

Konfigurieren von Remote-Desktop-Funktionen in Horizon 7

DEZ 2019

VMware Horizon 7 7.11



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 © 2018–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Konfigurieren von Remote-Desktop-Funktionen in Horizon 7	8
2	Konfigurieren von Remote-Desktop-Funktionen	9
	Konfigurieren von Unity Touch	10
	Systemanforderungen für Unity Touch	10
	Konfigurieren von Favoritenanwendungen durch Unity Touch	11
	Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming	13
	Systemanforderungen für die Flash-URL-Umleitung	15
	Sicherstellen, dass die Flash-URL-Umleitung installiert ist	16
	Einrichten der Webseiten für die Flash-URL-Umleitung	16
	Einrichten von Clientgeräten für die Flash-URL-Umleitung	17
	Deaktivieren oder Aktivieren der Flash-URL-Umleitung	18
	Konfigurieren der Flash-Umleitung	19
	Systemanforderungen für die Flash-Umleitung	20
	Installieren und Konfigurieren der Flash-Umleitung	20
	Verwenden der Windows-Registrierungseinstellungen zur Konfiguration der Flash-Umleitung	23
	Konfigurieren der HTML5-Multimedia-Umleitung	25
	Systemanforderungen für die HTML5-Multimedia-Umleitung	25
	Installieren und Konfigurieren der HTML5-Multimedia-Umleitung	27
	Installieren der VMware Horizon HTML5-Umleitungserweiterung für Chrome	29
	Installieren der VMware Horizon HTML5-Umleitungserweiterung für Edge	30
	Einschränkungen bei der HTML5-Multimedia-Umleitung	31
	Konfigurieren der Browserumleitung	31
	Systemanforderungen für die Browser-Umleitung	32
	Installieren und Konfigurieren der Browser-Umleitung	32
	Installieren der VMware Horizon Browser-Umleitungserweiterung für Chrome	38
	Einschränkungen der Browser-Umleitung	39
	Konfigurieren der Geolocation-Umleitung	40
	Systemanforderungen für die Geolocation-Umleitung	41
	Installieren und Konfigurieren der Geolocation-Umleitung	42
	Aktivieren des Internet Explorer-Plug-ins für die VMware Horizon Geolocation-Umleitung	44
	Aktivieren des Chrome-Plug-Ins für die VMware Horizon Geolocation-Umleitung	45
	Konfigurieren von Echtzeit-Audio/Video	46
	Konfigurationsmöglichkeiten für Echtzeit-Audio/Video	46
	Systemanforderungen für Echtzeit-Audio/Video	47
	Sicherstellen, dass anstelle der USB-Umleitung Echtzeit-Audio/Video verwendet wird	48
	Auswählen von bevorzugten Webcams und Mikrofonen	49
	Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video	50

Bandbreite für Echtzeit-Audio/Video	54
Konfigurieren von Microsoft Teams mit Echtzeit-Audio/Video	55
Konfigurieren der Scannerumleitung	56
Systemanforderungen für Scannerumleitung	56
Bedienung der Scannerumleitung durch den Benutzer	57
Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung	59
Konfigurieren der Umleitung serieller Ports	64
Systemanforderungen für die Umleitung serieller Ports	64
Bedienung der Umleitung serieller Ports durch den Benutzer	66
Richtlinien für die Konfiguration der Umleitung für serielle Ports	67
Konfigurieren der Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports	68
Konfigurieren von USB-Seriell-Adaptern	73
Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows (MMR)	74
Aktivieren von Multimedia-Umleitung in Horizon 7	74
Systemanforderungen für Windows Media MMR	74
Verwenden von Windows Media MMR basierend auf Netzwerklatenz	76
Verwalten des Zugriffs auf die Clientlaufwerksumleitung	77
Verwenden der Clientlaufwerksumleitung in einer Unified Access Gateway-Implementierung	78
Verwenden einer Gruppenrichtlinie zur Deaktivierung der Clientlaufwerkumleitung	78
Verwenden von Gruppenrichtlinien zum Konfigurieren des Laufwerkbuchstaben-Verhaltens	79
Verwenden der Registrierungseinstellungen zur Konfiguration der Clientlaufwerksumleitung	80
Konfigurieren der Drag & Drop-Funktion	82
Konfigurieren der SDO-Sensor-Umleitung	83
Konfigurieren der Funktion „Session Collaboration“	84
VMware Virtualization Pack für Skype for Business konfigurieren	85
Erfassen von Protokollen zur Behebung von Problemen mit Skype for Business	90
Konfigurieren der Umleitung „VMware Integrated Printing“	91

3 Konfigurieren der URL-Inhaltsumleitung 95

Grundlegendes zur URL-Inhaltsumleitung	95
Anforderungen für die URL-Inhaltsumleitung	96
Verwenden der URL-Inhaltsumleitung in einer Cloud-Pod-Architektur-Umgebung	97
Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung	98
Konfigurieren der Agent-zu-Client-Umleitung	98
Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO	99
Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung	100
Syntax der Regeln für die URL-Inhaltsumleitung	102
Regeln für reguläre Ausdrücke, die von der URL-Inhaltsumleitung unterstützt werden	104
Beispiel einer Gruppenrichtlinie für eine Agent-zu-Client-Umleitung	105
Konfigurieren der Client-zu-Agent-Umleitung	106
Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz	107

Syntax für die Option „--agentURLPattern“	109
Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung	109
Erstellen einer globalen Einstellung für die URL-Inhaltsumleitung	111
Zuweisen einer Einstellung für die URL-Inhaltsumleitung zu einem Benutzer oder einer Gruppe	114
Installieren von Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung	115
Testen einer Einstellung für die URL-Inhaltsumleitung	115
Verwalten der Einstellungen für die URL-Inhaltsumleitung	116
Verwenden von Gruppenrichtlinieneinstellungen für die Konfiguration der Client-zu-Agent-Umleitung	118
Einschränkungen der URL-Inhaltsumleitung	118
Nicht unterstützte Funktionen der URL-Inhaltsumleitung	119
Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows	120
Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome auf einem Mac	122
4 Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen	123
Einschränkungen in Bezug auf USB-Gerätetypen	124
Empfehlungen zur USB-Umleitung	125
Überblick über das Einrichten der USB-Umleitung	126
Konfigurieren der Fingerabdruckscannerumleitung	127
Konfigurieren der Kartenlesegerät-Umleitung	127
Netzwerkdatenverkehr und USB-Umleitung	128
Aktivieren der Funktion „USB über Sitzungserweiterungs-SDK“	129
Automatische Verbindungen mit USB-Geräten	129
Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung	130
Deaktivieren der USB-Umleitung für alle Gerätetypen	130
Deaktivieren der USB-Umleitung für bestimmte Geräte	132
Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs	134
Verwenden von Richtlinien zum Steuern der USB-Umleitung	134
Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte	135
Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte	138
USB-Gerätefamilien	143
USB-Einstellungen in der ADMX-Vorlage für die Horizon Agent-Konfiguration	144
Fehlerbehebung bei Problemen mit der USB-Umleitung	147
5 Konfigurieren von Richtlinien für Desktop- und Anwendungspools	150
Festlegen von Richtlinien in Horizon Administrator	151
Konfigurieren globaler Richtlinieneinstellungen	151
Konfigurieren von Richtlinien für Desktop-Pools	151
Konfigurieren von Richtlinien für Benutzer	152
Horizon 7-Richtlinien	152

Verwenden von Intelligente Richtlinien	153
Anforderungen für Intelligente Richtlinien	154
Installieren von Dynamic Environment Manager	154
Konfigurieren von Dynamic Environment Manager	154
Einstellungen für intelligente Horizon-Richtlinien	155
Bandbreitenprofil-Referenz	156
Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen	156
Erstellen einer intelligenten Horizon-Richtlinie in Dynamic Environment Manager	159
Verwenden von Active Directory-Gruppenrichtlinien	161
Erstellen einer OU für Remote-Desktops	161
Aktivieren der Loopback-Verarbeitung für Remote-Desktops	162
Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7	162
Horizon 7-ADMX-Vorlagendateien	163
Hinzufügen der ADMX-Vorlagendateien in Active Directory	165
ADMX-Vorlageneinstellungen für die VMware View Agent-Konfiguration	166
An Remote-Desktops gesendete Clientsysteminformationen	177
Ausführen von Befehlen auf Horizon-Desktops	182
Richtlinieneinstellungen für die Funktion „Session Collaboration“	182
Richtlinieneinstellungen für die Clientlaufwerksumleitung	183
Richtlinieneinstellungen für die VMware HTML5-Funktion	185
Richtlinieneinstellungen des VMware Virtualization Pack für Skype for Business	189
Richtlinieneinstellungen für VMware Horizon Performance Tracker	190
Richtlinieneinstellungen für den VMware-Integrationsdruck	191
PCoIP-Richtlinieneinstellungen	192
Allgemeine PCoIP-Einstellungen	193
PCoIP-Zwischenablagen- und Drag & Drop-Einstellungen	203
Einstellungen für die PCoIP-Bandbreite	208
PCoIP-Tastatureinstellungen	212
PCoIP Build-to-Lossless-Funktion	213
Richtlinieneinstellungen für VMware Blast	213
Aktivieren der verlustfreien Komprimierung für VMware Blast	219
Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste	220
Kompatibilitätseinstellungen für Remote-Desktop-Dienstanwendungen	220
Einstellungen für Remote-Desktop-Dienstverbindungen	222
Einstellungen zur Umleitung von RDS-Geräten und Ressourcen	227
Einstellungen für die Remote-Desktop-Dienstlizenzierung	233
Einstellungen für die Druckerumleitung für Remote-Desktop-Dienste	235
Einstellungen zu RDS-Profilen	239
Einstellungen für den RDS-Verbindungsserver	243
Umgebungseinstellungen zur RDS-Remote-Sitzung	248
Sicherheitseinstellungen für Remote-Desktop-Dienste	257

Zeitbeschränkung von RDS-Sitzungen	263
Einstellungen zu temporären RDS-Ordern	267
Filtern von Druckern für den virtuellen Druck	269
Einrichten des standortbasierten Drucks	270
Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck	271
Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck	272
Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck	273
Verwalten von speziellen Unity-Fenstern	276
Beispiel einer Active Directory-Gruppenrichtlinie	277
Erstellen einer OU für Horizon 7-Computer	277
Erstellen von GPOs für Horizon 7-Gruppenrichtlinien	278
Hinzufügen einer Horizon 7-ADMX-Vorlagendatei zu einem GPO	279
Aktivieren der Loopback-Verarbeitung für Remote-Desktops	280

Konfigurieren von Remote-Desktop-Funktionen in Horizon 7



Konfigurieren von Remote-Desktop-Funktionen in Horizon 7 beschreibt die Konfiguration von Remote-Desktop-Funktionen, die mit Horizon Agent auf virtuellen Desktops oder auf einem RDS-Host installiert werden. Sie können durch Konfiguration von Richtlinien auch das Verhalten von Desktop- und Anwendungspools, Computern und Benutzern steuern.

Zielgruppe

Diese Informationen richten sich an alle, die Remote-Desktop-Funktionen oder -Richtlinien auf virtuellen Desktops oder auf RDS-Hosts konfigurieren möchten. Diese Informationen sind für Windows-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und Vorgängen in Datacentern vertraut sind.

Konfigurieren von Remote-Desktop-Funktionen

2

Bestimmte Remote Desktop-Funktionen, die mit Horizon Agent installiert wurden, können in Horizon 7-Versionen aktualisiert werden. Sie können diese Funktionen so konfigurieren, dass die Remote-Desktop-Erfahrung Ihrer Endbenutzer verbessert wird.

Diese Funktionen beinhalten HTML Access, Unity Touch, Flash URL-Umleitung, HTML5-Multimedia-Umleitung, Geolocation-Umleitung, Echtzeit-Audio/Video, Windows Media Multimedia-Umleitung (MMR), USB-Umleitung, Scannerumleitung, die Umleitung für serielle Ports, Fingerabdruckscanner-Umleitung, Session Collaboration, Skype for Business und die URL-Inhaltsumleitung.

Informationen zu HTML Access finden Sie im Dokument *VMware Horizon HTML Access Installations- und Einrichtungshandbuch*. Informationen zur USB-Umleitung finden Sie unter [Kapitel 4 Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen](#). Informationen zur URL-Inhaltsumleitung finden Sie im Abschnitt [Kapitel 3 Konfigurieren der URL-Inhaltsumleitung](#).

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Unity Touch](#)
- [Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming](#)
- [Konfigurieren der Flash-Umleitung](#)
- [Konfigurieren der HTML5-Multimedia-Umleitung](#)
- [Konfigurieren der Browserumleitung](#)
- [Konfigurieren der Geolocation-Umleitung](#)
- [Konfigurieren von Echtzeit-Audio/Video](#)
- [Konfigurieren von Microsoft Teams mit Echtzeit-Audio/Video](#)
- [Konfigurieren der Scannerumleitung](#)
- [Konfigurieren der Umleitung serieller Ports](#)
- [Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows \(MMR\)](#)
- [Verwalten des Zugriffs auf die Clientlaufwerksumleitung](#)
- [Konfigurieren der Drag & Drop-Funktion](#)
- [Konfigurieren der SDO-Sensor-Umleitung](#)

- [Konfigurieren der Funktion „Session Collaboration“](#)
- [VMware Virtualization Pack für Skype for Business konfigurieren](#)
- [Konfigurieren der Umleitung „VMware Integrated Printing“](#)

Konfigurieren von Unity Touch

Mit Unity Touch können Tablet- und Smartphone-Benutzer Windows-Anwendungen und -Dateien bequem durchsuchen, suchen und öffnen, Lieblingsanwendungen und -dateien auswählen und bequem zwischen ausgeführten Anwendungen wechseln, ohne das Start-Menü oder die Taskleiste zu verwenden. Sie können eine Standardliste der beliebtesten Anwendungen konfigurieren, die in der Unity Touch-Sidebar angezeigt werden.

Sie können die Unity Touch-Funktion deaktivieren, nachdem Horizon Agent installiert ist, indem Sie die Gruppenrichtlinieneinstellung **Unity Touch aktivieren** in der ADMX-Vorlagendatei für die Horizon Agent-Konfiguration (`vdm_agent.admx`) konfigurieren.

Die Dokumente zu VMware Horizon Client für iOS-, Android- und Chrome OS-Geräte enthalten weitere Informationen zu Endbenutzerfunktionen, die über Unity Touch bereitgestellt werden. Weitere Informationen finden Sie unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

Systemanforderungen für Unity Touch

Die Horizon Client-Software und die mobilen Geräte, auf denen Sie Horizon Client installieren, müssen zur Unterstützung von Unity Touch bestimmte Versionsanforderungen erfüllen.

Remote-Desktop

Zur Unterstützung von Unity Touch muss in der virtuellen Maschine, auf die der Endbenutzer zugreift, die folgende Software installiert sein:

- Die Unity Touch-Funktion installieren Sie durch die Installation von View Agent 6.0 oder höher oder von Horizon Agent 7.0 oder höher. Informationen dazu finden Sie unter „Installieren von Horizon Agent auf einer virtuellen Maschine“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Betriebssysteme: Windows 7 (32 Bit oder 64 Bit), Windows 8 (32 Bit oder 64 Bit), Windows 8.1 (32 Bit oder 64 Bit), Windows Server 2008 R2 oder Windows Server 2012 R2, Windows 10 (32 Bit oder 64 Bit)

Horizon Client-Software

Unity Touch wird auf den folgenden Horizon Client-Versionen unterstützt:

- Horizon Client für iOS
- Horizon Client für Android
- Horizon Client für Chrome OS

Konfigurieren von Favoritenanwendungen durch Unity Touch

Mit der Unity Touch-Funktion können Tablet- und Smartphone-Benutzer von einer Unity Touch-Sidebar aus schnell zu einer Remote-Desktop-Anwendung oder -Datei navigieren. Wenngleich Endbenutzer festlegen können, welche Favoritenanwendungen in der Sidebar angezeigt werden sollen, können Administratoren zur Verbesserung der Benutzerfreundlichkeit eine Standardliste mit Favoritenanwendungen konfigurieren.

Wenn Sie Desktop-Pools mit dynamischer Zuweisung einsetzen, gehen die von den Endbenutzern festgelegten Favoritenanwendungen und -dateien verloren, wenn die Endbenutzer die Verbindung mit einem Desktop trennen. Dies gilt nicht, wenn Sie in Active Directory die Verwendung von Roamingbenutzerprofilen aktivieren.

Die Standardliste der Favoritenanwendungen bleibt erhalten, wenn sich ein Endbenutzer zum ersten Mal mit einem Desktop verbindet, der für Unity Touch aktiviert ist. Wenn der Benutzer jedoch eigene Favoritenanwendungen konfiguriert, wird die Standardliste ignoriert. Die vom Benutzer definierte Liste der Favoritenanwendungen wird im Roamingbenutzerprofil abgelegt und ist verfügbar, wenn sich der Benutzer in einem dynamischen oder dedizierten Pool bei anderen Computern anmeldet.

Wenn Sie eine Standardliste mit Favoritenanwendungen erstellen und mindestens eine der Anwendungen nicht auf dem Remote-Desktop-Betriebssystem installiert ist oder die Pfade zu diesen Anwendungen nicht im Startmenü gefunden werden, wird die Anwendung nicht in der Favoritenliste angezeigt. Sie können dieses Verhalten dazu nutzen, um eine Master-Standardliste mit Favoritenanwendungen einzurichten, die anschließend auf mehrere virtuelle Maschinen-Images angewendet werden kann, auf denen unterschiedliche Anwendungen installiert sind.

Wenn beispielsweise Microsoft Office und Microsoft Visio auf einer virtuellen Maschine installiert sind und Windows Powershell und VMware vSphere Client auf einer zweiten virtuellen Maschine, können Sie eine Liste erstellen, die alle vier Anwendungen enthält. Es werden nur die installierten Anwendungen als standardmäßige Favoritenanwendungen auf den jeweiligen Desktops angezeigt.

Sie können unterschiedliche Methoden zur Festlegung einer Standardliste mit Favoritenanwendungen einsetzen.

- Fügen Sie der Windows-Registrierung auf den virtuellen Desktop-Maschinen im Desktop-Pool einen Wert hinzu.
- Erstellen Sie ein administratives Installationspaket aus dem Horizon Agent-Installationsprogramm und verteilen Sie das Paket an die virtuellen Maschinen.
- Führen Sie auf den virtuellen Maschinen das Horizon Agent-Installationsprogramm von der Befehlszeile aus.

Hinweis Für Unity Touch wird davon ausgegangen, dass sich Verknüpfungen für Anwendungen im Programmordner des Menüs **Start** befinden. Wenn sich eine Verknüpfung außerhalb des Programmordners befindet, fügen Sie das Präfix **Programs** in den Verknüpfungspfad ein. Beispiel: Windows Update.lnk befindet sich im Ordner ProgramData\Microsoft\Windows\Start Menu. Zur Veröffentlichung dieser Verknüpfung als standardmäßige Favoritenanwendung fügen Sie dem Verknüpfungspfad das Präfix **Programs** hinzu. Beispiel: "Programs/Windows Update.lnk".

Voraussetzungen

- Stellen Sie sicher, dass Horizon Agent auf der virtuellen Maschine installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen. Für dieses Verfahren müssen Sie möglicherweise eine Registrierungseinstellung bearbeiten.
- Wenn Sie Desktop-Pools mit dynamischer Zuweisung einsetzen, verwenden Sie Active Directory zum Einrichten von Roamingbenutzerprofilen. Folgen Sie den von Microsoft bereitgestellten Anweisungen. Benutzer von Desktop-Pools mit dynamischer Zuweisung sind in der Lage, ihre Liste mit Favoritanwendungen und -dateien bei jeder Anmeldung anzuzeigen.

Verfahren

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritanwendungen, indem Sie der Windows-Registrierung einen Wert hinzufügen.
 - a Öffnen Sie regedit und navigieren Sie zur Registrierungseinstellung HKLM\Software\VMware, Inc.\VMware Unity.

Navigieren Sie auf einer virtuellen Maschine mit 64 Bit zum Verzeichnis HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity.
 - b Erstellen Sie einen Zeichenfolgenwert mit dem Namen FavAppList.
 - c Geben Sie die standardmäßigen Favoritanwendungen an.

Verwenden Sie das folgende Format, um die Verknüpfungspfade zu den Anwendungen im Menü **Start** anzugeben.

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

Beispiel:

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
```

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie ein administratives Installationspaket aus dem Horizon Agent-Installationsprogramm erstellen.

- a Verwenden Sie an der Befehlszeile das folgende Format, um das administrative Installationspaket zu erstellen.

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""eine Netzwerkfreigabe zum Speichern des administrativen Installationspakets"" UNITY_DEFAULT_APPS=""die Liste der Standardfavoritenanwendungen, die in der Registrierung festgelegt werden sollen""
```

Beispiel:

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\
ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of
Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows
PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google
Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft
SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/
WebEx/Productivity Tools/WebEx Settings.lnk|""
```

- b Verteilen Sie das administrative Installationspaket von der Netzwerkfreigabe auf den virtuellen Desktop-Maschinen, indem Sie eine standardmäßige MSI-Bereitstellungsmethode (Microsoft Windows Installer) einsetzen, die in Ihrer Organisation verwendet wird.

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie das Horizon Agent-Installationsprogramm an der Befehlszeile einer virtuellen Maschine direkt ausführen.

Verwenden Sie das folgende Format.

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""die Liste der Standardfavoritenanwendungen, die in der Registrierung festgelegt werden sollen""
```

Hinweis Der oben gezeigte Befehl kombiniert die Installation des Horizon Agent mit der Festlegung einer Standardliste mit Favoritenanwendungen. Sie müssen den Horizon Agent nicht installieren, bevor Sie diesen Befehl ausführen.

Nächste Schritte

Wenn Sie diese Aufgabe direkt auf einer virtuellen Maschine ausführen (indem Sie die Windows-Registrierung bearbeiten oder den Horizon Agent über die Befehlszeile installieren), müssen Sie die neu konfigurierte virtuelle Maschine bereitstellen. Sie können einen Snapshot oder eine Vorlage und einen Desktop-Pool erstellen oder Sie stellen einen vorhandenen Pool neu zusammen. Alternativ können Sie eine Active Directory-Gruppenrichtlinie zur Bereitstellung der neuen Konfiguration erstellen.

Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming

Kunden können ab sofort Adobe Media Server und Multicast oder Unicast zur Bereitstellung von Live-Videoereignissen in einer VDI-Umgebung (Virtual Desktop Infrastructure) nutzen. Zur Bereitstellung von

Multicast- oder Unicast-Videostreams in einer VDI-Umgebung sollte der Medienstream unter Umgehung der Remote-Desktops direkt von der Medienquelle an die Endpunkte gesendet werden. Die Flash-URL-Umleitung unterstützt diese Funktion, indem die ShockWave-Datei (SWF) abgefangen und vom Remote-Desktop an den Clientendpunkt umgeleitet wird.

Die Flash-Inhalte werden dann mithilfe der lokalen Flash-Medienplayer wiedergegeben.

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf die Clientendpunkte wird die Datenlast auf dem ESXi-Host im Rechenzentrum gesenkt, das zusätzliche Routing über das Rechenzentrum vermieden und die erforderliche Bandbreite zum simultanen Streaming von Flash-Inhalten an mehrere Clientendpunkte verringert.

Die Flash-URL-Umleitung verwendet ein JavaScript, das durch den Webseitenadministrator in eine HTML-Webseite eingebettet wird. Immer dann, wenn ein Benutzer eines Remote-Desktops aus einer Webseite auf den festgelegten URL-Link klickt, fängt das JavaScript die SWF-Datei von der Remote-Desktop-Sitzung ab und leitet sie an den Clientendpunkt um. Der Endpunkt kann anschließend außerhalb der Remote-Desktop-Sitzung einen lokalen Flash Projector öffnen und den Medienstream lokal abspielen.

Zum Konfigurieren der Flash-URL-Umleitung müssen Sie Ihre HTML-Webseite und Ihre Clientgeräte einrichten.

Verfahren

1 Systemanforderungen für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung muss Ihre Horizon 7-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

2 Sicherstellen, dass die Flash-URL-Umleitung installiert ist

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass die Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

3 Einrichten der Webseiten für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer zeigen diese Webseiten in den Browsern auf ihren Remote-Desktops an, um auf die Video-Streams zuzugreifen.

4 Einrichten von Clientgeräten für die Flash-URL-Umleitung

Die Flash-URL-Umleitung leitet die SWF-Datei von Remote-Desktops an Client-Geräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

5 Deaktivieren oder Aktivieren der Flash-URL-Umleitung

Die Flash-URL-Umleitung ist aktiviert, wenn Sie eine unbeaufsichtigte Installation von Horizon Agent mit der Eigenschaft `VDM_FLASH_URL_REDIRECTION=1` durchführen. Sie können die Flash-URL-Umleitung-Funktion auf ausgewählten Remote-Desktops deaktivieren oder erneut aktivieren, indem Sie einen Wert auf einem Windows-Registrierungsschlüssel auf diesen virtuellen Maschinen festlegen.

Systemanforderungen für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung muss Ihre Horizon 7-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Remote-Desktop

- Sie installieren die Flash-URL-Umleitung durch Eingabe der `VDM_FLASH_URL_REDIRECTION`-Eigenschaft an der Befehlszeile im Rahmen einer unbeaufsichtigten Installation von View Agent 6.0 oder höher bzw. Horizon Agent 7.0 oder höher. Informationen dazu finden Sie unter „Eigenschaften der unbeaufsichtigten Installation von Horizon Agent“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Auf den Desktops muss ein 64-Bit- oder 32-Bit-Betriebssystem mit Windows 7 ausgeführt werden.
- Zu den unterstützten Desktop-Browsern gehören der Internet Explorer 8, 9 und 10, Chrome 29.x sowie Firefox 20.x.

Flash Media Player und ShockWave Flash (SWF)

Sie müssen einen entsprechenden Flash Media Player wie z. B. Strobe Media Playback in Ihre Website integrieren. Zum Streamen von Multicast-Inhalt können Sie `multicastplayer.swf` oder `StrobeMediaPlayback.swf` in Ihren Webseiten verwenden. Zum Streamen von Live-Unicast-Inhalt müssen Sie `StrobeMediaPlayback.swf` verwenden. Sie können `StrobeMediaPlayback.swf` auch für andere unterstützte Funktionen wie RTMP-Streaming und dynamisches HTTP-Streaming verwenden.

Horizon Client-Software

Die folgenden Horizon Client-Versionen unterstützen Multicast und Unicast:

- Horizon Client 2.2 für Linux oder höher
- Horizon Client 2.2 für Windows oder höher

Die folgenden Horizon Client-Versionen unterstützen nur Multicast. (Sie bieten keine Unterstützung für Unicast):

- Horizon Client 2.0 oder 2.1 für Linux

Horizon Client-Computer oder Clientzugriffsgerät

- Horizon Client 5.4 für Windows
- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, die Horizon Client für Linux auf x86 Thin Client-Geräten ausführen. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, auf denen Horizon Client für Windows ausgeführt wird. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.
- Auf Windows-Clientgeräten müssen Sie Adobe Flash Player 10.1 oder höher für Internet Explorer installieren.
- Auf Linux Thin Client-Geräten müssen Sie die Dateien „libexpat.so.0“ und „libflashplayer.so“ installieren. Siehe [Einrichten von Clientgeräten für die Flash-URL-Umleitung](#).

Hinweis Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die ShockWave Flash-Datei (SWF) zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

Sicherstellen, dass die Flash-URL-Umleitung installiert ist

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass die Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

Die Flash-URL-Umleitung muss auf jedem Desktop vorhanden sein, auf dem Sie die Multicast- oder Unicast-Umleitung unterstützen möchten. Anweisungen zur Installation von Horizon Agent finden Sie unter „Eigenschaften der unbeaufsichtigten Installation für Horizon Agent“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Verfahren

- 1 Starten Sie eine Remote-Desktop-Sitzung, die PCoIP verwendet.
- 2 Öffnen Sie den Task-Manager.
- 3 Stellen Sie sicher, dass der Prozess ViewMPServer.exe auf dem Desktop ausgeführt wird.

Einrichten der Webseiten für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer

zeigen diese Webseiten in den Browsern auf ihren Remote-Desktops an, um auf die Video-Streams zuzugreifen.

Darüber hinaus können Sie die englische Fehlermeldung anpassen, die dem Endbenutzer angezeigt wird, wenn ein Problem bei der Flash-URL-Umleitung auftritt. Führen Sie diesen optionalen Schritt aus, wenn Sie Ihren Endbenutzern eine lokalisierte Fehlermeldung anzeigen möchten. Sie müssen die Konfiguration „var vmwareScriptErrorMessage“ zusammen mit dem lokalisierten Text in die MHTML-Webseite einbetten.

Voraussetzungen

Stellen Sie sicher, dass die Bibliothek `swfobject.js` in die MHTML-Webseite importiert wurde.

Verfahren

- 1 Betten Sie den JavaScript-Befehl `viewmp.js` in die MHTML-Webseite ein.

Beispiel: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

- 2 (Optional) Passen Sie die Fehlermeldung zur Flash-URL-Umleitung an, die den Endbenutzern gesendet wird.

Beispiel: `"var vmwareScriptErrorMessage= lokalisierte Fehlermeldung"`

- 3 Stellen Sie sicher, dass Sie den JavaScript-Befehl „`viewmp.js`“ einbetten und optional die Fehlermeldung zur Flash-URL-Umleitung anpassen, bevor Sie die ShockWave Flash-Datei (SWF) in die MHTML-Webseite importieren.

Wenn ein Benutzer die Webseite in einem Remote-Desktop anzeigt, löst der JavaScript-Befehl `viewmp.js` den Flash-URL-Umleitungsmechanismus auf dem Remote-Desktop aus, der die SWF-Datei vom Desktop an das hostende Clientgerät umleitet.

Einrichten von Clientgeräten für die Flash-URL-Umleitung

Die Flash-URL-Umleitung leitet die SWF-Datei von Remote-Desktops an Client-Geräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

Hinweis Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die SWF-Datei zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

Verfahren

- ◆ Installieren Sie Adobe Flash Player auf Ihren Clientgeräten.

Betriebssystem	Aktion
Windows	Installieren Sie Adobe Flash Player 10.1 oder höher für Internet Explorer.
Linux	<p>a Installieren Sie die Datei „libexpat.so.0“ oder stellen Sie sicher, dass diese Datei bereits installiert ist.</p> <p>Stellen Sie sicher, dass die Datei im Verzeichnis „/usr/lib“ oder „/usr/local/lib“ installiert ist.</p> <p>b Installieren Sie die Datei libflashplayer.so oder stellen Sie sicher, dass diese Datei bereits installiert ist.</p> <p>Vergewissern Sie sich, dass die Datei im geeigneten Flash-Plug-In-Verzeichnis für Ihr Linux-Betriebssystem installiert ist.</p> <p>c Installieren Sie das Programm wget oder stellen Sie sicher, dass die Programmdatei bereits installiert ist.</p>

Deaktivieren oder Aktivieren der Flash-URL-Umleitung

Die Flash-URL-Umleitung ist aktiviert, wenn Sie eine unbeaufsichtigte Installation von Horizon Agent mit der Eigenschaft VDM_FLASH_URL_REDIRECTION=1 durchführen. Sie können die Flash-URL-Umleitung-Funktion auf ausgewählten Remote-Desktops deaktivieren oder erneut aktivieren, indem Sie einen Wert auf einem Windows-Registrierungsschlüssel auf diesen virtuellen Maschinen festlegen.

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf der virtuellen Maschine.
- 2 Navigieren Sie zum Windows-Registrierungsschlüssel, der die Flash-URL-Umleitung steuert.

Option	Beschreibung
Windows 7, 64-Bit	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMP\enabled = Wert
Windows 7, 32 Bit	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMP\enabled = Wert

- 3 Legen Sie den Wert zum Deaktivieren oder Aktivieren der Flash-URL-Umleitung fest.

Option	Wert
Deaktiviert	0
Aktiviert	1

Standardmäßig ist der Wert auf 1 festgelegt.

Konfigurieren der Flash-Umleitung

Bei aktivierter Flash-Umleitung wird, wenn der Endbenutzer den Internet Explorer (Versionen 9, 10, 11) verwendet, der Flash-Inhalt an das Clientsystem gesendet, wodurch die Last auf dem ESXi-Host reduziert wird. Das Clientsystem gibt den Medieninhalt in einem Flash-Container-Fenster unter Verwendung der Flash Player ActiveX-Version wieder.

Auch wenn der Name dieser Funktion dem der Funktion „Flash-URL-Umleitung“ ähnelt, bestehen zwischen diesen Funktionen wichtige Unterschiede, die in der folgenden Tabelle beschrieben sind.

Tabelle 2-1. Vergleich von Flash-Umleitung und Flash-URL-Umleitung

Unterscheidungsmerkmal	Flash-Umleitung	Flash URL-Umleitung
Horizon Client-Typen, die diese Funktion unterstützen	Nur Windows-Client	Windows-Client und Unix-Client
Anzeigeprotokoll	PCoIP und VMware Blast	PCoIP
Browser	Internet Explorer 9, 10 oder 11 für den Remote-Desktop	Alle Browser, die derzeit auf Horizon Client und Horizon Agent unterstützt werden
Konfigurationsmechanismus	Verwenden Sie eine Horizon Agent-Gruppenrichtlinieneinstellung, um eine Positivliste oder eine Schwarze Liste mit Websites anzulegen, die die Flash-Umleitung verwenden bzw. nicht verwenden dürfen.	Ändern Sie den Quellcode auf der Webseite, um das erforderliche JavaScript einzubetten.

Funktionseinschränkungen

Für die Flash-Umleitungsfunktion gelten folgende Einschränkungen:

- Wenn in einem Flash Player-Fenster auf einen URL-Link geklickt wird, wird der Browser statt im Remote-Desktop (Agent-Seite) auf dem Client geöffnet.
- Einige Websites können bei Verwendung der Flash-Umleitung in einigen Browserversionen nicht dargestellt werden. Dies gilt beispielsweise für die Website vimeo.com in Internet Explorer 11.
- Flash- und Java-Skripts funktionieren möglicherweise nicht erwartungsgemäß.
- Das Horizon Client-Fenster kann während der Wiedergabe von Flash-Inhalten einfrieren. Allerdings lässt sich dieses Problem durch eine entsprechende Windows-Registrierungseinstellung umgehen.

Legen Sie auf einem 32-Bit-Client den Wert HKLM\Software\VMware, Inc.\VMware VDM\Client\Enabled3DRenderer auf „FALSE“ fest und auf einem 64-Bit-Client legen Sie HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Enabled3DRenderer auf „FALSE“ fest.

- YouTube unterstützt nicht mehr Flash-Medien.
- Die Flash-Umleitung funktioniert nicht für redbox.com.
- Das Flash-Kontextmenü (wird durch Klicken auf die rechte Maustaste aktiviert) ist deaktiviert.

- Wenn Horizon Client 4.1 über PCoIP eine Verbindung zu einem Remote-Desktop herstellt, kann die Flash-Umleitung fehlschlagen. Horizon Client gibt den Flash-Inhalt im systemeigenen Player des Remote-Desktops wieder oder dem Benutzer wird ein weißer Bildschirm angezeigt.

Systemanforderungen für die Flash-Umleitung

Horizon Agent, Horizon Client und die Remote-Desktops und Clientsysteme, auf denen Sie den Agent und die Client-Software installieren, müssen bestimmte Anforderungen zur Unterstützung der Flash-Umleitungsfunktion erfüllen.

Remote-Desktop

- Auf virtuellen Desktops muss Horizon Agent 7.0 oder höher mit ausgewählter benutzerdefinierter Setup-Option „Flash-Umleitung“ installiert sein. Die benutzerdefinierte Setup-Option „Flash-Umleitung“ ist standardmäßig nicht ausgewählt. Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Es müssen auch die erforderlichen Gruppenrichtlinieneinstellungen konfiguriert werden. Siehe [Installieren und Konfigurieren der Flash-Umleitung](#).
- Die Flash-Umleitung wird auf virtuellen Windows 7-, Windows 8-, Windows 8.1- und Windows 10-Desktops unterstützt.
- Internet Explorer 9, 10 oder 11 muss dazu mit dem entsprechenden Flash ActiveX-Plug-In installiert werden.
- Nach der Installation muss im Internet Explorer das VMware View FlashMMR Server-Add-On aktiviert werden.

Horizon Client-Computer oder Clientzugriffsgerät

- Horizon Client 4.0 oder höher muss installiert sein. Die Flash-Umleitung ist standardmäßig aktiviert. Informationen zur Installation von Horizon Client finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.
- Die Flash-URL-Umleitung wird auf Windows 7, Windows 8, Windows 8.1 und Windows 10 unterstützt.
- Das Flash ActiveX-Plug-In muss installiert und aktiviert sein

Anzeigeprotokolle für die Remote-Sitzung

- PCoIP
- VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Installieren und Konfigurieren der Flash-Umleitung

Um den Flash-Inhalt von einem Remote-Desktop zu einem Flash Player-Fenster auf dem lokalen Clientsystem umleiten zu können, muss die Flash-Umleitungsfunktion auf dem Remote-Desktop sowie auf dem Clientsystem installiert sein und es muss angegeben werden, welche Websites diese Funktion verwenden sollen.

Um diese Funktion zu aktivieren und festzulegen, welche Websites diese Funktion verwenden, konfigurieren Sie Gruppenrichtlinieneinstellungen. Alternativ können Sie mit den Windows-Registrierungseinstellungen auf dem Remote-Desktop eine Positivliste für die Websites konfigurieren, die die Flash-Umleitung verwenden sollen. Siehe [Verwenden der Windows-Registrierungseinstellungen zur Konfiguration der Flash-Umleitung](#).

Voraussetzungen

- Installieren Sie Horizon Client auf dem Clientsystem und installieren Sie Horizon Agent auf dem Remote-Desktop, wobei die Funktion „Flash-Umleitung“ aktiviert sein muss. Informationen zu den erforderlichen Versionen, Setup-Optionen und vollständigen Systemanforderungen finden Sie im Abschnitt [Systemanforderungen für die Flash-Umleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie die ADMX-Vorlagendatei für die Konfiguration von Horizon Agent (Datei `vdm_agent.admx`) der Organisationseinheit (OU) für den Remote-Desktop hinzu. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).
- Kompilieren Sie eine Liste der Websites, die den Flash-Inhalt umleiten können (eine Positivliste) oder nicht (eine Schwarze Liste).
- Stellen Sie sicher, dass Flash Active X installiert ist und ordnungsgemäß funktioniert. Führen Sie zum Überprüfen der Installation Internet Explorer aus und wechseln Sie zu <https://helpx.adobe.com/flash-player.html>.

Verfahren

- 1 Installieren Sie auf dem Clientsystem ggf. die ActiveX-Version von Flash Player (anstelle der NPAPI-Version).

Flash Player wird standardmäßig in Internet Explorer 10 und 11 installiert. Für Internet Explorer 9 müssen Sie möglicherweise zu <https://get.adobe.com/flashplayer/> navigieren, um den Flash Player herunterzuladen und zu installieren.

- 2 Führen Sie die folgenden Installationsschritte auf dem Remote-Desktop aus.

- a Installieren Sie Internet Explorer 9, 10 oder 11.
- b Installieren Sie ggf. die ActiveX-Version von Flash Player (anstelle der NPAPI-Version).

Flash Player wird standardmäßig in Internet Explorer 10 und 11 installiert. Für Internet Explorer 9 müssen Sie möglicherweise zu <https://get.adobe.com/flashplayer/> navigieren, um den Flash Player herunterzuladen und zu installieren.

- 3 Auf dem Remote-Desktop wählen Sie in Internet Explorer in der Menüleiste **Extras > Add-Ons verwalten** aus und stellen Sie sicher, dass im gleichnamigen Dialogfeld **VMware View FlashMMR Server** aufgeführt und aktiviert ist.

- 4 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und konfigurieren Sie die Richtlinieneinstellungen für die Flash-Umleitung im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware FlashMMR**

Einstellung	Beschreibung
Flash-Multimedia-Umleitung aktivieren	Legt fest, ob die Flash-Umleitung (FlashMMR) auf dem Remote-Desktop aktiviert ist (Agent-seitig). Ist dies der Fall, leitet die Funktion die Flash-Multimedia-Daten der entsprechenden URLs über den TCP-Kanal an den Client weiter und ruft den lokalen Flash Player auf dem Clientsystem auf. Diese Funktion reduziert die Agent-seitige Inanspruchnahme von CPU und Netzwerkbandbreite erheblich.
Mindestgröße des Rechtecks zur Aktivierung von Flash-MMR	Legt die Mindestbreite und -höhe des Rechtecks in Pixeln fest, in dem der Flash-Inhalt abgespielt wird. Beispielsweise legt die Angabe 400, 300 eine Breite von 400 Pixeln und eine Höhe von 300 Pixeln fest. Die Flash-Umleitung ist nur wirksam, wenn der Flash-Inhalt mindestens so groß wie die in dieser Richtlinie angegebenen Werte ist. Ist dieses GPO nicht konfiguriert, wird als Standardwert 320, 200 verwendet.

- 5 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und konfigurieren Sie die Richtlinieneinstellungen für die Flash-Umleitung im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware FlashMMR**.
- Um eine Liste der Host-URLs zur Verwendung für die Flash-Umleitung zu definieren, öffnen Sie die Einstellung **Verwendung der FlashMMR-URL-Liste festlegen** und wählen Sie die Option **Aktiviert** aus.
 - Wählen Sie im Dropdown-Menü **Verwendung der FlashMMR-URL-Liste festlegen** die Option **Positivliste aktivieren** oder **Schwarze Liste aktivieren** aus und klicken Sie dann auf **OK**.
Standardmäßig ist die Positivliste aktiviert.
 - Um die Liste der Host-URLs hinzuzufügen, die die Flash-Umleitung verwenden oder nicht verwenden, öffnen Sie die Einstellung **Host-URL-Liste zur Aktivierung von FlashMMR** und wählen Sie die Option **Aktiviert** aus.

- d Klicken Sie auf **Anzeigen** und geben Sie die vollständigen URLs, die Sie für die Positivliste oder die Schwarze Liste kompiliert haben, in die Spalte „Wertname“ ein.

Fügen Sie der URL das Präfix `http://` oder `https://` hinzu. Dafür können reguläre Ausdrücke verwendet werden. Beispiele: `https://*.google.com` und `http://www.cnn.com/*`.

In der Spalte „Wert“ können Sie optional `requireIECompatibility=true`, `appMode=0` oder beides festlegen. Verwenden Sie ein Komma zum Trennen der zwei Zeichenfolgen.

Standardmäßig ist die externe Schnittstellenunterstützung aktiviert, wenn die Flash-Umleitung ausgeführt wird. Dadurch kann die Leistung beeinträchtigt werden. In bestimmten Situationen kann das Festlegen von `appMode=0` die Leistung verbessern und eine bessere Benutzerfreundlichkeit nach sich ziehen.

- e Klicken Sie auf **OK**, um die URL-Liste zu speichern, und dann erneut auf **OK**, um die Richtlinieneinstellung zu speichern.

- 6 Um die Positiv- oder Negativliste zu Internet Explorer hinzuzufügen, öffnen Sie eine Eingabeaufforderung und führen Sie den Befehl `cscript "%ProgramFiles%\Common Files\VMware\Remote Experience\mergeflashmmrwhitelist.vbs"` aus.

- 7 Starten Sie Internet Explorer neu.

Die Sites, für die der Parameter `requireIECompatibility=true` festgelegt wurde, werden zur Kompatibilitätsansicht von Internet Explorer hinzugefügt. Wählen Sie zum Überprüfen der Sites in der Kompatibilitätsansicht **Extras > Einstellungen der Kompatibilitätsansicht** über die Menüleiste aus.

Die Sites werden zudem der Liste der vertrauenswürdigen Sites von Internet Explorer hinzugefügt. Um die vertrauenswürdigen Sites zu überprüfen, wählen Sie aus der Menüleiste von Internet Explorer **Extras > Internetoptionen** aus und klicken Sie dann auf der Registerkarte **Sicherheit** auf **Sites**.

Verwenden der Windows-Registrierungseinstellungen zur Konfiguration der Flash-Umleitung

Wenn Sie als Domänenbenutzer nicht über Administratorrechte auf dem Active Directory-Server verfügen, haben Sie alternativ die Möglichkeit, die Flash-Umleitung durch Einstellung der erforderlichen Werte in den Windows-Registrierungsschlüsseln auf dem Remote-Desktop zu konfigurieren.

Diese Vorgehensweise bietet eine Alternative zur Konfiguration der Flash-Umleitung mithilfe von Gruppenrichtlinieneinstellungen.

Voraussetzungen

- Stellen Sie eine Positivliste zusammen, um sicherzustellen, dass nur die in der Liste angegebenen URLs den Flash-Inhalt umleiten können. Sie können nicht die Windows-Registrierungseinstellungen verwenden, um eine Schwarze Liste zu aktivieren. Verwenden Sie zur Aktivierung einer Schwarzen Liste die Gruppenrichtlinieneinstellungen für die Flash-Umleitung.
- Stellen Sie sicher, dass auf dem Remote-Desktop Horizon Agent 7.0 oder höher, Flash Player und Internet Explorer 9, 10 oder 11 installiert sind. Siehe [Systemanforderungen für die Flash-Umleitung](#).

- Stellen Sie sicher, dass Horizon Client 4.0 oder höher und eine Flash Player ActiveX-Version auf dem Clientsystem installiert sind.

Verfahren

- 1 Verwenden Sie Horizon Client, um auf den Remote-Desktop zuzugreifen.
- 2 Öffnen Sie den Windows-Registrierungs-Editor (`regedit.exe`) auf dem Remote-Desktop, navigieren Sie zum Ordner `HKLM\Software\VMware, Inc.\VMware FlashMMR` und legen Sie für **FlashRedirection** den Wert **1** fest.

Hinweis Diese Einstellung aktiviert die Flash-Umleitungsfunktion. Wenn diese Einstellung allerdings in `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR` deaktiviert ist (d. h. auf 0 gesetzt ist), wird die Flash-Umleitung domänenübergreifend deaktiviert. Diese kann dann nur durch einen Domänenadministrator aktiviert werden.

- 3 Navigieren Sie zum Ordner `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR`. Wenn dieser Ordner nicht vorhanden ist, erstellen Sie ihn.
- 4 Im Ordner `VMware FlashMMR` erstellen Sie einen Unterschlüssel mit dem Namen **UrlWhiteList**.
- 5 Klicken Sie mit der rechten Maustaste auf den Schlüssel **UrlWhiteList**, wählen Sie **Neu > Zeichenfolgenwert** aus und geben Sie für den Namen die URL einer Website ein, für die die Flash-Umleitungsfunktion verwendet werden soll.

Dafür können reguläre Ausdrücke verwendet werden. Beispielsweise können Sie **`https://*.google.com`** angeben. Lassen Sie das Feld **Daten** leer.

- 6 (Optional) Fügen Sie im Datenfeld des neuen Registrierungswerts die Daten **`requireIECompatibility=true, appMode=0`** oder beide hinzu.

Verwenden Sie ein Komma zum Trennen der zwei Zeichenfolgen. Standardmäßig ist die externe Schnittstellenunterstützung aktiviert, wenn die Flash-Umleitung ausgeführt wird. Dadurch kann die Leistung beeinträchtigt werden. In bestimmten Situationen kann die Festlegung von **`appMode=0`** die Leistung verbessern und die Festlegung von **`appMode=1`** eine höhere Benutzerfreundlichkeit nach sich ziehen.

- 7 Wiederholen Sie den vorherigen Schritt, um zusätzliche URLs hinzuzufügen. Schließen Sie anschließend den Registrierungs-Editor.
- 8 Öffnen Sie auf dem Remote-Desktop eine Eingabeaufforderung, und navigieren Sie zum Verzeichnis `%Program Files%\Common Files\VMware\Remote Experience`.
- 9 Führen Sie den `cscript mergeflashmmrwhitelist.vbs`-Befehl aus, um die Positivliste zum Internet Explorer hinzuzufügen.
- 10 Starten Sie Internet Explorer neu.

Die Sites, für die der Parameter **`requireIECompatibility=true`** festgelegt wurde, werden zur Kompatibilitätsansicht von Internet Explorer hinzugefügt. Wählen Sie zum Überprüfen der Sites in der Kompatibilitätsansicht **Extras > Einstellungen der Kompatibilitätsansicht** über die Menüleiste aus.

Die Sites werden zudem der Liste der vertrauenswürdigen Sites von Internet Explorer hinzugefügt. Um die vertrauenswürdigen Sites zu überprüfen, wählen Sie aus der Menüleiste von Internet Explorer **Extras > Internetoptionen** aus und klicken Sie dann auf der Registerkarte **Sicherheit** auf **Sites**.

Konfigurieren der HTML5-Multimedia-Umleitung

Bei aktivierter HTML5-Multimedia-Umleitung wird, wenn der Endbenutzer den Google Chrome- oder den Microsoft Edge-Browser über einen Remote-Desktop verwendet, der HTML5-Multimedia-Inhalt an das Clientsystem gesendet, wodurch die Last auf dem ESXi-Host reduziert wird. Das Clientsystem gibt den Multimedia-Inhalt wieder und dem Endbenutzer wird ein besseres Audio- und Videoerlebnis geboten.

Systemanforderungen für die HTML5-Multimedia-Umleitung

Horizon Agent, Horizon Client und die Remote-Desktops und Clientsysteme, auf denen Sie die Agent- und die Client-Software installieren, müssen bestimmte Anforderungen zur Unterstützung der HTML5-Multimedia-Umleitungsfunktion erfüllen.

Remote-Desktop

- Auf virtuellen Desktops muss Horizon Agent 7.3.2 oder höher für Chrome bzw. Horizon Agent 7.5 oder höher für Edge mit der aktivierten benutzerdefinierten Setup-Option für die HTML5-Multimedia-Umleitung installiert sein. Diese Option ist nicht standardmäßig ausgewählt. Ab Horizon Agent 7.10 wird die benutzerdefinierte Setup-Option für die HTML5-Multimedia-Umleitung entfernt und die HTML5-Multimedia-Umleitung standardmäßig installiert. Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Auf RDS-Hosts für veröffentlichte Desktops muss Horizon Agent 7.3.2 oder höher mit ausgewählter benutzerdefinierter Setup-Option „HTML5-Multimedia-Umleitung“ installiert sein. Diese Option ist nicht standardmäßig ausgewählt. Ab Horizon Agent 7.10 wird die benutzerdefinierte Setup-Option für die HTML5-Multimedia-Umleitung entfernt und die HTML5-Multimedia-Umleitung standardmäßig installiert. Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Die Gruppenrichtlinieneinstellungen für die HTML5-Multimedia-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Siehe [Installieren und Konfigurieren der HTML5-Multimedia-Umleitung](#).
- Der Chrome- oder Edge-Browser muss installiert sein.

- Die Erweiterung „VMware Horizon HTML5-Multimedia-Umleitung“ muss im Chrome- oder Edge-Browser installiert sein. Siehe [Installieren der VMware Horizon HTML5-Umleitungserweiterung für Chrome](#) oder [Installieren der VMware Horizon HTML5-Umleitungserweiterung für Edge](#).

Clientsystem

- Für Windows-Clientsysteme muss Horizon Client 4.6 oder höher für Chrome installiert sein bzw. Horizon Client 4.8 oder höher für Edge, und benutzerdefinierte Setup-Option für die Unterstützung für die HTML5-Multimedia-Umleitung und die Browser-Umleitung muss aktiviert sein. Diese Option ist standardmäßig ausgewählt. Informationen zur Installation von Horizon Client finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.
- Für Linux-Clientsysteme muss Horizon Client 5.1 oder höher mit ausgewählter benutzerdefinierter Setup-Option „Unterstützung für die HTML5-Multimedia-Umleitung“ installiert sein. Diese Option ist standardmäßig ausgewählt. Informationen zur Installation von Horizon Client finden Sie im *VMware Horizon Client für Linux Installations- und Einrichtungshandbuch*.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

Einschränkungen

Für die HTML5-Multimedia-Umleitungsfunktion gelten folgende Einschränkungen:

- Die relative Mausfunktion von Horizon Client wird nicht unterstützt.
- Es ist nicht möglich, die Funktionen **Webseite stummschalten** (Chrome-Browser) oder **Registerkarte stummschalten** (Edge-Browser) zu verwenden.
- Um die HTML5-Multimedia-Umleitung von Chrome auf einem Linux-Clientsystem zu verwenden, öffnen Sie höchstens einen Chrome-Browser, der von einem RDS-Host veröffentlicht wird. Die HTML5-Multimedia-Umleitung funktioniert nicht ordnungsgemäß, wenn Sie einen zusätzlichen Chrome-Browser öffnen, der von einem anderen RDS-Host veröffentlicht wurde.
- Wenn bei der Wiedergabe von umgeleiteten Multimedia-Inhalten auf einem Linux-Clientsystem, das Thin-Client-Hardware mit niedrigerer Kapazität verwendet, die Leistung schlecht ist, können Sie die

Systemleistung wie hier beschrieben optimieren. Fügen Sie den Eintrag `disableGPU.html5mmr=true` zu einer der folgenden drei Konfigurationsdateien hinzu. Die Konfigurationsdateien werden in der aufgeführten Reihenfolge verarbeitet:

- a `/usr/lib/vmware/config`
- b `/etc/vmware/config`
- c `~/.vmware/config`

Installieren und Konfigurieren der HTML5-Multimedia-Umleitung

Um den HTML5-Multimedia-Inhalt von einem Remote-Desktop zu einem lokalen Clientsystem umleiten zu können, muss die HTML5-Multimedia-Umleitungsfunktion und der Chrome- oder Edge-Browser auf dem Remote-Desktop installiert und die Funktion „HTML5-Multimedia-Umleitung“ aktiviert sein und es muss angegeben werden, welche Websites diese Funktion verwenden sollen.

Um die HTML5-Multimedia-Umleitung zu aktivieren und festzulegen, welche Websites diese Funktion verwenden, konfigurieren Sie Gruppenrichtlinieneinstellungen auf dem Active Directory-Server. Sie müssen eine Liste von URLs für die Websites kompilieren, die den HTML5-Multimedia-Inhalt umleiten können. Fügen Sie den URLs das Präfix `http://` oder `https://` hinzu. Sie können den URL-Musterabgleich verwenden.

Beispiel: Um alle Videos auf YouTube umzuleiten, geben Sie `https://www.youtube.com/*` an. Um alle Videos auf Vimeo umzuleiten, geben Sie `https://www.vimeo.com/*` an. Weitere Informationen dazu finden Sie auf https://developer.chrome.com/extensions/match_patterns.

Voraussetzungen

- Installieren Sie Horizon Client auf dem Clientsystem und installieren Sie Horizon Agent auf dem Remote-Desktop, wobei die Funktion „HTML5-Multimedia-Umleitung“ aktiviert sein muss. Informationen zu den erforderlichen Versionen, Setup-Optionen und vollständigen Systemanforderungen finden Sie im Abschnitt [Systemanforderungen für die HTML5-Multimedia-Umleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie die VMware View Agent-ADMX-Vorlagendatei `vdm_agent.admx` für die Konfiguration von einem GPO, das mit der OU für den virtuellen Desktop verknüpft ist, oder dem RDS-Host für den veröffentlichten Desktop hinzu. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).
- Kompilieren Sie eine Liste der URLs für die Websites, die den HTML5-Multimedia-Inhalt umleiten können.

Verfahren

- 1 Installieren Sie den Chrome- oder Edge-Browser auf dem Remote-Desktop.
- 2 Öffnen Sie auf Ihrem Active Directory-Server den Editor zur Gruppenrichtlinienverwaltung.
- 3 Wechseln Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen**.
- 4 Öffnen Sie die Einstellung **VMware HTML5-Funktionen aktivieren**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.
- 5 Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware HTML5 Multimedia-Umleitung**.
- 6 Öffnen Sie die Einstellung **VMware HTML5 Multimedia-Umleitung aktivieren**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.
- 7 Führen Sie für den Chrome-Browser die folgenden Schritte durch.
 - a Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware HTML5 Multimedia-Umleitung**.
 - b Öffnen Sie die Einstellung **Chrome-Browser für VMware HTML5 Multimedia-Umleitung aktivieren**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.
- 8 Führen Sie für den Edge-Browser die folgenden Schritte durch.
 - a Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware HTML5 Multimedia-Umleitung**.
 - b Öffnen Sie die Einstellung **Edge-Browser für VMware HTML5 Multimedia-Umleitung aktivieren**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.
 - c Wechseln Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen**.
 - d Öffnen Sie die Einstellung **Automatische Intranet-Erkennung deaktivieren**, wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.
- 9 Geben Sie an, welche Websites die Funktion zur HTML5 Multimedia-Umleitung verwenden dürfen.
 - a Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware HTML5 Multimedia-Umleitung**.
 - b Öffnen Sie die Einstellung **URL-Liste für VMware HTML5 Multimedia-Umleitung aktivieren** und wählen Sie **Aktiviert** aus.

- c Klicken Sie auf **Anzeigen** und geben Sie die URLs, die Sie kompiliert haben, in die Spalte „Wertname“ ein.

Nur die URLs, die Sie dort angeben, können HTML5-Multimedia-Inhalte umleiten. Standardmäßig werden keine URLs hinzugefügt. Lassen Sie die Spalte „Wert“ leer.

- d Klicken Sie auf **OK**, um die URL-Liste zu speichern, und dann auf **OK**, um die Richtlinieneinstellung zu speichern.

Nächste Schritte

Installieren Sie zur Verwendung des Chrome-Browsers die Erweiterung zur VMware Horizon HTML5-Umleitung für Chrome im Chrome-Browser am Remote-Desktop. Siehe [Installieren der VMware Horizon HTML5-Umleitungserweiterung für Chrome](#).

Installieren Sie zur Verwendung des Edge-Browsers die Erweiterung zur VMware Horizon HTML5-Umleitung für Edge im Edge-Browser auf dem Remote-Desktop. Siehe [Installieren der VMware Horizon HTML5-Umleitungserweiterung für Edge](#).

Installieren der VMware Horizon HTML5-Umleitungserweiterung für Chrome

Um die Funktion „HTML5-Multimedia-Umleitung“ im Chrome-Browser verwenden zu können, müssen Sie die Erweiterung „VMware Horizon HTML5-Umleitung“ auf dem Remote-Desktop zwangsweise installieren. Konfigurieren Sie für eine erzwungene Installation eine Google Chrome-Gruppenrichtlinieneinstellung auf dem Active Directory-Server.

Um die Chrome-Gruppenrichtlinieneinstellung auf dem Remote-Desktop anzuwenden, müssen Sie die ADMX-Vorlagendatei zu einem GPO auf dem Active Directory-Server hinzufügen. Bei einem virtuellen Desktop muss das GPO mit der OU verknüpft werden, die den virtuellen Desktop enthält. Bei einem veröffentlichten Desktop muss das GPO mit der OU verknüpft werden, die den RDS-Host enthält.

Voraussetzungen

- Konfigurieren Sie die Funktion „HTML5-Multimedia-Umleitung“. Siehe [Installieren und Konfigurieren der HTML5-Multimedia-Umleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- 1 Laden Sie die Google Chrome-Datei `policy_templates.zip` unter https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip herunter.

- 2 Entpacken Sie die Datei `policy_templates.zip` und kopieren Sie die Dateien `chrome.admx` und `chrome.adml` auf Ihren Active Directory-Server.

Die Datei `chrome.admx` befindet sich im Ordner `\windows\admx` und die Datei `chrome.adml` im Ordner `\windows\admx\Sprache` der Datei `policy_templates.zip`.

- a Kopieren Sie die Datei `chrome.admx` in den Ordner `%systemroot%\PolicyDefinitions` auf Ihrem Active Directory-Server.
- b Kopieren Sie die Sprachressourcendatei `chrome.adml` in den entsprechenden Sprachen-Unterordner des Ordners `%systemroot%\PolicyDefinitions` auf Ihrem Active Directory-Server.

Kopieren Sie beispielsweise die `en_us`-Version der Datei `chrome.adml` in den Unterordner `%systemroot%\PolicyDefinitions\en_us` auf Ihrem Active Directory-Server.

- 3 Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf dem Active Directory-Server und navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Google Chrome > Erweiterungen**.
- 4 Öffnen Sie die Richtlinieneinstellung **Liste der zwangsweise installierten Anwendungen und Erweiterungen konfigurieren** und klicken Sie auf **Aktiviert**.
- 5 Klicken Sie auf **Anzeigen** und geben Sie `ljmaegmnepbjgkghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx` in die Spalte „Wert“ ein.
- 6 Klicken Sie auf **OK**, um die Erweiterungs-ID/Update-URL zu speichern, und dann auf **OK**, um die Richtlinieneinstellung zu speichern.
- 7 Stellen Sie sicher, dass die Erweiterung „HTML5-Multimedia-Umleitung“ auf dem Remote-Desktop installiert ist.
 - a Stellen Sie eine Verbindung zum Remote-Desktop her und starten Sie Chrome.
 - b Geben Sie in der Adressleiste von Chrome `chrome://extensions` ein.

Erweiterung VMware Horizon HTML5-Umleitung wird in die Liste der Erweiterungen angezeigt.

Installieren der VMware Horizon HTML5-Umleitungserweiterung für Edge

Um die Funktion der HTML5-Multimedia-Umleitung für den Edge-Browser verwenden zu können, müssen Sie die VMware Horizon HTML5-Umleitungserweiterung für Edge vom Microsoft Store auf dem Remote-Desktop installieren.

Voraussetzungen

Konfigurieren Sie die Funktion „HTML5-Multimedia-Umleitung“. Siehe [Installieren und Konfigurieren der HTML5-Multimedia-Umleitung](#).

Verfahren

- 1 Stellen Sie eine Verbindung mit dem Remote-Desktop her.

- 2 Laden Sie die Erweiterung **VMware Horizon HTML5-Umleitungserweiterung für Edge** vom Microsoft Store herunter und installieren Sie sie.

Nach Installation der Erweiterung wird das Symbol für die **VMware HTML5 Multimedia-Umleitung** oben rechts im Fenster des Edge-Browsers angezeigt. Wenn die Funktion zur HTML5-Multimedia-Umleitung funktioniert, erscheinen die Buchstaben REDR oberhalb des Symbols.

Einschränkungen bei der HTML5-Multimedia-Umleitung

Für die HTML5-Multimedia-Umleitungsfunktion gelten bestimmte Einschränkungen:

- 360-Videos werden von HTML5-Multimedia-Umleitung nicht unterstützt. Das Erweiterungssymbol für die HTML5-Multimedia-Umleitung ist mit dem REDR-Badge gekennzeichnet, obwohl das Video nicht unterstützt wird.
- Mit der Funktion „HTML5-Multimedia-Umleitung“ können keine HTML-Multimedia-Inhalte von `http://huffingtonpost.com` umgeleitet werden. Mit der Funktion „HTML5-Multimedia-Umleitung“ können HTML5-Multimedia-Inhalte von `http://www.yahoo.com` umgeleitet werden, doch möglicherweise wird eine Meldung angezeigt, dass die Seite nicht mehr reagiert.
- Wenn Sie die URL einer vertrauenswürdigen Microsoft Edge-Site in der Liste der Websites in der Gruppenrichtlinieneinstellung **URL-Liste für VMware HTML5-Multimedia-Umleitung aktivieren** einschließen, funktioniert die HTML5-Multimedia-Umleitung für diese URL nicht. Sie können diese Einschränkung vermeiden, indem Sie die Host-Sicherheit mithilfe des Befehls **CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"** verringern.
- Mit dem Microsoft Edge-Browser kann die Funktion zur HTML5-Multimedia-Umleitung HTML-Multimedia-Inhalt von Websites nicht umleiten, die das Videoformat m3u8 verwenden, z. B. `ted.com`.
- Wenn die Einrichtungsoption **Scannerumleitung** in Horizon Agent in einem Remote-Desktop aktiviert ist, reagiert die Erweiterung zur VMware Horizon HTML5-Umleitung für die Edge-Erweiterung manchmal nicht mehr, nachdem der Microsoft Edge-Browser auf dem Remote-Desktop gestartet wurde. Dieses Problem tritt in der Regel in Umgebungen mit großen Monitoren und unter starker Belastung auf.
- Wenn Benutzer ein HTML5-Video wiedergeben, das eine statische Video-URL auf einem Remote-Desktop verwendet, hat der Client Computer von Benutzern keinen Zugriff auf die statische URL und die Wiedergabe verfällt wieder auf den Remote-Desktop.

Konfigurieren der Browserumleitung

Wenn ein Endbenutzer bei der Browser-Umleitung den Google Chrome-Browser auf einem Remote-Desktop verwendet, wird die Webseite auf dem Clientsystem anstelle des Agent-Systems gerendert und im Viewport des Remote Browsers angezeigt. Der Viewport ist der Teil des Browserfensters, der den Inhalt einer Webseite anzeigt.

Systemanforderungen für die Browser-Umleitung

Die Remote-Desktops und Clientsysteme, auf denen Sie den Agent und die Client-Software installieren, müssen bestimmte Anforderungen zur Unterstützung der Browser-Umleitungsfunktion erfüllen.

Remote-Desktops

- Auf virtuellen Desktops muss Horizon Agent 7.10 oder höher installiert sein. Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Für RDS-Hosts für veröffentlichte Desktops muss Horizon Agent 7.10 oder höher installiert sein. Weitere Informationen finden Sie in den Themen zur Installation von Horizon Agent im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Die Gruppenrichtlinieneinstellungen für die VMware Browser-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Siehe [Installieren und Konfigurieren der Browser-Umleitung](#).
- Der Chrome-Browsers muss installiert sein.
- Die Erweiterung „VMware Horizon-Browser-Umleitung“ muss im Chrome-Browser installiert sein. Siehe [Installieren der VMware Horizon Browser-Umleitungserweiterung für Chrome](#).

Clientsystem

Horizon Client 5.2 für Windows oder höher muss mit ausgewählter Setup-Option für die Unterstützung für die HTML5-Multimedia-Umleitung und die Browser Umleitung installiert werden. Diese Option ist standardmäßig ausgewählt. Informationen zur Installation von Horizon Client finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*. Es werden nur Windows-Clientsysteme unterstützt.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

Installieren und Konfigurieren der Browser-Umleitung

Das Installieren und Konfigurieren der Browser-Umleitungsfunktion beinhaltet die Installation des Chrome-Browsers, die Aktivierung der Browser-Umleitungsfunktion auf dem Agent-Computer und die Angabe der URLs für die Umleitung.

Optional können Sie die URLs angeben, zu denen Benutzer von umgeleiteten URLs navigieren können, und das Fallback-Verhalten für Verstöße gegen Positivlisten anpassen. Sie können auch clientseitige Gruppenrichtlinieneinstellungen für die Verwendung von Mikrofonen und Kameras, den Umgang mit Zertifikatsfehlern und den Browser-Cache-Speicher konfigurieren.

Um die Browser-Umleitung zu aktivieren und die URLs für die Umleitung anzugeben, müssen Sie agentenseitige Gruppenrichtlinieneinstellungen auf Ihrem Active Directory-Server konfigurieren. Kompilieren Sie eine Liste der URLs für Websites, die umgeleitet werden können, und optional für die Websites, zu denen Benutzer von umgeleiteten URLs navigieren können. Fügen Sie den URLs das Präfix **http://** oder **https://** hinzu. Sie können den URL-Musterabgleich verwenden. Um z. B. alle Yahoo-Inhalte umzuleiten, geben Sie **https://www.yahoo.com/*** ein. Weitere Informationen finden Sie unter https://developer.chrome.com/extensions/match_patterns.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie die VMware View Agent-ADMX-Vorlagendatei (`vdm_agent.admx`) für die Konfiguration einem GPO hinzu, das mit der OU für den virtuellen Desktop verknüpft ist, oder dem RDS-Host für den veröffentlichten Desktop. Wenn Sie eine der optionalen clientseitigen Gruppenrichtlinieneinstellungen konfigurieren möchten, fügen Sie auch die ADMX-Vorlagendatei für die Horizon Client-Konfiguration (`vdm_client.admx`) hinzu. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).
- Kompilieren Sie eine Liste mit URLs für Websites, die die Browser-Umleitungsfunktion verwenden können.

Verfahren

- 1 Installieren Sie den Chrome-Browser auf dem Remote-Desktop.
- 2 Öffnen Sie auf Ihrem Active Directory-Server den Editor zur Gruppenrichtlinienverwaltung.
- 3 Wechseln Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen**.
- 4 Öffnen Sie die Einstellung **VMware HTML5-Funktionen aktivieren**, wählen Sie **Aktiviert** aus, und klicken Sie dann auf **OK**.
- 5 Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware Browser-Umleitung**.
- 6 Öffnen Sie die Einstellung **VMware Browser-Umleitung aktivieren**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.

7 Geben Sie die URLs für die Browser-Umleitungsfunktion an.

Benutzer können diese URLs besuchen, indem sie sie entweder in die Chrome-Adressleiste oder in die benutzerdefinierte Adressleiste eingeben. Benutzer können diese URLs auch aufrufen, indem sie ausgehend von einer anderen URL in der Liste oder von einer beliebigen agentenseitig gerenderten Seite zu ihnen navigieren. Nur die von Ihnen angegebenen URLs werden umgeleitet. Standardmäßig werden keine URLs hinzugefügt.

- a Öffnen Sie die Einstellung **URL-Liste für VMware Browser-Umleitung aktivieren** und wählen Sie **Aktiviert** aus.
- b Klicken Sie auf **Anzeigen**, geben Sie die URLs in die Wertnamensspalte ein und klicken Sie auf **OK**.

Lassen Sie die Spalte „Wert“ leer.

- c Um die Richtlinieneinstellung zu speichern, klicken Sie auf **OK**.

8 (Optional) Konfigurieren Sie eine oder mehrere der optionalen agentenseitigen Gruppenrichtlinieneinstellungen.

In der folgenden Tabelle werden die optionalen agentenseitigen Gruppenrichtlinieneinstellungen beschrieben.

Option	Bezeichnung
Navigations-URL-Liste für VMware Browser-Umleitung aktivieren	<p>Mit dieser Einstellung können Sie die URLs angeben, zu denen ein Benutzer von einer URL, die in der Positivliste URL-Liste für VMware Browser-Umleitung aktivieren angegeben ist, navigieren darf (entweder durch Eingabe der URL direkt in die benutzerdefinierte Adressleiste oder durch Navigieren zur URL von einer URL in der Positivliste).</p> <p>Benutzer können diese URLs nicht direkt aufrufen, indem sie sie in die Chrome-Adressleiste eingeben oder von einer agentenseitig gerenderten Seite dorthin navigieren.</p> <p>Um die URLs anzugeben, klicken Sie auf Anzeigen, geben Sie die URLs in die Wertnamensspalte ein und klicken Sie auf OK. Lassen Sie die Spalte „Wert“ leer.</p>
Enable automatic fallback after a whitelist violation	<p>Wenn diese Einstellung aktiviert ist und ein Benutzer zu einer URL navigiert, die nicht in einer der Positivlisten für die Browser-Umleitung angegeben ist, entweder durch Eingabe in die benutzerdefinierte Adressleiste oder durch Navigieren von einer URL in einer der Positivlisten, wird die Umleitung für diese Registerkarte angehalten. Die URL wird dann abgerufen und stattdessen auf dem Agent angezeigt.</p> <p>Hinweis Wenn ein Benutzer versucht, zu einer URL zu navigieren, die nicht in der Einstellung URL-Liste für VMware Browser-Umleitung aktivieren angegeben ist, fällt die Registerkarte immer wieder auf das Abrufen und Rendern der URL auf dem Agent zurück, unabhängig davon, ob diese Einstellung aktiviert ist.</p>
Show a page with error information before automatic fallback	<p>Wenn Sie diese Einstellung aktivieren und ein Verstoß gegen eine Positivliste auftritt, wird eine Seite angezeigt, die einen Countdown von fünf Sekunden anzeigt. Nach Ablauf von fünf Sekunden fällt die Registerkarte auf das Abrufen und Rendern der URL zurück, die den Verstoß auf dem Agent verursacht hat. Wenn diese Einstellung deaktiviert ist, wird die Seite mit der Warnung von fünf Sekunden nicht angezeigt. Diese Einstellung wird nur wirksam, wenn Automatisches Fallback nach einem Whitelist-Verstoß aktivieren ebenfalls aktiviert ist.</p>

- 9 (Optional) Um eine oder mehrere der optionalen clientseitigen Gruppenrichtlinieneinstellungen zu konfigurieren, navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware Horizon Client-Konfiguration > VMware Browser-Umleitung**.

In der folgenden Tabelle werden die clientseitigen Gruppenrichtlinieneinstellungen beschrieben.

Option	Bezeichnung
WebRTC-Kamera und Mikrofonzugriff für die Browserumleitung aktivieren	Wenn Sie diese Einstellung aktivieren, haben umgeleitete Seiten, die WebRTC verwenden, Zugriff auf die Kamera und das Mikrofon des Clientsystems. Diese Einstellung ist standardmäßig aktiviert.
Zertifikatfehler für die Browserumleitung ignorieren	Wenn Sie diese Einstellung aktivieren, werden Zertifikatfehler, die auf einer umgeleiteten Seite auftreten, ignoriert, und das Browsen wird fortgesetzt. Diese Einstellung ist standardmäßig deaktiviert.
Cache für die Browserumleitung aktivieren	<p>Wenn Sie diese Einstellung aktivieren, wird der Browserverlauf, einschließlich Cookies, auf dem Clientsystem gespeichert. Diese Einstellung ist standardmäßig aktiviert.</p> <p>Hinweis Durch das Deaktivieren dieser Einstellung wird der Cache nicht gelöscht. Wenn Sie diese Einstellung deaktivieren und dann erneut aktivieren, wird der Cache wieder verwendet.</p>

Beispiel

`https://play.google.com` und `https://news.google.com` haben eine gemeinsame Anmeldeseite: `https://accounts.google.com`.

Im folgenden Beispiel sind `https://play.google.com/*` und `https://accounts.google.com/*` in **URL-Liste für VMware Browser-Umleitung aktivieren** enthalten. Die folgende Tabelle beschreibt das Verhalten, das in diesem Szenario auftritt.

Ein Benutzer besucht `https://play.google.com`

- `https://play.google.com` wird an den Client Computer umgeleitet.
- Wenn sich der Benutzer anmeldet, wird `https://accounts.google.com` auf dem Client Computer geöffnet, und der Benutzer authentifiziert sich auf dem Client Computer.
- Nach erfolgreicher Authentifizierung leitet die Website wieder auf `https://play.google.com` auf dem Client Computer um, und der Benutzer wird ordnungsgemäß angemeldet.

Ein Benutzer besucht `https://news.google.com`

- `https://news.google.com` wird auf dem Agent-Computer gerendert.
- Wenn sich der Benutzer anmeldet, wird `https://accounts.google.com` an den Client Computer umgeleitet, und der Benutzer authentifiziert sich auf dem Client Computer.
- Nach erfolgreicher Authentifizierung ist der Benutzer nicht ordnungsgemäß angemeldet, da `https://news.google.com` auf dem Agent-Computer gerendert wird, aber die Authentifizierung auf dem Client Computer erfolgt ist.

Ein Benutzer öffnet `https://accounts.google.com` direkt in der Adressleiste

`https://accounts.google.com` wird an den Client Computer umgeleitet.

Im nächsten Beispiel ist `https://play.google.com/*` in **URL-Liste für VMware Browser-Umleitung aktivieren** enthalten und `https://accounts.google.com/*` in **Navigations-URL-Liste für VMware Browser-Umleitung aktivieren**. Die folgende Tabelle beschreibt das Verhalten, das in diesem Szenario auftritt.

Ein Benutzer besucht <code>https://play.google.com</code>	<ul style="list-style-type: none"> ■ <code>https://play.google.com</code> wird an den Client Computer umgeleitet. ■ Wenn sich der Benutzer anmeldet, wird <code>https://accounts.google.com</code> auf dem Client Computer geöffnet, und der Benutzer authentifiziert sich auf dem Client Computer. ■ Nach erfolgreicher Authentifizierung leitet die Website wieder auf <code>https://play.google.com</code> auf dem Client Computer um, und der Benutzer wird ordnungsgemäß angemeldet.
Ein Benutzer besucht <code>https://news.google.com</code>	<ul style="list-style-type: none"> ■ <code>https://news.google.com</code> wird auf dem Agent-Computer gerendert. ■ Wenn sich der Benutzer anmeldet, wird <code>https://accounts.google.com</code> auf dem Agent-Computer gerendert, und der Benutzer wird auf dem Agent-Computer authentifiziert. ■ Nach erfolgreicher Authentifizierung leitet die Website wieder auf <code>https://news.google.com</code> auf dem Agent-Computer um, und der Benutzer wird ordnungsgemäß angemeldet.
Ein Benutzer öffnet <code>https://accounts.google.com</code> direkt in der Adressleiste	<code>https://accounts.google.com</code> wird auf dem Agent-Computer gerendert.

Nächste Schritte

[Installieren der VMware Horizon Browser-Umleitungserweiterung für Chrome.](#)

Installieren der VMware Horizon Browser-Umleitungserweiterung für Chrome

Um die Browser-Umleitungsfunktion im Chrome-Browser verwenden zu können, müssen Sie die Erweiterung „VMware Horizon Browser-Umleitung“ auf dem Remote-Desktop zwangsweise installieren. Konfigurieren Sie für eine erzwungene Installation eine Google Chrome-Gruppenrichtlinieneinstellung auf dem Active Directory-Server.

Um die Chrome-Gruppenrichtlinieneinstellung auf dem Remote-Desktop anzuwenden, müssen Sie die ADMX-Vorlagendatei zu einem GPO auf dem Active Directory-Server hinzufügen. Bei einem virtuellen Desktop muss das GPO mit der OU verknüpft werden, die den virtuellen Desktop enthält. Bei einem veröffentlichten Desktop muss das GPO mit der OU verknüpft werden, die den RDS-Host enthält.

Voraussetzungen

- Konfigurieren der Browser-Umleitungsfunktion. Siehe [Installieren und Konfigurieren der Browser-Umleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- 1 Laden Sie die Google Chrome-Datei `policy_templates.zip` unter https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip herunter.
- 2 Entpacken Sie die Datei `policy_templates.zip` und kopieren Sie die Dateien `chrome.admx` und `chrome.adml` auf Ihren Active Directory-Server.

Die Datei `chrome.admx` befindet sich im Ordner `\windows\admx` und die Datei `chrome.adml` im Ordner `\windows\admx\Sprache` der Datei `policy_templates.zip`.
 - a Kopieren Sie die Datei `chrome.admx` in den Ordner `%systemroot%\PolicyDefinitions` auf Ihrem Active Directory-Server.
 - b Kopieren Sie die Sprachressourcendatei `chrome.adml` in den entsprechenden Sprachen-Unterordner des Ordners `%systemroot%\PolicyDefinitions` auf Ihrem Active Directory-Server.

Kopieren Sie beispielsweise die `en_us`-Version der Datei `chrome.adml` in den Unterordner `%systemroot%\PolicyDefinitions\en_us` auf Ihrem Active Directory-Server.
- 3 Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf dem Active Directory-Server, und navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Google Chrome > Erweiterungen**.
- 4 Öffnen Sie die Richtlinieneinstellung **Liste der zwangsweise installierten Anwendungen und Erweiterungen konfigurieren** und klicken Sie auf **Aktiviert**.
- 5 Klicken Sie auf **Anzeigen** und geben Sie `demgbalbngngkkgjcofhdiipjblblob;https://clients2.google.com/service/update2/crx` in die Spalte „Wert“ ein.
- 6 Klicken Sie auf **OK**, um die Erweiterungs-ID/Update-URL zu speichern, und dann auf **OK**, um die Richtlinieneinstellung zu speichern.
- 7 Stellen Sie sicher, dass die Erweiterung „VMware Horizon-Browser-Umleitung“ auf dem Remote-Desktop installiert ist.
 - a Stellen Sie eine Verbindung zum Remote-Desktop her und starten Sie Chrome.
 - b Geben Sie in der Adressleiste von Chrome `chrome://extensions` ein.

VMware Horizon-Browsererweiterung wird in der Liste der Erweiterungen angezeigt.

Einschränkungen der Browser-Umleitung

Für die Browser-Umleitungsfunktion gelten bestimmte Einschränkungen.

- Diese Funktion wird nur für Windows-Clients unterstützt.
- Nur die VMware Blast- und PCoIP-Anzeigeprotokolle werden unterstützt. Das RDP-Protokoll wird nicht unterstützt.

- Die Browser-Umleitung funktioniert nicht mit den folgenden Funktionen der Horizon 7-Umleitung:
 - URL-Inhaltsumleitung.
 - Funktion der HTML5-Multimedia-Umleitung in Chrome. Wenn die Erweiterung „VMware Horizon-Browser-Umleitung“ und die Erweiterung „HTML5-Multimedia-Umleitung“ in Chrome installiert sind und die Gruppenrichtlinieneinstellungen für beide Funktionen ordnungsgemäß konfiguriert sind, funktioniert nur die Browser-Umleitung.
 - Geolocation-Umleitung. Wenn beide Funktionen konfiguriert sind, hat die Browser-Umleitung Vorrang.
- Andere Protokolle als http und https, wie z. B. mailto, werden nicht unterstützt.
- Diese Funktion wird nur für Chrome-Browser unterstützt.
- Die Browser-Umleitung funktioniert nicht, wenn Sie Chrome mit einem Ausführungsbefehl starten, z. B. **chrome *url***, auf eine URL in einem Editor klicken oder ein Lesezeichen-Element aus dem Chrome-Menü **Lesezeichen** in den Remote-Desktop ziehen und auf das Verknüpfungssymbol doppelklicken.
- Wenn Sie die Browser-Umleitungsfunktion im Chrome-Browser verwenden, treten möglicherweise die folgenden browserbezogenen Einschränkungen auf.
 - Popup-Fenster werden immer in einer neuen Registerkarte geöffnet.
 - Popup-Fenster zu Berechtigungen werden nicht angezeigt.
 - Es ist nicht möglich, einen Link im umgeleiteten Ansichtsfenster in die Adressleiste zu ziehen.
 - Es ist nicht möglich, eine Datei herunterzuladen oder ein Image zu speichern.
 - Es ist nicht möglich, Kennwörter für Websites zu speichern, für die eine Authentifizierung erforderlich ist.
 - Um eine Registerkarte zu schließen, wechseln Sie mit dem Fokus zur Browser-Registerkarte. Wenn Sie ALT+F4, STRG+F4 oder STRG+W drücken, während sich der Fokus auf dem Viewport befindet, kann dies zu unerwartetem Verhalten führen.
 - Das Löschen von Browserdaten, einschließlich Cookies, hat keine Auswirkungen.
 - Manchmal ist es nicht möglich, zur vorherigen Seite zurückzukehren oder weiterzuleiten.

Konfigurieren der Geolocation-Umleitung

Mit der Funktion der Geolocation-Umleitung können Remote-Desktops und veröffentlichte Anwendungen die Geolocation-Informationen des Clientgeräts verwenden.

Systemanforderungen für die Geolocation-Umleitung

Horizon Agent und Horizon Client und der virtuelle Desktop oder RDS-Host und der Client-Computer, auf dem Sie die Agent- und Client-Software installieren, müssen bestimmte Anforderungen erfüllen, um die Geolocation-Umleitungsfunktion zu unterstützen.

Virtueller Desktop oder RDS-Host

- Die Windows-Einstellung **Standortdienste** muss unter **Einstellungen > DatenschutzStandort** aktiviert sein.
- Die Geolocation-Umleitung unterstützt folgende Remote-Desktop-Anwendungen.

Anwendung	Plattform
Google Chrome (neueste Version)	Alle virtuellen Desktops oder RDS-Hosts
Internet Explorer 11	Alle virtuellen Desktops oder RDS-Hosts
Edge, Maps, Weather und andere Win32- und UWP-Apps	Windows 8,1 und Windows 10

Die Berechtigungseinstellung für den **Standort** muss, falls vorhanden, einzeln in jedem unterstützten Browser aktiviert werden.

- Für Horizon Agent 7.6 oder höher muss bei der Installation die benutzerdefinierte Setup-Option für die Geolocation-Umleitung aktiviert werden. Diese Option ist nicht standardmäßig ausgewählt. Weitere Informationen finden Sie in den Abschnitten zum Installieren von Horizon Agent in den Dokumenten *Einrichten von virtuellen Desktops in Horizon 7* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Die Gruppenrichtlinieneinstellungen für die VMware Geolocation-Umleitung müssen auf dem Active Directory-Server konfiguriert werden. Siehe [Installieren und Konfigurieren der Geolocation-Umleitung](#).
- Für Internet Explorer 11 muss das Internet Explorer-Plug-in für die VMware Horizon Geolocation-Umleitung für virtuelle Windows 7-Desktops und RDS-Hosts aktiviert werden. Siehe [Aktivieren des Internet Explorer-Plug-ins für die VMware Horizon Geolocation-Umleitung](#). Sie müssen das IE-Plug-in für die VMware Horizon Geolocation-Umleitung für virtuelle Windows 8.1- und Windows 10-Desktops nicht aktivieren. Internet Explorer wird auf virtuellen Windows 8.1- und Windows 10-Desktops mit dem VMware Geolocation-Umleitungstreiber unterstützt.

- Bei Chrome muss das Chrome-Plug-in für die VMware Horizon Geolocation-Umleitung aktiviert werden. Siehe [Aktivieren des Chrome-Plug-Ins für die VMware Horizon Geolocation-Umleitung](#).

Clientsystem

- Damit Horizon auf den Standort zugreifen kann, muss für Windows 8.1- und Windows 10-Client-Systeme für die Windows-Einstellung **Positionsdienst** unter **Einstellungen > Datenschutz > PositionEin** festgelegt werden.
- Sie müssen Horizon Client für Windows 4.9 oder höher auf dem Client-System installieren und die Standortinformationen des Client-Systems freigeben, indem Sie die **Geolocation**-Einstellungen in Horizon Client für Windows konfigurieren. Nicht-Windows-Clients werden nicht unterstützt. Informationen hierzu finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

Das Anzeigeprotokoll für die Remote-Sitzung ist

- PCoIP
- VMware Blast

Installieren und Konfigurieren der Geolocation-Umleitung

Um Geolocation-Informationen vom Client-Gerät an Remote-Desktops oder veröffentlichte Anwendungen umzuleiten, müssen die Funktion für die Geolocation-Umleitung aktiviert, die Gruppenrichtlinieneinstellungen auf dem Active Directory-Server konfiguriert und die von dieser Funktion verwendeten Websites angegeben werden.

Um die Geolocation-Umleitung zu aktivieren und festzulegen, welche Websites diese Funktion verwenden, konfigurieren Sie Gruppenrichtlinieneinstellungen auf dem Active Directory-Server. Sie müssen eine Liste mit URLs für Websites kompilieren, die die umgeleiteten Geolocation-Informationen verwenden können. Fügen Sie den URLs das Präfix `http://` oder `https://` hinzu. Sie können den URL-Musterabgleich verwenden.

Voraussetzungen

- Installieren Sie Horizon Client auf dem Client-System und installieren Sie Horizon Agent im virtuellen Desktop oder RDS-Host mit aktivierter Geolocation-Umleitung. Informationen zu den erforderlichen Versionen, Setup-Optionen und vollständigen Systemanforderungen finden Sie im Abschnitt [Systemanforderungen für die Geolocation-Umleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Stellen Sie sicher, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.

- Fügen Sie die VMware View Agent-ADMX-Vorlagendatei für die Konfiguration (`vdm_agent.admx`) zu einem GPO hinzu, das mit der Organisationseinheit für den virtuellen Desktop oder RDS-Host verknüpft ist. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).
- Kompilieren Sie eine Liste mit URLs für Websites, die die umgeleiteten Geolocation-Informationen verwenden können.
- Installieren Sie Internet Explorer 11 oder Chrome auf dem Agent-Computer.

Verfahren

- 1 Öffnen Sie auf Ihrem Active Directory-Server den Editor zur Gruppenrichtlinienverwaltung.
- 2 Wechseln Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen**.
- 3 Öffnen Sie die Einstellung **Automatische Intranet-Erkennung deaktivieren**, wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.
- 4 Öffnen Sie die Einstellung **VMware HTML5-Funktionen aktivieren**, wählen Sie **Aktiviert** aus, und klicken Sie dann auf **OK**.
- 5 Navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware Geolocation-Umleitung**.
- 6 Öffnen Sie die Einstellung **VMware Geolocation-Umleitung**, wählen Sie **Aktiviert** aus und klicken Sie dann auf **OK**.
- 7 Geben Sie an, welche Websites die Geolocation-Umleitung verwenden können.

Die Chrome-Plug-in für die VMware Horizon Geolocation-Umleitung verwendet diese Websitelliste in allen RDS-Host- und virtuellen Desktop-Umgebungen. Das IE-Plug-In für die VMware Horizon Geolocation-Umleitung verwendet diese Websitelliste in RDS-Host- und virtuellen Windows 7-Desktop-Umgebungen.

- a Öffnen Sie die Einstellung **URL-Liste für VMware Geolocation-Umleitung aktivieren** und wählen Sie **Aktiviert** aus.
- b Klicken Sie auf **Anzeigen** und geben Sie die URLs, die Sie kompiliert haben, in die Spalte „Wertname“ ein.

Nur die angegebenen URLs können die umgeleiteten Geolocation-Informationen verwenden. Standardmäßig werden keine URLs hinzugefügt. Lassen Sie die Spalte „Wert“ leer.

- c Klicken Sie auf **OK**, um die URL-Liste zu speichern, und dann auf **OK**, um die Richtlinieneinstellung zu speichern.

- 8 Öffnen Sie die Einstellung **Mindestentfernung zum Melden von Standort-Updates festlegen**, wählen Sie **Aktiviert** aus, und geben Sie die Mindestentfernung (in Metern) zwischen einem Standort-Update auf dem Client und dem zuletzt an den Agent gemeldeten Update, für das der neue Standort aktualisiert werden muss, an.

Standardmäßig liegt die Mindestentfernung bei 75 Metern.

Nächste Schritte

Wenn Sie Internet Explorer auf einem virtuellen Windows 7-Desktop oder einem RDS-Hostagent-Computer installiert haben, müssen Sie auch das IE-Plug-in für die VMware Horizon Geolocation-Umleitung aktivieren. Weitere Informationen hierzu finden Sie unter [Aktivieren des Internet Explorer-Plug-ins für die VMware Horizon Geolocation-Umleitung](#).

Hinweis Internet Explorer wird auf virtuellen Windows 8.1- und Windows 10-Desktops mit dem VMware Geolocation-Umleitungstreiber unterstützt. Sie müssen das IE-Plug-in für die VMware Horizon Geolocation-Umleitung für virtuelle Windows 8.1- und Windows 10-Desktops nicht aktivieren.

Wenn Sie Chrome auf dem Agent-Computer installiert haben, müssen Sie auch das Chrome-Plug-in für die VMware Horizon Geolocation-Umleitung aktivieren. Weitere Informationen hierzu finden Sie unter [Aktivieren des Chrome-Plug-Ins für die VMware Horizon Geolocation-Umleitung](#).

Aktivieren des Internet Explorer-Plug-ins für die VMware Horizon Geolocation-Umleitung

Um Internet Explorer auf einem virtuellen Desktop oder veröffentlichten Desktop unter Windows 7 mit der Funktion der Geolocation-Umleitung zu verwenden, müssen Sie das IE-Plug-in für die VMware Horizon Geolocation-Umleitung auf dem virtuellen Desktop oder RDS-Host aktivieren.

Internet Explorer wird auf virtuellen Windows 8.1- und Windows 10-Desktops mit dem VMware Geolocation-Umleitungstreiber unterstützt. Sie müssen das IE-Plug-in für die VMware Horizon Geolocation-Umleitung für virtuelle Windows 8.1- und Windows 10-Desktops nicht aktivieren.

Voraussetzungen

- [Installieren und Konfigurieren der Geolocation-Umleitung](#).
- Prüfen Sie, ob in Internet Explorer 11 die Option **Erweiterter Schutzmodus** ausgeschaltet ist. Das Plug-In funktioniert nicht, wenn diese Funktion aktiviert ist.
- Stellen Sie für Windows Server-Betriebssysteme sicher, dass die **Verstärkte Sicherheitskonfiguration für Internet Explorer** deaktiviert ist. Das Plug-In funktioniert nicht, wenn diese Funktion aktiviert ist.

Verfahren

- 1 Öffnen Sie Internet Explorer 11 auf dem virtuellen Desktop oder RDS-Host, auf dem die Geolocation-Umleitungsfunktion aktiviert ist.
- 2 Klicken Sie rechts oben im Browserfenster auf das Symbol **Extras** und wählen Sie **Add-ons verwalten** aus.

- 3 Führen Sie einen Bildlauf zum Abschnitt „VMware, Inc.“ durch, wählen Sie das **Internet Explorer-Plug-In für die VMware Horizon Geolocation-Umleitung** aus und klicken Sie auf **Aktivieren**.
- 4 Starten Sie Internet Explorer 11 neu.

Aktivieren des Chrome-Plug-Ins für die VMware Horizon Geolocation-Umleitung

Um die Geolocation-Umleitungsfunktion mit Chrome zu verwenden, müssen Sie das Chrome-Plug-in für die VMware Horizon Geolocation-Umleitung aktivieren.

Voraussetzungen

[Installieren und Konfigurieren der Geolocation-Umleitung.](#)

Verfahren

- 1 Laden Sie die Datei https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip auf Ihrem Active Directory-Server herunter.
- 2 Extrahieren Sie die Datei `chrome.admx` und kopieren Sie sie in den Ordner `%systemroot%\PolicyDefinitions` auf Ihrem Active Directory-Server.
- 3 Entpacken Sie die Sprachressourcendatei `chrome.adml`, und kopieren Sie sie in den entsprechenden Sprachen-Unterordner des Ordners `%systemroot%\PolicyDefinitions\` auf Ihrem Active Directory-Server.

Kopieren Sie beispielsweise die `en_us`-Version der Datei `chrome.adml` in den Unterordner `%systemroot%\PolicyDefinitions\en_us` auf Ihrem Active Directory-Server.
- 4 Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf dem Active Directory-Server, und navigieren Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Google Chrome > Erweiterungen**.
- 5 Öffnen Sie die Gruppenrichtlinieneinstellung **Liste der zwangsweise installierten Anwendungen und Erweiterungen konfigurieren**, und klicken Sie auf **Aktiviert**.
- 6 Klicken Sie auf **Anzeigen**, geben Sie `Indponbebpoechnoblfgdfeiegeaokcf;https://clients2.google.com/service/update2/crx` in das Textfeld **Wert** ein, und klicken Sie auf **OK**.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
- 8 Um sicherzustellen, dass die Erweiterung VMware Horizon Geolocation-Umleitung auf dem Remote-Desktop installiert ist, führen Sie die folgenden Schritte aus.
 - a Stellen Sie eine Verbindung zum Remote-Desktop her und starten Sie Chrome.
 - b Geben Sie in der Adressleiste von Chrome `chrome://extensions` ein.
 - c Überprüfen Sie, ob die VMware Horizon Geolocation-Umleitung in die Liste der Erweiterungen angezeigt wird.

Konfigurieren von Echtzeit-Audio/Video

Die Echtzeit-Audio/Video-Funktion ermöglicht es Horizon 7-Benutzern, Skype, Webex, Google Hangouts, Microsoft Teams und andere Anwendungen für Onlinekonferenzen auf ihren Remote-Sitzungen auszuführen. Mit der Echtzeit-Audio/Video-Funktion werden Webcams und Audiogeräte, die lokal an das Clientsystem angeschlossen sind, an den Remote-Sitzungen umgeleitet. Diese Funktion leitet Video- und Audio-Daten mit deutlich weniger Bandbreite um, als mit der USB-Umleitung erreicht werden kann.

Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Bei der Einrichtung einer Anwendung wie Skype, Webex, Google Hangouts oder Microsoft Teams können Benutzer Ein- und Ausgabegeräte aus Menüs in der Anwendung auswählen.

- Bei virtuellen Desktops mit Horizon Client für Windows 5.2 und höher kann Echtzeit-Audio/Video mehrere Audiogeräte und Videogeräte umleiten. Die Namen der umgeleiteten Geräte im virtuellen Desktop sind die tatsächlichen Gerätenamen, allerdings mit dem Zusatz „(VDI)“. Beispiel: C670i FHD Webcam (VDI).
- Für virtuelle Desktops mit Horizon Client für Windows 5.1 oder früher oder mit einem Nicht-Windows-Client kann Echtzeit-Audio/Video nur ein Audiogerät und nur ein Videogerät zu einem virtuellen Desktop umleiten. Die Gerätenamen sind im virtuellen Desktop „Virtuelles VMware-Mikrofon“ und „Virtuelle VMware-Webcam“.
- Für veröffentlichte Desktops und veröffentlichte Anwendungen kann Echtzeit-Audio/Video nur ein Audiogerät und nur ein Video Gerät umleiten. Die Gerätenamen sind in Remote-Sitzungen „Remotearaudiogerät“ und „virtuelle VMware-Webcam“.

Die virtuelle VMware-Webcam verwendet einen Kernel-Webcam-Treiber, der eine bessere Kompatibilität mit browserbasierten Videoanwendungen und anderer Konferenzsoftware von Drittanbietern bietet.

Beim Start einer Konferenz- oder Videoanwendung werden diese virtuellen VMware-Geräte angezeigt und verwendet und sorgen für die Audio/Video-Umleitung von den lokal angeschlossenen Geräten auf dem Client.

Die Treiber für die Audiogeräte und Webcams müssen auf den Horizon Client-Systemen installiert sein, um die Umleitung zu aktivieren.

Konfigurationsmöglichkeiten für Echtzeit-Audio/Video

Nachdem Sie Horizon Agent mit Echtzeit-Audio/Video installiert haben, funktioniert diese Funktion bei Remotesitzungen ohne eine weitere Konfiguration. Die Standardwerte für Webcam-Bildrate und -Bildauflösung werden für die meisten Standardgeräte und -anwendungen empfohlen.

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um diese Standardwerte an bestimmte Anwendungen, Webcams oder Umgebungen anzupassen. Sie können auch eine Richtlinie festlegen, um die Funktion zu deaktivieren oder zu aktivieren. Mit einer ADMX-Vorlagendatei können Sie Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video in Active Directory oder auf einzelnen Desktops installieren. Siehe [Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video](#).

Wenn Benutzer über mehrere integrierte oder an ihre Clientcomputer angeschlossene Webcams und Audioeingabegeräte verfügen, müssen Sie bevorzugte Webcams und Audioeingabegeräte unter Umständen konfigurieren, um sie umzuleiten. Weitere Informationen hierzu finden Sie unter [Auswählen von bevorzugten Webcams und Mikrofonen](#).

Hinweis Sie können ein bevorzugtes Audiogerät auswählen, es stehen jedoch keine weiteren Optionen für die Audiokonfiguration zur Verfügung.

Wenn Webcambilder und Audioeingangsdaten an eine Remotesitzung umgeleitet werden, können Sie auf dem lokalen Computer nicht auf die Webcam oder die Audiogeräte zugreifen. Ebenso können diese Geräte nicht bei der Remotesitzung verwendet werden, wenn auf dem lokalen Computer darauf zugegriffen wird.

Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video funktioniert mit Standard-Webcams, USB-Audiogeräten und analogen Audiogeräten. Die Funktion funktioniert auch mit Standard-Konferenzanwendungen. Zur Unterstützung von Echtzeit-Audio/Video muss Ihre Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Virtuelle Desktops

Bei der Verwendung von Microsoft-Teams mit Echtzeit-Audio/Video empfiehlt VMware ein Minimum von 4 vCPUs und 4 GB RAM für virtuelle Desktops.

Horizon Client-Software

- Horizon Client für Windows, Version 2.2 oder höher. Um mehr als eine Webcam oder ein Mikrofon in einem virtuellen Desktop verwenden zu können, muss Horizon Client für Windows 5.2 oder höher installiert sein.
- Horizon Client für Linux, Version 2.2 oder höher. Für Version 3.1 oder eine ältere Version steht diese Funktion nur mit der von Drittanbietern bereitgestellten Horizon Client-Version für Linux zur Verfügung. Für Version 3.2 und höher steht diese Funktion auch mit der über VMware verfügbaren Clientversion zur Verfügung.
- Horizon Client für Mac, Version 2.3 oder höher.
- Horizon Client für iOS, Version 4.0 oder höher.
- Horizon Client für Android, Version 4.0 oder höher.
- Horizon Client für Chrome OS, Version 4.3 oder höher
- Horizon Client für Chrome, Version 4.8 oder höher.
- Horizon Client für Windows 10 UWP, Version 5.2 oder höher.

Horizon Client-Computer oder Clientzugriffsgerät

- Alle Betriebssysteme, auf denen Horizon Client für Windows, iOS, Android, Chrome OS, Chrome und Windows 10 UWP ausgeführt werden.

- Alle Betriebssysteme, unter denen Horizon Client für Linux auf x86-Geräten ausgeführt wird. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- Mac OS X Mountain Lion (10.8) und höher. Auf allen älteren Mac OS X-Betriebssystemen ist diese Funktion deaktiviert.
- Weitere Informationen zu den unterstützten Clientbetriebssystemen finden Sie im Dokument zur Installation und Einrichtung von Horizon Client für das entsprechende System oder Gerät.
- Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Es ist nicht erforderlich, die Gerätetreiber auf dem Computer zu installieren, auf dem der Agent installiert ist.

Anzeigeprotokolle

- PCoIP

Hinweis In Horizon Client für Windows 10 UWP wird Echtzeit-Audio/Video mit PCoIP nicht unterstützt.

- VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Sicherstellen, dass anstelle der USB-Umleitung Echtzeit-Audio/Video verwendet wird

Echtzeit-Audio/Video unterstützt die Umleitung von Webcam- und Audio-Eingaben für die Verwendung in Konferenzanwendungen. Die Funktion zur USB-Umleitung, die gemeinsam mit Horizon Agent installiert werden kann, unterstützt die Webcam-Umleitung nicht. Wenn Sie Audioeingabegeräte über die USB-Umleitung umleiten, wird der Audio-Stream in Echtzeit-Audio/Video-Sitzungen nicht korrekt mit dem Video synchronisiert und Sie büßen außerdem den Vorteil der verringerten Anforderungen an die Netzwerkbandbreite ein. Mithilfe dieser Schritte können Sie sicherstellen, dass Webcams und Audio-Eingabegeräte über Echtzeit-Audio/Video zu Ihren Desktops umgeleitet werden und nicht über die USB-Umleitung.

Wenn Ihre Desktops mit der USB-Umleitung konfiguriert sind, können Endbenutzer ihre lokal verbundenen USB-Geräte verbinden und anzeigen, indem sie in der Menüleiste des Windows-Clients die Option **USB-Gerät verbinden** oder im Mac-Client die Option **Desktop > USB** auswählen. Linux-Clients blockieren standardmäßig die USB-Umleitung von Audio- und Videogeräten und bieten keine USB-Geräte-Optionen für Endbenutzer.

Wenn ein Endbenutzer ein USB-Gerät aus der Liste unter **USB-Gerät verbinden** oder **Desktop > USB** auswählt, kann dieses Gerät nicht mehr für Video- oder Audiokonferenzen verwendet werden. Wenn ein Benutzer beispielsweise einen Skype-Anruf durchführt, wird das Video-Bild möglicherweise nicht angezeigt oder der Audio-Stream ist möglicherweise nur eingeschränkt verfügbar. Wenn ein Endbenutzer während einer Konferenzsitzung ein Gerät auswählt, wird die Webcam- oder Audio-Umleitung unterbrochen.

Um diese Geräte für Endbenutzer auszublenden und potenzielle Störungen zu vermeiden, können Sie Gruppenrichtlinieneinstellungen für die USB-Umleitung konfigurieren. Auf diese Weise können Sie die Anzeige von Webcams und Audioeingabegeräten in VMware Horizon Client deaktivieren.

Sie können insbesondere Filterregeln für die USB-Umleitung für Horizon Agent erstellen und angeben, dass die Gerätefamilien `audio-in` und `video` deaktiviert werden. Weitere Informationen zum Festlegen von Gruppenrichtlinien und zum Angeben von Filterregeln für die USB-Umleitung finden Sie unter [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#).

Vorsicht Wenn Sie keine Filterregeln für die USB-Umleitung einrichten, um die USB-Gerätefamilien zu deaktivieren, informieren Sie Ihre Endbenutzer darüber, dass sie aus der Liste unter **USB-Gerät verbinden** oder **Desktop > USB** in der VMware Horizon Client-Menüleiste keine Webcam- oder Audio-Geräte auswählen können.

Auswählen von bevorzugten Webcams und Mikrofonen

Wenn ein Clientcomputer über mehrere Webcams und Mikrofone verfügt, können Sie eine bevorzugte Webcam und ein Mikrofon konfigurieren, die bzw. das über die Echtzeit-Audio/Video-Funktion an den Remote-Desktop oder die veröffentlichte Anwendung umgeleitet wird. Diese Geräte können in den Clientcomputer integriert oder mit diesem verbunden sein.

Die Echtzeit-Audio/Video-Funktion leitet die bevorzugte Webcam um, sofern diese verfügbar ist. Wenn die bevorzugte Webcam nicht verfügbar ist, verwendet Echtzeit-Audio/Video die erste durch die System-Enumeration bereitgestellte Webcam.

Windows-Clientcomputer

Wenn bei einem veröffentlichten Desktop oder einer veröffentlichten Anwendung Horizon Client für Windows 4.2 oder eine spätere Version auf dem Clientcomputer installiert ist, wählen Sie eine bevorzugte Webcam bzw. ein bevorzugtes Mikrofon aus, indem Sie die Einstellungen für Echtzeit-Audio/Video im Dialogfeld „Horizon Client-Einstellungen“ konfigurieren.

Wenn bei einem virtuellen Desktop Horizon Client für Windows 4.2 bis 5.1 auf dem Clientcomputer installiert ist, können Sie eine bevorzugte Webcam bzw. ein bevorzugtes Mikrofon auswählen, indem Sie die Einstellungen für Echtzeit-Audio/Video im Dialogfeld „Horizon Client-Einstellungen“ konfigurieren. Ab Horizon Client für Windows 5.2 und Horizon Agent 7.10 kann die Echtzeit-Audio/Video-Funktion mehr als eine Webcam und ein Mikrofon an einen virtuellen Desktop umleiten. Außerdem müssen Sie keine bevorzugte Webcam bzw. kein bevorzugtes Mikrofon auswählen.

Bei Horizon Client für frühere Windows-Versionen als 4.2 müssen Sie die Registrierungseinstellungen anpassen, um eine bevorzugte Webcam auszuwählen, und die Systemsteuerungsoption für den Sound des Windows-Betriebssystems nutzen, um ein Standardmikrofon auszuwählen.

	Weitere Informationen finden Sie im Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
Mac-Clientcomputer	Sie geben eine bevorzugte Webcam oder ein bevorzugtes Mikrofon mithilfe des Mac-Standardsystems an. Weitere Informationen finden Sie im Dokument <i>VMware Horizon Client für Mac Installations- und Einrichtungshandbuch</i> .
Linux-Clientcomputer	Sie geben eine bevorzugte Webcam an, indem Sie eine Konfigurationsdatei bearbeiten. Zur Auswahl eines Standardmikrofons konfigurieren Sie die Option „Sound“ im Linux-Betriebssystem auf dem Clientcomputer. Weitere Informationen finden Sie im Dokument <i>VMware Horizon Client für Linux Installations- und Einrichtungshandbuch</i> .
Chromebook-Clientcomputer	Wenn auf dem Chromebook Horizon Client für Chrome 4.8 oder eine spätere Version installiert ist, legen Sie eine bevorzugte Webcam bzw. ein bevorzugtes Mikrofon fest, indem Sie die Einstellungen für Echtzeit-Audio/Video im Dialogfeld „Horizon Client-Einstellungen“ konfigurieren. Weitere Informationen finden Sie im Dokument <i>VMware Horizon Client für Chrome Installations- und Einrichtungshandbuch</i> .
Windows 10 UWP-Clientcomputer	Wenn auf dem Windows 10 UWP-Computer Horizon Client für Windows 10 UWP 5.2 oder eine spätere Version installiert ist, legen Sie eine bevorzugte Webcam bzw. ein bevorzugtes Mikrofon fest, indem Sie die Einstellungen für Echtzeit-Audio/Video im Dialogfeld „Horizon Client-Einstellungen“ konfigurieren. Weitere Informationen finden Sie im Dokument <i>VMware Horizon Client für Windows 10 UWP Installations- und Einrichtungshandbuch</i> .

Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Echtzeit-Audio/Video-Funktion (Real-Time Audio-Video, RTAV) auf Ihren Remote-Desktops steuert. Mithilfe dieser Einstellungen wird die maximale Bildrate und -auflösung einer virtuellen Webcam festgelegt. Die Einstellungen ermöglichen es Ihnen, die maximale Bandbreite zu verwalten, die ein Benutzer belegen kann. Über eine zusätzliche Einstellung wird die RTAV-Funktion deaktiviert oder aktiviert.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Echtzeit-Audio/Video-Funktion verwendet die Bildrate und -auflösung, die für die Webcam auf den Clientsystemen festgelegt ist. Für die meisten Webcams und Audioanwendungen werden die Standardeinstellungen empfohlen.

Beispiele für die Bandbreitenbelegung durch die Echtzeit-Audio/Video-Funktion finden Sie unter [Bandbreite für Echtzeit-Audio/Video](#).

Diese Richtlinieneinstellungen wirken sich auf Ihre Remote-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen auf Ihren Desktops die administrative Vorlagendatei (ADMX) für die RTAV-Gruppenrichtlinie in Active Directory hinzu.

Informationen zum Konfigurieren von Einstellungen auf Clientsystemen finden Sie im VMware KB-Artikel *Festlegen von Frame-Raten und Auflösung für Echtzeit-Audio/Video auf Horizon View Clients* unter <http://kb.vmware.com/kb/2053644>.

Hinzufügen der RTAV ADMX-Vorlage in Active Directory und Konfigurieren der Einstellungen

Sie können die Richtlinieneinstellungen in der RTAV-ADMX-Datei (`vdm_agent_rtav.admx`) zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und die Einstellungen im Gruppenrichtlinienobjekt-Editor konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass die Setup-Option „RTAV“ auf den Desktops für virtuelle Maschinen und RDS-Hosts installiert ist. Diese Setupoption wird standardmäßig installiert, kann aber während der Installation abgewählt werden. Die Einstellungen haben keine Auswirkungen, wenn RTAV nicht installiert ist. Informationen zur Installation von Horizon Agent finden Sie in Ihrem Dokument für die Einrichtung.
- Stellen Sie sicher, dass Active Directory-GPOs für die RTAV-Gruppenrichtlinieneinstellungen erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die die Desktops für virtuelle Maschinen oder RDS-Hosts enthält. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).
- Vergewissern Sie sich, dass Microsoft Management Console (MMC) und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den RTAV-Gruppenrichtlinieneinstellungen vertraut. Siehe [Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video](#).

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip und kopieren Sie die ADMX-Dateien auf Ihren Active Directory-Server.
 - a Kopieren Sie die Datei vdm_agent_rtav.admx und den Ordner en-US in den Ordner C:\Windows\PolicyDefinitions auf Ihrem Active Directory-Server.
 - b (Optional) Kopieren Sie die Sprachressourcendatei (vdm_agent_rtav.adml) in den entsprechenden Unterordner in C:\Windows\PolicyDefinitions\ auf Ihrem Active Directory-Server.
- 3 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und geben Sie dort den Pfad zur Vorlagendatei ein.

Die Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > View-RTAV-Konfiguration** enthalten.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Mithilfe der Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video (RTAV) werden die maximale Frame-Rate und -Auflösung einer virtuellen Webcam gesteuert. Über eine zusätzliche Einstellung können Sie die RTAV-Funktion deaktivieren oder aktivieren. Diese Richtlinieneinstellungen wirken sich auf Remote-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind.

Wenn Sie die RTAV-Gruppenrichtlinieneinstellungen nicht konfigurieren, verwendet RTAV die Werte, die auf den Clientsystemen festgelegt sind. Die standardmäßige Webcam-Bildrate auf Clientsystemen beträgt 15 Frames pro Sekunde. Die standardmäßige Bildauflösung für die Webcam beträgt 320x240 Pixel.

Die Gruppenrichtlinieneinstellungen für die Auflösung bestimmen die Maximalwerte, die verwendet werden können. Die Frame-Rate und -Auflösung, die auf den Clientsystemen festgelegt sind, sind absolute Werte. Beispiel: Wenn Sie die RTAV-Einstellungen für die maximale Bildauflösung auf 640x480 Pixel konfigurieren, zeigt die Webcam alle Auflösungen an, die auf dem Client auf bis zu 640x480 Pixel festgelegt wurde. Wenn Sie die Bildauflösung auf dem Client auf einen Wert über 640x480 Pixel festlegen, beträgt die Obergrenze der Client-Auflösung 640x480 Pixel.

Nicht alle Konfigurationen können die maximalen Gruppenrichtlinieneinstellungen mit einer Auflösung von 1920x1080 bei 25 Frames pro Sekunde erreichen. Welche maximale Frame-Rate Ihre Konfiguration für eine bestimmte Auflösung erreichen kann, hängt von der Webcam, die noch verwendet wird, von der Clientsystem-Hardware, der virtuellen Horizon Agent-Hardware und der verfügbaren Bandbreite ab.

Die Gruppenrichtlinieneinstellungen für die Auflösung bestimmen die standardmäßigen Werte, die verwendet werden, wenn die Auflösungswerte nicht vom Benutzer festgelegt werden.

Gruppenrichtlinieneinstellung	Beschreibung
Disable RTAV	<p>Wenn Sie diese Einstellung aktivieren, wird die Echtzeit-Audio/Video-Funktion deaktiviert.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird Echtzeit-Audio/Video aktiviert.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration im Gruppenrichtlinienverwaltungs-Editor.</p>
Max frames per second	<p>Bestimmt die maximale Rate pro Sekunde, in der die Webcam Frames aufnehmen kann. Sie können diese Einstellung verwenden, um die Frame-Rate der Webcam in Netzwerkumgebungen mit einer geringen Bandbreite einzuschränken.</p> <p>Der Minimalwert beträgt ein Frame pro Sekunde. Der Maximalwert beträgt 25 Frames pro Sekunde.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Frame-Rate festgelegt. Echtzeit-Audio/Video verwendet die Frame-Rate, die für die Webcam auf dem Clientsystem ausgewählt wurde.</p> <p>Standardmäßig verfügen Webcams über eine Frame-Rate von 15 Frames pro Sekunde.</p> <p>Wenn keine Einstellung auf dem Clientsystem konfiguriert ist und die Einstellung Maximale Bilder pro Sekunde nicht konfiguriert oder deaktiviert ist, erfasst die Webcam 15 Frames pro Sekunde.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings im Gruppenrichtlinienverwaltungs-Editor.</p>
Resolution – Max image width in pixels	<p>Bestimmt die maximale Breite von Bildframes in Pixel, die von der Webcam erfasst werden. Durch das Festlegen einer niedrigen, maximalen Bildbreite können Sie die Auflösung von erfassten Frames verringern, die die Erfahrung bei der Bildverarbeitung in Netzwerkumgebungen mit einer geringen Bandbreite verbessern können.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Bildbreite festgelegt. RTAV verwendet die Bildbreite, die auf dem Clientsystem festgelegt wurde. Die Standardbreite eines Webcam-Bildes auf einem Clientsystem beträgt 320 Pixel.</p> <p>Die maximale Größe für ein Webcam-Bild beträgt 1920x1080 Pixel. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der 1920 Pixel überschreitet, beträgt die effektive, maximale Bildbreite 1920 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings im Gruppenrichtlinienverwaltungs-Editor.</p>
Resolution – Max image height in pixels	<p>Bestimmt die maximale Höhe von Bildframes in Pixel, die von der Webcam erfasst werden. Durch das Festlegen einer niedrigen, maximalen Bildhöhe können Sie die Auflösung von erfassten Frames verringern, die die Erfahrung bei der Bildverarbeitung in Netzwerkumgebungen mit einer geringen Bandbreite verbessern können.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Bildhöhe festgelegt. RTAV verwendet die Bildhöhe, die auf dem Clientsystem festgelegt wurde. Die Standardhöhe eines Webcam-Bildes auf einem Clientsystem beträgt 240 Pixel.</p> <p>Die maximale Größe für ein Webcam-Bild beträgt 1920x1080 Pixel. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der 1080 Pixel überschreitet, beträgt die effektive, maximale Bildhöhe 1080 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings im Gruppenrichtlinienverwaltungs-Editor.</p>

Gruppenrichtlinieneinstellung	Beschreibung
Resolution – Default image resolution width in pixels	<p>Bestimmt die standardmäßige Auflösungsbreite von Bildframes in Pixel, die von der Webcam erfasst werden. Diese Einstellung wird verwendet, wenn kein Auflösungswert vom Benutzer definiert wird.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, beträgt die standardmäßige Bildbreite 320 Pixel.</p> <p>Der Wert, der von der Richtlinieneinstellung konfiguriert wird, ist nur wirksam, wenn View Agent 6.0 oder höher sowie Horizon Client 3.0 oder höher verwendet werden. Diese Richtlinieneinstellung ist für ältere Versionen von View Agent und Horizon Client nicht wirksam. Zudem beträgt die standardmäßige Bildbreite 320 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings im Gruppenrichtlinienverwaltungs-Editor.</p>
Resolution – Default image resolution height in pixels	<p>Bestimmt die standardmäßige Auflösungshöhe von Bildframes in Pixel, die von der Webcam erfasst werden. Diese Einstellung wird verwendet, wenn kein Auflösungswert vom Benutzer definiert wird.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, beträgt die standardmäßige Bildhöhe 240 Pixel.</p> <p>Der Wert, der von der Richtlinieneinstellung konfiguriert wird, ist nur wirksam, wenn View Agent 6.0 oder höher sowie Horizon Client 3.0 oder höher verwendet werden. Diese Richtlinieneinstellung ist für ältere Versionen von View Agent und Horizon Client nicht wirksam. Zudem beträgt die standardmäßige Bildhöhe 240 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings im Gruppenrichtlinienverwaltungs-Editor.</p>

Bandbreite für Echtzeit-Audio/Video

Die Bandbreite für Echtzeit-Audio/Video variiert entsprechend der Webcam-Frame-Rate und -Bildauflösung und der erfassten Bild- und Audiodaten.

Die in [Tabelle 2-2. Beispielhafte Bandbreitenergebnisse für das Senden von Echtzeit-Audio/Video-Daten von Horizon Client an Horizon Agent](#) dargestellten Beispieltests messen die Bandbreite, die die Echtzeit-Audio/Video-Funktion in einer Horizon 7-Umgebung mit Standard-Webcams und Audioeingabegeräten verwendet. Diese Tests messen die Bandbreite für das Senden von Video- und Audiodaten von Horizon Client an Horizon Agent. Die für das Ausführen einer Desktop-Sitzung von Horizon Client erforderliche Gesamtbandbreite ist möglicherweise größer als diese Zahlen. Bei diesen Tests erfasst die Webcam Bilder bei 15 Frames pro Sekunde für jede Bildauflösung.

Tabelle 2-2. Beispielhafte Bandbreitenergebnisse für das Senden von Echtzeit-Audio/Video-Daten von Horizon Client an Horizon Agent

Bildauflösung (Breite x Höhe)	Verwendete Bandbreite (KBit/s)
160 x 120	225
320 x 240	320
640 x 480	600

Konfigurieren von Microsoft Teams mit Echtzeit-Audio/Video

Mit Echtzeit-Audio/Video können Benutzer Microsoft Teams in ihren Remote-Sitzungen ausführen.

Webcam- und Audiogeräte, die lokal mit dem Clientsystem verbunden sind, werden an die Remotesitzungen umgeleitet und verwenden eine deutlich geringere Bandbreite als bei der Verwendung der USB-Umleitung.

Wenn Sie die Microsoft-Teams-Anwendung in einem Remote-Desktop starten, wählen Sie virtuelle Ein- und Ausgabegeräte für VMware aus den Menüs in der Anwendung aus. Die virtuellen VMware-Geräte leiten die Audio- und Videogeräte um, die mit dem Clientcomputer verbunden sind.

- Bei virtuellen Desktops mit Horizon Client für Windows 5.2 und höher kann Echtzeit-Audio/Video mehrere Audiogeräte und Videogeräte umleiten. Die Namen der umgeleiteten Geräte im virtuellen Desktop sind die tatsächlichen Gerätenamen, allerdings mit dem Zusatz „(VDI)“. Beispiel: C670i FHD Webcam (VDI).
- Für virtuelle Desktops mit Horizon Client für Windows 5.1 oder früher oder mit einem Nicht-Windows-Client kann Echtzeit-Audio/Video nur ein Audiogerät und nur ein Videogerät zu einem virtuellen Desktop umleiten. Die Gerätenamen sind im virtuellen Desktop „Virtuelles VMware-Mikrofon“ und „Virtuelle VMware-Webcam“.
- Für veröffentlichte Desktops und veröffentlichte Anwendungen kann Echtzeit-Audio/Video nur ein Audiogerät und nur ein Video Gerät umleiten. Die Gerätenamen sind in Remote-Sitzungen „Remoteaudiogerät“ und „virtuelle VMware-Webcam“.

Um Echtzeit-Audio/Video mit Microsoft Teams zu verwenden, müssen Sie die Audio- und Webcam-Gerätetreiber auf Ihren Horizon Client-Systemen installieren.

Nachdem Sie Horizon Agent mit Echtzeit-Audio/Video installiert haben, funktioniert Microsoft Teams bei Remotesitzungen ohne weitere Konfiguration. Siehe [Konfigurieren von Echtzeit-Audio/Video](#).

Empfehlungen für die Verwendung von Microsoft Teams mit Echtzeit-Audio/Video

Um Microsoft Teams mit Echtzeit-Audio/Video zu verwenden, befolgen Sie diese Empfehlungen:

- Microsoft Teams mit Echtzeit-Audio/Video wird in Horizon Agent 7.9 und später auf Windows-, Linux- und Mac-Clients unterstützt.
- Microsoft Teams mit Echtzeit-Audio/Video erfordert eine Konfiguration mit mindestens 4 vCPU und 4 GB RAM mit einer maximalen Videoauflösung von 640 x 480 Pixel. Konfigurationen mit zusätzlichen vCPUs und mehr Speicher bieten ein besseres Erlebnis.
- Die standardmäßige Videoauflösung für Echtzeit-Audio/Video ist 320 x 240 Pixel. Sie können die Auflösung ändern, indem Sie die Einstellung im Ordner **VMware View Agent-Konfiguration > View-RTAV-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor ändern.

Konfigurieren der Scannerumleitung

Durch Verwenden der Scannerumleitung können Endbenutzer Informationen in ihren Remote-Desktops und -anwendungen mit Scan- und Bildverarbeitungsgeräten scannen, die lokal an ihren Clientcomputern angeschlossen sind.

Die Scannerumleitung unterstützt Standard-Scan- und Bildverarbeitungsgeräte, die mit den TWAIN- und WIA-Formaten kompatibel sind, sowie SANE auf Linux-Clients.

Nach der Installation von Horizon Agent mithilfe des Scannerumleitungs-Setup funktioniert die Funktion auf Ihren Remote-Desktops und -anwendungen, ohne dass eine weitere Konfiguration erforderlich ist. Sie müssen keine scannerspezifischen Treiber auf Remote-Desktops oder -anwendungen konfigurieren.

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um Standardwerte an bestimmte Scan- und Bildanwendungen oder -umgebungen anzupassen. Sie können auch eine Richtlinie festlegen, um die Funktion insgesamt zu deaktivieren oder zu aktivieren. Mit einer ADMX-Vorlagendatei können Sie Gruppenrichtlinieneinstellungen für die Scannerumleitung auf Ihrem Active Directory-Server oder auf einzelnen Desktops installieren. Siehe [Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

Wenn Scandaten an einen Remote-Desktop oder eine Remoteanwendung weitergeleitet werden, können Sie nicht auf das Scan- oder Bildverarbeitungsgerät auf dem lokalen Computer zugreifen. Ebenso kann dieses Gerät nicht auf dem Remote-Desktop oder der Remoteanwendung verwendet werden, wenn auf dem lokalen Computer darauf zugegriffen wird.

Systemanforderungen für Scannerumleitung

Zur Unterstützung der Scannerumleitung muss Ihre Horizon 7-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Remote-Desktop oder veröffentlichte Anwendung

Diese Funktion wird an veröffentlichten Desktops und in veröffentlichten Anwendungen auf RDS-Hosts unterstützt sowie an virtuellen Desktops, die auf virtuellen Maschinen für Einzelbenutzer bereitgestellt sind.

Sie müssen Horizon Agent 7.0 oder höher mit aktivierter Setup-Option „Scannerumleitung“ auf übergeordneten virtuellen Maschinen oder virtuellen Vorlagenmaschinen bzw. auf RDS-Hosts installieren.

Auf Windows-Desktop- und Windows-Server-Gastbetriebssystemen ist die Horizon Agent-Setup-Option „Scannerumleitung“ standardmäßig deaktiviert.

Die folgenden Gastbetriebssysteme werden auf Einzelbenutzer-VMs und, sofern angegeben, auf RDS-Hosts unterstützt:

- Windows 7, 32 oder 64 Bit
- Windows 8, 32 oder 64 Bitx
- Windows 10, 32 oder 64 Bit

- Windows Server 2008 R2, als Desktop oder RDS-Host konfiguriert
- Windows Server 2012 R2, als Desktop oder RDS-Host konfiguriert

Wichtig Auf den Windows Server-Gastbetriebssystemen muss die Funktion „Desktopdarstellung“ installiert sein. Dies gilt unabhängig davon, ob sie als Desktops oder RDS-Hosts konfiguriert sind.

Es ist nicht erforderlich, die Gerätetreiber für den Scanner auf dem Desktop-Betriebssystem zu installieren, auf dem Horizon Agent installiert ist.

**Horizon Client für
Windows-Software**

Horizon Client 4.0 oder höher.

**Horizon Client-
Computer oder
Clientzugriffsgerät**

Unterstützte Betriebssysteme:

- Windows 7, 32 oder 64 Bit
- Windows 8, 32 oder 64 Bitx
- Windows 10, 32 oder 64 Bit

Auf dem Clientcomputer müssen Treiber für das Scannergerät installiert sein, und der Scanner muss betriebsbereit sein.

Scangerät-Standard

TWAIN oder WIA

Anzeigeprotokoll

PCoIP

VMware Blast (erfordert Horizon Client 4.0 oder höher und Horizon Agent 7.0 oder höher)

Scannerumleitung wird in RDP-Desktop-Sitzungen nicht unterstützt.

Bedienung der Scannerumleitung durch den Benutzer

Mithilfe der Scannerumleitung können Benutzer physische Scanner und Bildverarbeitungsgeräte, die mit ihren Clientcomputern verbunden sind, als virtuelle Geräte handhaben, die Scanarbeitsgänge im Kontext ihrer Remote-Desktops und Remoteanwendungen ausführen können.

Benutzer können ihre virtuellen Scanner auf sehr ähnliche Weise handhaben wie die Scanner, die mit ihren lokalen Clientcomputern verbunden sind.

- Nach der Installation der Option zur Scannerumleitung mit Horizon Agent erscheint ein Scanner-Taskleistensymbol (🖨️) auf dem Desktop. In veröffentlichten Anwendungen wird das Taskleistensymbol zum lokalen Clientcomputer umgeleitet.

Es besteht keine Notwendigkeit, das Scanner-Taskleistensymbol zu verwenden. Die Umleitung von Scanvorgängen funktioniert ohne weitere Konfiguration. Sie können das Symbol dazu verwenden, Optionen zu konfigurieren und beispielsweise die Festlegung, welche Geräte zu verwenden sind, wenn mehrere Geräte mit dem Clientcomputer verbunden sind, zu ändern.

- Wenn Sie auf das Scanner-Symbol klicken, wird das Menü „Scannerumleitung für VMware Horizon“ angezeigt. Wenn inkompatible Scanner mit dem Clientcomputer verbunden sind, werden keine Scanner in der Menüliste aufgeführt.
- Scannergeräte werden standardmäßig automatisch ausgewählt. Die Auswahl von TWAIN- und WIA-Scannern erfolgt separat. Zu einem gegebenen Zeitpunkt kann jeweils nur ein TWAIN-Scanner und ein WIA-Scanner ausgewählt sein.
- Wenn mehrere lokal verbundene Scanner konfiguriert sind, haben Sie die Möglichkeit, statt des standardmäßig ausgewählten einen anderen Scanner auszuwählen.
- WIA-Scanner werden im Gerätemanager-Menü des Remote-Desktops unter **Bildverarbeitungsgeräte** angezeigt. Der Name für den WIA-Scanner lautet **Virtueller VMware-WIA-Scanner**.
- Im Menü „Scannerumleitung für VMware Horizon“ können Sie auf die Option **Einstellungen** klicken und Optionen wie das Ausblenden von Webcams im Scannerumleitungsmenü und die Vorgehensweise bei der Auswahl des Standardscanners auswählen.

Außerdem können Sie diese Funktionen durch Konfigurieren der Gruppenrichtlinieneinstellungen für die Scannerumleitung in Active Directory steuern. Siehe [Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

- Wenn Sie mit einem TWAIN-Scanner arbeiten, bietet das Menü „Scannerumleitung für VMware Horizon“ des TWAIN-Scanners zusätzliche Optionen für die Auswahl von Bildbereichen, das Scannen in Farbe, Schwarzweiß oder Graustufen und die Auswahl anderer üblicher Funktionen.
- Um das Fenster der TWAIN-Benutzeroberfläche für TWAIN-Scansoftware anzuzeigen, die das Fenster nicht standardmäßig anzeigt, können Sie die Option **Dialogfeld 'Scannereinstellungen' immer einblenden** im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ auswählen.

Beachten Sie, dass die meisten TWAIN-Scansoftware-Produkte das Fenster mit der TWAIN-Benutzeroberfläche standardmäßig anzeigen. Für diese Software wird das Fenster immer angezeigt, unabhängig davon, ob Sie die Option **Dialogfeld 'Scannereinstellungen' immer einblenden** aktivieren oder deaktivieren.

Hinweis Wenn Sie zwei veröffentlichte Anwendungen ausführen, die auf unterschiedlichen Farmen gehostet werden, zeigt die Taskleiste auf dem Clientcomputer zwei Scannerumleitungssymbole an. In der Regel ist nur ein Scanner mit einem Clientcomputer verbunden. In diesem Fall steuern beide Symbole dasselbe Gerät, und es ist nicht von Belang, welches Symbol Sie auswählen. In einigen Situationen kann es vorkommen, dass zwei veröffentlichte Anwendungen auf unterschiedlichen Farmen ausgeführt werden und zwei Scanner lokal verbunden sind. In diesem Fall müssen Sie jedes Symbol öffnen, um herauszufinden, welches Scannerumleitungsmenü welche veröffentlichte Anwendung steuert.

Endbenutzeranleitungen für die Handhabung umgeleiteter Scanner finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Scannerumleitung auf Ihren Remote-Desktops und -Anwendungen steuern. Mit diesen Richtlinieneinstellungen können Sie die Optionen, die im Dialogfenster „VMware Horizon Scannerumleitungs-Präferenzen“ auf Desktops und Anwendungen von Benutzern verfügbar sind, zentral aus dem Active Directory steuern.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Scannerumleitung funktioniert mit den Standardeinstellungen, die für Scanner auf Remote-Desktops und Clientsystemen konfiguriert sind.

Diese Richtlinieneinstellungen wirken sich auf Ihre Remote-Desktops aus, nicht auf die Clientsysteme, an die die physischen Scanner angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen auf Ihren Desktops und in Ihren Anwendungen die administrative Vorlagendatei (ADMX) für die Scannerumleitungs-Gruppenrichtlinie in Active Directory hinzu.

Hinzufügen der ADMX-Vorlagen für die Scannerumleitung in Active Directory

Sie können die Richtlinieneinstellungen in der Scannerumleitungs-ADMX-Vorlagendatei (`vdm_agent_scanner.admx`) zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und die Einstellungen im Gruppenrichtlinienobjekt-Editor konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass die Setup-Option „Scannerumleitung“ auf den Desktops für virtuelle Maschinen und RDS-Hosts installiert ist. Die Gruppenrichtlinieneinstellungen haben keine Auswirkungen, wenn die Scannerumleitung nicht installiert ist. Informationen zur Installation von Horizon Agent finden Sie in Ihrem Dokument für die Einrichtung.
- Stellen Sie sicher, dass Active Directory-GPOs für die Gruppenrichtlinieneinstellungen für die Scannerumleitung erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die die virtuellen Desktops oder RDS-Hosts enthält. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den Gruppenrichtlinieneinstellungen für die Scannerumleitung vertraut. Siehe [Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip und kopieren Sie die ADMX-Dateien auf Ihren Active Directory-Server.
 - a Kopieren Sie die Datei vdm_agent_scanner.admx und den Ordner en-US in den Ordner C:\Windows\PolicyDefinitions auf Ihrem Active Directory-Server.
 - b (Optional) Kopieren Sie die Sprachressourcendatei (vdm_agent_scanner.adml) in den entsprechenden Unterordner in C:\Windows\PolicyDefinitions\ auf Ihrem Active Directory-Server.
- 3 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und geben Sie dort den Pfad zur Vorlagendatei ein.

Die Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Scannerumleitung** enthalten.

Die meisten Einstellungen werden auch dem Ordner **Benutzerkonfiguration** hinzugefügt, der sich im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Scannerumleitung** befindet.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

Gruppenrichtlinieneinstellungen für Scannerumleitung

Die Gruppenrichtlinieneinstellungen für Scannerumleitung steuern die Optionen, die im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ auf Desktops und in Anwendungen für Benutzer verfügbar sind.

Die ADMX-Vorlagendatei für die Scannerumleitung enthält sowohl Richtlinien für die Computerkonfiguration als auch Richtlinien für die Benutzerkonfiguration. Die Richtlinien für die Benutzerkonfiguration ermöglichen es Ihnen, unterschiedliche Konfigurationen für Benutzer von virtuellen Desktops, veröffentlichten Desktops und veröffentlichten Anwendungen einzurichten. Unterschiedliche Benutzerkonfigurationsrichtlinien können selbst dann wirksam werden, wenn Desktop-Sitzungen und -Anwendungen von Benutzern auf denselben RDS-Hosts ausgeführt werden. Alle Einstellungen befinden sich im Ordner **VMware Horizon Agent Configuration > Scanner Redirection** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 2-3. Gruppenrichtlinieneinstellungen für Scannerumleitung

Einstellung	Computer	Benutzer	Beschreibung
BandwidthLimit		X	Gibt die maximal zulässige Bandbreite in Kilobyte pro Sekunde für die Übertragung von gescannten Daten an eine Benutzersitzung an. Wenn Sie 0 oder keinen Wert angeben, ist die Bandbreite unbegrenzt.
Compression		X	<p>Gibt die Bildkomprimierungsrate während der Bildübertragung an einen Remote-Desktop bzw. eine veröffentlichte Anwendung an.</p> <p>Sie können einen der folgenden Komprimierungsmodi auswählen:</p> <ul style="list-style-type: none"> ■ Deaktivieren – Die Bildkomprimierung ist deaktiviert. ■ Verlustfrei – Es wird eine verlustfreie (zlib-)Komprimierung ohne Bildqualitätsverlust verwendet. ■ JPEG – Es wird eine JPEG-Komprimierung mit Einbußen bei der Bildqualität verwendet. Sie wählen den Grad der Bildqualität aus dem Dropdown-Menü JPEG-Kompressionsqualität aus. Die Einstellung für „JPEG-Kompressionsqualität“ muss ein Wert zwischen 0 und 100 sein. <p>Wenn Sie diese Einstellung aktivieren, wird der ausgewählte Komprimierungsmodus für alle von dieser Richtlinie betroffenen Benutzer festgelegt. Benutzer können die Option Komprimierung im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ ändern und damit die Richtlinieneinstellung überschreiben.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird der JPEG-Komprimierungsmodus nicht verwendet.</p>
Default Color Mode			Wenn diese Einstellung aktiviert ist, können Sie den Standard-Farbmodus konfigurieren: Schwarzweiß, Graustufen oder Farbe. Diese Einstellung wird unter Windows XP Professional oder Windows Server 2003 oder höher unterstützt.
Default Duplex			Wenn diese Einstellung aktiviert ist, können Sie den Standard-Scanmodus konfigurieren: Simplex oder Duplex. Im Duplex-Modus muss die Scan-Anwendung den Duplex-Scan unterstützen und beim Scanner zwei Seiten anfordern. Diese Einstellung wird unter Windows XP Professional oder Windows Server 2003 oder höher unterstützt.

Tabelle 2-3. Gruppenrichtlinieneinstellungen für Scannerumleitung (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
Default Scanner	X	X	<p>Ermöglicht eine zentrale Verwaltung der automatischen Scannerauswahl. Sie können Optionen für die automatische Scannerauswahl separat für TWAIN- und WIA-Scanner auswählen. Sie können eine der folgenden Optionen für die automatische Auswahl auswählen:</p> <ul style="list-style-type: none"> ■ Keine. Scanner werden nicht automatisch ausgewählt. ■ Automatische Auswahl Der lokal verbundene Scanner wird automatisch ausgewählt. ■ Zuletzt verwendet Der zuletzt verwendete Scanner wird automatisch ausgewählt. ■ Angegeben Der Scanner, dessen Namen Sie in das Textfeld Angebener Scanner eingeben, wird ausgewählt. <p>Wenn Sie diese Einstellung als Computerkonfigurationsrichtlinie aktivieren, bestimmt die Einstellung den Modus der automatischen Scannerauswahl für alle Benutzer der betroffenen Computer. Benutzer können die Option Standardscanner im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ nicht ändern.</p> <p>Wenn Sie diese Einstellung als Benutzerkonfigurationsrichtlinie aktivieren, bestimmt die Einstellung den Modus der automatischen Scannerauswahl für alle betroffenen Benutzer. Benutzer können jedoch die Option Standardscanner im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ ändern.</p> <p>Wenn Sie diese Einstellung sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration aktivieren, hat der Modus für die automatische Scannerauswahl in der Computerkonfiguration Vorrang vor der entsprechenden Richtlinieneinstellung in der Benutzerkonfiguration für alle Benutzer der betroffenen Computer.</p> <p>Wenn Sie diese Einstellung deaktivieren oder nicht in beiden Richtlinienkonfigurationen konfigurieren, wird der Modus für die automatische Scannerauswahl durch die entsprechende Richtlinieneinstellung (entweder der Benutzerkonfiguration oder der Computerkonfiguration) oder durch Benutzerauswahl im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ bestimmt.</p>
Disable functionality	X		<p>Deaktiviert die Scannerumleitungsfunktion.</p> <p>Wenn Sie diese Einstellung aktivieren, können Scanner nicht umgeleitet werden. Sie werden auch nicht im Scanner-Menü auf den Desktops bzw. in den Anwendungen der Benutzer angezeigt.</p> <p>Wenn Sie die Einstellung deaktivieren oder nicht konfigurieren, funktioniert die Scannerumleitung und die Scanner werden im Scanner-Menü angezeigt.</p>
Force the TWAIN Scanning Properties dialog		X	<p>Wenn diese Einstellung aktiviert ist, wird das Dialogfeld „TWAIN-Scanner-Eigenschaften“ immer angezeigt, auch falls eine Scananwendung nicht im Dialogfeld „Scannen“ angezeigt wird.</p>

Tabelle 2-3. Gruppenrichtlinieneinstellungen für Scannerumleitung (Fortsetzung)

Einstellung	Comp uter	Be nut zer	Beschreibung
Hide Webcam	X	X	<p>Verhindert, dass Webcams im Scannerauswahlmenü im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ angezeigt werden. Webcams können standardmäßig zu Desktops und Anwendungen umgeleitet werden. Benutzer können Webcams auswählen und sie als virtuelle Scanner zum Aufnehmen von Bildern verwenden.</p> <p>Wenn Sie diese Einstellung als Computerkonfigurationsrichtlinie aktivieren, werden Webcams für alle Benutzer der betroffenen Computer ausgeblendet. Benutzer können die Option Webcam ausblenden im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ nicht ändern.</p> <p>Wenn Sie diese Einstellung als Benutzerkonfigurationsrichtlinie aktivieren, werden Webcams für alle betroffenen Benutzer ausgeblendet. Benutzer können jedoch die Option Webcam ausblenden im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ ändern.</p> <p>Wenn Sie diese Einstellung sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration aktivieren, hat die Einstellung von Webcam ausblenden in der Computerkonfiguration Vorrang vor der entsprechenden Richtlinieneinstellung in der Benutzerkonfiguration für alle Benutzer der betroffenen Computer.</p> <p>Wenn Sie diese Einstellung deaktivieren oder nicht in beiden Richtlinienkonfigurationen konfigurieren, wird die Einstellung von Webcam ausblenden durch die entsprechende Richtlinieneinstellung (entweder der Benutzerkonfiguration oder der Computerkonfiguration) oder durch Benutzerauswahl im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ bestimmt.</p>
Lock config	X		<p>Sperrt die Benutzeroberfläche für die Scannerumleitung und verhindert, dass Benutzer Konfigurationsoptionen auf ihren Desktops und in ihren Anwendungen ändern.</p> <p>Wenn Sie diese Einstellung aktivieren, können Benutzer die Optionen, die über das Taskleisten-Menü auf ihren Desktops und in ihren Anwendungen verfügbar sind, nicht konfigurieren. Benutzer können zwar das Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ öffnen, doch die Optionen sind inaktiv und ihre Einstellungen können nicht geändert werden.</p> <p>Wenn Sie die Einstellung deaktivieren oder nicht konfigurieren, können Benutzer die Optionen im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ konfigurieren.</p>
TWAIN Scanner Properties dialog location		X	<p>Gibt an, wo das Dialogfeld „TWAIN-Scanner-Eigenschaften“ angezeigt wird. Sie können eine der folgenden Optionen auswählen:</p> <ul style="list-style-type: none"> ■ Agent – Das Dialogfeld „VMware-Scanner-Eigenschaften“ wird auf der Agent-Seite angezeigt. ■ Client – Das native TWAIN-Dialogfeld für den Scanner des Anbieters auf der Clientseite angezeigt. (Diese Option wird für den Linux-Client nicht unterstützt.)

Konfigurieren der Umleitung serieller Ports

Mithilfe der Umleitung serieller Ports können Benutzer lokal verbundene, serielle Ports (COM-Ports) wie integrierte RS232-Ports oder USB-Seriell-Adapter umleiten. Geräte wie Drucker, Barcodeleser und andere serielle Geräte können mit diesen Ports verbunden und an Remote-Desktops und in veröffentlichten Anwendungen verwendet werden.

Nach der Installation von Horizon Agent und der Einrichtung der Funktion zur Umleitung für serielle Ports kann diese Funktion für Ihre Remote-Desktops und veröffentlichten Anwendungen ohne weitere Konfiguration eingesetzt werden. Beispielsweise kann ein COM1-Port auf dem lokalen Clientsystem als COM1-Port auf einen Remote-Desktop und ein COM2-Port als COM2-Port umgeleitet sein, wenn auf dem Remote-Desktop ein COM-Port vorhanden ist. Ist dies der Fall, wird der COM-Port zur Vermeidung von Konflikten neu zugeordnet. Wenn beispielsweise der COM1- und der COM2-Port bereits auf dem Remote-Desktop vorhanden sind, wird der COM1-Port standardmäßig dem COM3-Port zugeordnet. Sie müssen dazu weder die COM-Ports konfigurieren noch Gerätetreiber auf den Remote-Desktops installieren.

Um den umgeleiteten COM-Port zu aktivieren, wählt der Benutzer während einer Desktop-Sitzung die Option **Verbinden** aus dem Menü des Taskleistensymbols des seriellen Ports aus. Ein Benutzer kann für ein COM-Port-Gerät auch die automatische Herstellung der Verbindung einrichten, wenn der Benutzer sich beim Remote-Desktop oder bei der veröffentlichten Anwendung anmeldet. Siehe [Bedienung der Umleitung serieller Ports durch den Benutzer](#).

Sie können für eine Änderung der Standardkonfiguration die Gruppenrichtlinieneinstellungen entsprechend konfigurieren. Beispielsweise lassen sich die Einstellungen sperren, sodass Benutzer die COM-Port-Zuordnungen oder -Eigenschaften nicht verändern können. Sie können auch eine Richtlinie festlegen, um die Funktion insgesamt zu deaktivieren oder zu aktivieren. Mit einer ADMX-Vorlagendatei können Sie Gruppenrichtlinieneinstellungen für die Umleitung für serielle Ports in Active Directory oder auf einzelnen Computern installieren. Siehe [Konfigurieren der Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports](#).

Wenn ein umgeleiteter COM-Port an einem Remote-Desktop oder in einer veröffentlichten Anwendung geöffnet und verwendet wird, können Sie auf diesen Port auf dem lokalen Computer nicht zugreifen. Umgekehrt können Sie auf den COM-Port am Remote-Desktop oder in der veröffentlichten Anwendung nicht zugreifen, wenn dieser Port auf dem lokalen Computer verwendet wird.

Systemanforderungen für die Umleitung serieller Ports

Mit der Umleitung serieller Ports können Endbenutzer lokal verbundene serielle Ports (COM-Ports) wie integrierte RS232-Ports oder USB-Seriell-Adapter an ihre Remote-Desktops und veröffentlichten Anwendungen umleiten. Zur Unterstützung der Umleitung für serielle Ports muss Ihre Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.


Virtuelle Desktops

Auf virtuellen Desktops (virtuellen Einzelsitzungsmaschinen) muss View Agent 6.2.x oder höher oder Horizon Agent 7.0 oder höher mit aktivierter Setup-Option für die Umleitung serieller Ports installiert sein. Diese Setup-Option ist standardmäßig nicht ausgewählt.

	<p>Die folgenden Betriebssysteme werden auf virtuellen Desktops unterstützt.</p> <ul style="list-style-type: none">■ Windows 7, 32 oder 64 Bit■ Windows 8.x, 32 oder 64 Bit■ Windows 10, 32 oder 64 Bit■ Windows Server 2008 R2■ Windows Server 2012 R2■ Windows Server 2016■ Windows Server 2019 <p>Gerätetreiber für serielle Ports müssen nicht auf dem virtuellen Desktop installiert sein.</p>
Veröffentlichte Desktops und veröffentlichte Anwendungen	<p>Auf RDS-Hosts muss Horizon Agent 7.6 oder höher mit aktivierter Setup-Option für die Umleitung serieller Ports installiert sein. Diese Setup-Option ist standardmäßig nicht ausgewählt.</p> <p>Die folgenden Betriebssysteme werden für veröffentlichte Desktops und veröffentlichte Anwendungen unterstützt.</p> <ul style="list-style-type: none">■ Windows Server 2008 R2■ Windows Server 2012 R2■ Windows Server 2016■ Windows Server 2019 <p>Gerätetreiber für serielle Ports müssen nicht im RDS-Host installiert sein.</p>
Horizon Client-Computer oder Clientzugriffsgerät	<p>Die Umleitung serieller Ports wird auf Windows 7-, Windows 8.x- und Windows 10-Clientsystemen unterstützt. Die erforderlichen Gerätetreiber für serielle Ports müssen installiert sein, und der serielle Port muss betriebsbereit sein. Die Umleitung serieller Ports ist mit Horizon Client für Windows 3.4 und höhere Versionen verfügbar.</p>
Anzeigeprotokolle	<ul style="list-style-type: none">■ PCoIP■ VMware Blast (erfordert Horizon Agent 7.0 oder höher) <p>Die Umleitung serieller Ports wird in RDP-Desktop-Sitzungen nicht unterstützt.</p>

Bedienung der Umleitung serieller Ports durch den Benutzer

Benutzer können physische COM-Port-Geräte, die mit ihren Clientcomputern verbunden sind, nutzen und diese Geräte mithilfe der Virtualisierung serieller Ports mit ihren Remote-Desktops verbinden, auf denen dann von Drittanbieteranwendungen auf diese Geräte zugegriffen werden kann.

- Nach der Installation der Option zur Umleitung serieller Ports mit Horizon Agent erscheint ein Taskleistensymbol für die serielle Umleitung () auf dem Remote-Desktop. Bei veröffentlichten Anwendungen wird das Symbol zum lokalen Clientcomputer umgeleitet.

Dieses Symbol wird nur angezeigt, wenn Sie die erforderlichen Versionen von Horizon Agent und Horizon Client für Windows verwenden und eine Verbindung über PCoIP hergestellt haben. Es erscheint nicht, wenn Sie sich mit einem Remote-Desktop von einem Mac-, Linux- oder einem mobilen Client aus verbinden.

Sie können mit diesem Symbol die Optionen zum Herstellen von Verbindungen, zum Aufheben von Verbindungen und zum Anpassen zugeordneter COM-Ports konfigurieren.

- Wenn Sie auf das Symbol des seriellen Ports klicken, erscheint das Menü **Umleitung serieller COM-Ports für VMware Horizon**.
- Standardmäßig werden die lokal verbundenen COM-Ports den entsprechenden COM-Ports auf dem Remote-Desktop zugeordnet. Beispiel: **COM1 wird COM3 zugeordnet**. Die zugeordneten Ports sind nicht standardmäßig miteinander verbunden.
- Für die Verwendung eines zugeordneten COM-Ports müssen Sie entweder die Option **Verbinden** manuell im Menü **Umleitung serieller COM-Ports für VMware Horizon** auswählen oder die Option **Automatische Verbindung herstellen** während einer vorherigen Desktop-Sitzung aktivieren oder eine Gruppenrichtlinieneinstellung konfigurieren. **Automatische Verbindung herstellen** konfiguriert einen zugeordneten Port für die automatische Herstellung einer Verbindung, wenn eine Remote-Desktop-Sitzung gestartet wird.
- Mit der Auswahl der Option **Verbinden** ist der umgeleitete Port aktiv. Im Gerätemanager des Gastbetriebssystems auf dem Remote-Desktop wird der umgeleitete Port als **Umleitung für seriellen Port für VMware Horizon (COMn)** angezeigt.

Wenn der COM-Port verbunden ist, können Sie den Port in einer Drittanbieteranwendung öffnen, in der sich Daten mit dem COM-Port-Gerät austauschen lassen, das mit dem Clientcomputer verbunden ist. Wenn ein Port in einer Anwendung geöffnet ist, lässt sich dieser nicht im Menü **Umleitung serieller COM-Ports für VMware Horizon** trennen.

Bevor Sie die Verbindung mit dem COM-Port trennen können, muss der Port in der Anwendung oder die Anwendung selbst geschlossen werden. Sie können dann die Option **Verbindung trennen** auswählen und den physischen COM-Port dann für die Verwendung auf dem Clientcomputer zur Verfügung stellen.

- Im Menü **Umleitung serieller COM-Ports für VMware Horizon** klicken Sie mit der rechten Maustaste auf einen umgeleiteten Port und wählen aus dem eingeblendeten Kontextmenü die Option **Porteigenschaften**.

Im Dialogfeld der COM-Eigenschaften können Sie einen Port für die automatische Herstellung einer Verbindung beim Beginn einer Remote-Desktop-Sitzung konfigurieren. Außerdem haben Sie die Möglichkeit festzulegen, dass das DSR-Signal (Data Set Ready) ignoriert, der Port als permanenter Port aktiviert und der lokale Port einem anderen COM-Port auf dem Remote-Desktop durch Auswahl eines Ports in der Dropdown-Menü **Name des benutzerdefinierten Ports** zugeordnet wird.

Ein Remote-Desktop-Port wird eventuell als überlappend angezeigt. Beispielsweise kann **COM1 (Überlappend)** angezeigt werden. In diesem Fall ist die virtuelle Maschine mit einem COM-Port in der virtuellen Hardware auf dem ESXi-Host konfiguriert. Sie können einen umgeleiteten Port auch verwenden, wenn dieser einem überlappenden Port auf der virtuellen Maschine zugeordnet ist. Die virtuelle Maschine empfängt serielle Daten vom ESXi-Host oder vom Clientsystem über den Port.

- Im Gerätemanager des Gastbetriebssystems können Sie mit der Registerkarte **Eigenschaften > Porteinstellungen** die Einstellungen für einen umgeleiteten COM-Port konfigurieren. Beispielsweise haben Sie hier die Möglichkeit, die Standard-Baud-Rate und die Standard-Daten-Bits festzulegen. Beachten Sie, dass die im Gerätemanager konfigurierten Einstellungen ignoriert werden, wenn die Anwendung die Porteinstellungen festlegt.

Endbenutzeranleitungen für die Handhabung umgeleiteter serieller COM-Ports finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

Richtlinien für die Konfiguration der Umleitung für serielle Ports

Mithilfe der Gruppenrichtlinieneinstellungen haben Sie die Möglichkeit, die Umleitung serieller Ports zu konfigurieren und das Ausmaß festzulegen, in dem Benutzer umgeleitete COM-Ports anpassen können. Ihre Wahl hängt von den Benutzerrollen und den Drittanbieteranwendungen in Ihrem Unternehmen ab.

Weitere Informationen zu den Gruppenrichtlinieneinstellungen finden Sie im Abschnitt [Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports](#).

- Wenn Ihre Benutzer dieselben Drittanbieteranwendungen und COM-Port-Geräte verwenden, müssen Sie sicherstellen, dass die umgeleiteten Ports in derselben Art und Weise konfiguriert sind. Beispielsweise müssen Sie in einer Bank oder einem Einzelhandelsgeschäft mit Point-of-Sale-Geräten gewährleisten, dass alle COM-Port-Geräte mit denselben Ports auf den Clientendpunkten verbunden und alle Ports denselben umgeleiteten COM-Ports auf den Remote-Desktops zugeordnet sind.

Wählen Sie die Richtlinieneinstellung **PortSettings** für die Zuordnung von Clientports zu umgeleiteten Ports. Wählen Sie das Element **Autoconnect** in **PortSettings**, um sicherzustellen, dass die umgeleiteten Ports beim Beginn jeder Desktop-Sitzung verbunden sind. Aktivieren Sie die Richtlinieneinstellung **Lock Configuration**, um zu verhindern, dass Benutzer die Portzuordnungen ändern oder die Portkonfiguration anpassen. In diesem Fall müssen Benutzer dann die Verbindungen nicht manuell herstellen oder aufheben und können auch nicht versehentlich den Zugriff einer Drittanbieteranwendung auf umgeleitete COM-Ports verhindern.

- Wenn es sich bei den Benutzern um Fachkräfte handelt, die verschiedene Drittanbieteranwendungen verwenden und möglicherweise auch ihre COM-Ports lokal auf ihren Clientcomputern nutzen, müssen Sie sicherstellen, dass diese Benutzer eine Verbindung zu den umgeleiteten COM-Ports herstellen bzw. diese aufheben können.

Sie können die **PortSettings**-Richtlinieneinstellung entsprechend ändern, wenn die Standardportzuordnungen nicht korrekt sind. Außerdem haben Sie die Möglichkeit, das **Autoconnect**-Element je nach den Anforderungen ihrer Benutzer entsprechend festzulegen. Aktivieren Sie keinesfalls die Richtlinieneinstellung **Lock Configuration**.

- Stellen Sie sicher, dass Ihre Drittanbieteranwendungen den COM-Port öffnen, der dem Remote-Desktop zugeordnet ist.
- Vergewissern Sie sich, dass die Baud-Rate für ein Gerät der möglichen Baud-Rate der Drittanbieteranwendung entspricht.
- Sie können einem Remote-Desktop bis zu fünf COM-Ports eines Clientsystems zuordnen.

Konfigurieren der Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Umleitung für serielle Ports in Ihren Remote-Sitzungen steuern. Mit diesen Richtlinieneinstellungen besteht die Möglichkeit, von Active Directory aus die verfügbaren Optionen im Menü **Umleitung serieller COM-Ports für VMware Horizon** in Remote-Desktops zu steuern.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Umleitung für serielle Ports funktioniert mit den Standardeinstellungen, die für umgeleitete COM-Ports in Remote-Sitzungen und auf Clientsystemen konfiguriert sind.

Diese Richtlinieneinstellungen wirken sich auf Ihre Remote-Sitzungen aus, nicht auf die Clientsysteme, an die die physischen COM-Port-Geräte angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen für Remote-Desktops und veröffentlichte Anwendungen die administrative Vorlagendatei (ADMX) für die Gruppenrichtlinie zur Umleitung für serielle Ports in Active Directory hinzu.

Hinzufügen der ADMX-Vorlage für die Umleitung serieller Ports in Active Directory

Sie können die Richtlinieneinstellungen in der ADMX-Datei (`vdm_agent_serialport.admx`) für die Umleitung für serielle Ports (serieller COM-Port) zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und die Einstellungen im Gruppenrichtlinienobjekt-Editor konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass die Setup-Option für die Umleitung serieller Ports auf den virtuellen Desktops oder RDS-Hosts installiert ist. Die Gruppenrichtlinieneinstellungen haben keine Auswirkungen, wenn die Umleitung serieller Ports nicht installiert ist. Informationen zum Installieren von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Stellen Sie sicher, dass Active Directory-GPOs für die Gruppenrichtlinieneinstellungen zur Umleitung serieller Ports erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die die virtuellen Desktops oder RDS-Hosts enthält. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).

- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den Gruppenrichtlinieneinstellungen für die Umleitung für serielle Ports vertraut. Siehe [Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports](#).

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.
- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip und kopieren Sie die ADMX-Dateien auf Ihren Active Directory-Server.
 - a Kopieren Sie die Datei vdm_agent_serialport.admx und den Ordner en-US in den Ordner C:\Windows\PolicyDefinitions auf Ihrem Active Directory-Server.
 - b (Optional) Kopieren Sie die Sprachressourcendatei (vdm_agent_rtav.adml) in den entsprechenden Unterordner des Ordners C:\Windows\PolicyDefinitions\ auf Ihrem Active Directory-Server.
- 3 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und geben Sie dort den Pfad zur Vorlagendatei ein.

Die Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Serieller COM-Port** enthalten.

Die meisten Einstellungen werden auch dem Ordner **Benutzerkonfiguration** hinzugefügt, der sich im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Serieller COM-Port** befindet.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports

Die Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports legen die Konfiguration umgeleiteter COM-Ports fest, inklusive der im Menü **Umleitung serieller COM-Ports für VMware Horizon** in Remote-Desktops verfügbaren Optionen.

Die ADMX-Datei für die Umleitung serieller Ports enthält sowohl Richtlinien für die Computerkonfiguration als auch Richtlinien für die Benutzerkonfiguration. Die Richtlinien für die Benutzerkonfiguration ermöglichen unterschiedliche Konfigurationen für einzelne Benutzer von Remote-Desktops. Die in der Computerkonfiguration konfigurierten Richtlinien haben Vorrang vor den entsprechenden Einstellungen der Benutzerkonfiguration.

Tabelle 2-4. Richtlinieneinstellungen für serielle Ports

Einstellung	Com pute r	B e n ut ze r	Beschreibung
PortSettings1	X	X	Die Porteeinstellungen legen die Zuordnung zwischen dem COM-Port auf dem Clientsystem und dem umgeleiteten COM-Port auf dem Desktop fest sowie weitere Einstellungen für den umgeleiteten COM-Port. Sie müssen jeden umgeleiteten COM-Port separat konfigurieren.
PortSettings2			
PortSettings3			
PortSettings4			
PortSettings5			<p>Es sind fünf Richtlinieneinstellungen für Porteeinstellungen verfügbar, mit denen Sie dem Remote-Desktop bis zu fünf COM-Ports des Clients zuordnen können. Wählen Sie je eine Richtlinieneinstellung für Porteeinstellungen für jeden COM-Port aus, der konfiguriert werden soll. Wenn Sie die Richtlinieneinstellung für Porteeinstellungen aktivieren, können Sie die folgenden Elemente für den umgeleiteten COM-Port konfigurieren:</p> <ul style="list-style-type: none"> ■ Die Source port number-Einstellung gibt die Nummer des physischen COM-Ports an, der mit dem Clientsystem verbunden ist. ■ Die Einstellung Destination virtual port number gibt die Nummer des umgeleiteten virtuellen COM-Ports auf dem Remote-Desktop an. ■ Die Autoconnect-Einstellung legt fest, dass der COM-Port beim Beginn jeder Desktop-Sitzung automatisch mit dem umgeleiteten COM-Port verbunden wird. ■ Bei aktivierter Einstellung IgnoreDSR ignoriert das Gerät des umgeleiteten COM-Ports das DSR-Signal (Data Set Ready). ■ Die Einstellung Pause before close port (in milliseconds) gibt die Wartezeit an (in Millisekunden), bis der umgeleitete Port nach dem Schließen durch den Benutzer tatsächlich geschlossen wird. Bestimmte USB-/Seriell-Adapter erfordern diese Verzögerung, damit die übermittelten Daten geschützt bleiben. Diese Einstellung dient der Fehlerbehebung. ■ Die Einstellung Serial2USBModeChangeEnabled behandelt Probleme bei USB-Seriell-Adaptoren mit dem Prolific-Chipsatz, inklusive GlobalSat BU353 GPS-Adaptoren. Wenn Sie diese Einstellung nicht für Prolific-Chipsatzadapter aktivieren, können verbundene Geräte Daten übertragen, aber nicht empfangen. ■ Die Einstellung Disable errors in wait mask deaktiviert den Fehlerwert in der COM-Port-Maske. Diese Einstellung zur Fehlerbehebung ist für bestimmte Anwendungen erforderlich. Einzelheiten dazu finden Sie in der Microsoft-Dokumentation zur <code>WaitCommEvent</code>-Funktion unter http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx. ■ Die HandleBtDisappear-Einstellung unterstützt die Bluetooth-Funktionalität eines COM-Ports. Diese Einstellung dient der Fehlerbehebung. ■ Die Einstellung UsbToComTroubleShooting behandelt verschiedene Probleme von USB-/Seriell-Adaptoren. Diese Einstellung dient der Fehlerbehebung. ■ Mit der Einstellung Dauerhaft wird der Status des umgeleiteten COM-Ports in der Remotesitzung beibehalten, auch wenn der Client getrennt wird. <p>Durch Aktivierung der Richtlinieneinstellung für Porteeinstellungen für einen bestimmten COM-Port können sich Benutzer mit dem umgeleiteten Port verbinden bzw. diese Verbindung wieder aufheben. Die Benutzer haben jedoch nicht die Möglichkeit, Eigenschaften des Ports auf dem Remote-Desktop zu konfigurieren.</p>

Tabelle 2-4. Richtlinieneinstellungen für serielle Ports (Fortsetzung)

Einstellung	Computer	Beschreibung
		<p>Beispielsweise können Benutzer den Port nicht für eine automatische Umleitung einrichten, wenn Sie sich beim Desktop anmelden, und Sie können das DSR-Signal nicht ignorieren. Diese Eigenschaften werden durch die Gruppenrichtlinieneinstellung gesteuert.</p> <hr/> <p>Hinweis Ein umgeleiteter COM-Port wird nur verbunden und ist aktiv, wenn der physische COM-Port lokal mit dem Clientsystem verbunden ist. Wenn Sie einen COM-Port zuordnen, der auf dem Client nicht vorhanden ist, wird der umgeleitete Port als inaktiv angezeigt und ist im Taskleisten-Menü des Remote-Desktops nicht verfügbar.</p> <hr/> <p>Wenn die Richtlinieneinstellung für Porteinstellungen deaktiviert oder nicht konfiguriert ist, verwendet der umgeleitete COM-Port die von den Benutzern auf dem Remote-Desktop konfigurierten Einstellungen. Die Menüoptionen unter Umleitung serieller COM-Ports für VMware Horizon sind aktiv und für Benutzer verfügbar.</p> <p>Diese Einstellungen befinden sich im Ordner VMware View Agent Configuration > Serial COM > PortSettings im Gruppenrichtlinienverwaltungs-Editor.</p>
Bandwidth limit	X	<p>Damit wird eine Obergrenze für die Geschwindigkeit der Datenübertragung zwischen dem umgeleiteten seriellen Port und Clientsystemen in Kilobytes pro Sekunde festgelegt.</p> <p>Wenn Sie diese Einstellung aktivieren, haben Sie die Möglichkeit, in das Feld Bandbreitenobergrenze (in Kilobytes pro Sekunde) einen Wert für die maximale Übertragungsgeschwindigkeit von Daten zwischen dem umgeleiteten seriellen Port und dem Client einzugeben. Bei der Eingabe eines Wertes von null ist keine Obergrenze wirksam.</p> <p>Wird diese Einstellung deaktiviert, ist keine Obergrenze für die Übertragungsgeschwindigkeit definiert.</p> <p>Wenn diese Einstellung nicht konfiguriert ist, legen die lokalen Programmeinstellungen auf dem Remote-Desktop fest, ob eine Bandbreitenobergrenze gültig ist.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > Serial COM im Gruppenrichtlinienverwaltungs-Editor.</p>
Disable functionality	X	<p>Deaktiviert die Funktion zur Umleitung serieller Ports.</p> <p>Ist diese Einstellung aktiviert, werden COM-Ports nicht zum Remote-Desktop umgeleitet. Das Taskleistensymbol des seriellen Ports auf dem Remote-Desktop wird nicht dargestellt.</p> <p>Ist diese Einstellung deaktiviert, ist die Umleitung serieller Ports aktiv, das Taskleistensymbol des seriellen Ports wird dargestellt und der COM-Port erscheint im Menü Umleitung serieller COM-Ports für VMware Horizon.</p> <p>Wenn diese Einstellung nicht konfiguriert wurde, legen die lokalen Einstellungen des Remote-Desktops fest, ob die Umleitung serieller Ports deaktiviert oder aktiviert ist.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > Serial COM im Gruppenrichtlinienverwaltungs-Editor.</p>

Tabelle 2-4. Richtlinieneinstellungen für serielle Ports (Fortsetzung)

Einstellung	Com pute r	B e n u t z e r	Beschreibung
Local settings priority	X	X	<p>Räumt den auf dem Remote-Desktop konfigurierten Einstellungen Priorität ein.</p> <p>Wenn Sie diese Richtlinie aktivieren, haben die vom Benutzer auf dem Remote-Desktop konfigurierten Einstellungen für die Umleitung serieller Ports Vorrang vor den Gruppenrichtlinieneinstellungen. Eine Gruppenrichtlinieneinstellung wird nur wirksam, wenn keine Einstellung auf dem Remote-Desktop konfiguriert ist.</p> <p>Ist diese Einstellung deaktiviert oder nicht konfiguriert, haben die Gruppenrichtlinieneinstellungen Vorrang vor den auf dem Remote-Desktop konfigurierten Einstellungen.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > Serial COM im Gruppenrichtlinienverwaltungs-Editor.</p>
Lock configuration	X	X	<p>Diese Einstellung sperrt die Benutzeroberfläche für die Umleitung serieller Ports und verhindert die Änderung von Konfigurationseinstellungen auf dem Remote-Desktop durch Benutzer.</p> <p>Wenn Sie diese Einstellung aktivieren, können Benutzer die Optionen, die über das Taskleisten-Menü auf ihren Desktops verfügbar sind, nicht konfigurieren. Benutzer haben zwar die Möglichkeit, das Menü Umleitung serieller COM-Ports für VMware Horizon darzustellen, dessen Optionen sind aber nicht aktiv und können nicht geändert werden.</p> <p>Wird diese Einstellung deaktiviert, können Benutzer die Optionen des Menüs Umleitung serieller COM-Ports für VMware Horizon konfigurieren.</p> <p>Wenn diese Einstellung nicht konfiguriert ist, legen die lokalen Programmeinstellungen auf dem Remote-Desktop fest, ob Benutzer die Einstellungen für die Umleitung von COM-Ports ändern können.</p> <p>Diese Einstellung befindet sich im Ordner VMware View Agent Configuration > Serial COM im Gruppenrichtlinienverwaltungs-Editor.</p>
COM Port Isolation Mode			<p>Gibt den Isolationsmodus für COM-Ports an. Wenn Sie diese Einstellung aktivieren, können Sie einen der folgenden Isolationsmodi auswählen:</p> <ul style="list-style-type: none"> ■ Vollständige Isolation – Virtuelle serielle Ports sind nur innerhalb von Benutzersitzungen sichtbar und zugänglich. COM-Ports können in unterschiedlichen Benutzersitzungen dieselben Namen haben. Systemdienste, wie z. B. <code>spoolsv.exe</code>, können in diesem Modus nicht auf isolierte serielle Ports zugreifen. ■ Isolation deaktiviert – Virtuelle serielle Ports sind global sichtbar. Von jeder beliebigen Sitzung aus kann auf jeden beliebigen Port zugegriffen werden. Da Ports in unterschiedlichen Benutzersitzungen nicht denselben Namen haben können, müssen die Portnamen für jeden Benutzer eindeutig sein. Systemdienste, wie z. B. <code>spoolsv.exe</code>, können auf jeden seriellen Port zugreifen. <p>Wenn diese Einstellung nicht konfiguriert ist, arbeitet die serielle Portumleitung im Modus Vollständige Isolation.</p>

Konfigurieren von USB-Seriell-Adaptern

Sie können USB-Seriell-Adapter zur Verwendung eines Prolific-Chipsatzes konfigurieren, der auf Remote-Sitzungen mithilfe der Funktion zur Umleitung für serielle Ports umgeleitet werden soll.

Um sicherzustellen, dass die Daten korrekt auf Prolific-Chipsätze übertragen werden, können Sie eine Gruppenrichtlinieneinstellung für die Umleitung für serielle Ports in Active Directory bzw. an einem einzelnen Desktop einer virtuellen Maschine oder auf dem RDS-Host aktivieren.

Wenn Sie keine Gruppenrichtlinieneinstellung zur Behandlung von Problemen der Prolific-Chipsatzadapter konfigurieren, können verbundene Geräte Daten übertragen, aber nicht empfangen.

Sie müssen keine Richtlinieneinstellungen oder Registrierungsschlüssel auf Clientsystemen konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass die Setup-Option „Umleitung für serielle Ports“ auf den Desktops für virtuelle Maschinen oder RDS-Hosts installiert ist. Die Gruppenrichtlinieneinstellungen haben keine Auswirkungen, wenn die Umleitung serieller Ports nicht installiert ist. Informationen zum Installieren von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Vergewissern Sie sich, dass die ADMX-Vorlagendatei für die Umleitung für serielle Ports in Active Directory hinzugefügt ist.
- Machen Sie sich mit dem Element **Serial2USBModeChangeEnabled** in der Gruppenrichtlinieneinstellung **PortSettings** vertraut. Siehe [Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports](#).

Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server den Editor für Gruppenrichtlinien-Verwaltungsobjekte.
- 2 Wechseln Sie zum Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Agent-Konfiguration > Serieller COM**.
- 3 Wählen Sie den Ordner **PortSettings**.
- 4 Wählen und aktivieren Sie eine **PortSettings**-Gruppenrichtlinieneinstellung.
- 5 Geben Sie für die Zuordnung des COM-Ports die Quell- und Zielnummern des COM-Ports an.
- 6 Aktivieren Sie das Kontrollkästchen **Serial2USBModeChangeEnabled**.
- 7 Konfigurieren Sie die anderen Elemente in der Richtlinieneinstellung **PortSettings** nach Bedarf.
- 8 Klicken Sie auf **OK** und schließen Sie den Editor für Gruppenrichtlinien-Verwaltungsobjekte.

USB-Seriell-Adapter können jetzt auf Remote-Sitzungen umgeleitet werden und erfolgreich Daten empfangen, wenn Benutzer ihre nächsten Sitzungen starten.

Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows (MMR)

Horizon 7 stellt die Windows Media MMR-Funktion für virtuelle Desktops, die auf Einzelbenutzercomputern ausgeführt werden, und für veröffentlichte Desktops auf RDS-Hosts bereit.

MMR stellt den Multimedia-Stream direkt auf den Clientcomputern bereit. Mit MMR wird der Multimediadatenstrom auf dem Clientsystem verarbeitet, d. h. entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und lagert so die Anforderung vom ESXi-Host aus.

MMR-Daten werden ohne anwendungsbasierte Verschlüsselung über das Netzwerk gesendet und können je nach umgeleitetem Inhalt vertrauliche Daten enthalten. Um sicherzustellen, dass diese Daten nicht auf dem Netzwerk nachverfolgt werden können, sollten Sie MMR nur auf einem sicheren Netzwerk verwenden.

Wenn der sichere Tunnel aktiviert ist, sind MMR-Verbindungen zwischen Clients und dem View Secure Gateway sicher. Verbindungen vom View Secure Gateway zu Desktop-Computern werden allerdings nicht verschlüsselt. Ist der sichere Tunnel deaktiviert, werden MMR-Verbindungen von Clients zu den Desktop-Computern nicht verschlüsselt.

Aktivieren von Multimedia-Umleitung in Horizon 7

Sie können Maßnahmen ergreifen, um sicherzustellen, dass nur Horizon Client-Systeme mit ausreichenden Ressourcen auf MMR zugreifen können, um die lokale Multimedia-Dekodierung zu verarbeiten, und in einem sicheren Netzwerk mit Horizon 7 verbunden sind.

Standardmäßig ist die globale Richtlinie in Horizon Administrator **Multimedia-Umleitung (MMR)** auf **Verweigern** festgelegt.

Für die Verwendung von MMR müssen Sie den Wert explizit auf **Zulassen** festlegen.

Wenn Sie den Zugriff auf MMR steuern möchten, haben Sie die Möglichkeit, die Richtlinie **Multimedia-Umleitung (MMR)** für einzelne Desktop-Pools oder für bestimmte Benutzer global zu aktivieren bzw. zu deaktivieren.

Anweisungen zum Festlegen von globalen Richtlinien in Horizon Administrator finden Sie unter [Horizon 7-Richtlinien](#).

Systemanforderungen für Windows Media MMR

Zur Unterstützung von Windows Media-Multimedia-Umleitung (MMR) muss Ihre Horizon 7-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen. Windows Media MMR wird mit Horizon 6.0.2 und neueren Versionen bereitgestellt.

Remote-Desktop

- Diese Funktion wird von Desktops virtueller Maschinen unterstützt, die auf virtuellen Einzelbenutzer-Maschinen und veröffentlichten Desktops auf RDS-Hosts bereitgestellt sind.

View Agent 6.1.1 oder höher oder Horizon Agent 7.0 oder höher ist erforderlich, um diese Funktion auf veröffentlichten Desktops zu unterstützen.

View Agent 6.0.2 oder höher oder Horizon Agent 7.0 oder höher ist für die Unterstützung dieser Funktion auf Einzelbenutzer-Maschinen erforderlich.

- Horizon 7 Version 7.9 oder höher ist für die Unterstützung von MMS (Microsoft Media Server) und RTSP (Real Time Streaming Protocol) erforderlich.
- Die folgenden Gastbetriebssysteme werden unterstützt:
 - Windows 10, 64 oder 32 Bit Windows Media Player wird unterstützt. Der standardmäßige TV & Movies-Player wird nicht unterstützt.
 - Windows Server 2016 ist eine Tech Preview-Funktion. Windows Media Player wird unterstützt. Der standardmäßige TV & Movies-Player wird nicht unterstützt.
 - 64-Bit- oder 32-Bit-Version von Windows 7 SP1 Enterprise oder Ultimate (Einzelbenutzer-Maschine). Windows 7 Professional wird nicht unterstützt.
 - 64-Bit- oder 32-Bit-Version von Windows 8/8.1 Professional oder Enterprise (Einzelbenutzer-Maschine).
 - Windows Server 2008 R2, als RDS-Host konfiguriert
 - Windows Server 2012 und 2012 R2, als RDS-Host konfiguriert
- **3D-Rendering** kann für den Desktop-Pool aktiviert oder deaktiviert werden.
- Benutzer müssen Videos in Windows Media Player 12 oder höher oder in Internet Explorer 8 oder höher wiedergeben.

Horizon Client-Software Horizon Client 3.2 für Windows oder höher ist erforderlich für die Unterstützung von Windows Media MMR auf Einzelbenutzer-Maschinen.

Horizon Client-Computer oder Clientzugriffsgerät Auf den Clients muss ein Windows 7-, Windows 8/8.1- oder Windows 10-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden.

Unterstützte Medienformate In Windows Media Player unterstützte Medienformate, beispielsweise: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3; WAV.

Horizon 7 Version 7.9 und höher unterstützt MMS und RTSP.

MP3 wird bei Verwendung von MMS und RTSP nicht unterstützt.

Hinweis DRM-geschützter Inhalt wird nicht über Windows Media MMR umgeleitet.

Horizon-Richtlinien	Legen Sie in Horizon Administrator die Richtlinie Multimedia-Umleitung (MMR) auf Zulassen fest. Der Standardwert lautet Verweigern .
Backend-Firewall	Wenn Ihre Horizon 7-Bereitstellung eine Backend-Firewall zwischen Ihren DMZ-basierten Sicherheitsservern und dem internen Netzwerk enthält, stellen Sie sicher, dass die Backend-Firewall den Datenverkehr zu Port 9427 auf Ihren Desktops zulässt.

Verwenden von Windows Media MMR basierend auf Netzwerklatenz

Standardmäßig passt sich Windows Media MMR an die Netzwerkbedingungen von Einzelbenutzer-Desktops an, auf denen Windows 8 oder höher ausgeführt wird, und von veröffentlichten Desktops mit Windows Server 2012 oder 2012 R2 oder höher. Falls die Netzwerklatenz zwischen Horizon Client und dem Remote-Desktop maximal 29 Millisekunden beträgt, wird das Video mit Windows Media MMR umgeleitet. Falls die Netzwerklatenz 30 Millisekunden oder mehr beträgt, wird das Video nicht umgeleitet. Stattdessen wird es auf dem ESXi-Host gerendert und über PCoIP an den Client gesendet.

Diese Funktion kann auf Einzelbenutzer-Desktops mit Windows 8 oder höher und auf veröffentlichte Desktops mit Windows Server 2012 oder 2012 R2 oder höher angewendet werden. Die Benutzer können jedes unterstützte Client-System, Windows 7 oder Windows 8/8.1, ausführen.

Diese Funktion ist nicht für Einzelbenutzer-Desktops mit Windows 7 und veröffentlichte Desktops mit Windows Server 2008 R2 verfügbar. Auf diesen Gastbetriebssystemen führt Windows Media MMR immer die Multimedia-Umleitung durch, unabhängig von der Netzwerklatenz.

Diese Funktion können Sie außer Kraft setzen und Windows Media MMR zwingen, die Multimedia-Umleitung unabhängig von der Netzwerklatenz durchzuführen, indem Sie die `RedirectionPolicy`-Registrierungseinstellung auf dem Desktop konfigurieren.

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem Remote-Desktop.

- 2 Navigieren Sie zum Windows-Registrierungsschlüssel, der die Umleitungsrichtlinie steuert.

Welchen Registrierungsschlüssel Sie für einen Remote-Desktop konfigurieren, hängt von der Bit-Version des Windows Media Player ab.

Option	Beschreibung
Windows Media Player (64-Bit)	<ul style="list-style-type: none"> Für einen 64-Bit-Desktop konfigurieren Sie den Registrierungsschlüssel: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr
Windows Media Player (32-Bit)	<ul style="list-style-type: none"> Für einen 32-Bit-Desktop konfigurieren Sie den Registrierungsschlüssel: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr Für einen 64-Bit-Desktop konfigurieren Sie den Registrierungsschlüssel: HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware tsmmr

- 3 Setzen Sie den Wert für RedirectionPolicy auf always.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

- 4 Starten Sie den Windows Media Player auf dem Desktop neu, um den aktualisierten Wert anzuwenden.

Verwalten des Zugriffs auf die Clientlaufwerksumleitung

Wenn Sie Horizon Client und Horizon Agent mithilfe der Clientlaufwerkumleitung bereitstellen, werden die Ordner und Dateien verschlüsselt über das Netzwerk versendet.

Verbindungen der Clientlaufwerksumleitung zwischen Clients und dem View Secure Gateway sowie Verbindungen vom View Secure Gateway zu Desktop-Maschinen sind sicher. Wenn VMware Blast aktiviert ist, werden die Dateien und Ordner verschlüsselt über einen virtuellen Kanal übertragen.

Zur Unterstützung der Clientlaufwerksumleitung sind TCP-Verbindungen für Port 9427 erforderlich. Wenn Ihre Horizon 7-Bereitstellung eine Backend-Firewall zwischen Ihren DMZ-basierten Sicherheitsservern und dem internen Netzwerk enthält, muss die Backend-Firewall den Datenverkehr zu Port 9427 auf Ihren Remote-Desktops zulassen. Wenn VMware Blast aktiviert ist, muss der TCP-Port 9427 nicht geöffnet sein, da die Daten bei der Clientlaufwerkumleitung über den virtuellen Kanal übertragen werden.

Die benutzerdefinierte Setup-Option **Clientlaufwerkumleitung** im Horizon Agent-Installationsprogramm ist standardmäßig aktiviert. Empfehlenswert ist die Aktivierung der benutzerdefinierten Setup-Option **Clientlaufwerkumleitung** nur auf Remote-Desktops, auf denen Benutzer diese Funktion benötigen.

Bei Horizon Client-Versionen, die älter als Version 3.5 sind, oder Horizon Agent-Versionen, die älter als Version 6.2 sind, werden die Ordner und Dateien der Clientlaufwerkumleitung unverschlüsselt über das Netzwerk versendet und können abhängig vom umgeleiteten Inhalt sensitive Daten enthalten. Wenn der sichere Tunnel aktiviert ist, sind Verbindungen der Clientlaufwerkumleitung zwischen Horizon Client und View Secure Gateway sicher. Verbindungen vom View Secure Gateway zu Desktop-Computern werden

allerdings nicht verschlüsselt. Wenn der sichere Tunnel deaktiviert ist, werden Verbindungen der Clientlaufwerksumleitung von Horizon Client zu Desktop-Computern nicht verschlüsselt. Um sicherzustellen, dass diese Daten bei älteren Client- und Agent-Versionen im Netzwerk nicht nachverfolgt werden können, verwenden Sie die Clientlaufwerkumleitung nur in einem sicheren Netzwerk.

Mit aktivierter Clientlaufwerksumleitung auf Horizon Agent 7.7 oder höher können Sie Dateien und Ordner zwischen Horizon Client 4.10 und höher und Remote-Desktops sowie veröffentlichten Anwendungen per Drag & Drop verschieben. Siehe [Konfigurieren der Drag & Drop-Funktion](#).

Verwenden der Clientlaufwerksumleitung in einer Unified Access Gateway-Implementierung

Wenn Ihre Horizon 7-Implementierung eine Unified Access Gateway-Appliance anstelle eines Sicherheitsservers verwendet, Benutzer die Clientlaufwerksumleitung mit dem PCoIP-Anzeigeprotokoll verwenden und die Horizon Client- und Horizon Agent-Maschinen sich in unterschiedlichen Netzwerken befinden, muss der UDP-Tunnel-Server für die Unified Access Gateway-Appliance aktiviert sein.

Zur Aktivierung des UDP-Tunnel-Servers legen Sie in der Administratorbenutzeroberfläche von Unified Access Gateway die Einstellung **UDP-Tunnel-Server aktiviert** auf **Ja** fest.

Wenn Sie den UDP-Tunnel-Server nicht aktivieren, können Benutzer die Funktion der Clientlaufwerksumleitung nicht mit dem PCoIP-Anzeigeprotokoll verwenden. Die Clientlaufwerksumleitung benötigt das VMware Blast-Anzeigeprotokoll, unabhängig davon, ob der UDP-Tunnel-Server aktiviert ist.

Weitere Informationen finden Sie in der Dokumentation Unified Access Gateway.

Verwenden einer Gruppenrichtlinie zur Deaktivierung der Clientlaufwerkumleitung

Sie können die Clientlaufwerkumleitung durch Konfigurieren einer Gruppenrichtlinieneinstellung für Ihre Remote-Desktops auf dem Active Directory-Server deaktivieren.

Diese Gruppenrichtlinieneinstellung überschreibt die lokalen Registrierungs- und Intelligente Richtlinien-Einstellungen, die die Funktion der Clientlaufwerkumleitung aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie die ADMX-Vorlagendatei `vmware_rdsh_server.admx` für Remotedesktopdienste einem GPO, das mit der OU für Ihre virtuellen Desktops verknüpft ist, oder dem RDS-Host für Ihre veröffentlichten Desktops hinzu. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).

Verfahren

- 1 Öffnen Sie auf Ihrem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und navigieren Sie zu **Computerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remote-Desktop-Sitzungshost\Umleitung von Geräten und Ressourcen**.
- 2 Öffnen Sie die Gruppenrichtlinieneinstellung **Laufwerksumleitung nicht zulassen**, wählen Sie Option **Aktiviert** aus und klicken Sie dann auf **OK**.

Verwenden von Gruppenrichtlinien zum Konfigurieren des Laufwerksbuchstaben-Verhaltens

Sie können Agent-Gruppenrichtlinieneinstellungen verwenden, um das Verhalten des Laufwerksbuchstaben für Laufwerke zu konfigurieren, die mit der Funktion der Clientlaufwerksumleitung umgeleitet werden.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie die ADMX-Vorlagendatei für die VMware Horizon Client-Laufwerksumleitung (`vdm_agent_cdr.admx`) einem GPO, das mit der OU für Ihre virtuellen Desktops verknüpft ist, oder dem RDS-Host für Ihre veröffentlichten Desktops hinzu. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).

Verfahren

- 1 Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf dem Active Directory-Server und navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware Horizon Client-Laufwerksumleitung**.
- 2 Um zu konfigurieren, ob ein Laufwerksbuchstabe für umgeleitete Laufwerke angezeigt werden soll, konfigurieren Sie die Gruppenrichtlinieneinstellung **Umgeleitetes Gerät mit Laufwerksbuchstaben anzeigen**.

Diese Einstellung ist standardmäßig aktiviert.
- 3 Um die Wartezeit in Millisekunden, bis der Windows Explorer einen Laufwerksbuchstaben für Laufwerke initialisiert und anzeigt, festzulegen, konfigurieren Sie die Gruppenrichtlinieneinstellung **Zeitüberschreitung für Laufwerksbuchstaben-Konfiguration**.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, beträgt der Standardwert 5.000 Millisekunden.

- 4 Um den Zuweisungsmodus für den Laufwerkbuchstaben festzulegen, konfigurieren Sie die Gruppenrichtlinieneinstellung **Laufwerkbuchstaben-Zuordnungsmodus konfigurieren**.

Sie können eine der folgenden Optionen auswählen:

Option	Bezeichnung
Eins-zu-Eins-Zuordnung	Ordnet den Laufwerkbuchstaben auf dem Clientcomputer demselben Laufwerkbuchstaben auf dem Agent-Computer zu. Beispielsweise wird Laufwerk X auf dem Clientcomputer Laufwerk X auf dem Agent-Computer zugeordnet.
Definierte Zuordnung	Ordnet Laufwerkbuchstaben auf dem Clientcomputer entsprechend einer Zuordnungstabelle bestimmten Laufwerkbuchstaben auf dem Agent-Computer zu, die in der Gruppenrichtlinieneinstellung Zuordnungstabelle für Laufwerksbuchstaben definieren definiert ist.

- 5 Konfigurieren Sie zum Zuordnen von Laufwerkbuchstaben die Gruppenrichtlinieneinstellung **Zuordnungstabelle für Laufwerksbuchstaben definieren**.

Sie klicken auf **Anzeigen**, um eine Zuordnungstabelle für Laufwerkbuchstaben zu definieren. Die Spalte **Wertname** gibt den Laufwerkbuchstaben auf dem Clientcomputer an, während die entsprechende Spalte **Wert** den Laufwerkbuchstaben angibt, der auf der Agent-Maschine verwendet werden soll.

Verwenden der Registrierungseinstellungen zur Konfiguration der Clientlaufwerksumleitung

Mit den Einstellungen des Windows-Registrierungsschlüssels können Sie das Verhalten der Clientlaufwerksumleitung auf einem Remote-Desktop steuern. Diese Funktion erfordert Horizon Agent 7.0 oder höher und Horizon Client 4.0 oder höher.

Die Windows-Registrierungseinstellungen, die das Verhalten der Clientlaufwerksumleitung auf einem Remote-Desktop steuern, sind unter folgendem Pfad gespeichert:

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

Sie können mit dem Windows Registrierungs-Editor auf dem Remote-Desktop die Einstellungen der Clientlaufwerksumleitung bearbeiten.

Hinweis Die mit Intelligente Richtlinien festgelegten Richtlinien für die Clientlaufwerksumleitung haben Vorrang vor den lokalen Registrierungseinstellungen.

Deaktivieren der Clientlaufwerksumleitung

Um die Clientlaufwerksumleitung zu deaktivieren, erstellen Sie eine Zeichenfolge mit dem Namen `disabled` und legen dafür den Wert `true` fest.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

Standardmäßig ist der Wert auf `false` (aktiviert) festgelegt.

Unterbinden des Schreibzugriffs auf freigegebene Ordner

Um zu verhindern, dass in alle Ordner, die mit einem Remote-Desktop freigegeben wurden, Daten geschrieben werden, erstellen Sie eine neue Zeichenfolge mit dem Namen `permissions` und legen Sie für diese eine Zeichenfolge fest, die mit `r` beginnt (außer `rw`).

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

Der Standardwert ist `rw` (d. h., alle freigegebenen Ordner können gelesen und in diese können Daten geschrieben werden).

Freigeben bestimmter Ordner

Um bestimmte Ordner mit dem Remote-Desktop freizugeben, erstellen Sie einen neuen Schlüssel mit dem Namen `default shares` und einen neuen Unterschlüssel für jeden Ordner, der mit dem Remote-Desktop freigegeben werden soll. Für jeden Unterschlüssel erstellen Sie eine neue Zeichenfolge mit dem Namen `name` und geben für diese den Pfad des Ordners an, der freigegeben werden soll. Das nachfolgende Beispiel gibt die Ordner `C:\ebooks` und `C:\spreadsheets` frei.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Wenn Sie für `name` den Wert `*all` festlegen, werden alle Clientlaufwerke mit dem Remote-Desktop freigegeben. Die Einstellung `*all` wird nur auf Windows-Clientsystemen unterstützt.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

Um zu verhindern, dass vom Client weitere Ordner (also Ordner, die nicht mit dem Schlüssel `default shares` festgelegt wurden) freigegeben werden, erstellen Sie eine Zeichenfolge mit dem Namen `ForcedByAdmin` und legen dafür den Wert `true` fest.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

Mit `true` wird das Dialogfeld „Freigabe“ nicht angezeigt, wenn Benutzer mit dem Remote-Desktop in Horizon Client eine Verbindung herstellen. Standardmäßig ist der Wert `false` eingestellt (d. h., Clients können weitere Ordner freigegeben).

Mit dem nachfolgenden Beispiel werden die Ordner `C:\ebooks` und `C:\spreadsheets` freigegeben, wobei beide Ordner schreibgeschützt sind, und es können vom Client keine weiteren Ordner freigegeben werden.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Hinweis Sie sollten die Funktion `ForcedByAdmin` nicht als Sicherheitsfunktion oder Freigabesteuerelement verwenden. Ein Benutzer kann die Einstellung `ForcedByAdmin=true` umleiten, indem ein Link zur vorhandenen Freigabe erstellt wird, der auf Ordner verweist, die nicht mit dem Schlüssel `default shares` angegeben wurden.

Konfigurieren der Drag & Drop-Funktion

Benutzer können Daten per Drag & Drop zwischen Clientsystemen und Remote-Desktops und veröffentlichten Anwendungen verschieben.

Clientanforderungen für Drag & Drop

- Es werden nur Windows- und Mac-Clientsysteme unterstützt. Andere Typen von Clientsystemen werden nicht unterstützt.
- Benutzer müssen das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden.
- Für Drag & Drop von Dateien und Ordnern muss die Funktion der Clientlaufwerksumleitung in Horizon Client für Windows aktiviert sein.
- Um die neuesten Drag & Drop-Funktionen verwenden zu können, müssen Benutzer über Horizon Client für Windows 5.1 oder höher oder Horizon Client für Mac 5.1 oder höher verfügen. Frühere Clientversionen bieten nur partielle Drag & Drop-Funktionen.

Informationen zur Verwendung der Drag & Drop-Funktion auf einem Windows-Client finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*. Informationen zur Verwendung der Drag & Drop-Funktion auf einem Mac-Client finden Sie im Dokument *VMware Horizon Client für Mac Installations- und Einrichtungshandbuch*.

Agent-Anforderungen für Drag & Drop

Um die Drag & Drop-Funktion mit Dateien und Ordnern verwenden zu können, müssen Sie bei der Installation von Horizon Agent die Option **Clientlaufwerksumleitung** aktivieren.

Verwenden von Gruppenrichtlinieneinstellungen zum Konfigurieren von Drag & Drop

Sie können die Drag & Drop-Richtung, die zulässigen Drag & Drop-Formate und den Grenzwert für die Drag & Drop-Größe konfigurieren, indem Sie Gruppenrichtlinieneinstellungen für die VMware Blast- und PCoIP-Anzeigeprotokolle bearbeiten. Siehe [Richtlinieneinstellungen für VMware Blast](#) und [PCoIP-Zwischenablagen- und Drag & Drop-Einstellungen](#).

Verwenden von Dynamic Environment Manager zum Konfigurieren von Drag & Drop

Mit Dynamic Environment Manager 9.8 oder höher und Horizon Client 5.1 oder höher können Sie mit Intelligente Richtlinien das Drag & Drop-Verhalten konfigurieren, einschließlich der Deaktivierung der gesamten Drag & Drop-Funktion. Siehe [Einstellungen für intelligente Horizon-Richtlinien](#).

Konfigurieren der SDO-Sensor-Umleitung

Die Funktion zur Umleitung des einfachen Geräteausrichtungssensors (Simple Device Orientation Sensor, SDO-Sensor) erkennt Änderungen in der Bildschirmausrichtung eines Client-Geräts und zeigt entsprechend auf dem Gerät eine andere Ansicht an.

Die SDO-Sensor-Umleitung ist in Ihrer Softwareanwendung im Horizon Agent integriert. Wenn Ihre Anwendung die SimpleOrientationSensor-Klasse <https://docs.microsoft.com/en-us/uwp/api/windows.devices.sensors.simpleorientationsensor> verwendet, kann die Anwendung Inhalte basierend auf der aktuellen Quadrantenausrichtung des Client-Geräts anzeigen.

Systemanforderungen für die SDO-Sensor-Umleitung

Die folgenden Geräte werden unterstützt:

Tabelle 2-5. Geräte, die die SDO-Sensor-Umleitung unterstützen

Gerät	Clientbetriebssystem	Windows-Betriebssystemserver	Protokolle
Surface Book	Windows 10 1709	Windows 10 1709 (64 Bit, 32 Bit)	PCoIP, Blast
Surface Pro	Windows 10 1709 Windows 8.1	Windows 10 1709 (64 Bit, 32 Bit)	PCoIP, Blast

Für Horizon Agent-Betriebssysteme wird nur Windows 10 32-Bit und 64-Bit unterstützt.

Installieren des SDO-Sensors

Die SDO-Sensor-Umleitung ist eine benutzerdefinierte Setup-Option im Horizon Agent-Installationsprogramm. Sie ist nicht standardmäßig ausgewählt. Sie müssen die SDO-Sensor-Umleitung zur Installation auswählen. Weitere Informationen zu den Eigenschaften der unbeaufsichtigten Installation für die SDO-Sensor-Umleitung finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Der Sensordienst muss am lokalen System aktiviert sein, damit der SDO-Treiber funktioniert. Der SDO-Sensor muss auf dem Client-Gerät aktiviert sein.

Protokolle

Horizon Client-Protokolle für die SDO-Sensor-Umleitung werden in der rdeSvc-Protokolldatei %TEMP%\vmware-%USERNAME%\vmware-rdeSvc-x-xxxxx.log aufgezeichnet.

Horizon Agent-Protokolle für die SDO-Sensor-Umleitung werden in der rdeSvc-Protokolldatei C:\Windows\Temp\vmware-SYSTEM*\vmware-rdeSvc-x-xxxx.log aufgezeichnet.

Konfigurieren der Funktion „Session Collaboration“

Mit der Funktion „Session Collaboration“ können Benutzer andere Benutzer zur Teilnahme an einer vorhandenen Windows-Remote-Desktop-Sitzung einladen. Informationen zum Einrichten der Session Collaboration auf Linux-Desktops finden Sie im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

Systemanforderungen für die Funktion „Session Collaboration“

Um die Funktion „Session Collaboration“ zu unterstützen, muss Ihre Horizon-Bereitstellung bestimmte Anforderungen erfüllen.

Tabelle 2-6. Systemanforderungen für die Funktion „Session Collaboration“

Komponente	Anforderungen
Clientsystem	Für Sitzungsbesitzer und Sitzungsteilnehmer muss Horizon Client 4.7 oder höher für Windows, Mac oder Linux auf dem Clientsystem installiert sein oder HTML Access 4.7 oder höher verwendet werden.
Windows-Remote-Desktops	Horizon Agent 7.4 oder höher muss auf dem virtuellen Desktop oder auf dem RDS-Host für veröffentlichte Anwendungen installiert sein. Die Funktion „Session Collaboration“ muss auf Desktop-Pool- oder Farmebene aktiviert sein. Informationen zur Aktivierung der Funktion „Session Collaboration“ für Desktop-Pools finden Sie im Dokument <i>Einrichten von virtuellen Desktops in Horizon 7</i> . Informationen zur Aktivierung der Funktion „Session Collaboration“ für eine Farm erhalten Sie im Dokument <i>Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7</i> .
Linux-Remote-Desktops	Anforderungen für Linux-Remote-Desktops finden Sie im Dokument <i>Einrichten von Horizon 7 für Linux-Desktops</i> .
Verbindungsserver	Die Verbindungsserver-Instanz verwendet eine Enterprise-Lizenz.
Anzeigeprotokoll	VMware Blast

Informationen zur Verwendung der „Session Collaboration“-Funktion finden Sie in der Dokumentation zu Horizon Client.

Konfigurieren der Gruppenrichtlinieneinstellungen für „Session Collaboration“

Verwenden Sie die Gruppenrichtlinieneinstellungen für „Collaboration“ in der ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (`vdm_agent.admx`), um die „Session Collaboration“ zu konfigurieren. Siehe [Richtlinieneinstellungen für die Funktion „Session Collaboration“](#).

Einschränkungen der Funktion „Session Collaboration“

Benutzern stehen die folgenden Remote-Desktop-Funktionen in einer gemeinsamen Sitzung nicht zur Verfügung.

- USB-Umleitung
- Echtzeit-Audio/Video (RTAV)
- Multimedia-Umleitung

- Clientlaufwerkumleitung
- Smartcard-Umleitung
- Virtueller Druck
- Microsoft Lync-Umleitung
- Dateiumleitung und Funktion „Im Dock behalten“
- Zwischenablagenumleitung

Benutzer können die Auflösung des Remote-Desktops in einer gemeinsamen Sitzung nicht ändern.

Benutzer dürfen nicht mehrere Collaboration-Sitzungen auf einem Client Computer ausführen.

VMware Virtualization Pack für Skype for Business konfigurieren

Sie können optimierte Audio- und Videoanrufe mit Skype for Business innerhalb eines virtuellen Desktops vornehmen, ohne die virtuelle Infrastruktur negativ zu beeinflussen oder das Netzwerk zu überladen. Alle Medienverarbeitungsabläufe während eines Audio- und Videoanrufs mit Skype erfolgen auf dem Clientcomputer und nicht auf dem virtuellen Desktop.

Funktionen des VMware Virtualization Pack für Skype for Business

VMware Virtualization Pack für Skype for Business bietet folgende Funktionen:

- Ausführen von Anrufen und Konferenzen über einen HTTPS-Proxy-Server
- Antwortgruppen
- Microsoft Office-Integration: Starten Sie einen Skype for Business-Anruf aus Word, Outlook, SharePoint, usw.
- Mit „Quality of Experience“ (QoE) können Skype for Business-Clients Anrufmetriken zum Generieren von Berichten an den Skype for Business-Server übergeben.
- Verwalten von Anrufen im Auftrag von jemand anderem als Stellvertreter
- Aktive Sprecheridentifikation
- Anruf über X (privat, geschäftlich usw.)
- Festlegen der Lautstärke vom Remote-Desktop aus
- E911-Anrufe
- Anruf halten und annehmen
- Externen Besprechungen anonym beitreten
- Anrufe auf Mobilgeräte umleiten
- Anrufstatistik
- Smartcard-Authentifizierung

- Audio-Anrufe von Punkt zu Punkt
- Video-Anrufe von Punkt zu Punkt
- PSTN-Anrufe über Wähltastatur
- Übertragen, Weiterleiten, Stummschalten und Fortsetzen eines Anrufs
- HID-Befehle
- Anrufe zu PSTN über Vermittlungsserver
- Remotekonnektivität und Anrufe über Edge-Server
- Wartemusik
- Benutzerdefinierte Klingeltöne
- Voicemailintegration
- USB-Smartphones
- Unterstützung veröffentlichter Anwendungen
- Weiterleitungsfehlerkorrektur (Forward Error Correction, FEC) mit Audio und Video
- Skype for Business-Online-Besprechung
- Konferenz mit der Funktion „Jetzt besprechen“
- Whiteboard-Nutzung und Bildschirmfreigabe

Systemanforderungen für VMware Virtualization Pack für Skype for Business

VMware Virtualization Pack für Skype for Business unterstützt diese Konfigurationen.

Tabelle 2-7. Systemanforderungen für VMware Virtualization Pack für Skype for Business

System	Anforderungen
Microsoft Server	Lync Server 2013, Skype for Business Server 2015, Office365, Skype for Business Server 2019
Microsoft-Client	<p>VMware empfiehlt dringend die Verwendung der aktuellen Client-Updates für Skype for Business.</p> <ul style="list-style-type: none"> ■ Skype for Business 2015-Client: 15.0.4933.100 oder höher ■ Skype for Business 2016 als Teil von Office 365 Plus: 16.0.7571.2072 oder höher ■ Skype for Business 2016 als Teil von Office 2016: 16.0.4561.1000 oder höher <p>Hinweis Skype for Business Basic 2015- oder 2016-Clients werden nicht unterstützt.</p>

Tabelle 2-7. Systemanforderungen für VMware Virtualization Pack für Skype for Business (Fortsetzung)

System	Anforderungen
Betriebssysteme für virtuelle Desktops	<p>Als Mindestanforderung müssen 2 vCPUs für diese Betriebssysteme vorhanden sein.</p> <ul style="list-style-type: none"> ■ Windows 7 SP1 <p>Hinweis Installieren Sie .NET 4.0 oder höher für Horizon Agent 7.10 und höher.</p> <ul style="list-style-type: none"> ■ Windows 8.1 ■ Persistente und nicht persistente Windows 10-Desktops ■ Windows 2008 R2 SP1-Desktops ■ Windows 2012 R2-Desktops ■ Windows 2008 R2 SP1 RDSH-Desktops ■ Windows 2012 R2 RDSH-Desktops ■ Windows Server 2016 RDSH-Desktops ■ Unterstützung veröffentlichter Anwendungen
Betriebssysteme für Clientcomputer:	<p>Mindesthardwareanforderung: 2,4 GHz Dual Core</p> <ul style="list-style-type: none"> ■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 ■ Windows Embedded Standard 7 ■ Windows 10 IoT ■ Windows Thin PC <p>VMware Virtualization Pack für Skype for Business unterstützt dieselben Linux-Betriebssysteme wie Horizon Client für Linux.</p> <p>VMware Virtualization Pack für Skype for Business unterstützt dieselben Mac-Betriebssysteme wie Horizon Client für Mac.</p>
Bereitstellungen	<ul style="list-style-type: none"> ■ VDI (lokal und Cloud) ■ Persistente und nicht persistente Desktops ■ RDS-Bereitstellungen (veröffentlichte Desktops und Anwendungen)
Anzeigeprotokolle	VMware Blast und PCoIP
Netzwerkports	Die gleichen Ports, die vom nativen Skype for Business-Client verwendet werden. Siehe Clientports unter https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols . Siehe auch https://kb.vmware.com/s/article/52558 .
Mikrofone und Webcams	Die gleichen Geräte, die für die Anwendung mit Skype for Business geeignet sind. Siehe unter https://docs.microsoft.com/en-us/SkypeForBusiness/certification/devices-usb-devices aufgeführte Webcams.
Audio- und Videocodecs	Die gleichen Audio- und Videocodecs, die vom nativen Skype for Business-Client verwendet werden. Siehe https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements .

Tabelle 2-7. Systemanforderungen für VMware Virtualization Pack für Skype for Business (Fortsetzung)

System	Anforderungen
Kompatible Skype for Business-Peer-Clients (nicht-VDI)	<ul style="list-style-type: none"> ■ Skype for Business 2016-Client mit aktuellen Updates ■ Skype for Business 2015-Client mit aktuellen Updates ■ Lync 2013-Client mit aktuellen Updates ■ Lync 2010-Client (nur Audioanrufe)
Media Feature Pack	Dieses Paket muss auf dem Remote-Desktop für Windows 10 N- und Windows 10 KN-Versionen installiert werden. Sie können das Media Feature Pack über https://www.microsoft.com/en-us/download/details.aspx?id=48231 installieren.

VMware Virtualization Pack für Skype for Business installieren

Um Skype for Business verwenden zu können, muss das VMware Virtualization Pack für Skype for Business auf dem Clientcomputer installiert sein. Die Software „VMware Virtualization Pack für Skype for Business“ wird standardmäßig im Rahmen der Installationsprogramme von Horizon Client für Windows (4.6 und höher), Horizon Client für Linux (4.6 und höher) und Horizon Client für Mac (4.7 oder höher) installiert. Weitere Informationen zur Installation von Horizon Client finden Sie im Installations- und Einrichtungshandbuch für die Version Horizon Client.

Ein Horizon-Administrator muss bei der Installation von Horizon Agent das VMware Virtualization Pack für Skype for Business auf dem virtuellen Desktop installieren. Weitere Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Das VMware Virtualization Pack für Skype for Business enthält folgende Softwaremodule:

- Horizon Media Proxy, das am virtuellen Desktop installiert ist
- Horizon Media Provider, das auf dem Client-Endpoint installiert ist.

Überprüfen Sie die folgenden Registrierungsschlüssel, um festzustellen, ob VMware Virtualization Pack für Skype for Business auf der virtuellen Maschinen installiert ist:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG_SZ)
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG_SZ)

Kombinationsmodi für eine Sitzung

Beim Starten wird mit Lync.exe das VMware Virtualization Pack für das Skype for Business-Plugin geladen. Das Plugin prüft, ob eine gültige Sitzung ausgeführt wird und schreibt den Kombinationsmodusstatus in die Registry. Überprüfen Sie zur Abfrage von Kombinationsmodi, ob Lync.exe in der Liste der Prozesse ausgeführt wird. Überprüfen Sie anschließend HKEY_CURRENT_USER\Software\VMware, Inc.\VMWMMAPugin – PairingMode(REG_SZ).

Die folgenden Kombinationsmodi sind gültig:

- Optimiert: eine gültige Sitzung
- Fallback: keine gültige Sitzung

- Optimiert (Versionen sind unterschiedlich)
- Fallback (Versionen sind unterschiedlich)
- Verbindung wird hergestellt
- Verbindung getrennt
- Nicht definiert

Wenn Lync.exe beendet wird, löscht das Plugin den Kombinationsmoduswert aus der Registry.

Benutzer benötigen keine Administratorrechte zum Prüfen des Kombinationsmodus. Mehrere an Remote-Desktops angemeldete Benutzer finden den Kombinationsmodus der einzelnen Benutzer in der HKCU-Struktur.

Gruppenrichtlinieneinstellungen des VMware Virtualization Pack für Skype for Business konfigurieren

Sie können für eine Änderung der Standardkonfiguration die Gruppenrichtlinieneinstellungen entsprechend konfigurieren. Siehe [Richtlinieneinstellungen des VMware Virtualization Pack für Skype for Business](#).

Einschränkungen des VMware Virtualization Pack für Skype for Business

VMware Virtualization Pack für Skype for Business hat folgende Einschränkungen:

- SOCKS- und HTTP-Proxy-Server werden nicht unterstützt.
- Die VMware Virtualization Pack for Skype for Business-Lösung bietet keine Interoperabilität mit Drittanbietermodulen für eine Mehr-Parteien-Konferenz wie Pexip.
- Die Galerieansicht wird derzeit nicht unterstützt.
- Anrufe können nicht aufgezeichnet werden.
- Medienumgehung wird nicht unterstützt. Weitere Informationen finden Sie unter <https://kb.vmware.com/s/article/56977>.
- Das Double-Hop-Szenario wie Horizon Agent verschachtelt mit Horizon Client wird nicht unterstützt.
- Die für Skype for Business optimierte VDI-Lösung ist in Bezug auf Interoperabilität nicht kompatibel mit Lync 2010-Clients.
- Die gleichzeitige Verwendung eines Lync- oder Skype for Business-Clients auf dem Clientcomputer mit einem optimierten Skype for Business-Client auf dem Remote-Desktop wird nicht unterstützt.
- Die Lync 2013-Client-Benutzeroberfläche wird nicht unterstützt, wenn der Skype 2015-Client mit einem Lync 2013-Server verbunden ist. Ein Administrator hat die Möglichkeit, die Skype-Client-Benutzeroberfläche auf dem Server zu konfigurieren: <https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx>

- Wenn Sie im Videovorschaufenster eine andere als die aufgeführte Kamera verwenden möchten, wählen Sie das gewünschte Gerät aus, schließen Sie das Dialogfeld und öffnen Sie es für die Vorschau erneut. Wenn Sie die Kamera dynamisch aktualisieren möchten, verwenden Sie das Click-to-Run-Installationsprogramm für Skype for Business 2016 der Version 16.0.11001.20097 oder höher.
- Wenn Sie bei der Installation von Skype for Business auf dem Remote-Desktop mit einem privaten Netzwerk verbunden sind, fügt das Installationsprogramm Firewallregeln für eingehende und ausgehende Verbindungen für dieses Netzwerkprofil hinzu. Wenn Sie sich beim Remote-Desktop von einem Domänennetzwerk aus anmelden und dann Skype for Business verwenden, wird eine Firewallausnahme angezeigt. Um das Problem zu beheben, fügen Sie den Firewallregeln für alle Netzwerkprofile manuell Firewallausnahmen für den Skype for Business-Client hinzu.

Erfassen von Protokollen zur Behebung von Problemen mit Skype for Business

Erfassen Sie zur Fehlerbehebung bei Problemen mit Skype for Business die Protokolle von Horizon Agent und Horizon Client für Windows.

Verfahren

- 1 Melden Sie sich von Horizon Agent aus bei einer virtuellen Maschine an, auf der Horizon Agent installiert ist, um Horizon-Protokolle, einschließlich der Media Proxy-Protokolle, zu erfassen.
- 2 Öffnen Sie eine Eingabeaufforderung und führen Sie `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat` aus.
- 3 Melden Sie sich von Horizon Client aus bei einer physischen oder virtuellen Maschine an, auf der Horizon Client installiert ist, um Horizon-Protokolle, einschließlich der Media Provider-Protokolle, zu erfassen.
- 4 Öffnen Sie eine Eingabeaufforderung und führen Sie `support.bat` aus.
 - 32 Bit: `C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat`
 - 64 Bit: `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

Es wird ein Ordner `vdm-sdct` mit komprimierten Protokolldateien auf dem Desktop angezeigt, der diese Verzeichnisse enthält. Darin befinden sich die Protokolle für das VMware Horizon Virtualization Pack für Skype for Business:

- Clientgerät: `%TEMP%\vmware-<username>\VMWMediaProvider`
- Virtueller Desktop:
 - `%TEMP%\vmware-<username>\VMWMediaProviderProxy`
 - `%TEMP%\vmware-<username>\VMWMediaProviderProxyLocal`
 - `%TEMP%\vmware-<username>\MMAPPlugin`

Die Standard-Protokollierungsebene ist 7, wo die Protokollgröße und die Absturzabbilder klein sind. Sie können die Protokollierungsebene auf 8 erhöhen, um Protokolle maximaler Größe und vollständige Absturzabbilder zu erhalten. Alle Einstellungen sind DWORD:

- Client: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProvider/DebugLogging/LoggingPriority = 8
- Agent: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8
- Agent: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8

Konfigurieren der Umleitung „VMware Integrated Printing“

Die Funktion „VMware Integrated Printing“ ermöglicht Benutzern das Drucken auf allen Druckern, die auf ihren Windows-, Mac- und Linux-Clientcomputern zur Verfügung stehen.

Die Funktion „VMware Integrated Printing“ unterstützt die Clientdruckerumleitung, das standortbasierte Drucken und die dauerhafte Druckereinstellung.

Clientdruckerumleitung

Mit der Clientdruckerumleitung können Benutzer von einem Remote-Desktop aus auf jedem lokalen oder Netzwerkdrucker drucken, der auf einem Windows-, Mac- und Linux-Client installiert ist. Bei Druckern, die von einem Windows-Client zu einem Remote-Desktop umgeleitet werden, unterstützt VMware Integrated Printing zwei Arten von Druckertreibern auf dem Remote-Desktop:

- Nativer Druckertreiber (NPD). Sie müssen auf dem Remote-Desktop denselben Druckertreiber wie beim Clientdrucker installieren. NPD unterstützt nur v3-Drucker.
- Universal-Druckertreiber (UPD). Sie müssen keine Treiber auf dem Remote-Desktop installieren.

Wenn Sie den nativen Treiber auf Horizon Agent installieren, wird NPD standardmäßig verwendet. Andernfalls wird UPD verwendet. Sie können den Druckertreibertyp, der auf einem Remote-Desktop verwendet werden soll, auswählen, indem Sie eine Gruppenrichtlinie festlegen.

Um zu prüfen, welcher Druckertreibertyp in einem Remote-Desktop verwendet wird, gehen Sie zu **Systemsteuerung > Hardware und Sound > Geräte und Drucker**, klicken Sie mit der rechten Maustaste auf den virtuellen Drucker, und wählen Sie aus dem Kontextmenü **Druckereigenschaften** aus. Wenn auf der Registerkarte **Allgemein** unter **Modell** der Treiber VMware Universal EMF angegeben ist, wird UPD verwendet. Andernfalls wird NPD verwendet.

Standortbasiertes Drucken

Die standortbasierte Druckfunktion ordnet Drucker, die sich physisch in der Nähe von Clientsystemen befinden, Remote-Desktops zu. Auf diese Weise können Benutzer von ihren Remote-Desktops über ihre Netzwerkdrucker drucken. Das standortbasierte Drucken wird auf folgenden Remote-Desktops und -Anwendungen unterstützt:

- Desktops, die auf Computern für Einzelbenutzer bereitgestellt werden, z. B. Windows Desktop- und Windows Server-Maschinen
- Veröffentlichte Desktops und veröffentlichte Anwendungen, die auf RDS-Hosts bereitgestellt werden, wobei die RDS-Hosts virtuelle Maschinen oder physische Computer sind

Um das standortbasierte Drucken zu nutzen, müssen Sie die korrekten Druckertreiber auf dem Remote-Desktop installieren und Übersetzungsregeln für jeden standortbasierten Drucker in einer LBP.xml-Datei definieren. Die Regeln legen fest, ob der Drucker zum Remote-Desktop für ein bestimmtes Clientsystem zugeordnet wird. Wenn sich ein Benutzer mit einem Remote-Desktop verbindet, vergleicht Horizon 7 das Clientsystem mit den Übersetzungsregeln. Wenn das Clientsystem allen Übersetzungsregeln entspricht, ordnet Horizon 7 den Drucker während der Benutzersitzung dem Remote-Desktop zu.

Sie können Übersetzungsregeln basierend auf dem Namen des beim Remote-Desktop angemeldeten Benutzers, der IP-Adresse des Clientsystems, dem Hostnamen und der MAC-Adresse definieren. Sie können für einen bestimmten Drucker eine Übersetzungsregel oder eine Kombination aus mehreren Übersetzungsregeln festlegen. Wenn Sie einen standortbasierten Drucker in der LBP.xml-Datei als Standard festlegen, wird er zum Standarddrucker auf dem Remote-Desktop anstelle des Standarddruckers auf dem Client-System.

Damit die Regeln in Kraft treten, speichern Sie die LBP.xml-Datei unter %ProgramData%\VMware auf dem Remote-Desktop, und verbinden Sie den Remote-Desktop oder die Remote-Anwendung neu.

Eine Vorlage der LBP.xml-Datei finden Sie im Ordner VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip. Siehe [Horizon 7-ADMX-Vorlagendateien](#).

Das standortbasierte Drucken kann deaktiviert werden, indem Sie eine Gruppenrichtlinie festlegen.

Umleitung im geschachtelten Modus

In einer Konfiguration im geschachtelten Modus können Sie lokale Drucker, die auf der ersten und zweiten Ebene installiert sind, auf den Remote-Desktop oder die Remoteanwendung auf der dritten Ebene umleiten. Abhängig von der GPO-Einstellung und der Installation nativer Druckertreiber können umgeleitete Drucker auf der dritten Ebene UPD oder NPD verwenden.

Statischer Druckername

Umgeleitete Drucker behalten ihre Namen mit dem Suffix vdi über Sitzungen hinweg bei, sodass der Benutzer den Drucker beim Herstellen einer Verbindung mit einer anderen Sitzung nicht manuell neu zuordnen muss. Der statische Druckername wird nur auf Einzelbenutzer-Maschinen unterstützt und wird auf Windows Server im VDI-Modus nicht unterstützt.

Persistente Druckeinstellung

Druckereinstellungen für umgeleitete Clientdrucker, einschließlich des nativen Druckertreibers und des Universal-Druckertreibers, oder standortbasierte Drucker bleiben erhalten, wenn ein Benutzer sich abmeldet oder die Verbindung zum Desktop trennt. Beispiel: Ein Benutzer konfiguriert einen umgeleiteten Clientdrucker oder einen standortbasierten Drucker für die Verwendung des Schwarz-Weiß-Modus. Nachdem sich der Benutzer abgemeldet und erneut bei dem Desktop angemeldet hat, ist die vorherige Druckeinstellung persistent.

Die persistente Druckeinstellung kann deaktiviert werden, indem Sie eine Gruppenrichtlinie festlegen.

Druckeinstellungen für universelle Druckertreiber

VMware Integrated Printing bietet die folgenden Druckeinstellungen für umgeleitete UPD-Drucker von Windows-Clientcomputern.

- **Ausrichtung:** Wählen Sie Hoch- oder Querformat für das Papier aus. Die Endbearbeitungsoptionen für das Heften und Lochen hängen von der Ausrichtung des Papiers ab.
- **Beidseitig drucken:** Wählen Sie den beidseitigen Druck für Drucker mit dieser Funktion aus.
- **Mehrere Seiten pro Blatt:** Wenn Sie mehrere Dokumentseiten auf einer physischen Seite drucken möchten, wählen Sie die Anzahl der Seiten aus, die auf einer physischen Seite gedruckt werden sollen, und dann das Layout der Seiten aus.
- **Papierquelle:** Wählen Sie das Fach aus, das Papier in der entsprechenden Größe enthält (z. B. Brief oder rechtliches Dokument).
- **Medien:** Wählen Sie den Medientyp aus, auf dem gedruckt werden soll.
- **Farbe:** Geben Sie an, ob ein Farbdrucker bunt oder einfarbig drucken soll.
- **DPI:** Geben Sie die Druckerauflösung an.
- **Druck und Vorschau:** Wählen Sie **Direkt drucken** oder **Druckvorschau** aus:
 - Mit der Option **Direkt drucken** wird, können Sie **mit Dialogfeld für Öffnungseinstellungen** auswählen, mit dem die Clientdruckereinstellungen vor dem Drucken geöffnet werden, sodass Sie die Druckeinstellungen ändern können.
 - Mit **Druckvorschau** ist die Option **mit Dialogfeld für Öffnungseinstellungen** nicht verfügbar.
- **Anzahl der Kopien:** Geben Sie die Anzahl der Kopien an.
- **Als Bild drucken:** Jede Seite als Bild drucken.
- **Komprimierung:** Geben Sie an, wie die Bilder des gedruckten Dokuments komprimiert werden sollen.
- **Endbearbeitung:** Legen Sie die Optionen für das Heften und Lochen für die angegebenen Drucker fest.

Native Druckertreiber-Endbearbeitungsoptionen

Diese umgeleiteten nativen Drucker unterstützen eine Endbearbeitungsoption, wenn die spezifische Hardware mit den Druckern verbunden ist:

Tabelle 2-8. Native Druckertreiber-Endbearbeitungsoptionen

Drucker-	Endbearbeitungsoption	Anforderungen auf dem lokalen Drucker des Clients
FX ApeosPort-IV C5575 PCL 6	Heftklammer, Broschüre	Stellen Sie sicher, dass das Hardwaregerät für die Endbearbeitung mit dem Drucker verbunden ist. Aktualisieren Sie Druckerinformationen mit bidirektionaler Kommunikation in den Druckereigenschaften. Aktivieren Sie die Endbearbeitungsoptionen in den Druckereinstellungen.
Ricoh MP C5003	Heften, lochen	Fügen Sie das Endbearbeitungsgerät manuell entsprechend seiner Geräteeinstellung hinzu, um die Endbearbeitungsoption zu aktivieren, die dann in den Druckereinstellungen verfügbar ist.

Installieren der Umleitung „VMware Integrated Printing“

VMware Integrated Printing ist eine benutzerdefinierte Setup-Option im Horizon Agent-Installationsprogramm. Sie ist nicht standardmäßig ausgewählt. Um sie zu installieren, müssen Sie „VMware Integrated Printing“ auswählen. Informationen zur Installation dieser Funktion auf einer virtuellen Maschine finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*. Informationen zur Installation dieser Funktion auf einem RDS-Host finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*. Die Veröffentlichungen sind verfügbar unter <https://docs.vmware.com/de/VMware-Horizon-7/index.html>. Informationen zum Festlegen von Druckereinstellungen auf einem Windows-Client finden Sie unter *Festlegen von Druckereinstellungen für die Funktion „VMware Integrated Printing“* im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch* unter <https://docs.vmware.com/de/VMware-Horizon-Client-for-Windows/index.html>.

Konfigurieren der Gruppenrichtlinieneinstellungen für die Umleitung „VMware Integrated Printing“

Verwenden Sie die Gruppenrichtlinieneinstellungen in der ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (printerRedirection.admx), um das standortbasierte Drucken zu deaktivieren, die Persistenz der Druckereinstellung zu deaktivieren und den Druckertreiber für einen umgeleiteten Clientdrucker auszuwählen. Siehe [Richtlinieneinstellungen für den VMware-Integrationsdruck](#).

Konfigurieren der URL-Inhaltsumleitung

3

Mit der Funktion der URL-Inhaltsumleitung können Sie bestimmte URLs so konfigurieren, dass diese auf dem Clientcomputer oder in einem Remote-Desktop bzw. in einer veröffentlichten Anwendung geöffnet werden. Damit lassen sich URLs umleiten, die Benutzer in die Adressleiste von Internet Explorer oder in einer Anwendung eingeben.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zur URL-Inhaltsumleitung](#)
- [Anforderungen für die URL-Inhaltsumleitung](#)
- [Verwenden der URL-Inhaltsumleitung in einer Cloud-Pod-Architektur-Umgebung](#)
- [Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung](#)
- [Konfigurieren der Agent-zu-Client-Umleitung](#)
- [Konfigurieren der Client-zu-Agent-Umleitung](#)
- [Einschränkungen der URL-Inhaltsumleitung](#)
- [Nicht unterstützte Funktionen der URL-Inhaltsumleitung](#)
- [Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows](#)
- [Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome auf einem Mac](#)

Grundlegendes zur URL-Inhaltsumleitung

Die Funktion der URL-Inhaltsumleitung unterstützt die Umleitung von einem Remote-Desktop bzw. von einer veröffentlichten Anwendung zu einem Client und umgekehrt.

Die Umleitung von einem Remote-Desktop oder einer veröffentlichten Anwendung zu einem Client wird als „Agent-zu-Client-Umleitung“ bezeichnet. Die Umleitung von einem Client zu einem Remote-Desktop oder zu einer veröffentlichten Anwendung wird „Client-zu-Agent-Umleitung“ genannt.

Agent-zu-Client-Umleitung

Bei der Agent-zu-Client-Umleitung sendet Horizon Agent die URL an Horizon Client. Dort wird die Standardanwendung für das Protokoll der URL auf dem Clientcomputer geöffnet.

Client-zu-Agent-Umleitung

Bei der Client-zu-Agent-Umleitung öffnet Horizon Client einen Remote-Desktop oder eine veröffentlichte Anwendung, den bzw. die Sie für die Verarbeitung der URL festgelegt haben. Wird die URL zu einem Remote-Desktop umgeleitet, wird der Link im Standardbrowser für das Protokoll auf dem Desktop geöffnet. Wird die URL zu einer veröffentlichten Anwendung umgeleitet, wird der Link von der festgelegten Anwendung geöffnet. Der Endbenutzer muss über eine Berechtigung für den Desktop- oder Anwendungspool verfügen.

Es lassen sich URLs von einem Remote-Desktop oder von einer veröffentlichten Anwendung zum Client und URLs von einem Client zu einem Remote-Desktop oder zu einer veröffentlichten Anwendung umleiten. Sie können eine beliebige Anzahl von Protokollen inklusive HTTP, HTTPS, mailto und callto umleiten. Das Callto-Protokoll wird für die Umleitung mit dem Chrome-Browser nicht unterstützt.

Anforderungen für die URL-Inhaltsumleitung

Um die Funktion der URL-Inhaltsumleitung anwenden zu können, müssen Ihre Clientcomputer, Remote-Desktop-Computer und RDS-Hosts bestimmte Anforderungen erfüllen.

Webbrowser

- Internet Explorer 9, 10 und 11
- Chrome 60.0.3112.101 oder höher (offizielles Build), 64 Bit oder 32 Bit

Um den Chrome-Browser mit der URL-Inhaltsumleitung verwenden zu können, muss die Erweiterung „VMware Horizon URL Content Redirection Helper“ installiert und in Chrome aktiviert sein. Installationsanweisungen für Windows finden Sie unter [Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows](#).

Installationsanweisungen für Mac erhalten Sie unter [Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome auf einem Mac](#).

Windows-Clients

- Horizon Client 4.0 für Windows oder höher.
- Um den Chrome-Browser mit der URL-Inhaltsumleitung verwenden zu können, müssen Sie Horizon Client 4.7 oder höher installieren.

- Damit Sie die Client-zu-Agent-Umleitung nutzen können, müssen Sie die Funktion der URL-Inhaltsumleitung bei der Installation von Horizon Client für Windows aktivieren.

Hinweis Für die Agent-zu-Client-Umleitung müssen Sie die Funktion der URL-Inhaltsumleitung in Horizon Client für Windows nicht aktivieren.

Macintosh-Clients

- Horizon Client 4.2 für Mac oder höher

Hinweis In Horizon Client 4.2 und 4.3 für Mac ist die URL-Inhaltsumleitung eine Tech-Preview-Funktion. Dabei wird nur die Agent-zu-Client-Umleitung unterstützt. In Horizon Client 4.4 für Mac und höher wird die URL-Inhaltsumleitung sowohl für die Agent-zu-Client-Umleitung als auch für die Client-zu-Agent-Umleitung offiziell unterstützt.

- Um den Chrome-Browser mit der URL-Inhaltsumleitung verwenden zu können, müssen Sie Horizon Client 4.7 oder höher installieren.

Virtuelle Desktop-Maschinen und RDS-Hosts

- Horizon Agent 7.0 oder höher auf virtuellen Remote-Desktop-Maschinen und RDS-Hosts, die veröffentlichte Desktops und veröffentlichte Anwendungen zur Verfügung stellen.
- Um den Chrome-Browser mit der URL-Inhaltsumleitung verwenden zu können, müssen Sie Horizon Agent 7.4 oder höher installieren.
- Sie müssen die Funktion der URL-Inhaltsumleitung bei der Installation von Horizon Agent aktivieren.

Anzeigeprotokolle

- VMware Blast
- PCoIP

Verwenden der URL-Inhaltsumleitung in einer Cloud-Pod-Architektur-Umgebung

In einer Cloud-Pod-Architektur-Umgebung können Sie zusätzlich zu den lokalen Einstellungen globale Einstellungen für die URL-Inhaltsumleitung konfigurieren.

Anders als lokale Einstellungen für die URL-Inhaltsumleitung, die nur im lokalen Pod angezeigt werden, sind globale Einstellungen im gesamten Pod-Verbund sichtbar. Mit globalen Einstellungen für die URL-Inhaltsumleitung können Sie URL-Links im Client zu globalen Ressourcen wie globale Desktop- und Anwendungsberechtigungen umleiten.

Wenn ein Benutzer sich bei einer Verbindungsserver-Instanz im Pod-Verbund mit Horizon Client anmeldet, überprüft die Verbindungsserver-Instanz alle lokalen und globalen Einstellungen für die URL-Inhaltsumleitung, die dem Benutzer zugewiesen wurden. Die lokalen und globalen Einstellungen werden zusammengeführt und immer dann verwendet, wenn der Benutzer auf eine URL auf dem Clientcomputer klickt.

Vollständige Informationen zur Konfiguration und Verwaltung einer Cloud-Pod-Architektur-Umgebung finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung

Um URL-Inhalte von einem Remote-Desktop oder einer veröffentlichten Anwendung zu einem Client (Agent-zu-Client-Umleitung) oder von einem Client zu einem Remote-Desktop oder einer veröffentlichten Anwendung (Client-zu-Agent-Umleitung) umleiten zu können, müssen Sie bei der Installation von Horizon Agent die URL-Inhaltsumleitung aktivieren.

Statt durch Doppelklicken auf die Installationsdatei starten Sie die Horizon Agent-Installation durch Ausführung des folgenden Befehls in einem Befehlszeilenfenster:

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

Folgen Sie den Anweisungen und schließen Sie die Installation ab.

Um sicherzustellen, dass die Funktion der URL-Inhaltsumleitung installiert ist, vergewissern Sie sich, dass die Dateien `vmware-url-protocol-launch-helper.exe` und `vmware-url-filtering-plugin.dll` im Verzeichnis `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection` enthalten sind. Wenn Sie die Funktion zur URL-Inhaltsumleitung mit Internet Explorer verwenden, müssen Sie auch sicherstellen, dass das VMware Horizon View Plug-In zur URL-Filterung als Internet Explorer-Add-on aktiviert ist.

Konfigurieren der Agent-zu-Client-Umleitung

Bei der Agent-zu-Client-Umleitung sendet Horizon Agent die URL an Horizon Client. Dort wird die Standardanwendung für das Protokoll der URL geöffnet.

Für die Aktivierung der Agent-zu-Client-Umleitung müssen Sie die nachfolgend aufgeführten Konfigurationsaufgaben durchführen.

- Aktivieren Sie in Horizon Agent die Funktion der URL-Inhaltsumleitung. Siehe [Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung](#).
- Wenden Sie die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung auf Ihre Remote-Desktops und veröffentlichten Anwendungen an. Siehe [Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO](#).
- Konfigurieren Sie die Gruppenrichtlinieneinstellungen, um für jedes Protokoll festzulegen, wie Horizon Agent die URL umleiten soll. Siehe [Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung](#).

- (Optional) Für die Verwendung der URL-Inhaltsumleitung im Chrome-Browser müssen Sie die Erweiterung „VMware Horizon URL Content Redirection Helper“ installieren und aktivieren. Siehe [Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows](#).

Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO

Die ADMX-Vorlagendatei `urlRedirection.admx` für die URL-Inhaltsumleitung enthält Einstellungen, mit denen Sie festlegen können, ob ein URL-Link auf dem Client (Agent-zu-Client-Umleitung) oder auf einem Remote-Desktop bzw. in einer Remoteanwendung (Client-zu-Agent-Umleitung) geöffnet wird.

Um die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung auf Ihre Remote-Desktops und -anwendungen anzuwenden, fügen Sie den GPOs auf Ihrem Active Directory-Server die ADMX-Vorlagendatei hinzu. Für Regeln bezüglich URL-Links, auf die in Remote-Desktops oder veröffentlichten Anwendungen geklickt wird, müssen die GPOs mit der Organisationseinheit, die die virtuellen Desktops und RDS-Hosts enthält, verknüpft werden.

Sie können die Gruppenrichtlinieneinstellungen auch auf ein GPO anwenden, das mit der Organisationseinheit verknüpft ist, in der sich Ihre Windows-Clientcomputer befinden. Für die Konfiguration der Client-zu-Agent-Umleitung wird aber die Verwendung des `vdmutl`-Befehlszeilendienstprogramms empfohlen. Da MacOS keine GPOs unterstützt, müssen Sie für Mac-Clients `vdmutl` verwenden.

Voraussetzungen

- Stellen Sie sicher, dass bei der Installation von Horizon Agent auch die Funktion der URL-Inhaltsumleitung installiert wird. Siehe [Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung](#).
- Stellen Sie sicher, dass Active Directory-GPOs für die Gruppenrichtlinieneinstellungen zur URL-Inhaltsumleitung erstellt wurden.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienverwaltungs-Editor“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` (x.x.x ist die Version, yyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip und kopieren Sie die ADMX-Datei für die URL-Inhaltsumleitung auf Ihren Active Directory-Server.
 - a Kopieren Sie die Datei urlRedirection.admx in den Ordner C:\Windows\PolicyDefinitions\.
 - b Kopieren Sie die Sprachressourcendatei urlRedirection.adml in den entsprechenden Unterordner des Ordners C:\Windows\PolicyDefinitions.

So kopieren Sie beispielsweise für das Gebietsschema EN die Datei urlRedirection.adml in den Ordner C:\Windows\PolicyDefinitions\en-US.
 - 3 Öffnen Sie auf Ihrem Active Directory-Server den Editor zur Gruppenrichtlinienverwaltung.
- Die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung werden in **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware Horizon-URL-Umleitung** installiert.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen. Siehe [Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung](#).

Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung

Die Vorlagendatei für die URL-Inhaltsumleitung enthält Gruppenrichtlinieneinstellungen zur Erstellung von Regeln für die Agent-zu-Client- und Client-zu-Agent-Umleitung. Die Vorlagendatei enthält sowohl Richtlinien für die Computerkonfiguration als auch Richtlinien für die Benutzerkonfiguration. Alle Einstellungen befinden sich im Ordner **VMware Horizon URL Redirection** im Gruppenrichtlinienverwaltungs-Editor.

In der folgenden Tabelle werden die Gruppenrichtlinieneinstellungen in der Vorlagendatei für die URL-Inhaltsumleitung beschrieben.

Tabelle 3-1. Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung

Einstellung	Computer	Benutzer	Eigenschaften
IE Policy: Prevent users from changing URL Redirection plugin loading behavior	X		Legt fest, ob Benutzer die Funktion der URL-Inhaltsumleitung deaktivieren können. Diese Einstellung ist standardmäßig nicht konfiguriert.
IE Policy: Automatically enable URL Redirection plugin	X		Legt fest, ob neu installierte Internet Explorer Plug-Ins automatisch aktiviert werden. Diese Einstellung ist standardmäßig nicht konfiguriert.
Url Redirection Enabled	X		Legt fest, ob die URL-Inhaltsumleitung aktiviert wird. Sie können mit dieser Einstellung die Funktion der URL-Inhaltsumleitung deaktivieren, auch wenn diese Funktion auf dem Client oder Agent installiert wurde. Diese Einstellung ist standardmäßig nicht konfiguriert.

Tabelle 3-1. Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Url Redirection Protocol 'http'	X		<p>Legt für alle URLs, die das HTTP-Protokoll verwenden, fest, welche URLs umgeleitet werden. Diese Einstellung verfügt über die folgenden Optionen:</p> <ul style="list-style-type: none"> ■ Broker-Hostname – IP-Adresse oder vollqualifizierter Name des Verbindungsserver-Hosts für die Umleitung von URLs auf einen Remote-Desktop oder eine Remoteanwendung. ■ Remote-Element – Anzeigename des Remote-Desktop- oder Remoteanwendungspools, der die in Agent-Regeln angegebenen URLs verarbeiten kann. ■ Clientregeln – die URLs, die zum Client umgeleitet werden sollen. Beispiel: Sie setzen Clientregeln auf .*.mycompany.com festlegen, werden alle URLs mit der Zeichenfolge mycompany.com zum Windows-basierten Client umgeleitet und dort in einem Standardbrowser geöffnet. ■ Agent-Regeln – die URLs, die zum in Remote-Element angegebenen Remote-Desktop oder zur dort angegebenen Remoteanwendung umgeleitet werden sollen. Beispiel: Sie setzen Agent-Regeln auf .*.mycompany.com festlegen, werden alle URLs, die die Zeichenfolge „mycompany.com“ enthalten, zum Remote-Desktop bzw. zur Remoteanwendung umgeleitet. <p>Sie können reguläre Ausdrücke in Clientregeln und Agent-Regeln eingeben. Wenn die Einstellung Url Redirection IP Rules Enabled aktiviert ist, können Sie auch eine bestimmte IP-Adresse oder einen IP-Adressbereich eingeben. Ausführliche Informationen zur Syntax finden Sie unter Syntax der Regeln für die URL-Inhaltsumleitung.</p> <p>Wenn Sie Agentregeln erstellen, müssen Sie mit der Option Broker-Hostname auch die IP-Adresse oder den vollqualifizierten Domännennamen (FQDN) des Verbindungsserver-Hosts und mit der Option Remote-Element den Anzeigenamen des Desktop- oder Anwendungspools festlegen.</p> <p>Als Best Practice wird empfohlen, die gleichen Umleitungseinstellungen für die HTTP- und HTTPS-Protokolle zu konfigurieren. Wenn ein Benutzer die URL dann teilweise in Internet Explorer eingibt, z. B. in der Form mycompany.com, und diese Site automatisch von HTTP nach HTTPS umgeleitet wird, wird die Funktion der URL-Inhaltsumleitung wie erwartet ausgeführt. Wenn Sie in diesem Beispiel eine Regel für HTTPS, aber nicht die gleiche Umleitungseinstellung für HTTP festlegen, wird die vom Benutzer eingegebene Teil-URL nicht umgeleitet.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Url Redirection Protocol 'https'	X		<p>Legt für alle URLs, die das HTTPS-Protokoll verwenden, fest, welche URLs umgeleitet werden.</p> <p>Die Optionen entsprechen jenen für Url Redirection Protocol 'http'.</p> <p>Diese Einstellung ist standardmäßig nicht konfiguriert.</p>

Tabelle 3-1. Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Url Redirection Protocol '[...]	X		<p>Sie können diese Einstellung für jedes Protokoll außer HTTP und HTTPS verwenden, wie zum Beispiel email oder callto.</p> <p>Die Optionen entsprechen jenen für Url Redirection Protocol 'http' und Url Redirection Protocol 'https'.</p> <p>Wenn Sie keine anderen Protokolle konfigurieren müssen, können Sie diesen Eintrag vor dem Hinzufügen der Vorlagendatei für die URL-Inhaltsumleitung zum Active Directory löschen oder auskommentieren.</p> <p>Diese Einstellung ist standardmäßig nicht konfiguriert.</p>
Install the Chrome extension that is required in the URL content redirection feature.		X	<p>Wenn diese Einstellung aktiviert ist, wird die Chrome-Erweiterung, die für die Funktion der URL-Inhaltsumleitung erforderlich ist, automatisch im Hintergrund installiert. Diese Installation umfasst auch das Gewähren der erforderlichen Berechtigungen. Um diese Installation rückgängig machen zu können, benötigen Sie Administratorrechte.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird die Chrome-Erweiterung, die für die URL-Inhaltsumleitung notwendig ist, nicht installiert. Die URL-Inhaltsumleitung kann dann nicht im Chrome-Browser angewendet werden, auch wenn sie festgelegt ist. Sie müssen in diesem Fall die Erweiterung aus dem Chrome Web Store installieren.</p> <p>Diese Einstellung ist standardmäßig nicht konfiguriert.</p>
Url Redirection IP Rules Enabled	X		<p>Wenn diese Einstellung aktiviert ist, können Sie eine bestimmte IP-Adresse oder einen IP-Adressbereich in Clientregeln oder Agent-Regeln eingeben. Weitere Informationen finden Sie unter Filtern der IP-Adresse und des IP-Adressbereichs.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Hinweis Diese Funktion wird nur mit Internet Explorer und IPv4 unterstützt.</p>

Wenn Sie für eine Client-zu-Agent-Umleitung ein Protokoll ohne einen Standardhandler konfigurieren, müssen Sie nach der Konfiguration einer Gruppenrichtlinieneinstellung für dieses Protokoll Horizon Client einmal starten, bevor URLs, die dieses Protokoll festlegen, umgeleitet werden.

Für die Konfiguration der Client-zu-Agent-Umleitung wird die Verwendung des `vdmtail`-Befehlszeilendienstprogramms statt der Gruppenrichtlinieneinstellungen empfohlen.

Syntax der Regeln für die URL-Inhaltsumleitung

Wenn Sie die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung verwenden, müssen Sie angeben, welche URLs am Client (Option **Clientregeln**) bzw. an einem Remote-Desktop oder in einer veröffentlichten Anwendung (Option **Agent-Regeln**) geöffnet werden sollen.

URLs

Sie können URLs in **Clientregeln** und **Agent-Regeln** eingeben. Sie können mit Platzhalterzeichen (*) ein URL-Muster für eine Gruppe von URLs angeben. Sie müssen vor einem Punkt ein Maskierungszeichen (\) hinzufügen, um einen Punkt in einem Regeleintrag anzugeben. Wenn Sie beispielsweise ".*\net" angeben, wird xxxx.net weitergeleitet, aber http://intranet nicht.

Die folgende Tabelle enthält Beispiele für Regeleinträge, die URLs enthalten.

Regeleintrag	Beschreibung
.*	Legt fest, dass alle URLs umgeleitet werden. Wenn Sie diese Einstellung für Agent-Regeln (Option Agent-Regeln) verwenden, werden alle URLs am angegebenen Desktop bzw. in der angegebenen veröffentlichten Anwendung geöffnet. Wenn Sie diese Einstellung für Clientregeln (Option Clientregeln) verwenden, werden alle URLs zum Client umgeleitet.
.*\acme.com;.* \example.com	Legt fest, dass alle URLs mit der Zeichenfolge .acme.com oder .example.com umgeleitet werden. Verwenden Sie Semikolons für das Trennen mehrerer Einträge. Leerzeichen zwischen den Einträgen sind nicht zulässig.
.*\acme.com/ software	Legt fest, dass alle URLs, die die Zeichenfolge .acme.com und das Unterverzeichnis /software enthalten, umgeleitet werden. Beispiel: http://www.acme.com/software wird umgeleitet. Auch http://www.acme.com/software/consumer wird umgeleitet.
[Leerzeichen oder leer lassen]	Legt fest, dass keine URLs umgeleitet werden. Wenn Sie beispielsweise die Option Clientregeln leer lassen, wird keine URL auf den Client umgeleitet.

Reguläre Ausdrücke

Sie können reguläre Ausdrücke in **Clientregeln** und **Agent-Regeln** eingeben. Informationen zur Syntax finden Sie unter [Regeln für reguläre Ausdrücke, die von der URL-Inhaltsumleitung unterstützt werden](#).

Filtern der IP-Adresse und des IP-Adressbereichs

Wenn Sie die Gruppenrichtlinieneinstellung „URL-Umleitungs-IP-Regeln aktiviert“ aktivieren, können Sie eine bestimmte IP-Adresse oder einen IP-Adressbereich in **Clientregeln** und **Agent-Regeln** eingeben.

Wenn Sie beispielsweise „URL-Umleitungs-IP-Regeln aktiviert“ aktivieren und ".*\mycompany.com;22.22.22.22;10.10.1.2-10.10.12.20" eingeben, werden die folgenden URLs und IP-Adressen umgeleitet.

- Alle URLs, die „mycompany.com“ enthalten
- IP-Adresse 22.22.22.22
- Alle IP-Adressen im Bereich 10.10.1.2 bis 10.10.12.20
- Alle URLs, die in die IP-Adresse 22.22.22.22 aufgelöst werden
- Alle URLs, die in den IP-Adressbereich 10.10.1.2 bis 10.10.12.20 aufgelöst werden

Wenn Sie sowohl eine URL als auch eine IP-Adresse oder einen IP-Adressbereich eingeben, hat die URL-Regel die höhere Priorität. Wenn die URL übereinstimmt, erfolgt die Umleitung direkt über die URL. Wenn die URL nicht übereinstimmt, führt Horizon eine DNS-Abfrage durch und übernimmt dann die Filterung der IP-Adresse oder des IP-Adressbereichs.

Diese Funktion wird nur mit Internet Explorer und IPv4 unterstützt. Die Richtlinie ist standardmäßig deaktiviert.

Regeln für reguläre Ausdrücke, die von der URL-Inhaltsumleitung unterstützt werden

Sie können einen regulären Ausdruck in **Clientregeln** und **Agent-Regeln** eingeben. Ein regulärer Ausdruck ist ein Objekt, das ein Zeichenmuster beschreibt. Reguläre Ausdrücke führen Funktionen zu Musterübereinstimmungen und Suche und Ersetzung in Texten aus.

Die URL-Inhaltsumleitung unterstützt die folgenden Regeln für reguläre Ausdrücke.

Regel	Einzelheiten
Klammern	[], [^], (), (? :), (? =)
\+Metazeichen oder Metazeichen	'\w', '\W', '\d', '\D', '\b', '\B'
Quantifizierer	+, *, ?, {x}, {x,y}, {x,}
Alternierung	

Detaillierte Informationen zu regulären Ausdrücken finden Sie unter https://de.wikipedia.org/wiki/Regul%C3%A4rer_Ausdruck.

Die folgende Tabelle enthält Beispiele für Regeln für reguläre Ausdrücke, die von der URL-Inhaltsumleitung unterstützt werden.

Regeleintrag	Beispiele für übereinstimmende URLs und IP-Adressen
.*\.net	www.hello.net, www.inter.net, train.word.net, test.train.net und train.chromeie.net.com.cn.
.*\.sth\.ctirial	example.sth.ctirial, www.google.sth.ctirial und www.google.com/test.sth.ctirial/editpage.action.
.*administra	www.administra.com, www.askadministra-tor.net und google.akmkda.eae/administra.cn.
.*a{4}custom\.com	world.banada.cn/aaaacustom.com, www.aaaacustom.com und exple.aaaacustom.com.net/nodepad.action.
.*a{2,3}custom\.com	world.banada.aacustom.com, www.aacustom.com und exple.aacustom.com.net/nodepad.action.
.*train[abc]\.net	hello.traina.net, hello.trainb.net, example.trainc.net.com und www.testtraina.net.com/edit.
.*train[^abc]\.net	hello.traind.net, hello.traine.net, example.train2.net.com und www.testtrain3.net.com/edit.
.*a+c*tra\.net	www.actra.net.com. aactra.net.cn, atra.net.www.train und aaccctra.networkd.
.*example(test)?\.cn	www.example.cn, www.exampletest.cn, example.cn/editpage und exampletest.cn/editpage.
sac(?:=sprt)	helloworld.sacsprt.net, examplesacsprt.com/text und www.sacsprtexam.com.

Regeleintrag	Beispiele für übereinstimmende URLs und IP-Adressen
sac(?!\sprt)	helloworld.sacspra.net, examplesacbpri.com/text und www.sacexam.com.
10\1\1\1\1[0-5]	10.1.1.10 bis 10.1.1.15.
10\1\1(1 2)\1[0-5]	10.1.1.10 bis 10.1.1.15 und 10.1.2.10 bis 10.1.2.15.
10\.[2-4]\19\12	10.2.19.12, 10.3.19.12 und 10.4.19.12.
10\[^\2-4]\19\12	10.6.19.12, 10.1.19.12, 10.5.19.12 und 10.7.19.12.
a(w)cd(d)345a.com	www.abccd2345a.com.net und train.adc2cd1345a.com/edit.action.
abc(W)cd(D)345a.com	google.abc+cda345a.com und test.train.net/abc&cda345a.com.
((25[0-5] 2[0-4][0-9] ([01]?[0-9]?[0-9])\.)\3){25[0-5] 2[0-4][0-9] ([01]?[0-9]?[0-9])}	Alle IPv4-Adressen.
.*example(test)?\1.cn;10\1\1\1\1[0-5];a(w)cd(d)345a.com	www.example.cn, example.cn/editpage, 10.1.1.10 to 10.1.1.15, www.abccd2345a.com.net und train.adc2cd1345a.com/edit.action.

Beispiel einer Gruppenrichtlinie für eine Agent-zu-Client-Umleitung

Sie können mit der Agent-zu-Client-Umleitung Ressourcen schonen oder diese Umleitung als zusätzliche Sicherheitsebene einsetzen. Wenn sich beispielsweise Mitarbeiter an einem Remote-Desktop oder in einer veröffentlichten Anwendung Videos ansehen, können Sie die entsprechenden URLs zum Clientcomputer umleiten, sodass das Datacenter nicht zusätzlich belastet wird. Wenn Mitarbeiter außerhalb des Firmennetzwerks arbeiten, ist es aus Sicherheitsgründen möglicherweise besser, dass alle URLs, die auf externe Standorte außerhalb des Firmennetzwerks verweisen, auf dem eigenen Client Computer des Mitarbeiters geöffnet werden.

Sie können beispielsweise Regeln konfigurieren, durch die URLs, die nicht auf das Firmennetzwerk verweisen, an den Client Computer umgeleitet und dort geöffnet werden. In diesem Beispiel können Sie folgende Einstellungen mit regulären Ausdrücken verwenden:

- Für **Agent-Regeln** : `.*.mycompany.com`

Mit dieser Regel wird jede URL mit der Zeichenfolge `mycompany.com` zu einem bestimmten Remote-Desktop oder zu einer veröffentlichten Anwendung (Agent) umgeleitet und dort geöffnet.

- Für **Clientregeln**: `.*`

Mit dieser Regel werden alle URLs zum Client umgeleitet und dort mit dem standardmäßigen Clientbrowser geöffnet.

Auf die Funktion der URL-Inhaltsumleitung werden mit dem folgenden Vorgang Client- und Agentregeln angewendet:

- 1 Wenn ein Benutzer auf einen Link in einer veröffentlichten Anwendung oder einem Remote-Desktop klickt, werden zuerst die Clientregeln überprüft.
- 2 Wenn die URL einer Clientregel entspricht, werden als Nächstes die Agentregeln überprüft.

- 3 Wenn zwischen dem Agenten und den Clientregeln ein Konflikt besteht, wird der Link lokal geöffnet. In diesem Beispiel wird die URL auf dem Agentencomputer geöffnet.
- 4 Wenn kein Konflikt besteht, wird die URL an den Client umgeleitet.

In diesem Beispiel besteht ein Konflikt zwischen den Client- und den Agentregeln, da URLs mit **mycompany.com** eine Teilmenge aller URLs darstellen. Deshalb werden URLs mit der Zeichenfolge **mycompany.com** lokal geöffnet. Wenn Sie an einem Remote-Desktop auf einen Link mit der Zeichenfolge **mycompany.com** in der URL klicken, wird die URL an diesem Remote-Desktop geöffnet. Wenn Sie in einem Clientsystem auf einen Link mit der Zeichenfolge **mycompany.com** in der URL klicken, wird die URL auf dem Client geöffnet.

Konfigurieren der Client-zu-Agent-Umleitung

Bei einer Client-zu-Agent-Umleitung öffnet Horizon Client einen Remote-Desktop oder eine veröffentlichte Anwendung zur Verarbeitung eines URL-Links, auf den ein Benutzer auf dem Client geklickt hat. Wird ein Remote-Desktop geöffnet, verarbeitet die Standardanwendung für das URL-Protokoll diese URL. Wird eine veröffentlichte Anwendung geöffnet, verarbeitet die Anwendung die URL.

Für die Verwendung der Agent-zu-Client-Umleitung müssen Sie die nachfolgend aufgeführten Konfigurationsaufgaben durchführen.

- Erstellen Sie mit dem `vdmut il`-Befehlszeilendienstprogramm in einer Verbindungsserverinstanz eine Einstellung für die URL-Inhaltsumleitung, die für jedes Protokoll angibt, wie Horizon Client die URLs umleitet. Siehe [Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung](#) oder [Erstellen einer globalen Einstellung für die URL-Inhaltsumleitung](#).
- Weisen Sie mit dem `vdmut il`-Befehlszeilen-Dienstprogramm in einer Verbindungsserverinstanz den Active Directory-Benutzern oder -Gruppen die Einstellung für die URL-Inhaltsumleitung zu. Siehe [Zuweisen einer Einstellung für die URL-Inhaltsumleitung zu einem Benutzer oder einer Gruppe](#).
- Aktivieren Sie in Horizon Agent die Funktion der URL-Inhaltsumleitung. Siehe [Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung](#).
- (Nur Windows-Clients) Aktivieren Sie die Funktion der URL-Inhaltsumleitung in Horizon Client für Windows. Siehe [Installieren von Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung](#).
- (Optional) Für die Verwendung der URL-Inhaltsumleitung im Chrome-Browser müssen Sie die Erweiterung „VMware Horizon URL Content Redirection Helper“ installieren und aktivieren. Informationen zu Windows-Clients finden Sie unter [Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows](#). Informationen zu Mac-Clients erhalten Sie unter [Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome auf einem Mac](#).

- Überprüfen Sie die Einstellung für die URL-Inhaltsumleitung. Siehe [Testen einer Einstellung für die URL-Inhaltsumleitung](#).

Wichtig Sie können mit Gruppenrichtlinieneinstellungen Regeln für die Client-zu-Agent-Umleitung konfigurieren. Es wird aber die Verwendung des `vdmuti1`-Befehlszeilendienstprogramms empfohlen. Weitere Informationen zu den Gruppenrichtlinieneinstellungen finden Sie im Abschnitt [Verwenden von Gruppenrichtlinieneinstellungen für die Konfiguration der Client-zu-Agent-Umleitung](#). Bei Mac-Clients müssen Sie `vdmuti1` zur Konfiguration einer Client-zu-Agent-Umleitung verwenden. Da macOS keine GPOs unterstützt, können Sie mit Mac-Clients keine Gruppenrichtlinieneinstellungen zum Konfigurieren der Client-zu-Agent-Umleitung verwenden.

Verwenden des `vdmuti1`-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz

Sie können mit der `vdmuti1`-Befehlszeilenschnittstelle in einer Verbindungsserverinstanz Einstellungen für die URL-Inhaltsumleitung zur Client-zu-Agent-Umleitung erstellen, zuweisen und verwalten.

Hinweis Sie müssen den `vdmuti1`-Befehl verwenden, um die Client-zu-Agent-Umleitung für Mac-Clients zu konfigurieren. Da macOS keine GPOs unterstützt, können Sie, wenn Sie über Mac-Clients verfügen, die Client-zu-Agent-Umleitung nicht mit GPOs konfigurieren.

Verwendung des Befehls

Mit der Syntax des `vdmuti1`-Befehls steuern Sie dessen Ausführung von der Windows-Eingabeaufforderung aus.

```
vdmuti1 Befehlsoption [Zusatzoption Argument] ...
```

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab.

Der Pfad zur ausführbaren Datei des Befehls `vdmuti1` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie ihn zur PATH-Umgebungsvariable hinzu.

Befehlsauthentifizierung

Sie müssen den `vdmuti1`-Befehl als Benutzer mit der Administratorrolle ausführen.

Sie können einem Benutzer die Administratorrolle mithilfe von Horizon Administrator zuweisen. Weitere Informationen finden Sie im Dokument *Horizon 7-Verwaltung*.

Der `vdmuti1`-Befehl umfasst Optionen zur Angabe des Benutzernamens, der Domäne und des Kennworts für die Authentifizierung. Sie müssen diese Authentifizierungsoptionen mit allen `vdmuti1`-Befehlsoptionen verwenden (Ausnahme: `--help` und `--verbose`).

Tabelle 3-2. vdmutil-Befehlsauthentifizierungsoptionen

Option	Beschreibung
<code>--authAs</code>	Benutzername eines Horizon-Administratorbenutzers zur Authentifizierung bei der Verbindungsserver-Instanz. Verwenden Sie nicht das Format Domäne\Benutzername oder das UPN-Format (Benutzerprinzipalname).
<code>--authDomain</code>	Der vollqualifizierte Domänenname für den mit der Option <code>--authAs</code> angegebenen Horizon-Administratorbenutzer.
<code>--authPassword</code>	Das Kennwort für den mit der Option <code>--authAs</code> angegebenen Horizon-Administratorbenutzer. Wenn "*" anstelle eines Kennworts eingegeben wird, fordert der Befehl <code>vdmutil</code> zur Eingabe des Kennworts auf. Vertrauliche Kennwörter werden dann nicht im Befehlsverlauf der Befehlszeile hinterlassen.

Beispielsweise meldet der nachfolgend dargestellte Befehl `vdmutil` den Benutzer `mydomain\johndoe` an.

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

Ausgabe des Befehls

Der Befehl `vdmutil` gibt 0 zurück, wenn ein Vorgang erfolgreich ist, und einen fehlerspezifischen Code ungleich null, wenn ein Vorgang fehlschlägt. Der Befehl `vdmutil` schreibt Fehlermeldungen in die Standardfehler. Wenn ein Vorgang eine Ausgabe erzeugt oder die ausführliche Protokollierung mithilfe der Option `--verbose` aktiviert ist, schreibt der Befehl `vdmutil` die Ausgabe auf Englisch in die Standardausgabe.

Optionen für die URL-Inhaltsumleitung

Mithilfe des im Folgenden dargestellten `vdmutil`-Befehls können Sie Einstellungen für die URL-Inhaltsumleitung erstellen, zuweisen und verwalten. Vor allen Optionen stehen zwei Bindestriche (--).

Tabelle 3-3. vdmutil-Befehloptionen für die URL-Inhaltsumleitung

Option	Beschreibung
<code>--addGroupURLSetting</code>	Weist eine Gruppe einer bestimmten Einstellung für die URL-Inhaltsumleitung zu.
<code>--addUserURLSetting</code>	Weist einen Benutzer einer bestimmten Einstellung für die URL-Inhaltsumleitung zu.
<code>--createUrlSetting</code>	Erstellt eine Einstellung für die URL-Inhaltsumleitung.
<code>--deleteURLSetting</code>	Löscht eine Einstellung für die URL-Inhaltsumleitung.
<code>--disableURLSetting</code>	Deaktiviert eine Einstellung für die URL-Inhaltsumleitung.
<code>--enableURLSetting</code>	Aktiviert eine Einstellung für die URL-Inhaltsumleitung, die mit der Option <code>--disableURLSetting</code> deaktiviert wurde.
<code>--listURLSetting</code>	Listet alle Einstellungen für die URL-Inhaltsumleitung auf der Verbindungsserver-Instanz auf.
<code>--readURLSetting</code>	Zeigt Informationen zur Einstellung für die URL-Inhaltsumleitung an.
<code>--removeGroupURLSetting</code>	Entfernt eine Gruppenzuweisung von einer Einstellung für die URL-Inhaltsumleitung.

Tabelle 3-3. vdmutil-Befehlsoptionen für die URL-Inhaltsumleitung (Fortsetzung)

Option	Beschreibung
<code>--removeUserURLSetting</code>	Entfernt eine Benutzerzuweisung von einer Einstellung für die URL-Inhaltsumleitung.
<code>--updateURLSetting</code>	Aktualisiert eine vorhandene Einstellung für die URL-Inhaltsumleitung.

Sie können für alle vdmutil-Optionen Syntaxinformationen durch Eingabe von **vdmutil --help** anzeigen. Um detaillierte Syntaxinformationen für eine bestimmte Option aufzurufen, geben Sie **vdmutil --option --help** ein.

Syntax für die Option „--agentURLPattern“

Wenn Sie mit dem vdmutil-Befehl eine URL-Inhaltsumleitungseinstellung in einer Verbindungsserverinstanz erstellen, geben Sie eine Zeichenfolge in Anführungszeichen ein, in der Sie die URL oder URLs angeben, die am Remote-Desktop oder veröffentlichten Anwendung in der Option `--agentURLPattern` geöffnet werden sollte(n).

Die in Anführungszeichen gesetzte Zeichenfolge enthält einen regulären Ausdruck und muss das Protokoll-Präfix enthalten. Sie können mit Platzhalterzeichen ein URL-Muster für eine Gruppe von URLs angeben.

In der folgenden Tabelle werden einige Beispiele von URL-Mustern beschrieben.

Agent-URL-Muster	Beschreibung
<code>".*"</code>	Alle Client-URLs werden an den Remote-Desktop oder die veröffentlichte Anwendung umgeleitet.
<code>"http://google.*"</code>	Alle Client-URLs, die die Zeichenfolge google enthalten, werden an den Remote-Desktop oder die veröffentlichte Anwendung umgeleitet.
<code>"http://acme.com/software"</code>	Alle Client-URLs, die die Zeichenfolge acme.com und das Unterverzeichnis /software enthalten, werden an den Remote-Desktop oder die veröffentlichte Anwendung umgeleitet. Beispiel: <code>http://www.acme.com/software</code> wird umgeleitet. Auch <code>http://www.acme.com/software/consumer</code> wird umgeleitet.

Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung

Sie können eine lokale Einstellung für die URL-Inhaltsumleitung erstellen, mit der bestimmte URLs zu einem Remote-Desktop oder zu einer veröffentlichten Anwendung umgeleitet und dort geöffnet werden. Eine lokale Einstellung für die URL-Inhaltsumleitung wird nur im lokalen Pod angezeigt.

Sie können eine beliebige Anzahl von Protokollen inklusive HTTP, HTTPS, mailto und callto konfigurieren. Das Callto-Protokoll wird für die Umleitung mit dem Chrome-Browser nicht unterstützt.

Als Best Practice wird empfohlen, die gleichen Umleitungseinstellungen für die HTTP- und HTTPS-Protokolle zu konfigurieren. Wenn ein Benutzer die URL dann teilweise in Internet Explorer eingibt, z. B. in der Form `mycompany.com`, und diese Site automatisch von HTTP nach HTTPS umgeleitet wird, wird die Funktion der URL-Inhaltsumleitung wie erwartet ausgeführt. Wenn Sie in diesem Beispiel eine Regel für HTTPS, aber nicht die gleiche Umleitungseinstellung für HTTP festlegen, wird die vom Benutzer eingegebene Teil-URL nicht umgeleitet.

VMware empfiehlt, nicht mehr als eine Einstellung für die URL-Inhaltsumleitung zu erstellen.

Erläuterungen zum Erstellen einer globalen Einstellung für die URL-Inhaltsumleitung, die im gesamten Pod-Verbund angezeigt wird, finden Sie unter [Erstellen einer globalen Einstellung für die URL-Inhaltsumleitung](#).

Voraussetzungen

- Machen Sie sich mit den Optionen und Anforderungen der vdmutil-Befehlszeilenschnittstelle vertraut und überprüfen Sie, ob Sie über die Berechtigung zur Ausführung des vdmutil-Befehls verfügen. Siehe [Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz](#).
- Machen Sie sich mit der Syntax für URLs in den Einstellungen für die URL-Inhaltsumleitung vertraut. Siehe [Syntax für die Option „--agentURLPattern“](#).

Verfahren

- 1 Melden Sie sich bei der Verbindungsserver-Instanz an.
- 2 Führen Sie den Befehl vdmutil mit der Option --createUrlSetting zum Erstellen der Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --createUrlSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description Wert] [--urlScheme Wert] [--entitledApplication Wert | --entitledDesktop Wert] [--agentURLPattern Wert]
```

Option	Beschreibung
--urlSettingName	Eindeutiger Name der Einstellung für die URL-Inhaltsumleitung. Der Name muss url-filtering sein.
--urlRedirectionScope	Geltungsbereich der Einstellung für die URL-Inhaltsumleitung. Damit die Einstellung nur im lokalen Pod angezeigt wird, geben Sie LOCAL an.
--description	Beschreibung der Einstellung für die URL-Inhaltsumleitung. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.
--urlScheme	Protokoll, für das die Einstellung für die URL-Inhaltsumleitung gültig ist, z. B. http, https, mailto oder callto.
--entitledApplication	Anzeigenname eines lokalen Anwendungspools für das Öffnen der angegebenen URLs (z. B. iexplore-2012). Sie können mit dieser Option auch den Anzeigenamen eines lokalen RDS-Desktop-Pools festlegen.
--entitledDesktop	Anzeigenname eines lokalen Desktop-Pools für das Öffnen der angegebenen URLs (z. B. Win10). Für RDS-Desktop-Pools verwenden Sie die Option --entitledApplication.
--agentURLPattern	Eine Zeichenfolge in Anführungszeichen, die die URL angibt, die auf einem Remote-Desktop oder in einer veröffentlichten Anwendung geöffnet werden soll.

- 3 (Optional) Führen Sie den Befehl `vdmutl` mit der Option `--updateURLSetting` aus, um der erstellten Einstellung für die URL-Inhaltsumleitung weitere Protokolle, URLs und lokale Ressourcen hinzuzufügen.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description Wert][--urlScheme Wert][--entitledApplication Wert | --entitledDesktop Wert] [--
agentURLPattern Wert]
```

Die Optionen sind identisch mit jenen für den Befehl `vdmutl` mit der Option `--createURLSetting`.

Beispiel: Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung

Im nachfolgend dargestellten Beispiel wird eine lokale Einstellung für die URL-Inhaltsumleitung namens `url-filtering` erstellt, mit der alle Client-URLs mit der Zeichenfolge `http://google` umgeleitet werden.* zum Anwendungspool `iexplore2012` umgeleitet werden.

```
VdmUtil --createURLSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

Im nächsten Beispiel wird die Einstellung `url-filtering` so geändert, dass auch alle Client-URLs mit der Zeichenfolge `https://google.*` zum Anwendungspool `iexplore2012` umgeleitet werden.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

Im folgenden abschließenden Beispiel wird die Einstellung `url-filtering` so geändert, dass alle Client-URLs mit der Zeichenfolge `mailto://*.mycompany.com` zum Anwendungspool `Outlook2008` umgeleitet werden.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

Nächste Schritte

Weisen Sie die Einstellung für die URL-Inhaltsumleitung einem Benutzer oder einer Gruppe zu. Siehe [Zuweisen einer Einstellung für die URL-Inhaltsumleitung zu einem Benutzer oder einer Gruppe](#).

Erstellen einer globalen Einstellung für die URL-Inhaltsumleitung

Wenn Sie in einer Cloud-Pod-Architektur-Umgebung arbeiten, können Sie eine globale Einstellung für die URL-Inhaltsumleitung erstellen, mit der bestimmte URLs auf einen Remote-Desktop oder eine veröffentlichte Anwendung in einem beliebigen Pod des Pod-Verbundes umgeleitet und dort geöffnet werden.

Eine globale Einstellung für die URL-Inhaltsumleitung wird im gesamten Pod-Verbund angezeigt. Mit einer globalen Einstellung für die URL-Inhaltsumleitung können Sie URLs auf globale Ressourcen wie globale Desktop- und Anwendungsberechtigungen umleiten.

Sie können eine beliebige Anzahl von Protokollen inklusive HTTP, HTTPS, mailto und callto konfigurieren. Das Callto-Protokoll wird für die Umleitung mit dem Chrome-Browser nicht unterstützt.

Als Best Practice wird empfohlen, die gleichen Umleitungseinstellungen für die HTTP- und HTTPS-Protokolle zu konfigurieren. Wenn ein Benutzer die URL dann teilweise in Internet Explorer eingibt, z. B. in der Form `mycompany.com`, und diese Site automatisch von HTTP nach HTTPS umgeleitet wird, wird die Funktion der URL-Inhaltsumleitung wie erwartet ausgeführt. Wenn Sie in diesem Beispiel eine Regel für HTTPS, aber nicht die gleiche Umleitungseinstellung für HTTP festlegen, wird die vom Benutzer eingegebene Teil-URL nicht umgeleitet.

Vollständige Informationen zur Konfiguration und Verwaltung einer Cloud-Pod-Architektur-Umgebung finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

VMware empfiehlt, nicht mehr als eine Einstellung für die URL-Inhaltsumleitung zu erstellen.

Erläuterungen zum Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung erhalten Sie unter [Erstellen einer lokalen Einstellung für die URL-Inhaltsumleitung](#).

Voraussetzungen

- Machen Sie sich mit den Optionen und Anforderungen der `vdmutl`-Befehlszeilenschnittstelle vertraut und überprüfen Sie, ob Sie über die Berechtigung zur Ausführung des `vdmutl`-Befehls verfügen. Siehe [Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz](#).
- Machen Sie sich mit der Syntax für URLs in den Einstellungen für die URL-Inhaltsumleitung vertraut. Siehe [Syntax für die Option „--agentURLPattern“](#).

Verfahren

- 1 Melden Sie sich bei einer Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Führen Sie den Befehl `vdmutl` mit der Option `--createUrlSetting` zum Erstellen der Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutl --createUrlSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
[--description Wert] [--urlScheme Wert] [--entitledApplication Wert | --entitledDesktop
Wert] [--agentURLPattern Wert]
```

Option	Beschreibung
<code>--urlSettingName</code>	Eindeutiger Name der Einstellung für die URL-Inhaltsumleitung. Der Name muss url-filtering sein.
<code>--urlRedirectionScope</code>	Geltungsbereich der Einstellung für die URL-Inhaltsumleitung. Wenn die Einstellung im gesamten Pod-Verbund angezeigt werden soll, geben Sie dafür GLOBAL an.
<code>--description</code>	Beschreibung der Einstellung für die URL-Inhaltsumleitung. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.
<code>--urlScheme</code>	Protokoll, für das die Einstellung für die URL-Inhaltsumleitung gültig ist, z. B. http, https, mailto oder callto.

Option	Beschreibung
--entitledApplication	Anzeigename einer globalen Anwendungsberechtigung für das Öffnen der angegebenen URLs.
--entitledDesktop	Anzeigename einer globalen Berechtigung für das Öffnen der angegebenen URLs (z. B. GE-1).
--agentURLPattern	Eine Zeichenfolge in Anführungszeichen, die die URL angibt, die auf einem Remote-Desktop oder in einer veröffentlichten Anwendung geöffnet werden soll.

- 3 (Optional) Führen Sie den Befehl `vdmutl` mit der Option `--updateURLSetting` aus, um der erstellten Einstellung für die URL-Inhaltsumleitung weitere Protokolle, URLs und globale Ressourcen hinzuzufügen.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
[--description Wert] [--urlScheme Wert] [--entitledApplication Wert | --entitledDesktop
Wert] [--agentURLPattern Wert]
```

Die Optionen sind identisch mit jenen für den Befehl `vdmutl` mit der Option `--createURLSetting`.

Beispiel: Konfigurieren einer globalen Einstellung für die URL-Inhaltsumleitung

Im nachfolgend dargestellten Beispiel wird eine globale Einstellung für die URL-Inhaltsumleitung namens `url-filtering` erstellt, mit der alle Client-URLs mit der Zeichenfolge `http://google` umgeleitet werden. `*` zu einer globalen Anwendungsberechtigung mit dem Namen `GAE1` umgeleitet werden.

```
vdmutl --createURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

Im nächsten Beispiel wird die Einstellung `url-filtering` so geändert, dass auch alle URLs mit der Zeichenfolge „`https://google`“ umgeleitet werden. `*` zu einer globalen Anwendungsberechtigung mit dem Namen `GAE1` umgeleitet werden.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

Im folgenden abschließenden Beispiel wird die Einstellung `url-filtering` so geändert, dass alle Client-URLs mit der Zeichenfolge „`mailto://`“ umgeleitet werden. `*.mycompany.com`“ zu einer globalen Anwendungsberechtigung mit dem Namen `GA2` umgeleitet werden.

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

Nächste Schritte

Weisen Sie die Einstellung für die URL-Inhaltsumleitung einem Benutzer oder einer Gruppe zu. Siehe [Zuweisen einer Einstellung für die URL-Inhaltsumleitung zu einem Benutzer oder einer Gruppe](#).

Zuweisen einer Einstellung für die URL-Inhaltsumleitung zu einem Benutzer oder einer Gruppe

Wenn Sie eine Einstellung für die URL-Inhaltsumleitung erstellt haben, können Sie diese einem Active Directory-Benutzer oder einer Active Directory-Gruppe zuweisen.

Voraussetzungen

Machen Sie sich mit den Optionen und Anforderungen der vdmutil-Befehlszeilenschnittstelle vertraut und überprüfen Sie, ob Sie über die Berechtigung zur Ausführung des vdmutil-Befehls verfügen. Siehe [Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz](#).

Verfahren

- Um einem Benutzer eine Einstellung für die URL-Inhaltsumleitung zuzuweisen, führen Sie in der Verbindungsserverinstanz den Befehl vdmutil mit der Option `--addUserURLSetting` aus.

```
vdmutil --addUserURLSetting --urlSettingName Wert --userName Wert
```

Option	Beschreibung
<code>--urlSettingName</code>	Name der Einstellung für die URL-Inhaltsumleitung, die zugewiesen werden soll. Es muss url-filtering sein.
<code>--userName</code>	Name des Active Directory-Benutzers im Format Domäne\Benutzername.

- Um einer Gruppe eine Einstellung für die URL-Inhaltsumleitung zuzuweisen, führen Sie den Befehl vdmutil mit der Option `--addGroupURLSetting` aus.

```
vdmutil --addGroupURLSetting --urlSettingName Wert --groupName Wert
```

Option	Beschreibung
<code>--urlSettingName</code>	Name der Einstellung für die URL-Inhaltsumleitung, die zugewiesen werden soll. Es muss url-filtering sein.
<code>--groupName</code>	Name der Active Directory-Gruppe im Format Domäne\Benutzergruppe.

Beispiel: Zuweisen einer Einstellung für die URL-Inhaltsumleitung

Im nachfolgend dargestellten Beispiel wird eine Einstellung für die URL-Inhaltsumleitung namens `url-filtering` dem Benutzer `mydomain\janedoe` zugewiesen.

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

Im nachfolgend dargestellten Beispiel wird eine Einstellung für die URL-Inhaltsumleitung namens `url-filtering` der Gruppe `mydomain\usergroup` zugewiesen.

```
vdmutil --addGroupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

Nächste Schritte

Überprüfen Sie Ihre Einstellungen für die URL-Inhaltsumleitung. Siehe [Testen einer Einstellung für die URL-Inhaltsumleitung](#).

Installieren von Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung

Um URL-Inhalte von einem Windows-Client zu einem Remote-Desktop oder einer veröffentlichten Anwendung umleiten zu können (Client-zu-Agent-Umleitung), müssen Sie Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung installieren.

Zur Aktivierung der URL-Inhaltsumleitung verwenden Sie das Installationsprogramm von Horizon Client für Windows mit einer Befehlszeilenoption. Statt durch Doppelklicken auf die Installationsdatei starten Sie die Installation durch Ausführung des folgenden Befehls in einem Befehlszeilenfenster:

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Um sicherzustellen, dass die Funktion zur URL-Inhaltsumleitung installiert ist, vergewissern Sie sich, dass die Dateien `vmware-url-protocol-launch-helper.exe` und `vmware-url-filtering-plugin.dll` im Verzeichnis `%PROGRAMFILES%\VMware\VMware Horizon View Client` enthalten sind. Wenn Sie die Funktion zur URL-Inhaltsumleitung mit Internet Explorer verwenden, müssen Sie auch sicherstellen, dass das VMware Horizon View Plug-In zur URL-Filterung als Internet Explorer-Add-on aktiviert ist.

Hinweis Horizon Client 4.4 für Mac unterstützt standardmäßig die Client-zu-Agent-Umleitung. Es sind dazu keine zusätzlichen Installationsschritte erforderlich. In Horizon Client 4.2 und 4.3 für Mac wird die Client-zu-Agent-Umleitung nicht unterstützt.

Testen einer Einstellung für die URL-Inhaltsumleitung

Nach dem Erstellen und Zuweisen einer Einstellung für die URL-Inhaltsumleitung können Sie mit bestimmten Schritten prüfen, ob die Einstellung korrekt funktioniert.

Voraussetzungen

Machen Sie sich mit den Optionen und Anforderungen der `vdmutl`-Befehlszeilenschnittstelle vertraut und überprüfen Sie, ob Sie über die Berechtigung zur Ausführung des `vdmutl`-Befehls verfügen. Siehe [Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz](#).

Verfahren

- 1 Melden Sie sich bei der Verbindungsserver-Instanz an.
- 2 Führen Sie den Befehl `vdmutl` mit der Option `--readURLSetting` aus.

Beispiel:

```
vdmutl --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

Der Befehl zeigt detaillierte Informationen zur Einstellung für die URL-Inhaltsumleitung an. So wird z. B. mit der im Folgenden dargestellten Befehlsausgabe für die Einstellung `url-filtering` angezeigt, dass die HTTP- und HTTPS-URLs mit der Zeichenfolge `google.*` vom Client zum lokalen Anwendungspool `iexplore2012` umgeleitet werden.

```
URL Redirection setting url-filtering
Description                               : null
Enabled                                   : true
Scope of URL Redirection Setting          : LOCAL
URL Scheme And Local Resource handler pairs
  URL Scheme                             : http
  Handler type                           : APPLICATION
  Handler Resource name                   : iexplore2012
  URL Scheme                             : https
  Handler type                           : APPLICATION
  Handler Resource name                   : iexplore2012
AgentPatterns
  https://google.*
  http://google.*
ClientPatterns
  No client patterns configured
```

- 3 Öffnen Sie auf einem Windows-Clientcomputer Horizon Client, stellen Sie eine Verbindung mit der Verbindungsserver-Instanz her, klicken Sie auf die URLs, die dem in der Einstellung konfigurierten URL-Muster entsprechen, und prüfen Sie, ob die URLs wie vorgesehen umgeleitet werden.
- 4 Öffnen Sie auf demselben Windows-Clientcomputer den Registrierungs-Editor (`regedit`) und überprüfen Sie die Registrierungsschlüssel im Pfad `\Computer\HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\URLRedirection\`.

Es muss hier ein Schlüssel für jedes in der Einstellung angegebene Protokoll angezeigt werden. Durch Klicken auf ein Protokoll werden die mit diesem Protokoll verknüpften Regeln eingeblendet. Beispielsweise zeigt `agentRules` die umgeleiteten URLs an und `brokerHostName` die IP-Adresse oder den vollqualifizierten Hostnamen der Verbindungsserver-Instanz, der für die Umleitung der URLs verwendet wird. `remoteItem` zeigt den Anzeigenamen des Desktop- oder Anwendungspools an, der die umgeleiteten URLs verarbeitet.

Verwalten der Einstellungen für die URL-Inhaltsumleitung

Sie können mithilfe der `vdmutl`-Befehle Ihre Einstellungen für die URL-Inhaltsumleitung verwalten.

Sie müssen bei allen Befehlen die Optionen `--authAs`, `--authDomain` und `--authPassword` angeben. Weitere Informationen finden Sie unter [Verwenden des vdmutil-Befehlszeilen-Dienstprogramms auf einer Verbindungsserverinstanz](#).

Anzeigen von Einstellungen

Führen Sie den Befehl `vdmutl` mit der Option `--listURLSetting` aus, um die Namen aller konfigurierten Einstellungen für die URL-Inhaltsumleitung darzustellen.

```
vdmutl --listURLSetting
```

Führen Sie den Befehl `vdmutil` mit der Option `--readURLSetting` aus, um detaillierte Informationen über eine bestimmte Einstellungen für die URL-Inhaltsumleitung anzuzeigen.

```
vdmutil --readURLSetting --urlSettingName Wert
```

Löschen einer Einstellung

Führen Sie den Befehl `vdmutil` mit der Option `--deleteURLSetting` zum Löschen einer Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --deleteURLSetting --urlSettingName Wert
```

Deaktivieren und Aktivieren einer Einstellung

Führen Sie den Befehl `vdmutil` mit der Option `--disableURLSetting` zum Deaktivieren einer Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --disableURLSetting --urlSettingName Wert
```

Führen Sie den Befehl `vdmutil` mit der Option `--enableURLSetting` zum Aktivieren einer deaktivierten Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --enableURLSetting --urlSettingName Wert
```

Entfernen eines Benutzers oder einer Gruppe aus einer Einstellung

Führen Sie den Befehl `vdmutil` mit der Option `--removeUserURLSetting` zum Entfernen eines Benutzers aus einer Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --removeUserURLSetting --urlSettingName Wert --userName Wert
```

Führen Sie den Befehl `vdmutil` mit der Option `--removeGroupURLSetting` zum Entfernen einer Gruppe aus einer Einstellung für die URL-Inhaltsumleitung aus.

```
vdmutil --removeGroupURLSetting --urlSettingName Wert --userGroup Wert
```

Für die Angabe eines Benutzer- oder Gruppennamens verwenden Sie das Format Domäne \Benutzername oder Domäne \Gruppenname.

Verwenden von Gruppenrichtlinieneinstellungen für die Konfiguration der Client-zu-Agent-Umleitung

Die ADMX-Vorlagendatei für die URL-Inhaltsumleitung (`urlRedirection.admx`) enthält Gruppenrichtlinieneinstellungen, mit denen Sie Regeln für die Umleitung von URLs vom Client zu einem Remote-Desktop oder zu einer veröffentlichten Anwendung (Client-zu-Agent-Umleitung) erstellen können.

Wichtig Für die Konfiguration der Client-zu-Agent-Umleitung wird die Verwendung des `vdmutil`-Befehlszeilendienstprogramms empfohlen. Da macOS keine Gruppenrichtlinien unterstützt, können Sie, wenn Sie über Mac-Clients verfügen, nicht die Gruppenrichtlinien zum Konfigurieren der Client-zu-Agent-Umleitung verwenden.

Um eine Regel für die Client-zu-Agent-Umleitung zu erstellen, legen Sie mit der Option **Remote-Element** den Anzeigenamen des Desktop- oder Anwendungspools und mit der Option **Agent-Regeln** die URLs, die zum Remote-Desktop oder zur veröffentlichten Anwendung umgeleitet werden sollen, fest. Sie müssen mit der Option **Broker-Hostname** auch die IP-Adresse oder den vollqualifizierten Domännennamen des Verbindungsserver-Hosts für die Umleitung der URLs auf einen Remote-Desktop oder eine veröffentlichte Anwendung angeben.

Beispielsweise können Sie aus Sicherheitsgründen festlegen, dass alle HTTP-URLs, die auf das Netzwerk des Unternehmens verweisen, in einem Remote-Desktop oder in einer veröffentlichten Anwendung geöffnet werden. In diesem Fall müssen Sie für die Option **Agent-Regeln** einen Wert wie z. B. **festlegen.*.mycompany.com** angeben.

Installationsanleitungen für die Vorlagendatei der URL-Inhaltsumleitung, Beschreibungen für die Gruppenrichtlinieneinstellungen und die Syntax der **Agent-Regeln**-Option finden Sie unter [Konfigurieren der Agent-zu-Client-Umleitung](#).

Einschränkungen der URL-Inhaltsumleitung

Die Funktion der URL-Inhaltsumleitung kann zu bestimmten unerwarteten Ergebnissen führen.

- Wenn die URL eine landesspezifische Seite auf der Basis des Gebietsschemas öffnet, bestimmt die Quelle des Links, welche lokale Seite geöffnet wird. Wenn sich beispielsweise der Remote-Desktop (Agentquelle) in einem Datacenter in Japan und der Computer des Benutzers sich in den USA befindet, wird auf dem US-Client die japanische Seite geöffnet, wenn die URL vom Agent- zum Clientcomputer umgeleitet wird.
- Wenn Benutzer Webseiten-Favoriten erstellen, werden die Favoriten auf dem Ziel der Umleitung angelegt. Wenn z. B. ein Benutzer einen Link auf dem Clientcomputer anklickt, die URL dann zu einem Remote-Desktop (Agent) umgeleitet wird und der Benutzer einen Favoriten für diese Seite erstellt, wird der Favorit auf dem Agent erstellt. Öffnet der Benutzer das nächste Mal den Browser auf dem Clientcomputer, geht er eventuell davon aus, dass er den Favoriten auf dem Clientcomputer vorfindet. Der Favorit wurde jedoch auf dem Remote-Desktop (Agentquelle) gespeichert.
- Von Benutzern heruntergeladene Dateien befinden sich auf dem Computer, auf dem mit dem Browser die URL geöffnet wurde, wenn etwa ein Benutzer auf dem Clientcomputer auf einen Link

klickt und die URL zu einem Remote-Desktop umgeleitet wird. Wurde über diesen Link eine Datei heruntergeladen oder handelt es sich um einen Link zu einer Webseite, auf der der Benutzer eine Datei herunterlädt, wird die Datei auf den Remote-Desktop anstatt auf dem Clientcomputer heruntergeladen.

- Wenn Sie Horizon Agent und Horizon Client auf demselben Computer installieren, können Sie die URL-Inhaltsumleitung nur in Horizon Agent oder in Horizon Client aktivieren, aber nicht in beiden Modulen gleichzeitig. Auf diesem Computer haben Sie die Möglichkeit, entweder eine Client-zu-Agent-Umleitung oder eine Agent-zu-Client-Umleitung einzurichten. Beides ist nicht möglich.

Nicht unterstützte Funktionen der URL-Inhaltsumleitung

Die Funktion der URL-Inhaltsumleitung ist unter bestimmten Umständen nicht wirksam.

Verkürzte URLs

Verkürzte URLs wie z. B. <https://goo.gl/abc> können auf der Basis von Filterregeln umgeleitet werden. Der Filtervorgang wertet aber nicht die ursprüngliche ungekürzte URL aus.

Wenn Sie beispielsweise mit einer Filterregel URLs mit `acme.com`, eine ursprüngliche URL wie z. B. <http://www.acme.com/some-really-long-path> und eine verkürzte URL der ursprünglichen URL wie etwa <https://goo.gl/xyz> umleiten, wird die ursprüngliche URL, aber nicht die verkürzte URL umgeleitet.

Sie können diese Einschränkung durch das Erstellen von Regeln zum Blockieren oder Umleiten von URLs von Websites umgehen, die am häufigsten für das Verkürzen von URLs verwendet werden.

Eingebettete HTML-Seiten

Für eingebettete HTML-Seiten wird die URL-Umleitung umgangen, wenn z. B. ein Benutzer zu einer URL wechselt, die keiner Regel für die URL-Umleitung entspricht. Wenn also eine Seite eine eingebettete HTML-Seite (iFrame oder Inline-Frame) mit einer URL enthält, für die eine Umleitungsregel festgelegt wurde, ist diese URL-Umleitungsregel nicht wirksam. Die Regel ist nur für die Top-Level-URL wirksam.

Deaktivierte Internet Explorer-Plug-Ins

Die URL-Inhaltsumleitung kann nicht verwendet werden, wenn die Internet Explorer-Plug-Ins deaktiviert sind, etwa, wenn ein Benutzer zum InPrivate-Browsen in Internet Explorer wechselt. In diesem Modus werden die Webseiten und die von Webseiten heruntergeladenen Dateien nicht im Browser- und Download-Verlauf des jeweiligen Computers protokolliert. Der Grund dafür ist, dass die Funktion der URL-Umleitung die Aktivierung bestimmter Internet Explorer-Plug-Ins erfordert, die vom InPrivate-Browsen deaktiviert werden.

Sie können diese Einschränkung mithilfe einer GPO-Einstellung umgehen, die es Benutzer unmöglich macht, Plug-Ins zu deaktivieren. Diese Einstellungen enthalten die Einträge: „Aktivierung bzw. Deaktivierung von Add-Ons für Benutzer nicht zulassen“ und „Neu installierte Add-Ons automatisch aktivieren“. Diese Einstellungen sind im Editor der Gruppenrichtlinienverwaltung unter **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer** enthalten.

Um diese Einschränkung speziell für Internet Explorer zu umgehen, deaktivieren Sie den InPrivate-Modus mit der GPO-Einstellung. Diese Einstellung lautet „InPrivate-Browsen deaktivieren“. Diese Einstellungen finden Sie im Editor der Gruppenrichtlinienverwaltung unter **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Datenschutz**.

Diese Problemumgehungen stellen empfohlene Best Practices dar. Damit lassen sich Probleme mit der Umleitung über das InPrivate-Browsen hinaus vermeiden.

Windows 10 Universal App ist der Standardhandler für ein Protokoll

Die URL-Umleitung wird nicht durchgeführt, wenn eine universelle Windows 10-App den Standardhandler für ein in einem Link angegebenes Protokoll darstellt. Universelle Anwendungen, die auf der universellen Windows-Plattform zum Herunterladen auf PCs, Tablet-Computern und Smartphones zur Verfügung stehen, sind beispielsweise der Microsoft Edge-Browser, Mail, Maps, Photos oder Groove Music.

Wenn Sie einen Link anklicken, für den eine dieser Anwendungen als Standardhandler fungiert, wird die URL nicht umgeleitet. Wenn beispielsweise ein Benutzer einen E-Mail-Link in einer Anwendung anklickt und die universelle Mail-App als standardmäßige E-Mail-Anwendung verwendet wird, wird die im Link angegebene URL nicht umgeleitet.

Sie können diese Einschränkung durch Festlegung einer anderen Anwendung als Standardhandler für das Protokoll der URLs, die umgeleitet werden sollen, umgehen. Wenn beispielsweise Edge der Standardbrowser ist, verwenden Sie dafür Internet Explorer.

Installieren und Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome unter Windows

Um den Chrome-Browser mit der Funktion der URL-Inhaltsumleitung auf einem Windows-Client- oder einem Windows-Agentcomputer zu verwenden, müssen Sie die Erweiterung „VMware Horizon URL Content Redirection Helper“ für Chrome installieren und aktivieren.

Sie können die Erweiterung „VMware Horizon URL Content Redirection Helper“ durch Aktivierung einer Gruppenrichtlinieneinstellung für die URL-Inhaltsumleitung installieren und aktivieren.

Diese Schritte beschreiben, wie Sie die Gruppenrichtlinieneinstellung für die URL-Inhaltsumleitung auf GPOs auf Ihrem Active Directory-Server anwenden. Auf Windows-Clientcomputern muss das GPO mit der Organisationseinheit verknüpft werden, in der sich Ihre Windows-Clientcomputer befinden. Für Remote-Desktops und -anwendungen muss das GPO mit der Organisationseinheit verknüpft werden, in der sich Ihre virtuellen Desktops und RDS-Hosts befinden.

Wenn Sie die Erweiterung „VMware Horizon URL Content Redirection Helper“ nicht mithilfe einer Gruppenrichtlinie installieren und aktivieren, müssen Sie diese manuell aus dem Chrome Web Store installieren.

Voraussetzungen

- Auf einem Windows-Clientcomputer installieren Sie Horizon Client 4.7 oder höher und aktivieren Sie die Funktion der URL-Inhaltsumleitung. Siehe [Installieren von Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung](#).
- Auf einem Windows-Agentcomputer installieren Sie Horizon Agent 7.4 oder höher und aktivieren die Funktion der URL-Inhaltsumleitung. Siehe [Installieren von Horizon Agent mit der Funktion der URL-Inhaltsumleitung](#).
- Installieren Sie den Chrome-Browser. Eine Liste der unterstützten Versionen finden Sie unter [Anforderungen für die URL-Inhaltsumleitung](#).
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Fügen Sie Ihrem Active Directory-Server die ADMX-Vorlagendatei für die URL-Inhaltsumleitung hinzu. Siehe [Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO](#).

Verfahren

- 1 Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf dem Active Directory-Server und wechseln Sie zum Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > VMware Horizon-URL-Umleitung**.
- 2 Öffnen Sie die Einstellung **Installieren Sie die Chrome-Erweiterung, die für die URL-Inhaltsumleitungsfunktion erforderlich ist**, wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.
- 3 Starten Sie Chrome auf dem Windows-Computer.

Die Erweiterung „VMware Horizon URL Content Redirection Helper“ wird automatisch im Hintergrund installiert.
- 4 Um sicherzustellen, dass die Chrome-Erweiterung installiert wurde, geben Sie im Chrome-Browser **chrome://extensions** ein.

In der Liste der Erweiterungen wird **VMware Horizon URL Content Redirection Helper** angezeigt und das Kontrollkästchen **Aktiviert** ausgewählt.

Nächste Schritte

Bei der ersten Umleitung einer URL aus dem Chrome-Browser des Clients wird der Benutzer aufgefordert, die URL in Horizon Client zu öffnen. Für die Durchführung der URL-Umleitung muss der Benutzer dann auf **Open URL:VMware Hori...lient Protocol** klicken. Wenn der Benutzer das Kontrollkästchen **Meine Wahl für URL:VMware Hori...lient Protocol-Links merken** aktiviert (empfohlen), wird diese Eingabeaufforderung nicht mehr angezeigt.

Aktivieren der Erweiterung „URL Content Redirection Helper“ für Chrome auf einem Mac

Um den Chrome-Browser mit der Funktion der URL-Inhaltsumleitung auf einem Mac-Client zu verwenden, müssen Sie die Erweiterung „VMware Horizon URL Content Redirection Helper“ für Chrome aktivieren.

Voraussetzungen

- Installieren Sie den Chrome-Browser auf dem Mac-Client. Eine Liste der unterstützten Versionen finden Sie unter [Anforderungen für die URL-Inhaltsumleitung](#).
- Installieren Sie Horizon Client 4.7 oder höher auf dem Mac. Informationen hierzu finden Sie im Dokument *VMware Horizon Client für Mac Installations- und Einrichtungshandbuch*.
- Konfigurieren Sie die Einstellungen für die URL-Inhaltsumleitung auf der Verbindungsserverinstanz. Siehe [Konfigurieren der Client-zu-Agent-Umleitung](#).

Verfahren

- 1 Starten Sie Horizon Client auf dem Mac und stellen Sie eine Verbindung mit einer Verbindungsserver-Instanz her, auf der Einstellungen für die URL-Inhaltsumleitung konfiguriert wurden.

Die Erweiterung „VMware Horizon URL Content Redirection Helper“ wird automatisch im Chrome-Browser auf dem Mac-Client installiert.

- 2 Starten Sie den Chrome-Browser auf dem Mac erneut.
- 3 Wenn Sie aufgefordert werden, die Erweiterung „VMware Horizon URL Content Redirection Helper“ zu aktivieren, klicken Sie auf **Erweiterung aktivieren**.

Sie müssen die Erweiterung für die Verwendung der URL-Inhaltsumleitung im Chrome-Browser aktivieren.

Hinweis Wenn Sie die Erweiterung entfernen, können Sie diese später wieder manuell aus dem Chrome Web Store installieren.

- 4 Um sicherzustellen, dass die Chrome-Erweiterung installiert wurde, geben Sie im Chrome-Browser **chrome://extensions** ein.

In der Liste der Erweiterungen wird **VMware Horizon URL Content Redirection Helper** angezeigt und das Kontrollkästchen **Aktiviert** ausgewählt.

Nächste Schritte

Bei der ersten Umleitung einer URL aus dem Chrome-Browser des Mac-Clients wird der Benutzer aufgefordert, die URL in Horizon Client zu öffnen. Für die Durchführung der URL-Umleitung muss der Benutzer dann auf **VMware Horizon Client öffnen** klicken. Wenn der Benutzer das Kontrollkästchen **Meine Wahl für VMware Horizon Client-Links merken** aktiviert (empfohlen), wird diese Eingabeaufforderung nicht mehr angezeigt.

Verwenden von USB-Geräten mit Remote-Desktops und -anwendungen

4

Administratoren können virtuelle Desktops so konfigurieren, dass USB-Geräte wie Flash-Laufwerke, Kameras, VoIP-Geräte und Drucker genutzt werden können. Diese Funktion wird als USB-Umleitung bezeichnet. Ein virtueller Desktop unterstützt maximal 255 USB-Geräte.

Sie können auch bestimmte lokal verbundene USB-Geräte umleiten, um sie an veröffentlichten Desktops und Anwendungen zu verwenden. Informationen zu den spezifischen unterstützten Gerätetypen finden Sie unter [Einschränkungen in Bezug auf USB-Gerätetypen](#).

Bei Verwendung dieser Funktion in Desktop-Pools, die auf Maschinen für Einzelbenutzer bereitgestellt werden, stehen die meisten USB-Geräte, die an das lokale Client-System angeschlossen sind, auf dem Remote-Desktop zur Verfügung. Es ist sogar möglich, von einem Remote-Desktop aus eine Verbindung mit einem iPad herzustellen und diesen zu verwalten. Sie können zum Beispiel Ihr iPad mit dem auf Ihrem Remote-Desktop installierten iTunes-Programm synchronisieren. Auf einigen Clientgeräten, beispielsweise auf Windows- und Mac-Computern, werden die USB-Geräte in einem Menü in Horizon Client aufgelistet. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

In den meisten Fällen ist es nicht möglich, ein USB-Gerät gleichzeitig auf einem Clientsystem und auf einem Remote-Desktop zu verwenden. Nur wenige Arten von USB-Geräten können von einem Remote-Desktop und dem lokalen Computer gemeinsam verwendet werden. Zu diesen Geräten zählen Smartcard-Leser und Eingabegeräte, wie beispielsweise Tastaturen und Zeigegeräte.

Administratoren können angeben, mit welchen Arten von USB-Geräten die Endbenutzer eine Verbindung herstellen dürfen. Für aus mehreren Gerätetypen zusammengesetzte Gerätegruppen, die etwa aus einem Videoeingabegerät und einem Speichergerät bestehen, können Administratoren auf einigen Clientsystemen die Gerätegruppe so aufgliedern, dass ein Gerät (wie etwa das Videoeingabegerät) zulässig ist, das andere Gerät (etwa das Speichergerät) jedoch nicht.

Die USB-Umleitung ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungs-Matrix im Horizon Client-Dokument zur Installation und Einrichtung für den spezifischen Typ von Clientgerät.

Wichtig Beim Bereitstellen der USB-Umleitungsfunktion können Sie Schritte zum Schutz Ihres Unternehmens vor den Sicherheitslücken im Zusammenhang mit USB-Geräten ergreifen. Siehe [Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung](#).

Dieses Kapitel enthält die folgenden Themen:

- [Einschränkungen in Bezug auf USB-Gerätetypen](#)
- [Empfehlungen zur USB-Umleitung](#)
- [Überblick über das Einrichten der USB-Umleitung](#)
- [Konfigurieren der Fingerabdruckscannerumleitung](#)
- [Konfigurieren der Kartenlesegerät-Umleitung](#)
- [Netzwerkdatenverkehr und USB-Umleitung](#)
- [Automatische Verbindungen mit USB-Geräten](#)
- [Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung](#)
- [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#)
- [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#)
- [Fehlerbehebung bei Problemen mit der USB-Umleitung](#)

Einschränkungen in Bezug auf USB-Gerätetypen

Obwohl Horizon 7 nicht verhindert, dass Geräte die USB-Umleitungsfunktion verwenden, funktionieren einige Geräte aufgrund von Faktoren wie Netzwerklatenz und Bandbreite besser als andere. Standardmäßig werden einige Geräte durch Filtern oder Sperren automatisch von der Verwendung ausgeschlossen.

Einschränkungen bei USB 3.0-Geräten

Ab Horizon 6 Version 6.0.1, zusammen mit Horizon Client 3.1 und höher, können Sie USB 3.0-Geräte an die USB 3.0-Ports auf dem Clientcomputer anschließen. Für USB 3.0-Geräte wird nur ein Stream unterstützt. Da die Unterstützung mehrerer Streams nicht implementiert ist, wurde die Leistung von USB-Geräten nicht verbessert. Manche USB 3.0-Geräte, die für ihren ordnungsgemäßen Gebrauch einen konstant hohen Durchsatz erfordern, funktionieren aufgrund der Netzwerklatenz möglicherweise nicht in einer Remote-Sitzung.

Einschränkungen für die USB-Umleitung bei virtuellen Desktops

Die folgenden USB-Gerätetypen eignen sich möglicherweise nicht für die USB-Umleitung an einen Remote-Desktop, der auf einer Maschine für Einzelbenutzer bereitgestellt wird:

- Aufgrund der Bandbreitenanforderungen von Webcams, die in der Regel mehr als 60 MBit/s Bandbreite verbrauchen, werden Webcams nicht über die USB-Umleitung unterstützt. Für Webcams können Sie die Echtzeit-Audio/Video-Funktion verwenden.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz. Wenn Sie die Echtzeit-Audio/Video-Funktion verwenden, arbeiten Audioeingabe- und Audioausgabegeräte ordnungsgemäß, und die Verwendung der USB-Umleitung ist für diese Geräte nicht erforderlich.
- Das CD-/DVD-Brennen über USB wird nicht unterstützt.

- Die Leistung einiger USB-Geräte variiert, insbesondere im WAN, abhängig von der Netzwerklatenz und Zuverlässigkeit sehr stark. Beispiel: Eine einzelne USB-Speichergerät-Leseanforderung benötigt drei Round-Trips zwischen dem Client und dem Remote-Desktop. Für Lesen einer vollständigen Datei sind möglicherweise mehrere USB-Lesevorgänge notwendig. Je größer die Latenz, desto mehr Zeit nimmt der Round-Trip in Anspruch.

Die Dateistruktur kann abhängig vom Format sehr groß sein. Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden. Das Formatieren eines USB-Geräts als NTFS anstatt FAT unterstützt das Verringern der ursprünglichen Verbindungszeit. Ein unzuverlässiger Netzwerk-Link führt zu Wiederholungen und die Leistung wird weiter reduziert.

Ebenso funktionieren USB-CD-/DVD-Lesegeräte und -Scanner nicht gut über ein latentes Netzwerk wie z. B. ein WAN.

- Das Umleiten von USB-Scannern hängt vom Zustand des Netzwerks ab und es kann länger als normal dauern, bis die Scans fertiggestellt sind.

Einschränkungen für die USB-Umleitung bei veröffentlichten Desktops und Anwendungen

Mit View Agent 6.2.x und höher oder mit Horizon Agent 7.0 und höher können Sie lokal angeschlossene USB-Thumb-Flashlaufwerke und Festplatten für die Verwendung in veröffentlichten Desktops und Anwendungen umleiten. Ab Horizon Agent 7.0.2 unterstützen veröffentlichte Desktops und Anwendungen auch weitere generische USB-Geräte wie das TOPAZ-Signaturpad, den Olympus-Diktatfußschalter und das Wacom-Signaturpad. Andere Arten von USB-Geräten, einschließlich Sicherheitsspeicherlaufwerke und USB-CD-ROM-Laufwerke, werden in veröffentlichten Desktops und Anwendungen nicht unterstützt.

Empfehlungen zur USB-Umleitung

Sie können empfohlene Lösungen für die USB-Umleitung für einige USB-Gerätetypen verwenden.

Anstatt die USB-Umleitung zu verwenden, nutzen Sie diese Umleitungsfunktionen, die eine bessere Leistung und Benutzerfreundlichkeit bieten:

- Verwenden Sie für Scanner die Scanner-Umleitung. Siehe [Konfigurieren der Scannerumleitung](#).
- Verwenden Sie für Drucker die Druckerumleitung. Siehe [Konfigurieren der Umleitung „VMware Integrated Printing“](#).
- Verwenden Sie für Smartcard-Leser die Smartcard-Umleitung. Weitere Informationen finden Sie im Dokument *Horizon 7-Verwaltung*.
- Verwenden Sie für Geräte mit seriellen Ports die Umleitung serieller Ports. Siehe [Konfigurieren der Umleitung serieller Ports](#).
- Verwenden Sie die Clientlaufwerksumleitung für die Dateifreigabe anstelle der USB-Umleitung für USB-Festplatten und massive Speichergeräte. Siehe [Verwalten des Zugriffs auf die Clientlaufwerksumleitung](#).

Überblick über das Einrichten der USB-Umleitung

Um Ihre Bereitstellung so einzurichten, dass Endbenutzer Wechselmedien wie USB-Flash-Laufwerke, Kameras und Headsets anschließen können, müssen Sie bestimmte Komponenten sowohl auf dem Remote-Desktop bzw. RDS-Host als auch auf dem Client-Gerät installieren, und Sie müssen überprüfen, ob die globale Einstellung für USB-Geräte in Horizon Administrator aktiviert ist.

Diese Prüfliste beinhaltet sowohl erforderliche als auch optionale Aufgaben zur Einrichtung einer USB-Umleitung in Ihrem Unternehmen.

Die USB-Umleitung ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungs-Matrix im Dokument zur Installation und Einrichtung für den spezifischen Typ von Clientgerät.

Wichtig Beim Bereitstellen der USB-Umleitungsfunktion können Sie Schritte zum Schutz Ihres Unternehmens vor den Sicherheitslücken im Zusammenhang mit USB-Geräten ergreifen. Beispielsweise können Sie Gruppenrichtlinieneinstellungen verwenden, um die USB-Umleitung für einige Remote-Desktops und Benutzer zu deaktivieren, oder um einzuschränken, welche Typen von USB-Geräten umgeleitet werden können. Siehe [Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung](#).

- 1 Wenn Sie den Horizon Agent-Installationsassistenten auf der Remote-Desktop-Quelle oder dem RDS-Host ausführen, müssen Sie die USB-Umleitungs-Komponente mitinstallieren.

Diese Komponente ist standardmäßig nicht ausgewählt. Um die Komponente zu installieren, müssen Sie sie auswählen.

- 2 Wenn Sie den VMware Horizon Client-Installationsassistenten auf dem Clientsystem ausführen, müssen Sie die USB-Umleitungs-Komponente hinzufügen.

Diese Komponente ist standardmäßig enthalten.

- 3 Überprüfen Sie, ob der Zugriff auf USB-Geräte von einem Remote-Desktop oder einer Remoteanwendung aus in Horizon Administrator aktiviert ist.

Wechseln Sie in Horizon Administrator zu **Richtlinien > Globale Richtlinien** und prüfen Sie, ob **USB-Zugriff** auf **Zulassen** festgelegt ist.

- 4 (Optional) Konfigurieren Sie Horizon Agent-Gruppenrichtlinien, um anzugeben, welche Typen von Geräten umgeleitet werden können.

Siehe [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#).

- 5 (Optional) Konfigurieren Sie ähnliche Einstellungen auf dem Clientgerät.

Sie können auch konfigurieren, ob Geräte automatisch angeschlossen werden sollen, wenn Horizon Client eine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herstellt oder wenn der Endbenutzer ein USB-Gerät einsteckt. Die Methode zur Konfigurierung von USB-Einstellungen auf dem Clientgerät hängt vom Typ des Geräts ab. Beispielsweise können Sie für Windows-Clients Gruppenrichtlinien konfigurieren. Für Mac-Clients verwenden Sie einen Befehlszeilenbefehl. Weitere Informationen finden Sie im Installations- und Einrichtungsdokument für den jeweiligen Typ des Clientgeräts.

- 6 Endbenutzer sollen eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung herstellen und ihre USB-Geräte in das lokale Client-System einstecken.

Wenn der Treiber für das USB-Gerät nicht bereits auf dem Remote-Desktop oder RDS-Host installiert ist, erkennt das Gastbetriebssystem das USB-Gerät und sucht genauso wie bei einem physischen Windows-Computer nach einem passenden Treiber.

Konfigurieren der Fingerabdruckscannerumleitung

Sie können biometrische Geräte, insbesondere Fingerabdruck-Scanner, die an den USB-Port eines Windows-Clientsystems angeschlossen sind, an virtuelle Desktops umleiten.

Um diese Fingerabdruck-Scanner umzuleiten, benötigen Sie mindestens eine Netzwerkbandbreite von 200 MBit/s auf dem Remote-Agent-Desktop.

Folgende Fingerabdruckscannergeräte werden unterstützt:

Tabelle 4-1. Unterstützte Fingerabdruck-Scanner

Gerät	Clientbetriebssystem	Windows-Betriebssystemserver	Protokolle
U.are.U 5160-Fingerabdruckleser	Windows 10 1809 64 Bit	Windows 10 1809 64 Bit	PCoIP, Blast
	Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	Windows 10 1903 64 Bit Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	
U.are.U 5300-Fingerabdruckleser	Windows 10 1809 64 Bit	Windows 10 1809 64 Bit	PCoIP, Blast
	Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	Windows 10 1903 64 Bit Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	

Konfigurieren der Kartenlesegerät-Umleitung

Sie können Kartenleser, die an einen USB-Port über den virtuellen PCoIP-Kanal auf einem Windows-Clientsystem angeschlossen sind, an virtuelle Desktops umleiten.

Diese Kartenleser werden unterstützt:

Tabelle 4-2. Unterstützte Kartenleser

Gerät	Clientbetriebssystem	Windows-Betriebssystemserver	Protokoll
Sony FeliCa RC-S320	Windows 10 1809 64 Bit	Windows 10 1809 64 Bit	PCoIP
	Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	Windows 10 1903 64 Bit Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	
Sony PaSoRi RC-S380	Windows 10 1809 64 Bit	Windows 10 1809 64 Bit	PCoIP
	Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	Windows 10 1903 64 Bit Windows 7 SP 1 Enterprise (32 Bit, 64 Bit)	

Virtuellen Kanal für USB über PCoIP konfigurieren

Um den virtuellen Kanal für USB über PCoIP mit UDP-Port 4172 zu konfigurieren, ändern Sie die Registrierung in Horizon Agent:

- 1 Legen Sie die Registrierung HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\UsbVirtualChannelEnabled (REG_SZ) auf „true“ fest.
- 2 Legen Sie die Registrierung HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection\sideChannelType (REG_SZ) auf „PCoIP“ fest.
- 3 Starten Sie die Horizon Agent-VM neu.

Um zu überprüfen, ob die Konfiguration übernommen wurde:

- 1 Verbinden Sie den Horizon Agent-Desktop mit dem PCoIP-Protokoll.
- 2 Überprüfen Sie das Horizon Client-Protokoll von „C:\Benutzer\<Benutzername>\AppData\Local\Temp\vmware-<Benutzername>\vmware-UsbRedirectionClient-xxxx.log“. Wenn die Konfiguration aktiv ist, finden Sie den „RPCManager::OnChannelDataObjectStateChanged(): Requesting virtual side channel“ in dieser Datei.

Netzwerkdatenverkehr und USB-Umleitung

Der Netzwerkdatenverkehr zwischen einem Client-System und einem Remote-Desktop oder einer Remoteanwendung kann über verschiedene Routen erfolgen, abhängig davon, ob das Client-System Teil des Unternehmensnetzwerks ist und für welche Sicherheitseinstellungen sich der Administrator entschieden hat.

Die USB-Umleitung erfolgt unabhängig vom Anzeigeprotokoll und der USB-Datenverkehr verwendet gewöhnlich den TCP-Port 32111.

Wenn das Clientsystem Teil des Unternehmensnetzwerks ist, sodass eine direkte Verbindung zwischen dem Client und dem Remote-Desktop oder der Anwendung hergestellt werden kann, verwendet der USB-Datenverkehr den TCP-Port 32111.

Wenn das Clientsystem nicht Teil des Unternehmensnetzwerks ist, kann der Client eine Verbindung über eine Unified Access Gateway-Appliance oder einen Sicherheitsserver in der DMZ herstellen. Unified Access Gateway-Appliances und Sicherheitsserver in der DMZ kommunizieren mit Verbindungsserver-Instanzen innerhalb der Unternehmens-Firewall und bieten eine weitere Sicherheitsebene, indem die Verbindungsserver-Instanzen vor dem öffentlichen Internet abgeschirmt werden.

Eine Unified Access Gateway-Appliance (die bevorzugte Methode) erfordert keine zusätzlichen Ports, die innerhalb der Firewall für den USB-Datenverkehr geöffnet werden müssen. Bei einem Sicherheitsserver muss der TCP-Port 32111 auf der Firewall für den USB-Datenverkehr geöffnet werden. Eine Liste der vollständigen Anforderungen an den Sicherheitsserver-Port sind dem Abschnitt „Firewall-Regeln für DMZ-basierte Sicherheitsserver“ im Dokument *Planung der Horizon 7-Architektur* zu entnehmen.

Sie können die Funktion „USB über Sitzungserweiterungs-SDK“ konfigurieren, um ein Öffnen des TCP-Ports 32111 zu vermeiden. Siehe [Aktivieren der Funktion „USB über Sitzungserweiterungs-SDK“](#).

Aktivieren der Funktion „USB über Sitzungserweiterungs-SDK“

Mit der Funktion „USB über Sitzungserweiterungs-SDK“ müssen Sie nicht mehr den TCP-Port 32111 für den USB-Datenverkehr öffnen. Diese Funktion wird sowohl für virtuelle Desktops als auch für veröffentlichte Desktops auf RDS-Hosts unterstützt.

Um die Funktion „USB über Sitzungserweiterungs-SDK“ zu aktivieren, öffnen Sie den Windows-Registrierungseditor (`regedit.exe`) auf dem Remote-Desktop, navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration` und setzen Sie den Schlüssel `UsbVirtualChannelEnabled` auf `true`.

Wenn diese Funktion aktiviert ist, verwendet der USB-Datenverkehr entweder die TCP-Verbindung, die das Anzeigeprotokoll nutzt, oder eine dedizierte TCP-Verbindung. Die vom USB-Datenverkehr verwendete Verbindung hängt von Ihrer Konfiguration ab.

Mit dem VMware Blast-Anzeigeprotokoll kann der USB-Datenverkehr zum Beispiel über den VVC (VMware Virtual Channel) oder den TCP-seitigen Kanal übertragen werden. Mit dem PCoIP-Anzeigeprotokoll verwendet der USB-Datenverkehr nur den TCP-seitigen Kanal.

Standardmäßig verwendet der TCP-seitige Kanal den TCP-Port 9427. Der VVC-seitige Kanal verwendet denselben Port wie das VMware Blast-Anzeigeprotokoll.

USB-Indikatoren, die mithilfe von PerfMon auf Windows-Agenten angezeigt werden, sind gültig, wenn der USB-Datenverkehr für die Verwendung von VVC konfiguriert ist.

Automatische Verbindungen mit USB-Geräten

Auf einigen Clientsystemen können Administratoren oder Endbenutzer oder beide automatische Verbindungen von USB-Geräten zu einem Remote-Desktop konfigurieren. Automatische Verbindungen können entweder hergestellt werden, sobald ein Benutzer ein USB-Gerät an das Client-System anschließt oder sobald der Client eine Verbindung zum Remote-Desktop herstellt.

Auf Windows-Clients gelten ab Horizon Client 4.7 die USB-Funktionen zum automatischen Herstellen einer Verbindung, einschließlich URI-Abfragen, Befehlszeilenoptionen und Gruppenrichtlinieneinstellungen nicht nur für Remote-Desktops, sondern auch für veröffentlichte Anwendungen.

Einige Geräte wie beispielsweise Smartphones und Tablets erfordern automatische Verbindungen, da diese Geräte während eines Upgrades neu gestartet und somit vom System getrennt werden. Wenn diese Geräte nicht auf automatische Verbindungswiederherstellung eingerichtet werden, stellen sie stattdessen während eines Upgrades und nach dem Neustart der Geräte eine Verbindung zum lokalen Clientsystem her.

Die Konfigurationseigenschaften für automatische USB-Verbindungen, die Administratoren auf dem Client einrichten oder die von Endbenutzern mithilfe eines Horizon Client Menüelements festgelegt werden, gelten für alle USB-Geräte, es sei denn, die Geräte sind für den Ausschluss von der USB-Umleitung konfiguriert. Einige Client-Versionen, Webcams und Mikrofone beispielsweise sind standardmäßig von der USB-Umleitung ausgenommen, da diese Geräte besser mit der Echtzeit-Audio/Video-Funktion funktionieren. Es kommt manchmal vor, dass ein USB-Gerät nicht standardmäßig von der

USB-Umleitung ausgenommen ist, aber ein Administrator für dieses Gerät dennoch explizit den Ausschluss von der USB-Umleitung vornehmen muss. Die folgenden USB-Gerätetypen eignen sich nicht für die USB-Umleitung; für sie darf keine automatische Verbindung zu einem Remote-Desktop oder einer Anwendung hergestellt werden:

- **USB-Ethernet-Geräte.** Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr Client-System möglicherweise die Verbindung zum Netzwerk, wenn es sich bei diesem Gerät um das einzige Ethernet-Gerät handelt.
- **Touchscreen-Geräte.** Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der Remote-Desktop oder die Anwendung Eingaben vom Touchscreen und nicht von der Tastatur.

Wenn Sie den Remote-Desktop oder die Anwendung zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte wie beispielsweise Touchscreen- und Netzwerkgeräte auszuschließen. Weitere Informationen finden Sie unter [Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte](#).

Bei Windows-Clients gibt es eine Alternative: Anstatt Einstellungen zu verwenden, die eine automatische Verbindung zu allen Geräten herstellen, wovon einige Geräte ausgenommen sind, können Sie eine Konfigurationsdatei auf dem Client bearbeiten, die Horizon Client für das Wiederherstellen einer Verbindung nur von einem oder mehreren bestimmten Geräten konfiguriert, z. B. Smartphones und Tablets. Die Anweisungen dazu finden Sie im *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*-Dokument.

Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung

USB-Geräte können für die Sicherheitsbedrohung mit der Bezeichnung BadUSB anfällig sein, bei der die Firmware auf USB-Geräten gehackt und durch Malware ersetzt wird. Beispielsweise kann ein Gerät veranlasst werden, Netzwerkdatenverkehr umzuleiten oder eine Tastatur zu emulieren und die Tastatureingabe aufzuzeichnen. Sie können die USB-Umleitungsfunktion konfigurieren, um Ihre Horizon 7-Bereitstellung vor dieser Sicherheitslücke zu schützen.

Durch Deaktivieren der USB-Umleitung können Sie verhindern, dass USB-Geräte an die Remote-Desktops und -Anwendungen Ihrer Benutzer umgeleitet werden. Alternativ können Sie die Umleitung bestimmter USB-Geräte deaktivieren, damit Benutzer nur auf bestimmte Geräte an ihren Remote-Desktops und -Anwendungen Zugriff haben.

Die Entscheidung, ob Sie diese Schritte ausführen sollten, hängt von den Sicherheitsanforderungen in Ihrem Unternehmen ab. Diese Schritte sind nicht obligatorisch. Sie können die USB-Umleitung installieren und diese Funktion für alle USB-Geräte in Ihrer Horizon 7-Bereitstellung aktiviert lassen. Sie sollten sich zumindest genau überlegen, in welchem Umfang Ihr Unternehmen versuchen sollte, die Anfälligkeit für diese Sicherheitslücke zu reduzieren.

Deaktivieren der USB-Umleitung für alle Gerätetypen

Für bestimmte Umgebungen mit hohen Sicherheitsanforderungen müssen Sie für alle USB-Geräte, die Benutzer an ihre Clientgeräte angeschlossen haben, die Umleitung an die Remote-Desktops und

-Anwendungen verhindern. Sie können die USB-Umleitung für alle Desktop-Pools, bestimmte Desktop-Pools oder bestimmte Benutzer in einem Desktop-Pool deaktivieren.

Sie können jede der folgenden Strategien Ihrer Situation entsprechend anwenden:

- Wenn Sie Horizon Agent auf einem Desktop-Image oder RDS-Host installieren, deaktivieren Sie die Setup-Option **USB-Umleitung**. (Diese Option ist standardmäßig deaktiviert.) Dadurch wird der Zugriff auf USB-Geräte auf allen Remote-Desktops und -Anwendungen verhindert, die über das Desktop-Image oder den RDS-Host bereitgestellt werden.
- Bearbeiten Sie in Horizon Administrator die Richtlinie **USB-Zugriff** für einen bestimmten Pool, um den Zugriff entweder zu verweigern oder zuzulassen. Bei dieser Vorgehensweise müssen Sie das Desktop-Image nicht ändern und können den Zugriff auf USB-Geräte in bestimmten Desktop-Pools und Anwendungspools steuern.

Nur die globale Richtlinie **USB-Zugriff** ist für veröffentlichte Desktop und -Anwendungspools verfügbar. Diese Richtlinie kann nicht für einzelne veröffentlichte Desktop oder Anwendungspools festgelegt werden.

- Nachdem Sie die Richtlinie in Horizon Administrator auf Desktop- oder Anwendungspool-Ebene festgelegt haben, können Sie die Richtlinie für einen bestimmten Benutzer im Pool außer Kraft setzen, indem Sie die Einstellung **Benutzer-Außerkraftsetzung** und anschließend einen Benutzer auswählen.
- Legen Sie die Richtlinie `Exclude All Devices` auf **true** fest, je nach Bedarf entweder auf Horizon Agent-Seite oder auf Client-Seite.
- Erstellen Sie mit Intelligente Richtlinien eine Richtlinie, die die Horizon-Richtlinieneinstellung **USB-Umleitung** deaktiviert. Mit diesem Vorgehen können Sie die USB-Umleitung auf einem bestimmten Remote-Desktop deaktivieren, wenn bestimmte Bedingungen erfüllt sind. Sie haben beispielsweise die Möglichkeit, eine Richtlinie zu konfigurieren, mit der die USB-Umleitung deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt.

Wenn Sie für die Richtlinie `Exclude All Devices` die Option **true** festlegen, verhindert Horizon Client, dass alle USB-Geräte umgeleitet werden. Sie können andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie für diese Richtlinie **false** festlegen, lässt Horizon Client zu, dass alle USB-Geräte umgeleitet werden, mit Ausnahme derer, die durch andere Richtlinieneinstellungen blockiert werden. Sie können die Richtlinie sowohl für Horizon Agent als auch für Horizon Client festlegen. Die folgende Tabelle zeigt, wie sich die Richtlinie `Exclude All Devices`, die Sie für Horizon Agent und Horizon Client festlegen können, zu einer effektiven Richtlinie für den Clientcomputer kombinieren lässt. Standardmäßig können alle USB-Geräte umgeleitet werden, es sei denn, sie wären anderweitig blockiert.

Tabelle 4-3. Auswirkungen der Kombination von „Exclude All Devices (Alle Geräte ausschließen)“

Richtlinie „Alle Geräte ausschließen“ auf Horizon Agent	Richtlinie „Alle Geräte ausschließen“ auf Horizon Client	Kombinierte effektive Richtlinie zum Ausschließen aller Geräte
false oder nicht definiert (alle USB-Geräte einschließen)	false oder nicht definiert (alle USB-Geräte einschließen)	Include all USB devices (Alle USB-Geräte einschließen)
false (alle USB-Geräte einschließen)	true (alle USB-Geräte ausschließen)	Exclude all USB devices (Alle USB-Geräte ausschließen)
true (alle USB-Geräte ausschließen)	Beliebig oder nicht definiert	Exclude all USB devices (Alle USB-Geräte ausschließen)

Wenn Sie die Richtlinie `Disable Remote Configuration Download` auf **true** setzen, wird der Wert von `Exclude All Devices` auf Horizon Agent nicht an Horizon Client weitergegeben. Horizon Agent und Horizon Client erzwingen dann den lokalen Wert von `Exclude All Devices`.

Diese Richtlinien sind in der ADMX-Vorlagendatei zur Konfiguration von Horizon Agent (`vdm_agent.admx`) enthalten.

Deaktivieren der USB-Umleitung für bestimmte Geräte

Manche Benutzer müssen möglicherweise bestimmte lokal angeschlossene USB-Geräte umleiten, damit sie Aufgaben auf ihren Remote-Desktops oder -Anwendungen ausführen können. Beispielsweise muss ein Arzt möglicherweise mithilfe eines USB-Diktiergeräts die medizinischen Daten von Patienten aufzeichnen. In diesen Fällen können Sie nicht den Zugriff auf alle USB-Geräte deaktivieren. Mithilfe von Gruppenrichtlinieneinstellungen können Sie die USB-Umleitung für bestimmte Geräte aktivieren bzw. deaktivieren.

Bevor Sie die USB-Umleitung für bestimmte Geräte aktivieren, sollten Sie sicherstellen, dass Sie den physischen Geräten vertrauen, die an Client-Computer in Ihrem Unternehmen angeschlossen sind. Stellen Sie sicher, dass Ihre Lieferkette vertrauenswürdig ist. Verfolgen Sie möglichst eine Kontrollkette für die USB-Geräte nach.

Darüber hinaus sollten Sie Ihre Mitarbeiter schulen, um sicherzustellen, dass sie keine Geräte unbekannter Herkunft anschließen. Beschränken Sie die Geräte in Ihrer Umgebung nach Möglichkeit auf jene Geräte, die nur signierte Firmware-Updates akzeptieren, FIPS 140-2 Level 3-zertifiziert sind und keinerlei vor Ort aktualisierbare Firmware unterstützen. Die Nachverfolgung dieser USB-Gerätetypen ist schwierig und je nach Ihren Geräteanforderungen sind sie möglicherweise nicht auffindbar. Diese Optionen mögen nicht wirklich praktisch sein, sollten aber in Erwägung gezogen werden.

Jedes USB-Gerät verfügt über eine eigene Hersteller- und Produkt-ID, mit der es gegenüber dem Computer identifiziert wird. Durch Konfigurieren der Gruppenrichtlinieneinstellungen für die Horizon Agent-Konfiguration können Sie eine Richtlinie für den Einschluss bekannter Gerätetypen festlegen. Durch diese Vorgehensweise entfällt das Risiko durch unbekannte Geräte in Ihrer Umgebung.

Beispielsweise können Sie verhindern, dass alle Geräte mit Ausnahme der Geräte von einem bekannten Gerätehersteller und mit einer bestimmten Produkt-ID (vid/pid=0123/abcd) an den Remote-Desktop oder die Remoteanwendung umgeleitet werden:

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

Hinweis Diese Beispielkonfiguration bietet Schutz, aber ein manipuliertes Gerät kann jede VID/PID melden, weshalb auch weiterhin Angriffe möglich sind.

Horizon 7 blockiert standardmäßig die Umleitung bestimmter Gerätefamilien an den Remote-Desktop oder die Remoteanwendung. Beispielsweise wird die Anzeige von Eingabegeräten (Human Interface Devices, HIDs) und Tastaturen für den Gast blockiert. Das Ziel von veröffentlichtem BadUSB-Code sind auch USB-Tastaturgeräte.

Sie können die Umleitung bestimmter Gerätefamilien an den Remote-Desktop oder die Remoteanwendung verhindern. Beispielsweise können Sie alle Video-, Audio- und Massenspeichergeräte blockieren:

```
ExcludeDeviceFamily  o:video;audio;storage
```

Umgekehrt können Sie eine Whitelist erstellen, indem Sie die Umleitung aller Geräte verhindern, aber die Verwendung einer bestimmten Gerätefamilie zulassen. Beispielsweise können Sie alle Geräte mit Ausnahme von Speichergeräten blockieren:

```
ExcludeAllDevices    Enabled

IncludeDeviceFamily  o:storage
```

Ein weiteres mögliches Risiko ergibt sich aus der Tatsache, dass sich ein Remotebenutzer bei einem Desktop oder einer Anwendung anmeldet und diesen bzw. diese infiziert. Sie können den USB-Zugriff auf alle Horizon 7-Verbindungen verhindern, die von außerhalb der Unternehmensfirewall hergestellt werden. Das USB-Gerät kann intern, aber nicht extern verwendet werden.

Beachten Sie: Wenn Sie TCP-Port 32111 blockieren, um den externen Zugriff auf USB-Geräte zu deaktivieren, funktioniert die Zeitzonensynchronisierung nicht, weil der Port 32111 auch für die Zeitzonensynchronisierung verwendet wird. Für Zero-Clients ist der USB-Datenverkehr in einen virtuellen Kanal auf UDP-Port 4172 eingebettet. Da Port 4172 für das Anzeigeprotokoll sowie für die USB-Umleitung verwendet wird, können Sie Port 4172 nicht blockieren. Bei Bedarf können Sie die USB-Umleitung auf Zero-Clients deaktivieren. Weitere Informationen hierzu erhalten Sie in der Begleitdokumentation zum Zero-Client oder vom Hersteller des Zero-Clients.

Die Festlegung von Richtlinien zum Blockieren bestimmter Gerätefamilien oder bestimmter Geräte kann das Risiko einer Infizierung mit BadUSB-Malware reduzieren. Durch diese Richtlinien kann das Risiko nicht vollständig eliminiert werden, aber sie stellen eine wirkungsvolle Komponente einer Gesamtstrategie für die Sicherheit dar.

Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs

Nützliche Protokolldateien für USB befinden sich sowohl auf dem Client-System als auch auf dem Remote-Desktop-Betriebssystem oder dem RDS-Host. Verwenden Sie die Protokolldateien an beiden Speicherorten zur Fehlerbehebung. Um Produkt-IDs für bestimmte Geräte zu suchen, verwenden Sie clientseitige Protokolle.

Wenn Sie versuchen, die USB-Geräteteilung oder -filterung zu konfigurieren, oder wenn Sie versuchen, festzustellen, warum ein spezielles Gerät nicht in einem Horizon Client-Menü angezeigt wird, sehen Sie in die Client-Protokolle. Client-Protokolle werden für den USB-Arbitrator und für den Horizon View USB-Dienst erzeugt. Die Anmeldung bei Windows- und Linux-Clients ist standardmäßig aktiviert. Auf Mac-Clients ist die Protokollierung standardmäßig deaktiviert. Informationen zur Aktivierung der Protokollierung auf Mac-Clients finden Sie im Dokument *VMware Horizon Client für Mac Installations- und Einrichtungshandbuch*.

Wenn Sie Richtlinien für das Teilen und Filtern von USB-Geräten konfigurieren, erfordern einige Werte, die Sie festlegen, die VID (Lieferanten-ID) und die PID (Produkt-ID) für das USB-Gerät. Die korrekte VID und PID finden Sie, indem Sie im Internet nach dem Produktnamen plus VID und PID suchen. Alternativ können Sie nach Anschluss des USB-Geräts an das lokale System bei Ausführung von Horizon Client auch in der USB-Protokolldatei nachsehen. Die folgende Tabelle zeigt den Standardspeicherort der Protokolldateien.

Tabelle 4-4. Protokolldateispeicherorte

Client oder Agent	Pfad zu Protokolldateien
Windows-Client	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt
Mac-Client	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Linux-Client	(Standardspeicherort) /tmp/vmware-root/vmware-view-usbd-*.log

Falls ein Problem mit dem Gerät auftritt, nachdem das Gerät an den Remote-Desktop oder die Remoteanwendung umgeleitet wurde, prüfen Sie die Protokolle sowohl auf dem Client als auch auf dem Agenten.

Verwenden von Richtlinien zum Steuern der USB-Umleitung

Sie können USB-Richtlinien sowohl für den Remote-Desktop oder die Remoteanwendung (Horizon Agent) als auch für Horizon Client konfigurieren. Diese Richtlinien geben an, ob das Clientgerät USB-Verbundgeräte für die Umleitung in separate Komponenten aufschlüsseln soll oder nicht. Sie können Geräte aufschlüsseln, um die Typen der USB-Geräte einzuschränken, die der Client zur Umleitung zur

Verfügung stellt, und damit Horizon Agent verhindert, dass bestimmte USB-Geräte von einem Client-Computer weitergeleitet werden.

Wenn Sie ältere Versionen von Horizon Agent oder Horizon Client installiert haben, sind nicht alle Funktionen der USB-Umleitungsrichtlinien verfügbar. Diese Tabelle zeigt, wie Horizon 7 die Richtlinien für unterschiedliche Kombinationen von Horizon Agent und Horizon Client anwendet.

Tabelle 4-5. Kompatibilität von USB-Richtlinieneinstellungen

Horizon Agent-Version	Horizon Client-Version	Auswirkungen von USB-Richtlinieneinstellungen auf die USB-Umleitung
5.1 oder höher	5.1 oder höher	<p>USB-Richtlinieneinstellungen gelten sowohl für Horizon Agent als auch für Horizon Client. Sie können in Horizon Agent USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. Horizon Agent kann Gerätesplitting- und Filterrichtlinieneinstellungen an Horizon Client senden. Sie können in Horizon Client USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht von einem Clientcomputer an einen Desktop weiterzuleiten.</p> <p>Hinweis In View Agent 6.1 oder höher, Horizon Agent 7.0 oder höher und Horizon Client 3.3 oder höher gelten diese Richtlinieneinstellungen für die USB-Umleitung für veröffentlichte Desktops und Anwendungen sowie für Remote-Desktops, die auf Maschinen für Einzelbenutzer ausgeführt werden.</p>
5.1 oder höher	5.0.x oder früher	<p>USB-Richtlinieneinstellungen gelten nur für Horizon Agent. Sie können in Horizon Agent USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. Sie können in Horizon Client keine USB-Richtlinieneinstellungen festlegen, die bestimmen, welche USB-Geräte von einem Clientcomputer an einen Desktop weitergeleitet werden können. Horizon Client kann keine Gerätesplitting- und Filterrichtlinieneinstellungen von Horizon Agent empfangen. Vorhandene Registrierungseinstellungen für die USB-Umleitung von Horizon Client bleiben gültig.</p>
5.0.x oder früher	5.1 oder höher	<p>USB-Richtlinieneinstellungen gelten nur für Horizon Client. Sie können in Horizon Client USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht von einem Clientcomputer an einen Desktop weiterzuleiten. Sie können in Horizon Agent keine USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. Horizon Agent kann keine Gerätesplitting- und Filterrichtlinieneinstellungen an Horizon Client senden.</p>
5.0.x oder früher	5.0.x oder früher	<p>USB-Richtlinieneinstellungen sind nicht anwendbar. Vorhandene Registrierungseinstellungen für die USB-Umleitung von Horizon Client bleiben gültig.</p>

Wenn Sie Horizon Client aktualisieren, bleiben alle vorhandenen Registrierungseinstellungen für die USB-Umleitung (z. B. `HardwareIdFilters`) so lange gültig, bis Sie USB-Richtlinien für Horizon Client definieren.

Auf Clientgeräten, die keine clientseitigen USB-Richtlinien unterstützen, können Sie mithilfe der USB-Richtlinien für Horizon Agent steuern, welche USB-Geräte vom Client an einen Desktop oder eine Anwendung weitergeleitet werden dürfen.

Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte

USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät oder einem Mikrofon und einem Mausgerät. Wenn

Sie möchten, dass eine oder mehrere Komponenten für die Umleitung zur Verfügung stehen sollen, können Sie das Verbundgerät in seine Komponentenschnittstellen splitten, bestimmte Schnittstellen von der Umleitung ausschließen und andere einschließen.

Sie können eine Richtlinie festlegen, die Verbundgeräte automatisch aufschlüsselt. Wenn das automatische Gerätesplitten bei einem bestimmten Gerät nicht funktioniert oder wenn das automatische Splitten nicht zu den von Ihrer Anwendung gewünschten Ergebnissen führt, können Sie Verbundgeräte manuell aufschlüsseln.

Automatisches Gerätesplitten

Wenn Sie das automatische Gerätesplitten aktivieren, versucht Horizon 7 die Funktionen oder Geräte in einem Verbundgerät den wirksamen Filterregeln gemäß aufzuschlüsseln. Beispiel: Ein Diktiermikrofon muss möglicherweise automatisch aufgeschlüsselt werden, sodass das Mausgerät für den Client lokal bleibt, der Rest der Geräte wird jedoch an den Remote-Desktop weitergeleitet.

Die folgende Tabelle zeigt, wie der Wert der Einstellung `Allow Auto Device Splitting` bestimmt, ob der Horizon Client versucht, USB-Verbundgeräte automatisch zu splitten. Standardmäßig ist das automatische Gerätesplitten deaktiviert.

Tabelle 4-6. Auswirkungen des Kombinierens von Richtlinien zum Deaktivieren des automatischen Splittens

Richtlinie zum Zulassen des automatischen Gerätesplittens bei Horizon Agent	Richtlinie zum Zulassen des automatischen Gerätesplittens bei Horizon Client	Kombinierte effektive Richtlinie zum Zulassen des automatischen Splittens von Geräten
Allow – Default Client Setting	false (automatisches Splitten deaktiviert)	Automatisches Splitten deaktiviert
Allow – Default Client Setting	true (automatisches Splitten aktiviert)	Automatisches Splitten aktiviert
Allow – Default Client Setting	Nicht definiert	Automatisches Splitten aktiviert
Allow – Override Client Setting	Beliebig oder nicht definiert	Automatisches Splitten aktiviert
Nicht definiert	Nicht definiert	Automatisches Splitten deaktiviert

Hinweis Diese Richtlinien sind in der ADMX-Vorlagendatei für die Horizon Agent-Konfiguration enthalten. Der Name der ADMX-Vorlagendatei lautet `vdm_agent.admx`.

Standardmäßig deaktiviert Horizon 7 das automatische Splitten und schließt alle Audioausgabe-, Tastatur-, Maus- oder Smartcard-Komponenten eines USB-Verbundgeräts von der Umleitung aus.

Horizon 7 wendet die Richtlinieneinstellungen zum Gerätesplitten vor den Filterrichtlinieneinstellungen an. Wenn Sie das automatische Splitten aktiviert haben und nicht explizit verhindern, dass ein USB-Verbundgerät gesplittet wird, indem Sie die Anbieter- und die Produkt-IDs angeben, prüft Horizon 7 jede Schnittstelle des USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen gemäß den Filterrichtlinieneinstellungen eingeschlossen oder ausgeschlossen werden sollten. Wenn Sie das automatische Gerätesplitten deaktiviert haben und nicht explizit die Anbieter- oder Produkt-ID eines USB-Verbundgeräts angeben, das Sie splitten möchten, wendet Horizon 7 die Filterrichtlinieneinstellungen auf das gesamte Gerät an.

Wenn Sie das automatische Splitten aktivieren, können Sie die Richtlinie Exclude Vid/Pid Device From Split verwenden, um das Composite USB-Gerät anzugeben, bei dem Sie das Splitten verhindern möchten.

Manuelles Gerätesplitten

Sie können die Richtlinie Split Vid/Pid Device verwenden, um die Anbieter- und Produkt-ID eines Composite USB-Gerätes anzugeben, das Sie splitten möchten. Sie können auch die Schnittstellen der Komponenten eines Composite USB-Gerätes angeben, das Sie von der Umleitung ausschließen möchten. Horizon 7 wendet keine Richtlinieneinstellungen auf Komponenten an, die Sie auf diese Weise ausschließen.

Wichtig Wenn Sie die Richtlinie Split Vid/Pid Device verwenden, schließt Horizon 7 nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. Include Vid/Pid Device angeben, um diese Komponenten einzuschließen.

Tabelle 4-7. Modifizierer für Richtlinieneinstellungen für das Gerätesplitten auf Horizon Agent zeigt die Modifizierer, die angeben, wie Horizon Client mit einer Horizon Agent-Richtlinie zum Gerätesplitten umgeht, wenn es eine äquivalente Richtlinieneinstellung für das Gerätesplitten für Horizon Client gibt. Diese Modifizierer gelten für alle Richtlinieneinstellungen zum Gerätesplitten.

Tabelle 4-7. Modifizierer für Richtlinieneinstellungen für das Gerätesplitten auf Horizon Agent

Modifizierer	Beschreibung
m (Zusammenführen)	Horizon Client wendet die Horizon Agent-Richtlinieneinstellung zum Gerätesplitten zusätzlich zur Horizon Client-Richtlinieneinstellung zum Gerätesplitten an.
o (Außer Kraft setzen)	Horizon Client wendet die Horizon Agent-Richtlinieneinstellung zum Gerätesplitten anstatt der Horizon Client-Richtlinieneinstellung zum Gerätesplitten an.

Tabelle 4-8. Beispiele für das Anwenden von Splittenmodifizierern auf die Richtlinieneinstellungen für das Gerätesplitten zeigt Beispiele dafür, wie Horizon Client die Einstellungen für Exclude Device From Split by Vendor/Product ID verarbeitet, wenn Sie verschiedene Splittenmodifizierer angeben.

Tabelle 4-8. Beispiele für das Anwenden von Splittenmodifizierern auf die Richtlinieneinstellungen für das Gerätesplitten

Gerät nach Anbieter-/Produkt-ID vom Splitten auf Horizon Agent ausschließen	Gerät nach Anbieter-/Produkt-ID vom Splitten auf Horizon Client ausschließen	Gerät nach von Horizon Client verwendeter Anbieter-/Produkt-ID-Richtlinie effektiv vom Splitten ausschließen
m:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX
m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY

Horizon Agent wendet die Richtlinieneinstellungen zum Splitten von Geräten auf seiner Seite der Verbindung nicht an.

Horizon Client prüft die Richtlinieneinstellungen zum Gerätesplitten in der folgenden Rangfolge.

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

Eine Richtlinieneinstellung zum Splitten von Geräten, in der ein Gerät vom Splitten ausgeschlossen wird, hat Vorrang vor jeder Richtlinie, nach der es gesplittet werden dürfte. Wenn Sie Schnittstellen oder Geräte festlegen, die vom Splitten ausgeschlossen werden sollen, schließt Horizon Client die entsprechenden Komponentengeräte von der Verfügbarkeit für die Umleitung aus.

Beispiele für das Festlegen von Richtlinien zum Splitten von USB-Geräten

Legen Sie Splittingrichtlinien für Desktops fest, um Geräte mit bestimmten Anbieter- und Produkt-IDs vom Umleiten nach dem automatischen Splitten auszuschließen, und geben Sie diese Richtlinien an Clientcomputer weiter:

- Legen Sie für Horizon Agent die Richtlinie Allow Auto Device Splitting auf Allow – Override Client Setting fest.
- Legen Sie für Horizon Agent die Richtlinie Exclude VidPid From Split auf **o:vid-xxx_pid-yyyy** fest, wobei es sich bei xxx und yyyy um die entsprechenden IDs handelt.

Lassen Sie das automatische Gerätesplitten für Desktops zu und geben Sie Richtlinien für das Splitten von festgelegten Geräten auf Clientcomputern an.

- Legen Sie für Horizon Agent die Richtlinie Allow Auto Device Splitting auf Allow – Override Client Setting fest.
- Legen Sie die Filterrichtlinie Include Vid/Pid Device für das Client-Gerät fest, um das bestimmte Gerät einzuschließen, das Sie splitten möchten. Beispiel: **vid-0781_pid-554c**.
- Legen Sie die Richtlinie Split Vid/Pid Device beispielsweise auf **vid-0781_pid-554c(exintf:00;exintf:01)** fest, um ein bestimmtes USB-Verbundgerät zu splitten, sodass die Schnittstellen 00 und 01 von der Umleitung ausgeschlossen werden.

Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte

Filterrichtlinieneinstellungen, die Sie für Horizon Agent und Horizon Client konfigurieren können, legen fest, welche USB-Geräte von einem Clientcomputer an einen Remote-Desktop oder eine Remoteanwendung umgeleitet werden können. Die USB-Gerätefilterung wird oft von Unternehmen verwendet, um die Verwendung von Massenspeichergeräten auf Remote-Desktops zu deaktivieren oder um die Weiterleitung eines bestimmten Gerätetyps wie eines USB-Ethernet-Adapters zu blockieren, der das Client-Gerät mit dem Remote-Desktop verbindet.

Wenn Sie eine Verbindung mit einem Desktop oder einer Anwendung herstellen, lädt Horizon Client die Horizon Agent-USB-Richtlinieneinstellungen herunter und verwendet diese in Verbindung mit den Horizon Client-USB-Richtlinieneinstellungen, um zu bestimmen, welche USB-Geräte Sie vom Clientcomputer umleiten dürfen.

Horizon 7 wendet jegliche Richtlinieneinstellungen zum Gerätesplitten an, bevor die Filterrichtlinieneinstellungen angewendet werden. Wenn Sie ein USB-Verbundgerät gesplittet haben, prüft Horizon 7 jede der Geräteschnittstellen, um zu entscheiden, welche gemäß den Filterrichtlinieneinstellungen ausgeschlossen oder eingeschlossen werden sollte. Wenn Sie kein USB-Verbundgerät gesplittet haben, wendet Horizon 7 die Filterrichtlinieneinstellungen auf das gesamte Gerät an.

Die Richtlinien zum Gerätesplitten sind in der ADMX-Vorlagendatei zur Konfiguration von Horizon Agent (`vdm_agent.admx`) enthalten.

Interaktion der von Agent erzwungenen USB-Einstellungen

Die folgende Tabelle zeigt die Modifizierer an, die festlegen, wie Horizon Client mit einer Horizon Agent-Filterrichtlinieneinstellung für eine Einstellung umgeht, die vom Agenten erzwungen werden kann, wenn eine äquivalente Filterrichtlinieneinstellung für Horizon Client vorhanden ist.

Tabelle 4-9. Filtermodifizierer für vom Agenten erzwingbare Einstellungen

Modifizierer	Beschreibung
m (Zusammenführen)	Horizon Client wendet die Horizon Agent-Filterrichtlinieneinstellung zusätzlich zur Horizon Client-Filterrichtlinieneinstellung an. Im Falle der booleschen Einstellungen „true/false“ werden die Agent-Einstellungen verwendet, wenn die Client-Richtlinie nicht festgelegt wurde. Wenn die Client-Richtlinie festgelegt wurde, werden die Agent-Einstellungen mit Ausnahme der Einstellung <code>Exclude All Devices</code> ignoriert. Wenn die Richtlinie <code>Exclude All Devices</code> auf der Agenten-Seite festgelegt wird, überschreibt die Richtlinie die Client-Einstellung.
o (Außer Kraft setzen)	Horizon Client verwendet die Horizon Agent-Filterrichtlinieneinstellung anstelle der Horizon Client-Filterrichtlinieneinstellung.

Beispiel: Die folgende Richtlinie auf der Agenten-Seite überschreibt alle Einbeziehungsregeln auf dem Client, und nur das Gerät VID-0911_PID-149a enthält eine angewendete Einbeziehungsregel:

```
IncludeVidPid: o:VID-0911_PID-149a
```

Sie können auch Sternchen als Platzhalterzeichen verwenden, wie beispielsweise:

```
o:vid-0911_pid-****
```

Wichtig Wenn Sie die Agenten-Seite ohne den Modifizierer **o** bzw. **m** konfigurieren, dann wird die Konfigurationsregel als ungültig betrachtet und ignoriert.

Interaktion der vom Client interpretierten USB-Einstellungen

Die folgende Tabelle zeigt die Modifizierer an, die festlegen, wie Horizon Client mit einer Horizon Agent-Filterrichtlinieneinstellung für eine Client-interpretierte Einstellung umgeht.

Tabelle 4-10. Filtermodifizierer für Client-interpretierte Einstellungen

Modifizierer	Beschreibung
Default (d in der Registrierungseinstellung)	Wenn keine Horizon Client-Filterrichtlinieneinstellung vorhanden ist, verwendet Horizon Client die Horizon Agent-Filterrichtlinieneinstellung. Wenn eine Horizon Client-Filterrichtlinieneinstellung vorhanden ist, wendet Horizon Client diese Richtlinieneinstellung an und ignoriert die Horizon Agent-Filterrichtlinieneinstellung.
Override (o in der Registrierungseinstellung)	Horizon Client verwendet die Horizon Agent-Filterrichtlinieneinstellung anstelle jeder entsprechenden Horizon Client-Filterrichtlinieneinstellung.

Horizon Agent wendet die Filterrichtlinieneinstellungen für Client-interpretierte Einstellungen auf seiner Seite der Verbindung nicht an.

Die folgende Tabelle zeigt Beispiele dafür an, wie Horizon Client die Einstellungen für Allow Smart Cards verarbeitet, wenn Sie verschiedene Filtermodifizierer verwenden.

Tabelle 4-11. Beispiele für das Anwenden von Filtermodifizierern auf Client-interpretierte Einstellungen

Einstellung „Smartcards zulassen“ auf Horizon Agent	Einstellung „Smartcards zulassen“ auf Horizon Client	Effektive, von Horizon Client verwendete Richtlinieneinstellung zum Zulassen von Smartcards
Disable – Default Client Setting (d:false in der Registrierungseinstellung)	true (Zulassen)	true (Zulassen)
Disable – Override Client Setting (o:false in der Registrierungseinstellung)	true (Zulassen)	false (Deaktivieren)

Wenn Sie die Richtlinie Disable Remote Configuration Download auf **true** setzen, ignoriert Horizon Client sämtliche Filterrichtlinieneinstellungen, die von Horizon Agent eingehen.

Horizon Agent wendet die Filterrichtlinieneinstellungen in durch den Agenten erzwingbaren Einstellungen auf seiner Seite der Verbindung immer an, selbst dann, wenn Sie Horizon Client so konfigurieren, dass eine andere Filterrichtlinieneinstellung verwendet werden soll oder Sie für Horizon Client festlegen, keine Filterrichtlinieneinstellungen von Horizon Agent herunterzuladen. Horizon Client informiert nicht darüber, dass Horizon Agent die Umleitung eines Geräts verhindert.

Rangfolge von Einstellungen

Horizon Client evaluiert die Filterrichtlinieneinstellungen entsprechend einer Rangfolge. Eine Filterrichtlinieneinstellung, die verhindert, dass ein passendes Gerät umgeleitet wird, hat Vorrang vor der äquivalenten Filterrichtlinieneinstellung, die das Gerät einschließt. Wenn Horizon Client keine Filterrichtlinieneinstellung findet, die ein Gerät ausschließt, lässt Horizon Client die Umleitung des Geräts zu, es sei denn, Sie haben die Richtlinie Exclude All Devices auf **true** gesetzt. Wenn Sie jedoch in Horizon Agent eine Filterrichtlinieneinstellung zum Ausschließen des Geräts konfiguriert haben, blockiert der Desktop bzw. die Anwendung jeden Versuch, das Gerät an ihn bzw. sie umzuleiten.

Horizon Client evaluiert die Filterrichtlinieneinstellungen in der Rangfolge, wobei die Horizon Client-Einstellungen und die Horizon Agent-Einstellungen zusammen mit den Modifiziererwerten beachtet werden, die für die Horizon Agent-Einstellungen gelten. Die folgende Liste zeigt die Rangfolge an, wobei Element 1 den höchsten Rang hat.

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device
- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family
- 7 Allow Audio Input Devices, Allow Audio Output Devices, Allow HIDBootable, Allow HID (Non Bootable and Not Mouse Keyboard), Allow Keyboard and Mouse Devices, Allow Smart Cards und Allow Video Devices
- 8 Kombinierte effektive Richtlinie zum Ausschließen aller Geräte (Exclude All Devices) evaluiert zum Ausschließen oder Einschließen aller USB-Geräte

Sie können die Filterrichtlinieneinstellungen Exclude Path und Include Path nur für Horizon Client festlegen. Die Filterrichtlinien Allow, die sich auf separate Gerätefamilien beziehen, haben denselben Rang.

Wenn Sie eine Richtlinieneinstellung zum Ausschließen von Geräten konfigurieren, die auf Anbieter- oder Produkt-ID-Werten basiert, schließt Horizon Client ein Gerät aus, dessen Anbieter- oder Produkt-ID-Werte dieser Richtlinieneinstellung entsprechen, obwohl Sie möglicherweise eine Richtlinieneinstellung Allow für die Familie konfiguriert haben, zu der das Gerät gehört.

Die Rangfolge für Richtlinieneinstellungen löst Konflikte zwischen den Richtlinieneinstellungen. Wenn Sie Allow Smart Cards konfigurieren, um die Umleitung von Smart Cards zuzulassen, hat jede Ausschlussrichtlinie höheren Ranges Vorrang vor dieser Richtlinie. Möglicherweise haben Sie eine Richtlinieneinstellung Exclude Vid/Pid Device konfiguriert, um Smartcard-Geräte mit übereinstimmenden Pfad-, Anbieter- oder Produkt-ID-Werten auszuschließen, oder vielleicht haben Sie eine Richtlinieneinstellung Exclude Device Family konfiguriert, die die smart-card-Gerätefamilie insgesamt ausschließt.

Wenn Sie beliebige Horizon Agent-Filterrichtlinieneinstellungen konfiguriert haben, evaluiert Horizon Agent diese und erzwingt die Filterrichtlinieneinstellungen in der folgenden Reihenfolge im Remote-Desktop bzw. in der Remoteanwendung, wobei Element 1 die höchste Priorität hat.

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family
- 4 Include Device Family

- 5 Ein vom Agenten erzwungener Richtliniensatz `Exclude All Devices`, der alle USB-Geräte ein- oder ausschließt

Horizon Agent erzwingt diesen begrenzten Satz Filterrichtlinieneinstellungen auf seiner Seite der Verbindung.

Durch das Definieren von Richtlinieneinstellungen für Horizon Agent können Sie eine Filterrichtlinie für nicht verwaltete Clientcomputer erstellen. Die Funktion ermöglicht es Ihnen auch, die Umleitung von Geräten von Clientcomputern zu blockieren, selbst dann, wenn die Filterrichtlinieneinstellungen für Horizon Client die Umleitung zulassen.

Wenn Sie z. B. eine Richtlinie konfigurieren, die zulässt, dass Horizon Client ein Gerät umleiten lässt, blockiert Horizon Agent das Gerät, wenn Sie eine Richtlinie für Horizon Agent konfigurieren, nach der das Gerät ausgeschlossen werden soll.

Beispiele für das Festlegen von Richtlinien zum Filtern von USB-Geräten

Die hier verwendeten Hersteller- und Produkt-IDs sind nur Beispiele. Weitere Informationen zum Festlegen der Hersteller- und Produkt-ID für ein bestimmtes Gerät finden Sie unter [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#).

- Schließen Sie auf dem Client ein bestimmtes Gerät von der Umleitung aus:

```
Exclude Vid/Pid Device:    Vid-0341_Pid-1a11
```

- Blockieren Sie alle Speichergeräte von der Umleitung an diesen Desktop- oder Anwendungspool. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Device Family:    o:storage
```

- Blockieren Sie Audio- und Videogeräte für alle Benutzer in einem Desktop-Pool, um sicherzustellen, dass diese Geräte immer für die Echtzeit-Audio/Video-Funktion verfügbar sind. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Device Family:    o:video;audio
```

Eine andere Strategie würde im Ausschließen bestimmter Geräte nach Hersteller- und Produkt-ID bestehen.

- Blockieren Sie auf dem Client alle Geräte von der Umleitung mit Ausnahme eines bestimmten Geräts:

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd
```

- Schließen Sie alle Geräte aus, die von einem bestimmten Unternehmen hergestellt wurden, da diese Geräte zu Problemen für Ihre Endbenutzer führen können. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Vid/Pid Device:    o:Vid-0341_Pid-*
```

- Schließen Sie auf dem Client zwei bestimmte Geräte ein, alle anderen Geräte jedoch aus:

```
Exclude All Devices:      true
Include Vid/Pid Device:  Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

USB-Gerätefamilien

Sie können eine USB-Gerätefamilie angeben, wenn Sie USB-Filterregeln für Horizon Client oder für View Agent oder Horizon Agent erstellen.

Hinweis Einige Geräte zeigen keine Gerätefamilie an.

Tabelle 4-12. USB-Gerätefamilien

Gerätefamilienname	Beschreibung
audio	Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.
audio-in	Audioeingabegeräte, z. B. Mikrofone.
audio-out	Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.
bluetooth	Per Bluetooth verbundene Geräte.
comm	Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.
hid	Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.
hid-bootable	Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte.
imaging	Bildverarbeitungsgeräte, z. B. Scanner.
keyboard	Tastaturgerät.
mouse	Zeigegerät, z. B. eine Maus.
other	Familie nicht angegeben.
pda	PDA (Personal Digital Assistant)
physical	Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.
printer	Druckergeräte.
security	Sicherheitsgeräte, z. B. Fingerabdruckleser.
smart-card	SmartCard-Geräte.
storage	Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.
unknown	Familie nicht bekannt.
vendor	Geräte mit herstellerspezifischen Funktionen.
video	Videoeingabegeräte.
wireless	Drahtlose Netzwerkadapter.
wusb	Drahtlose USB-Geräte.

USB-Einstellungen in der ADMX-Vorlage für die Horizon Agent-Konfiguration

Sie können USB-Richtlinieneinstellungen sowohl für Horizon Agent als auch für Horizon Client definieren. Nach dem Herstellen der Verbindung lädt Horizon Client die USB-Richtlinieneinstellungen von Horizon Agent herunter und verwendet diese zusammen mit den Horizon Client-USB-Richtlinieneinstellungen, um zu entscheiden, welche Geräte vom Clientcomputer umgeleitet werden dürfen.

Die ADMX-Vorlagendatei für die Horizon Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und die Umgebungskomponenten von Horizon Agent, einschließlich der USB-Umleitung. Der Name der ADMX-Vorlagendatei lautet `vdm_agent.admx`. Die Einstellungen gelten auf Computerebene. Horizon Agent liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`.

Einstellung für die Konfiguration der USB-Geräteaufschlüsselung

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Splitten von USB-Verbundgeräten in der ADMX-Vorlagendatei für die Horizon Agent-Konfiguration beschrieben. Alle Einstellungen befinden sich im Ordner **VMware Horizon Agent-Konfiguration > View USB-Konfiguration > Einstellungen für nur Download zum Client** im Gruppenrichtlinienverwaltungs-Editor. Horizon Agent erzwingt diese Einstellungen nicht. Horizon Agent übergibt die Einstellungen an Horizon Client zwecks Interpretation und Erzwingung in Abhängigkeit davon, ob Sie den Modifizierer zum Zusammenführen (m) oder Außerkraftsetzen (o) angeben. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob USB-Verbundgeräte in ihre Komponentengeräte gesplittet und die Komponentengeräte von der Verfügbarkeit für die Umleitung ausgeschlossen werden sollen. Eine Beschreibung dazu, wie Horizon die Richtlinien für das Splitten von Composite USB-Geräten anwendet, finden Sie unter [Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte](#).

Tabelle 4-13. Horizon Agent-Konfigurationsvorlage: Einstellungen für das Gerätesplitten

Einstellung	Eigenschaften
Allow Auto Device Splitting Eigenschaft: AllowAutoDeviceSplitting	Lässt das automatische Splitten von Composite USB-Geräten zu. Der Standardwert ist nicht definiert, was gleichbedeutend mit false ist.
Exclude Vid/Pid Device from Split Eigenschaft: SplitExcludeVidPid	Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format der Einstellung lautet {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: o:vid-0781_pid-55** Der Standardwert ist nicht definiert.
Split Vid/Pid Device Eigenschaft: SplitVidPid	Behandelt die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte. Das Format der Einstellung ist {m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) oder {m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) Sie können das Stichwort exintf verwenden, um Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: o:vid-0781_pid-554c(exintf:01;exintf:02) Hinweis Horizon 7 schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. Include Vid/Pid Device angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.

Von Horizon Agent erzwungene USB-Einstellungen

Die folgende Tabelle beschreibt alle von Agents erzwungenen Richtlinieneinstellungen für USB in der ADMX-Vorlagendatei für die Horizon Agent-Konfiguration. Alle Einstellungen befinden sich im Ordner **VMware Horizon Agent-Konfiguration > View USB-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor. Horizon Agent verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät zur Host-Maschine umgeleitet werden kann. Horizon Agent übergibt auch die Einstellungen an Horizon Client zwecks Interpretation und Erzwingung in Abhängigkeit davon, ob Sie den Modifizierer zum Zusammenführen (m) oder Außerkraftsetzen (o) angeben. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät für die Umleitung verfügbar ist. Da Horizon Agent immer eine vom Agent erzwungene Richtlinieneinstellung erzwingt, die Sie angeben, könnte die Konsequenz sein, dass Sie der Richtlinie entgegensteuern, die Sie für Horizon Client festgelegt haben. Eine Beschreibung, wie Horizon 7 die Richtlinien für das Filtern von Composite USB-Geräten anwendet, finden Sie unter [Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte](#).

Tabelle 4-14. Horizon Agent-Konfigurationsvorlage: vom Agent erzwungene Einstellungen

Einstellung	Eigenschaften
Exclude All Devices Eigenschaft: ExcludeAllDevices	<p>Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung true festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung false festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden.</p> <p>Wenn diese Einstellung auf true festgelegt ist und an Horizon Client übergeben wird, setzt diese Einstellung immer die Einstellung auf Horizon Client außer Kraft. Sie können die Modifizierer für das Zusammenführen (m) oder Außerkraftsetzen (o) mit dieser Einstellung nicht verwenden.</p> <p>Der Standardwert ist nicht definiert, was gleichbedeutend mit false ist.</p>
Exclude Device Family Eigenschaft: ExcludeFamily	<p>Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung ist {m o}:<i>Familiennname_1</i>[:<i>Familiennname_2</i>]...</p> <p>Beispiel: o:bluetooth;smart-card</p> <p>Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon 7 die Gerätefamilie jeder Schnittstelle eines USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen ausgeschlossen werden sollten. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon 7 die Gerätefamilie des gesamten USB-Verbundgeräts.</p> <p>Der Standardwert ist nicht definiert.</p>
Exclude Vid/Pid Device Eigenschaft: ExcludeVidPid	<p>Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format der Einstellung lautet {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...</p> <p>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.</p> <p>Beispiel: m:vid-0781_pid-****;vid-0561_pid-554c</p> <p>Der Standardwert ist nicht definiert.</p>
Include Device Family Eigenschaft: IncludeFamily	<p>Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung ist {m o}:<i>Familiennname_1</i>[:<i>Familiennname_2</i>]...</p> <p>Beispiel: m:storage</p> <p>Der Standardwert ist nicht definiert.</p>
Include Vid/Pid Device Eigenschaft: IncludeVidPid	<p>Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format der Einstellung lautet {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...</p> <p>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.</p> <p>Beispiel: o:vid-0561_pid-554c</p> <p>Der Standardwert ist nicht definiert.</p>

Von Client interpretierte USB-Einstellungen

Die folgende Tabelle beschreibt alle in der ADMX-Vorlagendatei für die Horizon Agent-Konfiguration enthaltenen Client-interpretierten Richtlinieneinstellungen. Alle Einstellungen befinden sich im Ordner **VMware Horizon Agent-Konfiguration > View USB-Konfiguration > Einstellungen für nur Download zum Client** im Gruppenrichtlinienverwaltungs-Editor. Horizon Agent erzwingt diese Einstellungen nicht. Horizon Agent übergibt diese Einstellungen an Horizon Client zur Interpretation und Erzwingung. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät für die Umleitung verfügbar ist.

Tabelle 4-15. Horizon Agent-Konfigurationsvorlage: Client-interpretierte Einstellungen

Einstellung	Eigenschaften
Allow Audio Input Devices Eigenschaft: AllowAudioIn	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit true ist.
Allow Audio Output Devices Eigenschaft: AllowAudioOut	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit false ist.
Allow HID-Bootable Eigenschaft: AllowHIDBootable	Lässt zu, dass Eingabegeräte außer Tastaturen und Mäuse, die zur Startzeit verfügbar sind (auch als HID-startfähige Geräte bekannt) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit true ist.
Allow Other Input Devices	Lässt zu, dass Eingabegeräte außer HID-startfähigen Geräten oder Tastaturen mit integrierten Zeigegeräten umgeleitet werden. Der Standardwert ist nicht definiert.
Allow Keyboard and Mouse Devices Eigenschaft: AllowKeyboardMouse	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit false ist.
Allow Smart Cards Eigenschaft: AllowSmartcard	Lässt zu, dass SmartCard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit false ist.
Allow Video Devices Eigenschaft: AllowVideo	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit true ist.

Fehlerbehebung bei Problemen mit der USB-Umleitung

Bei der USB-Umleitung in Horizon Client können verschiedene Probleme auftreten.

Problem

Bei der USB-Umleitung in Horizon Client werden lokale Geräte nicht am Remote-Desktop oder in der Remote-Anwendung verfügbar gemacht oder einige Geräte werden für die Umleitung in Horizon Client nicht als verfügbar angezeigt.

Ursache

Aus den folgenden Gründen funktioniert die USB-Umleitung möglicherweise nicht korrekt oder wie erwartet.

- Das Gerät ist ein Verbund-USB-Gerät und eines der enthaltenen Geräte wird standardmäßig gesperrt. Beispielsweise wird ein Diktiergerät mit einer Maus standardmäßig gesperrt, da Mauszeigergeräte standardmäßig gesperrt werden. Informationen zum Umgehen dieses Problems finden Sie unter [Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte](#).
- Die USB-Umleitung wird auf RDS-Hosts unter Windows Server 2008, die veröffentlichte Desktops und Anwendungen bereitstellen, nicht unterstützt.
- Das Gerät funktioniert nicht mit USB-Umleitung oder wird an veröffentlichten Desktops oder in veröffentlichten Anwendungen nicht unterstützt. Weitere Informationen finden Sie unter [Einschränkungen in Bezug auf USB-Gerätetypen](#).

- Die Umleitung wird für Webcams nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.
- Die USB-Umleitung wird für Startgeräte nicht unterstützt. Wenn Sie Horizon Client auf einem Windows-System ausführen, das von einem USB-Gerät startet, und Sie dieses Gerät auf den Remote-Desktop umleiten, reagiert das lokale Betriebssystem möglicherweise nicht oder kann nicht verwendet werden. Siehe <http://kb.vmware.com/kb/1021409>.
- Standardmäßig ermöglicht Ihnen Horizon Client für Windows nicht, Taste, Maus, Smartcard und Audio-Ausgangsgeräte zur Umleitung auszuwählen. Siehe <http://kb.vmware.com/kb/1011600>.
- RDP bietet keine Unterstützung für die Umleitung von USB-Eingabegeräten für die Konsolensitzung oder für Smartcard-Leser. Siehe <http://kb.vmware.com/kb/1011600>.
- Windows Mobile-Gerätecenter kann die Umleitung von USB-Geräten für RDP-Sitzungen verhindern. Siehe <http://kb.vmware.com/kb/1019205>.
- Für einige USB-Eingabegeräte müssen Sie die virtuelle Maschine so konfigurieren, dass die Position des Mauszeigers aktualisiert wird. Siehe <http://kb.vmware.com/kb/1022076>.
- Einige Audiogeräte erfordern möglicherweise Änderungen an Richtlinieneinstellungen oder Registrierungseinstellungen. Siehe <http://kb.vmware.com/kb/1023868>.
- Netzwerklatenz kann zu einer langsamen Geräteinteraktion führen. Zudem ist es möglich, dass Anwendungen nicht zu reagieren scheinen, da sie für die Interaktion mit lokalen Geräten konzipiert sind. Bei USB-Festplattenlaufwerken mit sehr hoher Kapazität kann es einige Minuten dauern, bis diese im Windows Explorer angezeigt werden.
- USB-Flashkarten, die mit dem FAT32-Dateisystem formatiert sind, werden langsam geladen. Siehe <http://kb.vmware.com/kb/1022836>.
- Ein Prozess oder Dienst auf dem lokalen System hat das Gerät geöffnet, bevor Sie eine Verbindung mit dem Remote-Desktop oder der Remoteanwendung hergestellt haben.
- Ein umgeleitetes USB-Gerät ist nicht mehr einsatzbereit, wenn Sie eine Desktop- oder Anwendungssitzung wiederherstellen – selbst wenn der Desktop oder die Anwendung anzeigt, dass das Gerät verfügbar ist.
- Die USB-Umleitung ist in Horizon Administrator deaktiviert.
- Fehlende oder deaktivierte Treiber für die USB-Umleitung auf dem Gast.

Lösung

- ◆ Verwenden Sie, soweit verfügbar, VMware Blast oder PCoIP anstelle von RDP als Protokoll.
- ◆ Wenn ein umgeleitetes Gerät weiterhin nicht verfügbar ist oder nach einer vorübergehenden Verbindungstrennung nicht mehr arbeitet, entfernen Sie das Gerät, schließen Sie es wieder an, und führen Sie erneut eine Umleitung durch.
- ◆ Wechseln Sie in Horizon Administrator zu **Richtlinien > Globale Richtlinien** und prüfen Sie, ob „USB-Zugriff“ unter „View-Richtlinien“ auf **Zulassen** gesetzt ist.

- ◆ Überprüfen Sie das Protokoll auf dem Gast auf Einträge der Klasse `ws_vhub` und das Protokoll auf dem Client auf Einträge der Klasse `vmware-view-usbd`.

Einträge dieser Klassen werden in die Protokolle geschrieben, wenn es sich bei einem Benutzer nicht um einen Administrator handelt oder wenn die Treiber für die USB-Umleitung nicht installiert sind oder nicht ordnungsgemäß funktionieren. Informationen zum Speicherort dieser Protokolldateien finden Sie unter [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#).

- ◆ Öffnen Sie auf dem Gast den Geräte-Manager, erweitern Sie die USB-Controller und installieren Sie die Treiber VMware View Virtual USB Host Controller und VMware View Virtual USB Hub erneut, wenn diese Treiber nicht vorhanden sind, bzw. aktivieren Sie die Treiber, wenn diese deaktiviert sind.

Konfigurieren von Richtlinien für Desktop- und Anwendungspools

5

Sie können Richtlinien konfigurieren, um das Verhalten von Desktop- und Anwendungspools, Computern und Benutzern zu steuern. Sie können mithilfe von Horizon Administrator Richtlinien für Clientsitzungen festlegen. Sie können über Active Directory-Gruppenrichtlinieneinstellungen das Verhalten von Horizon Agent, Horizon Client für Windows und Funktionen steuern, die sich auf einzelne Benutzer-Computer, auf RDS-Hosts, auf das PCoIP- oder das VMware Blast-Anzeigeprotokoll auswirken.

Dieses Kapitel enthält die folgenden Themen:

- [Festlegen von Richtlinien in Horizon Administrator](#)
- [Verwenden von Intelligente Richtlinien](#)
- [Verwenden von Active Directory-Gruppenrichtlinien](#)
- [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für Horizon 7](#)
- [Horizon 7-ADMX-Vorlagendateien](#)
- [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#)
- [ADMX-Vorlageneinstellungen für die VMware View Agent-Konfiguration](#)
- [Richtlinieneinstellungen für die Funktion „Session Collaboration“](#)
- [Richtlinieneinstellungen für die Clientlaufwerksumleitung](#)
- [Richtlinieneinstellungen für die VMware HTML5-Funktion](#)
- [Richtlinieneinstellungen des VMware Virtualization Pack für Skype for Business](#)
- [Richtlinieneinstellungen für VMware Horizon Performance Tracker](#)
- [Richtlinieneinstellungen für den VMware-Integrationsdruck](#)
- [PCoIP-Richtlinieneinstellungen](#)
- [Richtlinieneinstellungen für VMware Blast](#)
- [Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste](#)
- [Filtern von Druckern für den virtuellen Druck](#)
- [Einrichten des standortbasierten Drucks](#)
- [Verwalten von speziellen Unity-Fenstern](#)

■ Beispiel einer Active Directory-Gruppenrichtlinie

Festlegen von Richtlinien in Horizon Administrator

Sie können mithilfe von Horizon Administrator Richtlinien für Clientsitzungen konfigurieren.

Sie können diese Richtlinien so festlegen, dass sie auf bestimmte Benutzer, bestimmte Desktop-Pools oder auf alle Clientsitzungsb Benutzer angewendet werden. Richtlinien, die für bestimmte Benutzer und Desktop-Pools gelten, werden als Richtlinien auf Benutzer- und Desktop-Pool-Ebene bezeichnet. Richtlinien, die sich auf alle Sitzungen und Benutzer auswirken, werden als globale Richtlinien bezeichnet.

Richtlinien auf Benutzerebene erben Einstellungen von äquivalenten Richtlinieneinstellungen für Desktop-Pools. Ähnlich erben Richtlinien auf Desktop-Pool-Ebene Einstellungen von äquivalenten globalen Richtlinieneinstellungen. Eine Richtlinieneinstellung auf Desktop-Pool-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung. Eine Richtlinieneinstellung auf Benutzerebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung oder Richtlinieneinstellungen auf Pool-Ebene.

Richtlinieneinstellungen auf einer niedrigeren Ebene können mehr oder weniger restriktiv sein als die äquivalenten Einstellungen höherer Ebene. Beispiel: Sie können eine globale Richtlinie auf **Verweigern** und die äquivalente Richtlinie auf Desktop-Pool-Ebene auf **Zulassen** oder umgekehrt festlegen.

Hinweis Nur globale Richtlinien sind für veröffentlichte Desktop- und -Anwendungspools verfügbar. Sie können keine Richtlinien auf Benutzerebene oder Poolebene für veröffentlichte Desktop- und Anwendungspools festlegen.

Konfigurieren globaler Richtlinieneinstellungen

Sie können globale Richtlinien konfigurieren, um das Verhalten aller Clientsitzungsb Benutzer zu steuern.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Richtlinien > Globale Richtlinien** aus.
- 2 Klicken Sie im Fensterbereich **View-Richtlinien** auf **Richtlinien bearbeiten**.
- 3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Desktop-Pools

Sie können Richtlinien auf Desktop-Ebene konfigurieren, um diese auf spezifische Desktop-Pools anzuwenden. Eine Richtlinieneinstellung auf Desktop-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **Richtlinien**.
Die Registerkarte **Richtlinien** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **Desktop-Poolrichtlinie** der Wert **Vererben** angezeigt.
- 3 Klicken Sie im Fensterbereich **View-Richtlinien** auf **Richtlinien bearbeiten**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Benutzer

Sie können Richtlinien auf Benutzerebene konfigurieren, um diese auf spezifische Benutzer anzuwenden. Richtlinieneinstellungen auf Benutzerebene haben immer Vorrang vor äquivalenten globalen Richtlinieneinstellungen und Richtlinieneinstellungen auf Desktop-Pool-Ebene.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **Richtlinien**.
Die Registerkarte **Richtlinien** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **Desktop-Poolrichtlinie** der Wert **Vererben** angezeigt.
- 3 Klicken Sie auf **Benutzeraußerkraftsetzung** und anschließend auf **Benutzer hinzufügen**.
- 4 Um einen Benutzer zu suchen, klicken Sie auf **Hinzufügen**, geben den Namen oder die Beschreibung des Benutzers ein und klicken anschließend auf **Suchen**.
- 5 Wählen Sie einen oder mehrere Benutzer aus der Liste aus, klicken Sie auf **OK** und anschließend auf **Weiter**.
Das Dialogfeld „Einzelne Richtlinie hinzufügen“ wird angezeigt.
- 6 Konfigurieren Sie die Horizon-Richtlinien und klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Horizon 7-Richtlinien

Sie können Horizon 7-Richtlinien konfigurieren, die auf alle Clientsitzungen angewendet werden, Sie können die Richtlinien jedoch auch auf spezifische Desktop-Pools oder Benutzer anwenden.

Die folgende Tabelle beschreibt die einzelnen Horizon 7-Richtlinieneinstellungen.

Tabelle 5-1. Horizon-Richtlinien

Richtlinie	Beschreibung
Multimedia-Umleitung (MMR)	<p>Legt fest, ob MMR für Clientsysteme aktiviert ist.</p> <p>MMR ist ein Windows Media Foundation-Filter, der Multimediadaten von bestimmten Codecs auf Remote-Desktops direkt über einen TCP-Socket an das Clientsystem weiterleitet. Die Daten werden direkt auf dem Clientsystem decodiert, auf dem sie wiedergegeben werden.</p> <p>Der Standardwert lautet Verweigern.</p> <p>Wenn Clientsysteme über unzureichende Ressourcen zum Verarbeiten der lokalen Multimedia-Decodierung verfügen, lassen Sie die Einstellung auf Verweigern.</p> <p>MMR-Daten (Multimedia Redirection, Multimediaumleitung) werden über das Netzwerk ohne anwendungsbasierte Verschlüsselung gesendet und können sensitive Daten enthalten, abhängig vom umgeleiteten Inhalt. Um sicherzustellen, dass diese Daten nicht auf dem Netzwerk nachverfolgt werden können, sollten Sie MMR nur auf einem sicheren Netzwerk verwenden.</p>
USB-Zugriff	<p>Legt fest, ob Remote-Desktops USB-Geräte verwenden können, die mit dem Clientsystem verbunden sind.</p> <p>Der Standardwert lautet Zulassen. Um aus Sicherheitsgründen die Verwendung externer Geräte zu unterbinden, ändern Sie die Einstellung in Verweigern.</p>
PCoIP-Hardwarebeschleunigung	<p>Legt fest, ob die Hardwarebeschleunigung für das PCoIP-Anzeigeprotokoll aktiviert wird und legt die Beschleunigungspriorität fest, die der PCoIP-Benutzersitzung zugewiesen ist.</p> <p>Diese Einstellung hat nur dann Auswirkungen, wenn ein PCoIP-Hardwarebeschleunigungsgerät auf dem physischen Computer vorhanden ist, der den Remote-Desktop hostet.</p> <p>Der Standardwert lautet Zulassen, mit dem Prioritätswert Mittel.</p>

Verwenden von Intelligente Richtlinien

Sie können Intelligente Richtlinien für Benutzerumgebungseinstellungen in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung sowie für Computerumgebungseinstellungen verwenden, die beim Starten des Computers oder bei der Wiederherstellung der Sitzung angewendet werden.

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, können Sie eine ausgelöste Aufgabe konfigurieren.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden.

Mit Intelligente Richtlinien besteht die Möglichkeit, Richtlinien zu erstellen, die nur beim Eintreten bestimmter Bedingungen wirksam werden. Sie können beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

Anforderungen für Intelligente Richtlinien

Für die Verwendung von Intelligente Richtlinien muss Ihre Horizon 7-Umgebung bestimmte Anforderungen erfüllen.

- Sie müssen Horizon Agent 7.0 oder höher und VMware Dynamic Environment Manager 9.0 oder höher auf den Remote-Desktops installieren, die mit Intelligente Richtlinien verwaltet werden sollen.
- Benutzer benötigen für die Herstellung einer Verbindung mit Remote-Desktops, die Sie mit Intelligente Richtlinien verwalten, Horizon Client 4.0 oder höher.

Installieren von Dynamic Environment Manager

Wenn Sie mit Intelligente Richtlinien das Verhalten der Funktionen auf einem Remote-Desktop steuern möchten, müssen Sie Dynamic Environment Manager 9.0 oder höher auf den betreffenden Desktops installieren.

Das Dynamic Environment Manager-Installationsprogramm steht auf der VMware-Downloads-Seite zum Herunterladen zur Verfügung. Sie müssen VMware DEM FlexEngine auf jedem Remote-Desktop installieren, der mit Dynamic Environment Manager verwaltet werden soll. Sie können die Komponente der Dynamic Environment Manager-Verwaltungskonsole auf jedem Desktop installieren, von dem aus Sie die Dynamic Environment Manager-Umgebung verwalten möchten.

Für einen RDS-Desktop-Pool installieren Sie Dynamic Environment Manager auf dem RDS-Host, der die veröffentlichten Desktop-Sitzungen bereitstellt.

Informationen zu den Systemanforderungen von Dynamic Environment Manager und die kompletten Installationsanweisungen finden Sie im Dokument *Installieren und Konfigurieren von VMware Dynamic Environment Manager*.

Konfigurieren von Dynamic Environment Manager

Sie müssen Dynamic Environment Manager konfigurieren, ehe Sie damit intelligente Richtlinien für Remote-Desktop-Funktionen erstellen können.

Zum Konfigurieren von Dynamic Environment Manager führen Sie die entsprechenden Anweisungen in *Administratorhandbuch zu VMware Dynamic Environment Manager* aus. Die nachstehenden Konfigurationsschritte ergänzen die Informationen in diesem Dokument.

Zum Konfigurieren von Dynamic Environment Manager führen Sie die entsprechenden Anweisungen in *Administratorhandbuch zu VMware Dynamic Environment Manager* aus.

- Erstellen Sie bei der Konfiguration der Clientkomponente VMware DEM FlexEngine die FlexEngine-An- und Abmeldeskripts. Bei mehreren Sitzungen wie einem RDSH-Desktop und einer RDSH-Anwendung oder einer RDSH-Mehrfachanwendungssitzung für denselben Benutzer auf demselben RDSH-Host verwenden Sie für das Anmeldeskript den Parameter **–HorizonViewMultiSession –r**. Verwenden Sie für das Abmeldeskript den Parameter **–HorizonViewMultiSession –s**.

Hinweis Verwenden Sie keine Anmeldeskripts zum Starten anderer Anwendungen auf einem Remote-Desktop. Die Remote-Desktop-Anmeldung kann sich um bis zu 10 Minuten verzögern, wenn weitere Anmeldeskripts verwendet werden.

- Aktivieren Sie die Benutzer-Gruppenrichtlinieneinstellung Anmeldeskripts gleichzeitig ausführen auf Remote-Desktops. Diese Einstellung befindet sich im Ordner Benutzerkonfiguration\Administrative Vorlagen\System\Scripts.
- Aktivieren Sie die Computer-Gruppenrichtlinieneinstellung Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten auf Remote-Desktops. Diese Einstellung befindet sich im Ordner Computerkonfiguration\Administrative Vorlagen\System\Anmeldung.
- Deaktivieren Sie die Computer-Gruppenrichtlinieneinstellung Anmeldeskriptverzögerung konfigurieren für Remote-Windows 8.1-Desktops. Diese Einstellung befindet sich im Ordner Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinie.
- Wenn Benutzer ihre Verbindung zu Desktop-Sitzungen erneut herstellen, muss sichergestellt sein, dass die Einstellungen für intelligente Horizon-Richtlinien aktualisiert werden. Erstellen Sie dazu in der Dynamic Environment Manager Management Console eine ausgelöste Aufgabe. Setzen Sie den Trigger auf **Sitzung erneut verbinden**, legen Sie für die Aktion **User Environment aktualisieren** fest, und wählen Sie **Intelligente Horizon-Richtlinien** für die Aktualisierung aus.

Hinweis Wenn ein Benutzer bei einem Remote-Desktop angemeldet ist, während Sie die ausgelöste Aufgabe erstellen, wird die ausgelöste Aufgabe erst wirksam, wenn sich der Benutzer vom Desktop abgemeldet hat.

Einstellungen für intelligente Horizon-Richtlinien

Sie können das Verhalten von Remote-Funktionen in Dynamic Environment Manager durch Erstellen einer intelligenten Horizon-Richtlinie steuern.

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut

anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, können Sie eine ausgelöste Aufgabe konfigurieren. Weitere Informationen finden Sie in der vollständigen Liste der Richtlinien im Thema „Konfigurieren von Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen“ im *Administratorhandbuch für VMware Dynamic Environment Manager*.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Weitere Informationen finden Sie in der vollständigen Liste der Richtlinien im Thema „Konfigurieren von Horizon Smart-Richtlinien für Computerumgebungseinstellungen“ im *Administratorhandbuch für VMware Dynamic Environment Manager*.

Im Allgemeinen überschreiben Einstellungen für intelligente Horizon-Richtlinien, die Sie für Remote-Funktionen in Dynamic Environment Manager konfiguriert haben, die entsprechenden Registrierungsschlüssel und Gruppenrichtlinieneinstellungen.

Bandbreitenprofil-Referenz

Mit intelligenten Richtlinien können Sie mit der Profilrichtlinieneinstellung für die Bandbreite ein Bandbreitenprofil für PCoIP-Sitzungen auf Remote-Desktops konfigurieren.

Tabelle 5-2. Bandbreitenprofile

Bandbreitenprofil	Maximale Sitzungsbandbreite (KBit/s)	Mindestsitzungsbandbreite (KBit/s)	Build-to-Lossless (BTL) aktivieren	Maximale Startbildqualität	Mindestbildqualität	Maximale FPS	Maximale Audiobandbreite (KBit/s)	Bildqualitätseinstellung
Hochgeschwindigkeits-LAN	900000	64	Ja	100	50	60	1600	50
LAN	900000	64	Ja	90	50	30	1600	50
Dediziertes WAN	900000	64	Nein	80	40	30	500	50
Breitband-WAN	5000	64	Nein	70	40	20	500	50
Langsames WAN	2000	64	Nein	70	30	15	200	25
Extrem langsame Verbindung	1000	64	Nein	70	30	10	90	0

Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen

Wenn Sie eine intelligente Horizon-Richtlinie in Dynamic Environment Manager definieren, können Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit die Richtlinie wirksam wird. Sie können beispielsweise eine Bedingung hinzufügen, mit der die Clientlaufwerksumleitung nur dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt.

Für eine Remote-Desktop-Funktion können mehrere Bedingungen hinzugefügt werden. Sie haben z. B. die Möglichkeit, eine Bedingung hinzuzufügen, mit der die lokale Druckfunktion aktiviert wird, wenn der Benutzer Mitglied der HR-Gruppe ist, und eine weitere Bedingung, mit der die lokale Druckfunktion aktiviert wird, wenn sich der Remote-Desktop im Win7-Pool befindet.

Detaillierte Informationen zum Hinzufügen und Bearbeiten von Bedingungen in der Dynamic Environment Manager-Verwaltungskonsolle finden Sie unter *Administratorhandbuch zu VMware Dynamic Environment Manager*.

Verwenden der Bedingung „Horizon Client Property“

Wenn sich Benutzer mit einem Remote-Desktop verbinden oder erneut verbinden, ruft Horizon Client Informationen zum Clientcomputer ab und der Verbindungsserver sendet diese Informationen an den Remote-Desktop. Sie können einer Horizon-Richtliniendefinition die Bedingung „Horizon Client Property“ hinzufügen, um anhand der Informationen, die der Remote-Desktop empfängt, die Gültigkeit der Richtlinie festzulegen.

Hinweis Die Bedingung „Horizon Client Property“ ist nur wirksam, wenn der Remote-Desktop vom Benutzer mit dem PCoIP-Anzeigeprotokoll oder dem VMware Blast-Anzeigeprotokoll gestartet wird. Wenn der Benutzer den Remote-Desktop mit dem RDP-Anzeigeprotokoll startet, ist die Bedingung „Horizon Client Property“ unwirksam.

In [Tabelle 5-3. Vordefinierte Eigenschaften für die Bedingung „Horizon Client Property“](#) werden die vordefinierten Eigenschaften beschrieben, die im Dropdown-Menü **Eigenschaften** zur Auswahl stehen, wenn Sie die Bedingung „Horizon Client Property“ verwenden. Jede vordefinierte Eigenschaft entspricht einem ViewClient_-Registrierungsschlüssel.

Tabelle 5-3. Vordefinierte Eigenschaften für die Bedingung „Horizon Client Property“

Eigenschaft	Zugehöriger Registrierungsschlüssel	Beschreibung
Clientstandort	ViewClient_Broker_GatewayLocation	<p>Gibt den Standort des Clientsystems des Benutzers an. Folgende Werte sind gültig:</p> <ul style="list-style-type: none"> ■ Internal – Die Richtlinie wird nur wirksam, wenn der Benutzer von einem Gerät innerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt. ■ External – Die Richtlinie wird nur wirksam, wenn der Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt. <p>Informationen zum Festlegen des Gateway-Standorts für einen Verbindungsserver oder Sicherheitsserver-Host finden Sie im Dokument <i>Horizon 7-Verwaltung</i>.</p> <p>Informationen zum Festlegen des Gateway-Standorts für eine Access Point-Appliance finden Sie im Dokument <i>Bereitstellen und Konfigurieren von Unified Access Gateway</i>.</p>
Kennzeichen starten	ViewClient_Launch_Matched_Tags	<p>Gibt mindestens ein Kennzeichen an. Trennen Sie mehrere Kennzeichen durch ein Komma oder Semikolon. Die Richtlinie wird nur wirksam, wenn das Kennzeichen, das den Start des Remote-Desktops oder der Remoteanwendung ermöglicht hat, einem der angegebenen Kennzeichen entspricht.</p> <p>Informationen zum Zuweisen von Kennzeichen zu Verbindungsserver-Instanzen und Desktop-Pools finden Sie in Ihrem Dokument für die Einrichtung.</p>
Poolname	ViewClient_Launch_ID	<p>Legt die ID eines Desktop- oder Anwendungspools fest. Die Richtlinie wird nur wirksam, wenn die ID des Desktop- oder Anwendungspools, den der Benutzer beim Start des Remote-Desktops oder der Remotenanwendung ausgewählt hat, der angegebenen ID des Desktop- oder Anwendungspools entspricht. Beispielsweise wird die Richtlinie wirksam, wenn der Benutzer den Win7-Pool ausgewählt hat und diese Eigenschaft auf Win7 festgelegt ist.</p> <p>Hinweis Wenn mehr als ein Anwendungspool in einer RDS-Host-Sitzung gestartet wird, entspricht der Wert der ID der ersten Anwendung, die von Horizon Client aus gestartet wird.</p>

Das Dropdown-Menü **Eigenschaften** enthält auch ein Textfeld, sodass Sie jeden ViewClient_-Registrierungsschlüssel manuell in das Textfeld eingeben können. Lassen Sie das Präfix ViewClient_ bei der Eingabe des Registrierungsschlüssels weg. Um z. B. ViewClient_Broker_URL anzugeben, geben Sie Broker_URL ein.

Sie können mit dem Windows Registrierungs-Editor `regedit.exe` auf dem Remote-Desktop den `ViewClient_-Registrierungsschlüssel` anzeigen. Horizon Client schreibt die Clientcomputerinformationen in den Systemregistrierungspfad `HKEY_CURRENT_USER\Volatile Environment` auf Remote-Desktops, die auf Computern für Einzelbenutzer bereitgestellt sind. Bei Remote-Desktops, die in RDS-Sitzungen bereitgestellt sind, schreibt Horizon Client die Clientcomputerinformationen in den Systemregistrierungspfad `HKEY_CURRENT_USER\Volatile Environment\x`, wobei `x` die Sitzungs-ID auf dem RDS-Host darstellt.

Verwenden anderer Bedingungen

In der Dynamic Environment Manager-Verwaltungskonsole stehen viele Bedingungen zur Verfügung. Die folgenden Bedingungen können besonders beim Erstellen von Richtlinien für Remote-Desktop-Funktionen hilfreich sein.

Gruppenmitgliedschaft	Sie können mit dieser Bedingung eine Richtlinie konfigurieren, die nur dann wirksam wird, wenn der Benutzer Mitglied einer bestimmten Gruppe ist.
Remote-Anzeigeprotokoll	Sie können mit dieser Bedingung eine Richtlinie konfigurieren, die nur dann wirksam wird, wenn der Benutzer ein bestimmtes Anzeigeprotokoll auswählt. RDP, PCoIP und Blast sind zulässige Einstellungen für diese Bedingung.
IP-Adresse	Sie können mit dieser Bedingung eine Richtlinie konfigurieren, die nur dann wirksam wird, wenn der Benutzer von innerhalb oder außerhalb des Unternehmensnetzwerks eine Verbindung herstellt. In den Einstellungen für diese Bedingung lässt sich ein interner oder externer IP-Adressbereich angeben.

Hinweis Sie können hierfür auch die Eigenschaft **Clientstandort** der Bedingung „Horizon Client Property“ verwenden.

Beschreibungen aller verfügbaren Bedingungen finden Sie im Dokument *Administratorhandbuch zu VMware Dynamic Environment Manager*.

Erstellen einer intelligenten Horizon-Richtlinie in Dynamic Environment Manager

Mit der Dynamic Environment Manager Management Console können Sie eine intelligente Horizon-Richtlinie in Dynamic Environment Manager erstellen. Wenn Sie eine intelligente Horizon-Richtlinie definieren, können Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit die intelligente Richtlinie wirksam wird.

Voraussetzungen

- Installieren und konfigurieren Sie Dynamic Environment Manager. Siehe [Installieren von Dynamic Environment Manager](#) und [Konfigurieren von Dynamic Environment Manager](#).

- Machen Sie sich mit den Einstellungen der intelligenten Horizon-Richtlinie vertraut. Siehe [Einstellungen für intelligente Horizon-Richtlinien](#).
- Machen Sie sich mit den Bedingungen vertraut, die Sie den Definitionen einer intelligenten Horizon-Richtlinie hinzufügen können. Siehe [Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen](#).

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, konfigurieren Sie eine ausgelöste Aufgabe.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden.

Umfassende Informationen zur Verwendung der Dynamic Environment Manager Management Console finden Sie im Dokument *Administratorhandbuch zu VMware Dynamic Environment Manager*.

Verfahren

- 1 Wählen Sie in der Dynamic Environment Manager-Verwaltungskonsole die **Benutzerumgebung** aus, um eine Richtlinie für Benutzerumgebungseinstellungen zu erstellen, oder die Registerkarte **Computerumgebung**, um eine Richtlinie für Computerumgebungseinstellungen zu erstellen.

Falls Definitionen intelligenter Horizon-Richtlinien vorhanden sind, werden diese im Bereich „Intelligente Horizon-Richtlinien“ angezeigt.

- 2 Wählen Sie **Horizon Smart-Richtlinien** aus und klicken Sie auf **Erstellen**, um eine neue intelligente Richtlinie zu erstellen.
- 3 Aktivieren Sie die Registerkarte **Einstellungen**, und legen Sie die Einstellungen der intelligenten Richtlinie fest.

- a Geben Sie im Abschnitt „Allgemeine Einstellungen“ im Textfeld **Name** einen Namen für die intelligente Richtlinie ein.

Wenn beispielsweise die intelligente Richtlinie einen Einfluss auf die Clientlaufwerksumleitung hat, können Sie die intelligente Richtlinie „CLU“ nennen.

- b Wählen Sie im Abschnitt „Intelligente Horizon-Richtlinieneinstellungen“ die Remote-Desktop-Funktionen und -Einstellungen aus, die Sie in die intelligente Richtlinie aufnehmen möchten.

Sie können mehrere Remote-Desktop-Funktionen auswählen.

- 4 (Optional) Sie fügen der intelligenten Richtlinie eine Bedingung hinzu, indem Sie die Registerkarte **Bedingungen** aktivieren, auf **Hinzufügen** klicken und eine Bedingung auswählen.

Sie haben die Möglichkeit, einer Definition einer intelligenten Richtlinien mehrere Bedingungen hinzuzufügen.

- 5 Klicken Sie auf **Speichern**, um die intelligente Richtlinie zu speichern.

Dynamic Environment Manager verarbeitet die intelligente Horizon-Richtlinie jedes Mal, wenn ein Benutzer eine Verbindung mit dem Remote-Desktop herstellt oder erneut herstellt.

Dynamic Environment Manager verarbeitet mehrere intelligente Richtlinien in alphabetischer Reihenfolge basierend auf den Richtliniennamen. Die intelligenten Horizon-Richtlinien werden im Bereich „Intelligente Horizon-Richtlinien“ in alphabetischer Reihenfolge angezeigt. Wenn es bei den intelligenten Richtlinien zu Konflikten kommt, hat die zuletzt verarbeitete intelligente Richtlinie Vorrang. Beispiel: Angenommen, es gibt eine intelligente Richtlinie namens „Sue“, die die USB-Umleitung aktiviert, und eine andere intelligente Richtlinie namens „Pool“, die die USB-Umleitung für einen Desktop-Pool „Win7“ deaktiviert. Da die intelligente Richtlinie „Sue“ als Letztes verarbeitet wurde, wird die USB-Umleitungsfunktion aktiviert, wenn Sue eine Verbindung zu einem Remote-Desktop im Win7-Desktop-Pool herstellt.

Verwenden von Active Directory-Gruppenrichtlinien

Sie können Microsoft Windows-Gruppenrichtlinien dazu verwenden, Ihre Remote-Desktops zu optimieren und zu schützen, das Verhalten der Horizon 7-Komponenten zu steuern und den standortbasierten Druck zu konfigurieren.

Gruppenrichtlinien sind eine Funktion der Microsoft Windows-Betriebssysteme, die eine zentrale Verwaltung und Konfiguration von Computern und Remote-Benutzern in einer Active Directory-Umgebung ermöglichen.

Gruppenrichtlinieneinstellungen sind in Entitäten enthalten, die als GPOs (Group Policy Objects, Gruppenrichtlinienobjekte) bezeichnet werden. GPOs sind mit Active Directory-Objekten verknüpft. GPOs können auf Domänenebene auf Horizon 7-Komponenten angewendet werden, um verschiedene Bereiche der Horizon 7-Umgebung zu steuern. Nach der Aktivierung von GPOs werden GPO-Einstellungen in der lokalen Windows-Registrierung der betreffenden Komponente gespeichert.

Zur Verwaltung von Gruppenrichtlinieneinstellungen verwenden Sie den Gruppenrichtlinienobjekt-Editor von Microsoft Windows. Der Gruppenrichtlinienobjekt-Editor ist ein MMC-Snap-In (Microsoft Management Console). Die MMC ist Bestandteil der Gruppenrichtlinien-Verwaltungskonsolle von Microsoft.

Informationen zu Installation und Verwendung der Gruppenrichtlinien-Verwaltungskonsolle finden Sie auf der Microsoft TechNet-Website.

Erstellen einer OU für Remote-Desktops

Erstellen Sie in Active Directory eine Organisationseinheit (OU) speziell für Ihre Remote-Desktops.

Um zu verhindern, dass Gruppenrichtlinieneinstellungen auf andere Windows-Server oder -Arbeitsstationen in derselben Domäne wie Ihre Remote-Desktops angewendet werden, erstellen Sie ein Gruppenrichtlinienobjekt für Ihre Horizon 7-Gruppenrichtlinien und verknüpfen es mit der OU, die Ihre Remote-Desktops enthält.

Informationen zum Erstellen von OUs und GPOs finden Sie in der Microsoft Active Directory-Dokumentation auf der Microsoft TechNet-Website.

Aktivieren der Loopback-Verarbeitung für Remote-Desktops

Standardmäßig stammen die Richtlinieneinstellungen für einen Benutzer aus einem Satz an Gruppenrichtlinienobjekten (Group Policy Objects, GPOs), die in Active Directory auf das Benutzerobjekt angewendet werden. In der Horizon 7-Umgebung werden jedoch GPOs basierend auf dem Computer angewendet, bei dem sich der Benutzer anmeldet.

Wenn Sie die Loopback-Verarbeitung aktivieren, wird ein konsistenter Richtliniensatz auf alle Benutzer angewendet, die sich an einem bestimmten Computer anmelden – unabhängig von ihrer Position in Active Directory.

Informationen zum Aktivieren der Loopback-Verarbeitung finden Sie in der Dokumentation zu Microsoft Active Directory.

Hinweis Die Loopback-Verarbeitung ist nur ein Ansatz bei der Verarbeitung von GPOs in Horizon 7. Sie müssen möglicherweise einen anderen Ansatz implementieren.

Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7

Horizon 7 bietet verschiedene komponentenspezifische administrative ADMX-Vorlagendateien für Gruppenrichtlinien. Sie können Remote-Desktops und -anwendungen optimieren und schützen, indem Sie die Richtlinieneinstellungen in den ADMX-Vorlagendateien einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in der Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip verfügbar, wobei x.x.x für die Version und yyyyyyy für die Build-Nummer steht. Sie können die Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Die Horizon 7-ADMX-Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Die Richtlinien für die Computerkonfiguration gelten für alle Remote-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.
- Die Richtlinien für die Benutzerkonfiguration gelten für alle Benutzer, unabhängig davon, mit welchem Remote-Desktop oder mit welcher Remoteanwendung sie sich verbinden. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

Microsoft Windows wendet Richtlinien beim Start eines Desktops und bei der Benutzeranmeldung an.

Horizon 7-ADMX-Vorlagendateien

Die ADMX-Vorlagendateien von Horizon 7 stellen Gruppenrichtlinieneinstellungen bereit, mit denen Sie Horizon 7-Komponenten steuern und optimieren können.

Die ADMX-Dateien stehen in `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Tabelle 5-4. Horizon-ADMX-Vorlagendateien

Name der Vorlage	Vorlagendatei	Beschreibung
VMware View Agent-Konfiguration	<code>vdm_agent.admx</code>	Enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung sowie Umgebungskomponenten von Horizon Agent.
VMware Horizon Client-Konfiguration	<code>vdm_client.admx</code>	Enthält Richtlinieneinstellungen in Bezug auf Horizon Client für Windows. Für Clients, die von außerhalb der Verbindungsserver-Hostdomäne eine Verbindung herstellen, sind die auf Horizon Client angewendeten Richtlinien nicht gültig. Siehe das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
VMware Horizon-URL-Umleitung	<code>urlRedirection.admx</code>	Enthält die Richtlinieneinstellungen für die URL-Inhaltsumleitungsfunktion. Wenn Sie diese Vorlage einem GPO für einen Remote-Desktop- oder Anwendungspool hinzufügen, können bestimmte URL-Links, die im Remote-Desktop oder in der Remoteanwendung angeklickt werden, zu einem Windows-basierten Client umgeleitet und in einem clientseitigen Browser geöffnet werden. Wenn Sie diese Vorlage einem clientseitigen GPO hinzufügen und ein Benutzer bestimmte URL-Links in einem Windows-basierten Clientsystem anklickt, kann die URL in einem Remote-Desktop oder in einer Remoteanwendung geöffnet werden. Siehe Kapitel 3 Konfigurieren der URL-Inhaltsumleitung und siehe das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
VMware View Server-Konfiguration	<code>vdm_server.admx</code>	Enthält Richtlinieneinstellungen in Bezug auf den Verbindungsserver. Weitere Informationen finden Sie im Dokument <i>Administration von View</i> .

Tabelle 5-4. Horizon-ADMX-Vorlagendateien (Fortsetzung)

Name der Vorlage	Vorlagendatei	Beschreibung
Allgemeine VMware View-Konfiguration	vdm_common.admx	Enthält Richtlinieneinstellungen, die für alle Horizon-Komponenten gelten. Weitere Informationen finden Sie im Dokument <i>Administration von View</i> .
PCoIP-Sitzungsvariablen	pcoip.admx	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll.
PCoIP-Client-Sitzungsvariablen	pcoip.client.admx	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll, das Auswirkungen auf Horizon Client für Windows hat. Siehe das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
Persona-Verwaltung	ViewPM.admx	Enthält Richtlinieneinstellungen in Bezug auf Horizon Persona Management. Siehe das Dokument <i>Einrichten von virtuellen Desktops in Horizon 7</i> .
VMware Umleitung für virtuellen Druck	printerRedirection.admx	Enthält Richtlinieneinstellungen zur Deaktivierung des standortbasierten Druckens, zur Deaktivierung der dauerhaften Druckeinstellung und zur Auswahl des Druckertreibers für einen umgeleiteten Clientdrucker.
Standortbasiertes Drucken	LBP.xml	Vorlage zur Definition von Übersetzungsregeln für jeden standortbasierten Drucker für die virtuelle Druckfunktion von VMware.
View-RTAV-Konfiguration	vdm_agent_rtav.admx	Enthält Richtlinieneinstellungen in Bezug auf Webcams, die zusammen mit der Echtzeit-Audio/Video-Funktion verwendet werden. Siehe Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video .
Scannerumleitung	vdm_agent_scanner.admx	Enthält Richtlinieneinstellungen für Scangeräte, die zur Verwendung mit veröffentlichten Remote-Desktops und Remoteanwendungen umgeleitet werden. Siehe Gruppenrichtlinieneinstellungen für Scannerumleitung .
Serieller COM-Port	vdm_agent_serialport.admx	Enthält Richtlinieneinstellungen für serielle Ports (COM-Ports), die zur Verwendung mit virtuellen Desktops umgeleitet werden. Siehe Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports .
VMware Horizon-Druckerumleitung	vdm_agent_printing.admx	Enthält die Richtlinieneinstellungen in Bezug auf das Filtern von umgeleiteten Druckern. Siehe Filtern von Druckern für den virtuellen Druck .

Tabelle 5-4. Horizon-ADMX-Vorlagendateien (Fortsetzung)

Name der Vorlage	Vorlagendatei	Beschreibung
View Agent Direct-Connection	view_agent_direct_connection.admx	Enthält Richtlinieneinstellungen in Bezug auf das View Agent Direct-Connection-Plug-In. Weitere Informationen finden Sie im Dokument <i>Verwaltung des Plug-Ins „View Agent Direct-Connection“</i> .
VMware Horizon Performance Tracker	perf_tracker.admx	Enthält Richtlinieneinstellungen in Bezug auf die VMware Horizon Performance Tracker-Funktion. Siehe Richtlinieneinstellungen für VMware Horizon Performance Tracker .
VMware Horizon-Clientlaufwerkumleitung	vdm_agent_cdr.admx	Enthält die Richtlinieneinstellungen für die Clientlaufwerksumleitungsfunktion. Siehe Verwenden von Gruppenrichtlinien zum Konfigurieren des Laufwerkbuchstaben-Verhaltens .

Hinzufügen der ADMX-Vorlagendateien in Active Directory

Sie können die Richtlinieneinstellungen für bestimmte Remote-Desktop-Funktionen in den Horizon 7-ADMX-Dateien zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass die Setup-Option für die Remotedesktopfunktion, auf die Sie die Richtlinie anwenden, auf Ihren Desktops für virtuelle Maschinen und RDS-Hosts installiert ist. Die Gruppenrichtlinieneinstellungen haben keine Auswirkungen, wenn die Remote-Desktop-Funktion nicht installiert ist. Informationen zur Installation von Horizon Agent finden Sie in Ihrem Dokument für die Einrichtung.
- Erstellen Sie GPOs für die Remotedesktopfunktionen, auf die Sie die Gruppenrichtlinieneinstellungen anwenden möchten, und verknüpfen Sie diese mit der Organisationseinheit, die Ihre Desktops für virtuelle Maschinen und RDS-Hosts enthält.
- Überprüfen Sie den Namen der ADMX-Vorlagendatei, die Sie zu Active Directory hinzufügen möchten. Siehe [Horizon 7-ADMX-Vorlagendateien](#).
- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip und kopieren Sie die ADMX-Dateien auf Ihren Active Directory-Server.
 - a Kopieren Sie die .admx-Dateien und den Ordner en-US in den Ordner %systemroot%\PolicyDefinitions auf Ihrem Active Directory-Server.
 - b Kopieren Sie die Sprachressourcendateien (.adml) in den entsprechenden Unterordner des Ordners %systemroot%\PolicyDefinitions\ auf Ihrem Active Directory-Server.
- 3 Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und geben Sie den Pfad zu den Vorlagendateien an der Stelle ein, an der diese im Editor nach der Installation angezeigt werden.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

ADMX-Vorlageneinstellungen für die VMware View Agent-Konfiguration

Die ADMX-Vorlagendatei (vdm_agent.admx) für die VMware View Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und die Umgebungskomponenten von Horizon Agent.

Die ADMX-Dateien stehen in VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

In der folgenden Tabelle sind die Richtlinieneinstellungen in der ADMX-Vorlagendatei für die VMware View Agent-Konfiguration beschrieben. Die Vorlage enthält sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Agent-Konfigurationseinstellungen

Die Agent-Konfigurationseinstellungen befinden sich im Ordner **VMware View Agent-Konfiguration > Agent-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-5. Einstellungen für die Agent-Konfigurationsrichtlinie

Einstellung	Computer	Benutzer	Eigenschaften
AllowDirectRDP	X		<p>Legt fest, ob sich andere Clients außer Horizon Client-Geräten über RDP direkt mit Remote-Desktops verbinden können. Ist diese Einstellung deaktiviert, lässt der Agent nur Horizon-verwaltete Verbindungen über Horizon Client zu.</p> <p>Wenn Sie die Verbindung zu einem Remote-Desktop über Horizon Client für Mac herstellen möchten, dürfen Sie die Einstellung AllowDirectRDP nicht deaktivieren. Wenn diese Einstellung deaktiviert ist, schlägt die Verbindungsherstellung mit einem Fehler vom Typ Access is denied (Zugriff verweigert) fehl.</p> <p>Standardmäßig können Sie mit RDP eine Verbindung mit der virtuellen Maschine herstellen, während ein Benutzer bei einer Remote-Desktop-Sitzung angemeldet ist. Die RDP-Verbindung beendet die Remote-Desktop-Sitzung. Die nicht gespeicherten Daten sowie die Einstellungen des Benutzers gehen dann unter Umständen verloren. Der Benutzer kann sich erst dann am Desktop anmelden, wenn die externe RDP-Verbindung beendet wurde. Deaktivieren Sie die Einstellung AllowDirectRDP, um diese Situation zu vermeiden.</p> <hr/> <p>Wichtig Die Windows-Remotedesktopdienste müssen auf dem Gastbetriebssystem jedes Desktops ausgeführt werden. Sie können diese Einstellung verwenden, um Benutzer davon abzuhalten, direkte RDP-Verbindungen zu ihren Desktops herzustellen.</p> <hr/> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
AllowSingleSignon	X		<p>Legt fest, ob zur Verbindungsherstellung mit Desktops und Anwendungen die einmalige Anmeldung (Single Sign-On, SSO) zulässig ist. Wenn diese Einstellung aktiviert ist, müssen Benutzer ihre Anmeldedaten nur ein Mal eingeben, wenn sie sich beim Server anmelden. Ist diese Einstellung deaktiviert, müssen sich die Benutzer beim Herstellen einer Remote-Verbindung erneut authentifizieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
CommandsToRunOnConnect	X		<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die bei der ersten Verbindungsherstellung ausgeführt werden.</p> <p>Weitere Informationen finden Sie unter Ausführen von Befehlen auf Horizon-Desktops.</p>
CommandsToRunOnDisconnect	X		<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die ausgeführt werden, wenn eine Sitzung getrennt wird.</p> <p>Weitere Informationen finden Sie unter Ausführen von Befehlen auf Horizon-Desktops.</p>
CommandsToRunOnReconnect	X		<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird.</p> <p>Weitere Informationen finden Sie unter Ausführen von Befehlen auf Horizon-Desktops.</p>

Tabelle 5-5. Einstellungen für die Agent-Konfigurationsrichtlinie (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
ConnectionTicketTimeout	X		<p>Gibt die Gültigkeitsdauer des Horizon-Verbindungstickets in Sekunden an.</p> <p>Horizon Client-Geräte verwenden bei der Verbindungsherstellung mit dem Agenten zur Überprüfung und für die einmalige Anmeldung ein Verbindungsticket. Ein Verbindungsticket ist aus Sicherheitsgründen nur für einen begrenzten Zeitraum gültig. Wenn ein Benutzer eine Verbindung zu einem Remote-Desktop herstellt, muss die Authentifizierung innerhalb des Gültigkeitszeitraums des Verbindungstickets erfolgen, ansonsten wird die Sitzung aufgrund einer Zeitüberschreitung beendet. Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 900 Sekunden.</p>
CredentialFilterExceptions	X		<p>Gibt die ausführbaren Dateien an, die nicht zum Laden des CredentialFilter-Agenten berechtigt sind. Dateinamen dürfen weder einen Pfad noch ein Suffix enthalten. Verwenden Sie ein Semikolon zum Trennen mehrerer Dateinamen.</p>
Disable Time Zone Synchronization	X	X	<p>Legt fest, ob die Zeitzone des Remote-Desktops mit der des verbundenen Clients synchronisiert wird. Diese Einstellung wird bei Aktivierung nur angewendet, wenn die Einstellung Zeitzoneweiterleitung deaktivieren der Richtlinie für die Horizon Client-Konfiguration nicht auf „Deaktiviert“ gesetzt wurde.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Disconnect Session Time Limit (VDI)	X		<p>Gibt den Zeitraum an, nach dem sich eine getrennte Desktop-Sitzung automatisch abmeldet.</p> <ul style="list-style-type: none"> ■ Nie: getrennte Sitzungen auf diesem Computer werden nie abgemeldet. ■ Sofort: getrennte Sitzungen werden sofort abgemeldet. <p>Sie können auch das Zeitlimit in der Desktop-Pool-Einstellung Nach Verbindungstrennung automatisch abmelden in Horizon Administrator oder in Horizon Console konfigurieren. Wenn Sie jeweils diese Einstellung konfigurieren, hat der GPO-Wert Vorrang.</p> <p>Beispiel: Wenn Sie hier Nie auswählen, wird verhindert, dass eine getrennte Sitzung auf diesem Computer abgemeldet wird, unabhängig davon, was in Horizon Administrator oder Horizon Console festgelegt ist.</p>

Tabelle 5-5. Einstellungen für die Agent-Konfigurationsrichtlinie (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
DPI Synchronization	X	X	<p>Passt die systemweite DPI-Einstellung für die Remote-Sitzung an. Wenn diese Einstellung aktiviert oder nicht konfiguriert ist, wird für die systemweite DPI-Einstellung für die Remote-Sitzung der Wert der entsprechenden DPI-Einstellung des Client-Betriebssystems festgelegt. Wenn diese Einstellung deaktiviert ist, wird die systemweite DPI-Einstellung für die Remote-Sitzung nie geändert.</p> <p>Eine Liste der unterstützten Gastbetriebssysteme finden Sie unter „Verwenden der DPI-Synchronisierung“ im Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i>.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
DPI Synchronization Per Connection	X	X	<p>Legt fest, ob die DPI-Einstellung des Bildschirms angepasst wird, wenn ein Benutzer erneut eine Verbindung mit einer Remote-Sitzung herstellt.</p> <p>Wenn diese Einstellung aktiviert ist, wird die DPI-Einstellung des Bildschirms so festgelegt, dass Sie mit der entsprechenden DPI-Einstellung auf dem Clientsystem übereinstimmt, wenn ein Benutzer erneut eine Verbindung zu einer Remote-Sitzung herstellt. Die Einstellung DPI Synchronization muss ebenfalls aktiviert sein.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ändert sich die DPI-Einstellung des Bildschirms nicht, wenn ein Benutzer erneut eine Verbindung mit einer Remote-Sitzung herstellt.</p> <p>Eine Liste der unterstützten Gastbetriebssysteme finden Sie unter „Verwenden der DPI-Synchronisierung“ im Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i>.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Enable Battery State Redirection	X		<p>Legt fest, ob die Akkustandsumleitung aktiviert ist. Diese Funktion wird von Windows- und Linux-Clientsystemen unterstützt.</p> <p>Wenn diese Einstellung aktiviert ist, werden Informationen über den Akku des Windows- oder Linux-Clientsystems an einen Windows-Remote-Desktop umgeleitet. Das Akkusymbol in der Taskleiste auf dem Remote-Desktop zeigt die Akkuladung in Prozent an. Wenn die Akkuladung bei 10 Prozent oder weniger liegt, wird eine entsprechende Meldung eingeblendet.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>

Tabelle 5-5. Einstellungen für die Agent-Konfigurationsrichtlinie (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Enable multi-media acceleration	X		<p>Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem Remote-Desktop aktiviert ist.</p> <p>MMR ist ein Windows Media Foundation-Filter, der Multimediadaten von bestimmten Codecs auf dem Remote-System direkt über einen TCP-Socket an den Client weiterleitet. Die Daten werden direkt auf dem Client decodiert, auf dem sie wiedergegeben werden. Sie können MMR deaktivieren, wenn der Client nicht genügend Ressourcen hat, um eine lokale Multimedia-Decodierung durchzuführen.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Enable Unauthenticated Access	X		<p>Aktiviert bzw. deaktiviert die Funktion für den nicht authentifizierten Zugriff. Wenn diese Einstellung aktiviert ist, können Benutzer ohne Authentifizierung von einem Horizon Client aus ohne AD-Anmeldedaten auf veröffentlichte Anwendungen zugreifen. Ist diese Einstellung deaktiviert ist, haben Benutzer mit einem Zugriff ohne Authentifizierung nicht die Möglichkeit, von Horizon Client aus auf veröffentlichte Anwendungen ohne AD-Anmeldedaten zuzugreifen.</p> <p>Damit diese Einstellung wirksam wird, muss der RDS-Host neu gestartet werden.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Force MMR to use software overlay	X		<p>MMR versucht für die Videowiedergabe das Hardware-Overlay zu verwenden, um die Leistung zu verbessern. Bei Verwendung mehrerer Anzeigegeräte ist das Hardware-Overlay nur auf einem Anzeigegerät vorhanden, und zwar entweder auf dem primären Anzeigegerät oder auf dem Anzeigegerät, auf dem WMP gestartet wurde. Wird WMP in ein anderes Anzeigegerät gezogen, wird statt des Videos ein schwarzes Rechteck dargestellt. Mit dieser Option können Sie für MMR die Verwendung eines Software-Overlay festlegen, das auf allen Anzeigegeräten funktioniert.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Idle Time Until Disconnect (VDI)	X		<p>Gibt den Zeitraum an, nach dem eine Desktop-Sitzung aufgrund von Benutzerinaktivität getrennt wird.</p> <p>Wenn die Option deaktiviert, nicht konfiguriert oder auf Nie festgelegt wird, werden die Desktop-Sitzungen nie getrennt.</p> <p>Wenn der Desktop-Pool oder die Maschine so konfiguriert sind, dass sie nach einer Trennung automatisch abgemeldet werden, wird diese Einstellung berücksichtigt.</p>
ShowDiskActivityIcon	X		<p>Diese Einstellung wird in der vorliegenden Version nicht unterstützt.</p>

Tabelle 5-5. Einstellungen für die Agent-Konfigurationsrichtlinie (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Single sign-on retry timeout	X		Legt den Zeitraum in Millisekunden fest, nach dem erneut versucht wird, eine Single-Sign-On-Anmeldung durchzuführen. Wenn Sie die Wiederholung der Single-Sign-On-Anmeldung deaktivieren möchten, legen Sie den Wert 0 fest. Der Standardwert lautet 5000 Millisekunden. Diese Einstellung ist standardmäßig aktiviert.
Toggle Display Settings Control	X		Legt fest, ob in der Systemsteuerung unter Display (Anzeige) die Registerkarte Settings (Einstellungen) deaktiviert ist, wenn eine Clientsitzung das PCoIP-Anzeigeprotokoll verwendet. Diese Einstellung ist standardmäßig aktiviert.

Hinweis Die Einstellung `Connect using DNS Name` wurde in Horizon 6, Version 6.1 entfernt. Sie können das Horizon 7-LDAP-Attribut, **pae-PreferDNS**, festlegen, um Verbindungsserver anzuweisen, DNS-Namen beim Senden der Adressen von Desktop-Maschinen und RDS-Hosts an Clients und Gateways den Vorrang zu geben. Siehe „Vorrangige Behandlung von DNS-Namen beim Zurückgeben von Adressinformationen durch Horizon-Verbindungsserver“ im Dokument *Horizon 7-Installation*.

Agent-Sicherheitseinstellung

Die Agent-Sicherheitseinstellung befindet sich im Ordner **VMware View Agent-Konfiguration > Agent-Sicherheit** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-6. Einstellung für die Agent-Sicherheitsrichtlinie

Einstellung	Computer	Benutzer	Eigenschaften
Accept SSL encrypted framework channel		X	Aktiviert den TLS-verschlüsselten Framework-Kanal. Die folgenden Optionen stehen zur Verfügung: <ul style="list-style-type: none"> ■ Deaktivieren – TLS deaktivieren. ■ Aktivieren – TLS aktivieren. Ermöglicht älteren Clients die Herstellung einer Verbindung ohne TLS. ■ Erzwingen – TLS aktivieren. Verhindert die Verbindung mit älteren Clients. Diese Einstellung ist standardmäßig aktiviert.

Einstellungen für Session Collaboration

Die Session Collaboration-Einstellungen befinden sich im Ordner **VMware View Agent-Konfiguration > Collaboration** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Richtlinieneinstellungen für die Funktion „Session Collaboration“](#).

Persona Management-Einstellungen

Die Persona Management-Einstellungen befinden sich im Ordner **VMware View Agent-Konfiguration > Persona Management** im Gruppenrichtlinienverwaltungs-Editor. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Einstellungen für die Scannerumleitung

Die Einstellungen für die Scannerumleitung befinden sich im Ordner **VMware View Agent-Konfiguration > Scannerumleitung** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

Serielle COM-Einstellungen

Die seriellen COM-Einstellungen befindet sich im Ordner **VMware View Agent-Konfiguration > Serielle COM** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Gruppenrichtlinieneinstellungen für die Umleitung serieller Ports](#).

Einstellungen für die Smartcard-Umleitung

Die Einstellungen für die Smartcard-Umleitung befindet sich im Ordner **VMware View Agent-Konfiguration > Smartcard-Umleitung > Zugriff auf lokale Lesegeräte** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-7. Einstellungen für die Smartcard-Umleitungsrichtlinie

Einstellung	Computer	Benutzer	Eigenschaften
Allow applications access to Local Smart Card readers	X		<p>Wenn Sie diese Einstellung aktivieren, können Anwendungen auf alle lokalen Smartcard-Lesegeräte zugreifen, auch wenn die Funktion der Smartcard-Umleitung installiert ist. Ist diese Einstellung aktiviert, wird der Desktop auf lokale Lesegeräte überwacht. Werden solche Geräte ermittelt, wird die Smartcard-Umleitung ausgeschaltet und damit der Zugriff auf lokale Lesegeräte ermöglicht. Die Umleitung bleibt solange ausgeschaltet, bis der Benutzer wieder eine Verbindung mit der Sitzung herstellt. Wenn der lokale Zugriff aktiviert ist, können Anwendungen nicht mehr auf Remotelesegeräte auf dem Client zugreifen.</p> <p>Diese Einstellung wird für nicht RDP- oder RDS-Hosts angewendet, wenn die Remotedesktopdienste-Rolle aktiviert ist.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Local Reader Name	X		<p>Legt den Namen eines lokalen Lesegeräts fest, das überwacht werden soll, um den lokalen Zugriff zu aktivieren. Im Lesegerät muss standardmäßig eine Karte eingesteckt sein, um den lokalen Zugriff zu ermöglichen. Sie können diese Anforderung mit der <i>Require an inserted Smart Card</i>-Einstellung deaktivieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Require an inserted Smart Card	X		<p>Wenn diese Einstellung aktiviert ist, wird der lokale Zugriff auf Lesegeräte aktiviert, wenn in den Lesegeräten eine Smartcard eingesteckt ist. Wenn diese Einstellung deaktiviert ist, wird der lokale Zugriff aktiviert, wenn ein lokales Lesegerät ermittelt wird.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>

Einstellungen für die True-SSO-Konfiguration

Die True-SSO-Konfigurationseinstellungen befinden sich im Ordner **VMware View Agent-Konfiguration > True SSO-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor. Weitere Informationen finden Sie im Dokument *Horizon 7-Verwaltung*.

Einstellungen für Unity Touch und gehostete Anwendungen

Die Einstellungen für Unity Touch und gehostete Anwendungen befinden sich im Ordner **VMware View Agent-Konfiguration > Unity Touch und gehostete Anwendungen** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-8. Einstellungen für die Richtlinie zu Unity Touch und gehosteten Anwendungen

Einstellung	Computer	Benutzer	Eigenschaften
Send updates for empty or offscreen windows	X		<p>Legt fest, ob der Client Aktualisierungen für leere oder nicht sichtbare Fenster erhält. Wenn diese Einstellung deaktiviert ist, werden Informationen zu Fenstern, die kleiner als 2x2 Pixel oder komplett unsichtbar sind, nicht zum Client gesendet.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Enable UWP support on RDSH platforms	X		<p>Wenn diese Option aktiviert ist, können Universal Windows Platform(UWP)-Anwendungen auf virtuelle Windows 10-Desktop(WVD)-Hosts auf Horizon Cloud Service on Azure ausgeführt werden. Wenn diese Option deaktiviert ist, wird der Anwendungsstatus in Horizon Agent als nicht verfügbar angezeigt und Benutzer können nicht auf die Anwendung zugreifen. Starten Sie die Agent-VM neu, damit diese Einstellung wirksam wird.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Enable Unity Touch	X		<p>Legt fest, ob die Unity Touch-Funktionalität auf dem Remote-Desktop aktiviert ist. Unity Touch unterstützt das Bereitstellen von veröffentlichten Anwendungen in Horizon Client und ermöglicht den Benutzern mobiler Geräte den Zugriff auf Anwendungen in der Unity Touch-Sidebar.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Enable system tray redirection for Hosted Apps	X		<p>Legt fest, ob die Infobereich-Umleitung aktiviert ist, wenn ein Benutzer veröffentlichte Anwendungen ausführt.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Enable user profile customization for Hosted Apps	X	X	<p>Legt fest, ob das Benutzerprofil angepasst wird, wenn veröffentlichte Anwendungen verwendet werden. Wenn diese Einstellung aktiviert ist, wird ein Benutzerprofil generiert, das Windows-Design angepasst und es werden die Startanwendungen registriert.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Only launch new instances of Hosted Apps if arguments are different	X		<p>Diese Richtlinie steuert das Verhalten, wenn eine veröffentlichte Anwendung gestartet wird, aber bereits eine vorhandene Instanz der Anwendung innerhalb einer Sitzung mit getrenntem Protokoll ausgeführt wird. Bei Deaktivierung wird die vorhandene Instanz der Anwendung aktiviert. Bei Aktivierung wird die vorhandene Instanz der Anwendung nur aktiviert, wenn die Befehlszeilenparameter übereinstimmen.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>

Tabelle 5-8. Einstellungen für die Richtlinie zu Unity Touch und gehosteten Anwendungen (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Limit usage of Windows hooks	X		<p>Deaktiviert die meisten Hooks, wenn veröffentlichte Anwendungen oder Unity Touch verwendet werden. Diese Einstellung ist für Anwendungen mit Kompatibilitätsproblemen gedacht, die auftreten, wenn Hooks auf Betriebssystemebene festgelegt sind. Diese Einstellung deaktiviert beispielsweise die Verwendung der meisten Active Accessibility- und In-Process-Hooks von Windows.</p> <p>Diese Einstellung ist standardmäßig deaktiviert, d. h., es werden alle bevorzugten Hooks verwendet.</p>
Unity Filter rule list	X		<p>Gibt die Filterregeln für Unity-Fenster bei der Verwendung von veröffentlichten Anwendungen an. Horizon Agent verwendet diese Regeln, um benutzerdefinierte Anwendungen zu unterstützen. Weitere Informationen zum Erstellen von Filterregeln finden Sie unter Verwalten von speziellen Unity-Fenstern.</p> <p>Diese Einstellung ist standardmäßig nicht konfiguriert.</p>

Einstellungen für die Horizon Agent Direct-Connection-Konfiguration

Die Einstellungen für die Horizon Agent Direct-Connection-Konfiguration befinden sich im Ordner **VMware View Agent-Konfiguration > View Agent Direct-Connection-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor. Weitere Informationen finden Sie im Dokument *Verwaltung des Plug-Ins „View Agent Direct-Connection“*.

Einstellungen für die Konfiguration von Echtzeit-Audio/Video

Die RTAV-Konfigurationseinstellungen befinden sich im Ordner **VMware View Agent-Konfiguration > View RTAV-Konfiguration** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video](#).

USB-Konfigurationseinstellungen für Horizon Agent

Siehe [USB-Einstellungen in der ADMX-Vorlage für die Horizon Agent-Konfiguration](#).

VMware AppTap-Konfiguration

Die VMware AppTap-Konfigurationseinstellung befindet sich im Ordner **VMware View Agent-Konfiguration > VMware AppTap-Konfiguration** im Editor für die Gruppenrichtlinienverwaltung.

Tabelle 5-9. VMware AppTap-Konfigurationseinstellung

Einstellung	Computer	Benutzer	Eigenschaften
Processes to ignore when detecting empty application sessions	X		<p>Gibt die Liste der Prozesse an, die ignoriert werden sollen, wenn leere Anwendungssitzungen erkannt werden. Sie können entweder einen Prozessdateinamen oder einen vollständigen Pfad angeben. Bei den Werten wird die Groß-/Kleinschreibung nicht berücksichtigt. Verwenden Sie keine Umgebungsvariablen in Pfaden. UNC-Netzwerkpfade sind zulässig, Beispiel: \\vmware\temp\app.exe.</p> <p>Diese Einstellung ist standardmäßig nicht konfiguriert.</p>

Einstellungen für die VMware Client IP-Transparenz

Die Einstellungen für die VMware Client IP-Transparenz befinden sich im Ordner **VMware Client-IP-Transparenz > VMware Client IP-Transparenz** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-10. Einstellungen für die Richtlinie zur VMware Client IP-Transparenz

Einstellung	Computer	Benutzer	Eigenschaften
Default auto detect proxy	X		<p>Standardmäßige Verbindungseinstellung von Internet Explorer. Aktiviert Einstellungen automatisch erkennen unter „Internetoptionen“ > „Verbindungen“ > „Einstellungen für lokales Netzwerk“.</p> <p>Diese Einstellung ist standardmäßig nicht aktiviert.</p>
Default Proxy Server	X		<p>Standardmäßige Verbindungseinstellung von Internet Explorer für den Proxy-Server. Legt den Proxy-Server fest, der unter „Internetoptionen“ > „Verbindungen“ > „Einstellungen für lokales Netzwerk“ verwendet werden soll.</p> <p>Diese Einstellung ist standardmäßig nicht aktiviert.</p>
Enable	X		<p>Aktiviert die VMware Client IP-Transparenz. Remote-Verbindungen mit Internet Explorer verwenden die IP-Adresse des Clients anstelle der IP-Adresse des Remote-Desktop-Computers. Diese Einstellung wird nach der nächsten Anmeldung wirksam.</p> <p>Wenn die Option „VMware Client IP-Transparenz“ des benutzerdefinierten Setups im Installationsprogramm von Horizon Agent ausgewählt ist, wird diese Einstellung standardmäßig aktiviert.</p>
Set proxy for Java applet	X		<p>Legt den Proxy-Server für Java-Applets fest. Die folgenden Optionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> ■ Client IP-Transparenz für Java-Proxy verwenden – Legt für eine Remoteverbindung fest, dass die IP-Adresse des Clients und nicht die IP-Adresse des Remote-Desktop-Computers für Java-Applets verwendet wird. ■ Direkte Verbindung für Java-Proxy verwenden – Legt fest, dass eine direkte Verbindung verwendet wird, um die Browsereinstellung für Java-Applets zu umgehen. ■ Standardwert für Java-Proxy verwenden – Legt fest, dass die OriginalJava-Proxy-Einstellungen wiederhergestellt werden. <p>Diese Einstellung ist standardmäßig nicht aktiviert.</p>

Einstellungen für die Flash-Umleitung

Die Einstellungen für die Flash-Umleitung befinden sich im Ordner **VMware View Agent-Konfiguration > VMware FlashMMR** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-11. Einstellungen für die FlashMMR-Richtlinie

Einstellung	Computer	Benutzer	Eigenschaften
Enable flash multi-media redirection	X		Legt fest, ob die Flash-Umleitung auf dem Agenten aktiviert wird.
Minimum rect size to enable FlashMMR	X		Legt die Mindestgröße des Rechtecks für die Aktivierung der Flash-Umleitung fest. Die Standardbreite beträgt 320 Pixel und die Standardhöhe 200 Pixel.

Einstellungen für die HTML5-Multimedia-Umleitung

Die Einstellungen für die HTML5-Multimedia-Umleitung befinden sich im Ordner **VMware View Agent-Konfiguration > VMware HTML5-Multimedia-Umleitung** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Richtlinieneinstellungen für die VMware HTML5-Funktion](#).

Einstellungen für das VMware Virtualization Pack für Skype for Business

Die Einstellungen für die HTML5-Multimedia-Umleitung befinden sich im Ordner **VMware View Agent-Konfiguration > VMware Virtualization Pack für Skype for Business** im Gruppenrichtlinienverwaltungs-Editor. Siehe [Richtlinieneinstellungen des VMware Virtualization Pack für Skype for Business](#).

An Remote-Desktops gesendete Clientsysteminformationen

Wenn sich Benutzer mit einem Remote-Desktop verbinden oder erneut verbinden, ruft Horizon Client Informationen zum Clientsystem ab und der Verbindungsserver sendet diese Informationen an den Remote-Desktop.

Horizon Agent schreibt die Clientcomputerinformationen in den Systemregistrierungspfad HKCU \Volatile Environment auf Remote-Desktops, die auf Computern für Einzelbenutzer bereitgestellt sind. Bei Remote-Desktops, die in RDS-Sitzungen bereitgestellt sind, schreibt Horizon Agent die Clientcomputerinformationen in den Systemregistrierungspfad HKCU\Volatile Environment\x, wobei x die Sitzungs-ID auf dem RDS-Host darstellt.

Wenn Horizon Client in einer Remote-Desktop-Sitzung ausgeführt wird, werden anstelle der Informationen zur virtuellen Maschine die Informationen zum physischen Client an den Remote-Desktop gesendet. Wenn ein Benutzer z.B. von seinem Clientsystem eine Verbindung zu einem Remote-Desktop herstellt, dann startet Horizon Client im Remote-Desktop und stellt eine Verbindung zu einem anderen

Remote-Desktop her. Die IP-Adresse des physischen Clientsystems wird an den zweiten Remote-Desktop gesendet. Diese Funktion wird als Nested-Modus oder Doppelhop-Szenario bezeichnet. Horizon Client sendet ViewClient_Nested_Passthrough mit dem Wert „1“ zusammen mit den Clientsysteminformationen, um anzuzeigen, dass Nested-Modusinformationen gesendet werden.

Hinweis Mit Horizon Client 4.1 werden Clientsysteminformationen bei der ersten Protokollverbindung an den Second-Hop-Desktop gesendet. Mit Horizon Client 4.2 und höher werden Clientsysteminformationen auch aktualisiert, wenn die First-Hop-Protokollverbindung getrennt und neu hergestellt wird.

Sie können den Horizon Agent-Gruppenrichtlinieneinstellungen CommandsToRunOnConnect, CommandsToRunOnReconnect und CommandsToRunOnDisconnect Befehle hinzufügen, um Befehle oder Befehlsskripts auszuführen, die diese Informationen aus der Systemregistrierung lesen, wenn sich Benutzer mit Desktops verbinden oder erneut verbinden. Weitere Informationen finden Sie unter [Ausführen von Befehlen auf Horizon-Desktops](#).

Tabelle 5-12. Clientsysteminformationen beschreibt die Registrierungsschlüssel, die Clientsysteminformationen enthalten, und listet die Arten von Desktop- und Clientsystemen auf, die diese unterstützen. Wenn in der Spalte **Unterstützt Nested-Modus** „Ja“ angegeben ist, bedeutet dies, dass Informationen zum physischen Client (anstelle von Informationen zur virtuellen Maschine) an einen Second-Hop-Desktop gesendet werden.

Tabelle 5-12. Clientsysteminformationen

Registrierungsschlüssel	Beschreibung	Unterstützt Nested-Modus	Unterstützte Desktops	Unterstützte Client-Systeme
ViewClient_IP_Address	Die IP-Adresse des Clientsystems.	Ja	VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_MAC_Address	Die MAC-Adresse des Clientsystems.	Ja	VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android
ViewClient_Machine_Name	Der Computername des Clientsystems.	Ja	VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Machine_Domain	Die Domäne des Clientsystems.	Ja	VDI (Computer für Einzelbenutzer) RDS	Windows, Windows Store
ViewClient_LoggedOn_Username	Der Benutzername, der zur Anmeldung am Clientsystem verwendet wurde.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac

Tabelle 5-12. Clientsysteminformationen (Fortsetzung)

Registrierungsschlüssel	Beschreibung	Unterstützt Nested- Modus	Unterstützte Desktops	Unterstützte Client- Systeme
ViewClient_LoggedOn_Domain name	Der Domänenname, der zur Anmeldung am Clientsystem verwendet wurde.		VDI (Computer für Einzelbenutzer) RDS	Windows, Windows Store Informationen zu Linux- und Mac-Clients finden Sie unter ViewClient_Machine_Domain. ViewClient_LoggedOn_Domainname wird vom Linux- bzw. Mac-Client nicht bereitgestellt, da Linux- bzw. Mac-Konten nicht an Windows-Domänen gebunden sind.
ViewClient_Type	Der Thin Client-Name oder Betriebssystemtyp des Clientsystems.	Ja	VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Broker_DNS_Name	Der DNS-Name der View-Verbindungsserver-Instanz.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Broker_URL	Die URL der View-Verbindungsserver-Instanz.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Broker_Tunneled	Der Status der Tunnelverbindung für View-Verbindungsserver, der entweder true (aktiviert) oder false (deaktiviert) lauten kann.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Broker_Tunnel_URL	Die URL der View-Verbindungsserver-Tunnelverbindung, wenn die Tunnelverbindung aktiviert ist.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.

Tabelle 5-12. Clientsysteminformationen (Fortsetzung)

Registrierungsschlüssel	Beschreibung	Unterstützt Nested- Modus	Unterstützte Desktops	Unterstützte Client- Systeme
ViewClient_Broker_Remote_IP_Address	Die IP-Adresse des Clientsystems, die der View-Verbindungsserver-Instanz angezeigt wird.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_TZID	Die Olson-Zeitzone-ID. Zum Deaktivieren der Zeitzonensynchronisierung aktivieren Sie die Horizon Agent-Gruppenrichtlinieneinstellung Disable Time Zone Synchronization.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Windows_Timezone	Die GMT-Normalzeit. Zum Deaktivieren der Zeitzonensynchronisierung aktivieren Sie die Horizon Agent-Gruppenrichtlinieneinstellung Disable Time Zone Synchronization.		VDI (Computer für Einzelbenutzer) RDS	Windows, Windows Store
ViewClient_Broker_DomainName	Zur Authentifizierung beim View-Verbindungsserver verwendeter Domänenname.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Broker_UserName	Zur Authentifizierung beim View-Verbindungsserver verwendeter Benutzername.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Client_ID	Gibt die Unique Client HardwareId an, die als Link zum Lizenzschlüssel verwendet wird.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Displays.Number	Gibt die Anzahl an Monitoren an, die auf dem Client verwendet werden.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Tabelle 5-12. Clientsysteminformationen (Fortsetzung)

Registrierungsschlüssel	Beschreibung	Unterstützt Nested- Modus	Unterstützte Desktops	Unterstützte Client- Systeme
ViewClient_Displays.Topology	Gibt die Anordnung, Auflösung und Dimensionen von Anzeigen auf dem Client an.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Keyboard.Type	Gibt den Tastaturtyp an, der auf dem Client verwendet wird. Beispiel: Japanisch, Koreanisch.		VDI (Computer für Einzelbenutzer) RDS	Windows
ViewClient_Launch_SessionType	Gibt den Sitzungstyp an. Dabei kann es sich um eine Desktop-Sitzung oder eine Anwendungssitzung handeln.		VDI (Computer für Einzelbenutzer) RDS	Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben.
ViewClient_Mouse.Identifier	Gibt den Typ der Maus an.		VDI (Computer für Einzelbenutzer) RDS	Windows
ViewClient_Mouse.NumButtons	Gibt die Anzahl der Tasten an, die von der Maus unterstützt werden.		VDI (Computer für Einzelbenutzer) RDS	Windows
ViewClient_Mouse.SampleRate	Gibt in Berichten pro Sekunden die Rate an, in der Eingaben von einer PS/2-Maus aufgenommen werden.		VDI (Computer für Einzelbenutzer) RDS	Windows
ViewClient_Protocol	Gibt das verwendete Protokoll an.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Language	Gibt die Sprache des Betriebssystems an.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Launch_Matched_Tags	Gibt mindestens ein Kennzeichen an.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Launch_ID	Gibt die eindeutige Desktop- oder Anwendungspool-ID an.		VDI (Computer für Einzelbenutzer) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Broker_Farm_ID	Gibt die Farm-ID des Desktop- oder Anwendungspools auf einem RDS-Host an.		RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Hinweis Die Definitionen von ViewClient_LoggedOn_Username und ViewClient_LoggedOn_Domainname in [Tabelle 5-12. Clientsysteminformationen](#) gelten für Horizon Client 2.2 für Windows und spätere Versionen.

Bei Horizon Client 5.4 für Windows und früheren Versionen sendet ViewClient_LoggedOn_Username den in Horizon Client eingegebenen Benutzernamen, und ViewClient_LoggedOn_Domainname sendet den Domänennamen, der in Horizon Client eingegeben wurde.

Horizon Client 2.2 für Windows ist eine spätere Version als Horizon Client 5.4 für Windows. Ab Horizon Client 2.2 stimmen die Versionsnummern für Windows mit den Horizon Client-Versionen auf anderen Betriebssystemen und Geräten überein.

Ausführen von Befehlen auf Horizon-Desktops

Sie können mit den Horizon Agent-Gruppenrichtlinieneinstellungen CommandsToRunOnConnect, CommandsToRunOnReconnect und CommandsToRunOnDisconnect Befehle und Befehlsskripts auf Horizon-Desktops ausführen, wenn sich Benutzer verbinden, erneut verbinden oder ihre Verbindung trennen.

Um einen Befehl oder ein Befehlsskript auszuführen, fügen Sie den Befehlsnamen oder den Dateipfad des Skripts zur Liste der Befehle für die Gruppenrichtlinieneinstellung hinzu. Beispiel:

```
date
```

```
C:\Scripts\myscript.cmd
```

Um Skripts auszuführen, die einen Konsolenzugriff erfordern, stellen Sie die Option -C oder -c voran, gefolgt von einem Leerzeichen. Beispiel:

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procxp.exe
```

Zu den unterstützten Dateitypen gehören .CMD, .BAT und .EXE. .VBS-Dateien werden erst nach einer Analyse mit cscript.exe oder wscript.exe ausgeführt. Beispiel:

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

Die Gesamtlänge der Zeichenfolge, einschließlich der Option -C oder -c, darf 260 Zeichen nicht überschreiten.

Richtlinieneinstellungen für die Funktion „Session Collaboration“

Die ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (vdm_agent.admx) enthält Richtlinieneinstellungen für die Funktion „Session Collaboration“.

Diese Einstellungen finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner

Computerkonfiguration > Administrative Vorlagen > VMware View Agent Configuration > Zusammenarbeit.

Tabelle 5-13. Richtlinieneinstellungen für die Funktion „Session Collaboration“

Einstellung	Beschreibung
Allow control passing to collaborators	Wenn diese Option aktiviert ist, können Benutzer während der Zusammenarbeit die Eingabesteuerung an andere Mitarbeiter weitergeben. Wenn diese Option deaktiviert ist, wird der Umschalter nicht im Fenster der Zusammenarbeit angezeigt. Diese Einstellung ist standardmäßig aktiviert.
Allow inviting collaborators by e-mail	Ist diese Option aktiviert, können Sie Einladungen zur Zusammenarbeit mithilfe einer installierten E-Mail-Anwendung versenden. Ist diese Option deaktiviert, können Sie keine Einladungen zur Zusammenarbeit mit E-Mails versenden, auch wenn eine E-Mail-Anwendung installiert ist. Diese Einstellung ist standardmäßig aktiviert.
Allow inviting collaborators by IM	Ist diese Option aktiviert, können Sie Einladungen zur Zusammenarbeit mithilfe einer installierten Anwendung für Sofortnachrichten (Instant Messages, Chats) versenden. Ist diese Option deaktiviert, können Sie keine Einladungen zur Zusammenarbeit mit Sofortnachrichten versenden, auch wenn eine Anwendung für Sofortnachrichten installiert ist. Diese Einstellung ist standardmäßig aktiviert.
Separator used for multiple e-mail addresses in mailto: links	Konfiguriert das Trennzeichen für mehrere E-Mail-Adressen in „Senden an“-Links, um die Kompatibilität mit verschiedenen E-Mail-Clients zu verbessern. Ist diese Option nicht konfiguriert, ist das Standardzeichen zum Trennen von E-Mail-Adressen ein Semikolon ohne Leerzeichen. Wenn Ihr Standard-E-Mail-Client kein Semikolon als Trennzeichen erlaubt, versuchen Sie es mit anderen Kombinationen, wie z. B. ein Komma plus ein Leerzeichen oder ein Semikolon plus ein Leerzeichen.
Server URLs to include in invitation message	Legt die Server-URLs fest, die in Einladungen zur Zusammenarbeit enthalten sein sollen. Wenn Sie dies nicht konfigurieren, wird eine Standard-URL verwendet. Dies ist aber möglicherweise nur in den einfachsten Bereitstellungen korrekt.
Turn off collaboration	Wenn diese Option aktiviert ist, wird die Funktion „Session Collaboration“ vollständig deaktiviert. Wenn diese Option deaktiviert oder nicht konfiguriert ist, können Sie die Funktion auf Farm- oder Desktop-Poolebene festlegen. Diese Einstellung wird nach dem Neustart der Horizon Agent-Computer wirksam.
Maximum number of invited collaborators	Legt die maximale Anzahl der Benutzer fest, die Sie zur Teilnahme an einer Sitzung einladen können. Standardmäßig ist ein Höchstwert von 5 festgelegt. Der maximale Höchstwert beträgt 10.

Richtlinieneinstellungen für die Clientlaufwerksumleitung

Die ADMX-Vorlagendatei für die VMware Horizon Client-Laufwerksumleitung (`vdm_agent_cdr.admx`) enthält Richtlinieneinstellungen für die Funktion der Clientlaufwerksumleitung.

Die Einstellungen für die Clientlaufwerksumleitung befinden sich im Ordner **VMware View Agent-Konfiguration > VMware Horizon Client-Laufwerksumleitung** im Gruppenrichtlinienverwaltungs-Editor.

Tabelle 5-14. Einstellungen für die Clientlaufwerksumleitung

Einstellung	Computer	Benutzer	Eigenschaften
Configure drive letter mapping mode	X		<p>Gibt den Zuordnungsmodus für den Laufwerkbuchstaben an. Wenn diese Einstellung aktiviert ist, können Sie einen der folgenden Modi auswählen.</p> <ul style="list-style-type: none"> ■ Eins-zu-Eins-Zuordnung, bei der der Laufwerkbuchstabe auf dem Clientcomputer demselben Laufwerkbuchstaben auf dem Agent-Computer zuordnet wird. Beispielsweise wird Laufwerk X auf dem Clientcomputer Laufwerk X auf dem Agent-Computer zugeordnet. ■ Definierte Zuordnung, bei der Laufwerkbuchstaben auf dem Clientcomputer bestimmten Laufwerkbuchstaben auf dem Agent-Computer entsprechend einer Zuordnungstabelle zugeordnet werden, die in der Gruppenrichtlinieneinstellung Zuordnungstabelle für Laufwerkbuchstaben definieren definiert ist. <p>Wenn ein Konflikt bei den Laufwerkbuchstaben auftritt, beispielsweise wenn ein zuzuweisender Laufwerkbuchstabe bereits auf dem Agent-Computer verwendet wird, wird der erste verfügbare Laufwerkbuchstabe von Z bis A verwendet. Wenn kein Laufwerkbuchstabe verfügbar ist, wird kein Laufwerkbuchstabe zugewiesen.</p> <p>Diese Einstellung ist nur gültig, wenn die Gruppenrichtlinieneinstellung Umgeleitetes Gerät mit Laufwerkbuchstaben anzeigen nicht deaktiviert ist.</p>
Define drive letter mapping table	X		<p>Wenn diese Einstellung aktiviert ist, können Sie auf Anzeigen klicken und eine Tabelle mit Laufwerkbuchstabenzuordnungen definieren. Geben Sie in der Spalte Wertname den Laufwerkbuchstaben auf dem Clientcomputer ein. Geben Sie in der entsprechenden Spalte Wert den Laufwerkbuchstaben ein, der auf dem Agent-Computer verwendet werden soll.</p> <p>Diese Einstellung ist nur gültig, wenn Sie Definierte Zuordnung in der Gruppenrichtlinieneinstellung Laufwerkbuchstaben-Zuordnungsmodus konfigurieren auswählen.</p>
Display redirected device with drive letter	X		<p>Legt fest, ob ein Laufwerkbuchstabe für Laufwerke angezeigt wird, die mit der Funktion der Clientlaufwerksumleitung umgeleitet werden.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Timeout for drive letter initialization	X		<p>Gibt die Wartezeit in Millisekunden an, bis der Windows Explorer einen Laufwerkbuchstaben für Laufwerke initialisiert und anzeigt, die mit der Funktion der Clientlaufwerksumleitung umgeleitet werden.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, beträgt der Standardwert 5.000 Millisekunden.</p>

Richtlinieneinstellungen zum Filtern von Client-Geräten

Die Gerätefiltereinstellungen für die Clientlaufwerksumleitung finden Sie im Ordner **VMware View Agent-Konfiguration > VMware Horizon Client-Laufwerksumleitung > Gerätefilterung** im Gruppenrichtlinienverwaltungs-Editor.

Die Funktion zur Gerätefilterung funktioniert nur für Horizon Client für Windows, Mac und Linux-Versionen 5.1 und höher. Wenn diese Gerätefilter-Richtlinien festgelegt sind, wird die Clientlaufwerksumleitung für andere Clients, einschließlich Android, iOS und Chrome, sowie Horizon Client-Versionen 5.0 und früher deaktiviert.

Tabelle 5-15. Gerätefiltereinstellungen

Einstellung	Computer	Benutzer	Eigenschaften
Exclude Vid/Pid Device	X		<p>Schließt Geräte mit einer angegebenen Anbieter- und Produkt-ID aus, die mit der Funktion zur Clientlaufwerksumleitung umgeleitet werden.</p> <p>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Verwenden Sie ein Semikolon zum Trennen mehrerer Geräte. Beispiel:</p> <pre>vid-0781_pid-554c;vid-0781_pid-****</pre> <p>Der Standardwert ist „nicht definiert“ (keine Geräte ausgeschlossen).</p> <p>Diese Einstellung hat Vorrang vor der Einstellung VID-/PID-Gerät einschließen.</p> <p>Hinweis Um die Clientlaufwerksumleitung für alle Geräte zu deaktivieren, können Sie <code>vid-****_pid-****</code> angeben.</p>
Include Vid/Pid Device	X		<p>Gibt Geräte mit einer angegebenen Anbieter- und Produkt-ID an, die mit der Funktion zur Clientlaufwerksumleitung umgeleitet werden können.</p> <p>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Verwenden Sie ein Semikolon zum Trennen mehrerer Geräte. Beispiel:</p> <pre>vid-054C_pid-0099;vid-8888_pid-****</pre> <p>Der Standardwert ist „nicht definiert“ (alle Geräte eingeschlossen).</p>

Richtlinieneinstellungen für die VMware HTML5-Funktion

Die ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (`vdm_agent.admx`) enthält Richtlinieneinstellungen für die VMware HTML5-Funktionen.

Allgemeine Einstellungen für die VMware HTML5-Funktion

Allgemeine Einstellungen für die VMware HTML5-Funktion finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen**.

Tabelle 5-16. Allgemeine Einstellungen für die VMware HTML5-Funktion

Einstellung	Beschreibung
Enable VMware HTML5 Features	Aktiviert die VMware HTML5-Funktionen. Sie müssen diese Einstellung aktivieren, um die VMware HTML5 Multimedia-Umleitung, die Geolocation-Umleitung oder die Funktion zur Browser-Umleitung zu verwenden. Diese Einstellung wird nach der nächsten Anmeldung wirksam.
Disable Automatically Detect Intranet	<p>Wenn die Richtlinie aktiviert ist, werden die Intranet-Einstellungen „Alle lokalen Sites (Intranet), die nicht in anderen Zonen aufgeführt sind, einbeziehen“ und „Alle Sites, die den Proxyserver umgehen, einbeziehen“ bei der nächsten Anmeldung deaktiviert.</p> <p>Wenn diese Richtlinie deaktiviert ist, werden an der lokalen IE-Intranetzone keine Änderungen vorgenommen.</p> <p>Wichtig Sie müssen diese Einstellung aktivieren, wenn Sie den Edge-Browser für die HTML5-Multimedia-Umleitung aktivieren oder die Geolocation-Umleitung aktivieren.</p>

Einstellungen für die VMware HTML5-Multimedia-Umleitung

Die Einstellungen für die VMware HTML5 Multimedia-Umleitung finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware HTML5 Multimedia-Umleitung**.

Tabelle 5-17. Einstellungen für die Richtlinie zur HTML5-Multimedia-Umleitung

Einstellung	Beschreibung
Enable VMware HTML5 Multimedia Redirection	Aktiviert die Funktion zur VMware HTML5-Multimedia-Umleitung. Diese Einstellung wird nach der nächsten Anmeldung wirksam.
Enable URL list for VMware HTML5 Multimedia Redirection	<p>Gibt an, welche Websites die Funktion zur HTML5 Multimedia-Umleitung verwenden.</p> <p>Geben Sie die Liste der URLs für die Websites ein, die HTML5 Multimedia-Inhalte in die Spalte „Wertname“ umleiten können. Fügen Sie den URLs das Präfix <code>http://</code> oder <code>https://</code> hinzu. Sie können den URL-Musterabgleich verwenden.</p> <p>Geben Sie z. B. <code>https://www.youtube.com/*</code> ein, um alle Videos auf YouTube umzuleiten. Um alle Videos auf Vimeo umzuleiten, geben Sie <code>https://www.vimeo.com/*</code> ein.</p> <p>Lassen Sie die Spalte „Wert“ leer.</p>

Tabelle 5-17. Einstellungen für die Richtlinie zur HTML5-Multimedia-Umleitung (Fortsetzung)

Einstellung	Beschreibung
Enable Chrome Browser for VMware HTML5 Multimedia Redirection	Diese Richtlinie wird nur verwendet, wenn die Funktion zur VMware HTML5 Multimedia-Umleitung aktiviert ist. Wenn diese Richtlinie nicht konfiguriert ist, dann ist der Standardwert mit dem Wert der Einstellung „VMware HTML5 Multimedia-Umleitung aktivieren“ identisch.
Enable Edge Browser for VMware HTML5 Multimedia Redirection	Diese Richtlinie wird nur verwendet, wenn die Funktion zur VMware HTML5 Multimedia-Umleitung aktiviert ist. Wenn diese Richtlinie nicht konfiguriert ist, dann ist der Standardwert mit dem Wert der Einstellung „VMware HTML5 Multimedia-Umleitung aktivieren“ identisch.

Einstellungen für die VMware Geolocation-Umleitung

Die Einstellungen für die VMware Geolocation-Umleitung finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware GeoLocation-Umleitung**.

Tabelle 5-18. Einstellungen für die VMware Geolocation-Umleitung

Einstellung	Beschreibung
Enable VMware Geolocation Redirection	Aktiviert die Funktion zur Geolocation-Umleitung. Diese Einstellung wird nach der nächsten Anmeldung wirksam.
Enable URL list for VMware Geolocation Redirection	Gibt an, welche Websites die Funktion zur Geolocation-Umleitung verwenden. Geben Sie die Liste der URLs für die Websites ein, die Geolocation-Informationen in die Spalte „Wertname“ umleiten können. Fügen Sie den URLs das Präfix <code>http://</code> oder <code>https://</code> hinzu. Sie können den URL-Musterabgleich verwenden. Geben Sie z. B. <code>https://www.youtube.com/*</code> ein, um alle YouTube-Videos anzugeben. Geben Sie <code>https://www.vimeo.com/*</code> ein, um alle Vimeo-Videos anzugeben. Lassen Sie die Spalte „Wert“ leer.
Set the minimum distance for which to report location updates	Bestimmt die Mindestentfernung in Metern zwischen einem Standort-Update auf dem Client und dem zuletzt an den Agent gemeldeten Update, für das der neue Standort an den Agent gemeldet werden muss. Standardmäßig wird eine Mindestentfernung von 75 Metern verwendet.

Einstellungen für die VMware Browser-Umleitung

Die Einstellungen für die VMware Browser-Umleitungsfunktion finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware View Agent-Konfiguration > VMware HTML5-Funktionen > VMware Browser-Umleitung**.

Tabelle 5-19. Einstellungen für die VMware Browser-Umleitung

Einstellung	Beschreibung
Enable VMware Browser Redirection	Aktiviert die Browser-Umleitungsfunktion.
Enable URL list for VMware Browser Redirection	<p>Gibt alle URLs für die Browser-Umleitungsfunktion an. Benutzer können diese URLs besuchen, indem sie sie entweder in die Chrome-Adressleiste oder in die benutzerdefinierte Adressleiste eingeben. Benutzer können diese URLs auch aufrufen, indem sie ausgehend von einer anderen URL in der Liste oder von einer beliebigen agentenseitig gerenderten Seite zu ihnen navigieren.</p> <p>Geben Sie die URLs in die Wertnamensspalte ein. Fügen Sie den URLs das Präfix <code>http://</code> oder <code>https://</code> hinzu. Sie können den URL-Musterabgleich verwenden. Übereinstimmungsmuster müssen https://developer.chrome.com/extensions/match_patterns folgen.</p> <p>Geben Sie z. B. <code>https://www.youtube.com/*</code> ein, um den gesamten YouTube-Content anzugeben.</p> <p>Lassen Sie die Spalte „Wert“ leer.</p>
Enable Navigation URL list for VMware Browser Redirection	<p>Gibt die URLs an, zu denen ein Benutzer von einer URL, die in der Positivliste URL-Liste für VMware Browser-Umleitung aktivieren angegeben ist, navigieren darf (entweder durch Eingabe der URL direkt in die benutzerdefinierte Adressleiste oder durch Navigieren zur URL von einer URL in der Positivliste).</p> <p>Benutzer können diese URLs nicht direkt aufrufen, indem sie sie in die Chrome-Adressleiste eingeben oder von einer agentenseitig gerenderten Seite dorthin navigieren.</p> <p>Geben Sie die Liste der URLs in die Wertnamensspalte ein. Fügen Sie den URLs das Präfix <code>http://</code> oder <code>https://</code> hinzu. Sie können den URL-Musterabgleich verwenden. Übereinstimmungsmuster müssen https://developer.chrome.com/extensions/match_patterns folgen.</p> <p>Geben Sie z. B. <code>https://www.youtube.com/*</code> ein, um den gesamten YouTube-Content anzugeben.</p> <p>Lassen Sie die Spalte „Wert“ leer.</p>

Tabelle 5-19. Einstellungen für die VMware Browser-Umleitung (Fortsetzung)

Einstellung	Beschreibung
Enable automatic fallback after a whitelist violation	<p>Wenn diese Einstellung aktiviert ist und ein Benutzer zu einer URL navigiert, die nicht in einer der Positivlisten für die Browser-Umleitung angegeben ist, entweder durch Eingabe in die benutzerdefinierte Adressleiste oder durch Navigieren von einer URL in einer der Positivlisten, wird die Umleitung für diese Registerkarte angehalten. Die URL wird dann abgerufen und stattdessen auf dem Agent angezeigt.</p> <hr/> <p>Hinweis Wenn ein Benutzer versucht, zu einer URL zu navigieren, die nicht in der Einstellung URL-Liste für VMware Browser-Umleitung aktivieren angegeben ist, fällt die Registerkarte immer wieder auf das Abrufen und Rendern der URL auf dem Agent zurück, unabhängig davon, ob diese Einstellung aktiviert ist.</p>
Show a page with error information before automatic fallback	<p>Wenn diese Einstellung aktiviert ist und ein Verstoß gegen eine Positivliste auftritt, wird eine Seite angezeigt, die einen Countdown von fünf Sekunden anzeigt. Nach Ablauf von fünf Sekunden fällt die Registerkarte auf das Abrufen und Rendern der URL zurück, die den Verstoß auf dem Agent verursacht hat. Wenn diese Einstellung deaktiviert ist, wird die Seite mit der Warnung von fünf Sekunden nicht angezeigt.</p> <p>Diese Einstellung wird nur wirksam, wenn Automatisches Fallback nach einem Whitelist-Verstoß aktivieren ebenfalls aktiviert ist.</p>

Richtlinieneinstellungen des VMware Virtualization Pack für Skype for Business

Die ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (`vdm_agent.admx`) enthält Richtlinieneinstellungen für das VMware Virtualization Pack für Skype for Business.

Diese Einstellungen finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware View Agent Configuration > VMware Virtualization Pack für Skype for Business**.

Tabelle 5-20. Richtlinieneinstellungen für das Virtualization Pack für Skype for Business

Einstellung	Beschreibung
Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business	Standardmäßig aktiviert, bietet der erweiterte Filter für akustische Echo-Abbrüche eine bessere Echo- und Rückkopplungs-Löschung und ist besonders effektiv in Szenarien, in denen das Mikrofon und der Lautsprecher von Horizon Client systemnahe beieinander liegen. Aktivieren Sie diese Richtlinie, wenn Sie nicht möchten, dass VMware Virtualization Pack für Skype for Business diesen Filter verwendet.
EnableDetectProxySettings	Aktivieren Sie diese Richtlinie, um Verzögerungen zu reduzieren, wenn für das Horizon Client-System die Verwendung eines Proxy-Servers erforderlich ist. Wenn aktiviert, prüft das Virtualization Pack für Skype for Business, ob Proxy-Einstellungen auf dem Horizon Client-System vorhanden sind und verwendet diese Einstellungen für den Mediendatenverkehr. Sind keine Proxy-Einstellungen auf dem Horizon Client-System vorhanden, verwendet das Virtualization Pack für Skype for Business eine direkte Verbindung.
Force Skype for Business in non-optimized mode	Sie können erzwingen, dass Skype for Business für Horizon Client-Verbindungen im nicht optimierten Modus ausgeführt wird, indem Sie den Namen der Umgebungsvariablen festlegen, die zum Zeitpunkt der Verbindung auf dem Computer vorhanden ist, auf dem Horizon Agent installiert ist. Wenn der Name der Variablen festgelegt ist, wird das Virtualization Pack für Skype for Business auf den Fallback-Modus zurückgesetzt. Wenn beispielsweise die Umgebungsvariable ViewClient_F5_APM auf dem Remote-Desktop-Agent-Computer festgelegt ist, während der Horizon Client-Computer außerhalb des Netzwerks mithilfe des F5-Lastausgleichs eine Verbindung herstellt, und Sie den nicht optimierten Modus erzwingen möchten, legen Sie diesen Wert auf „ViewClient_F5_APM“ fest. Diese Richtlinie ist standardmäßig nicht konfiguriert.
Show Icon	Zeigt das Symbol für das Virtualization Pack für Skype for Business an. Diese Richtlinie ist standardmäßig aktiviert. Das Symbol wird nicht angezeigt, wenn die Richtlinie „Symbol anzeigen“ für das Virtualization Pack für Skype for Business deaktiviert ist. Wenn sie deaktiviert ist, können Sie die Anrufstatistik oder Nachrichten nicht anzeigen.
Show Messages	Zeigt Nachrichten für das Virtualization Pack für Skype for Business an. Diese Richtlinie ist standardmäßig aktiviert. Nachrichten werden nicht angezeigt, wenn die Richtlinie „Symbol anzeigen“ oder die Richtlinie „Nachrichten anzeigen“ für das Virtualization Pack für Skype for Business deaktiviert ist.
Suppress minor version mismatch warning	Im Benachrichtigungsbereich wird eine Warnung angezeigt, wenn das Virtualization Pack für Skype for Business auf dem Horizon Client-System und auf dem Horizon-Desktop nicht über dieselbe API-Nebenversion verfügt. Wenn diese Richtlinie aktiviert ist, wird diese Warnung unterdrückt. Beachten Sie, dass bei Nichtübereinstimmung der API-Nebenversionen Skype for Business-Aufrufe optimiert werden, aber das Virtualization Pack gegebenenfalls nicht über die neuesten Funktionen verfügt.

Richtlinieneinstellungen für VMware Horizon Performance Tracker

Die ADMX-Vorlagendatei des Horizon Performance Tracker (`perf_tracker.admx`) enthält Richtlinieneinstellungen in Bezug auf die VMware Horizon Performance Tracker-Funktion.

Informationen zum Konfigurieren und Verwenden der Horizon Performance Tracker-Funktion finden Sie im Dokument *Horizon 7-Verwaltung*.

Tabelle 5-21. Richtlinieneinstellungen für Horizon Performance Tracker

Einstellung	Beschreibung
Grundeinstellung für Horizon Performance Tracker	Wenn aktiviert, können Sie die Häufigkeit in Sekunden festlegen, in der der Horizon Performance Tracker Daten erfasst.
Automatischen Start von Horizon Performance Tracker in Remote-Desktop-Verbindung aktivieren	Wenn aktiviert, wird der Horizon Performance Tracker automatisch gestartet, wenn sich ein Benutzer bei einer Remote-Desktop-Verbindung anmeldet. Wählen Sie Deaktivieren aus, um diese GPO-Einstellung zu löschen.
Automatischen Start von Horizon Performance Tracker in Remoteanwendungsverbindung aktivieren	Wenn aktiviert, wird der Horizon Performance Tracker automatisch gestartet, wenn sich ein Benutzer bei einer Remoteanwendungsverbindung anmeldet. Wählen Sie Deaktivieren aus, um diese GPO-Einstellung zu löschen.

Richtlinieneinstellungen für den VMware-Integrationsdruck

Die ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (`printerRedirection.admx`) enthält Richtlinieneinstellungen im Zusammenhang mit dem VMware-Integrationsdruck.

Diese Einstellungen finden Sie im Gruppenrichtlinienverwaltungs-Editor im Ordner **Computerkonfiguration > Administrative Vorlagen > VMware-Integrationsdruck**.

Tabelle 5-22. Richtlinieneinstellungen für den VMware-Integrationsdruck

Einstellung	Beschreibung
Disable LBP	Gibt an, ob das standortbasierte Drucken aktiviert ist oder nicht. Wenn diese Einstellung aktiviert ist, ist das standortbasierte Drucken deaktiviert. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist das standortbasierte Drucken aktiviert.
Disable Printer Property Persistence	Geben Sie an, ob die Persistenz der Druckereigenschaften aktiviert ist oder nicht. Wenn diese Einstellung aktiviert ist, sind die Druckereigenschaften zwischen dem lokalen Clientdrucker und dem umgeleiteten Drucker nicht persistent. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, sind die Druckereigenschaften zwischen dem lokalen Clientdrucker und dem umgeleiteten Drucker persistent.
Print Preview Setting	<p>Druckauswahl deaktivieren bestimmt, ob das Druckziel aktiviert ist oder nicht. Sie ist standardmäßig nicht konfiguriert. Wenn diese Option aktiviert ist, kann der Benutzer das Druckziel nicht auswählen. Wenn diese Option deaktiviert oder nicht konfiguriert ist, kann der Benutzer das Druckziel auswählen.</p> <ul style="list-style-type: none"> ■ Direkt drucken : Die standardmäßige Druckoption in der Druck-Benutzeroberfläche ist das direkte Drucken. ■ Druckvorschau: Die standardmäßige Druckoption in der Druck-Benutzeroberfläche ist die Druckvorschau.

Tabelle 5-22. Richtlinieneinstellungen für den VMware-Integrationsdruck (Fortsetzung)

Einstellung	Beschreibung
Printer Driver Selection	<p>Geben Sie den Druckertreiber für den umgeleiteten Clientdrucker, den Universal-Druckertreiber (UPD) oder den nativen Druckertreiber (NPD) an. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ NPD immer verwenden – Der native Druckertreiber wird für den umgeleiteten Drucker verwendet. ■ UPD immer verwenden – Der Universal-Druckertreiber wird für den umgeleiteten Drucker verwendet. ■ Erst NPD, dann UPD verwenden – Es wird zunächst der native Druckertreiber verwendet, und wenn dieser nicht existiert, wird der Universal-Druckertreiber verwendet. ■ Erst UPD, dann NPD verwenden – Es wird zunächst der Universal-Druckertreiber verwendet, und wenn dieser nicht existiert, wird der native Druckertreiber verwendet. <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert Erst NPD, dann UPD verwenden.</p>
Specify a filter in redirecting client printers	<p>Wenn diese Option aktiviert ist, geben Sie eine Filterregel in das Textfeld Name des Registrierungswerts: PrinterFilterString ein. Bei der Filterregel handelt es sich um einen regulären Ausdruck, der angibt, dass der Drucker nicht umgeleitet werden soll (Schwarze Liste). Jeder Drucker, der nicht mit den Druckern in der Filterregel übereinstimmt, wird umgeleitet. Standardmäßig ist die Filterregel leer, was bedeutet, dass alle Clientdrucker umgeleitet werden.</p> <ul style="list-style-type: none"> ■ Attribute: DriverName, VendorName und PrinterName ■ Operatoren: UND, ODER und NICHT ■ Platzhalter: * und ? <p>Beispiele für Filterregeln:</p> <pre>(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e" PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF" PrinterName!=".*PDFCreator.*"</pre>

PCoIP-Richtlinieneinstellungen

Die PCoIP-ADMX-Vorlagendatei (`pcoip.admx`) enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Sie können die Einstellungen entweder mit den Standardwerten konfigurieren, die durch einen Administrator außer Kraft gesetzt werden können, oder die Einstellungen mit nicht überschreibbaren Werten konfigurieren.

Die ADMX-Dateien stehen in `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Die ADMX-Vorlagendatei für PCoIP-Sitzungsvariablen enthält zwei Unterkategorien:

Standardwerte, die durch einen Administrator außer Kraft gesetzt werden können	Legt Standardeinstellungen für PCoIP-Richtlinie fest. Diese Einstellungen können durch einen Administrator außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults geschrieben. Alle diese Einstellungen sind im Ordner Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Overridable Administrator Defaults im Gruppenrichtlinienverwaltungs-Editor enthalten.
Einstellungen, die nicht durch einen Administrator außer Kraft gesetzt werden können	Enthält dieselben Einstellungen wie die erste Unterkategorie, diese Einstellungen können jedoch von einem Administrator nicht außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin geschrieben. Alle diese Einstellungen sind im Ordner Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Not Overridable Administrator Settings im Gruppenrichtlinienverwaltungs-Editor enthalten.

Die Vorlage enthält sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration.

Nicht richtliniengesteuerte Registrierungsschlüssel

Wenn eine Einstellung auf einen lokalen Computer angewendet werden muss, die nicht in HKLM\Software\Policies\Teradici platziert werden kann, können die Einstellungen in Registrierungsschlüsseln unter HKLM\Software\Teradici eingefügt werden. In HKLM\Software\Teradici können dieselben Registrierungsschlüssel platziert werden wie in HKLM\Software\Policies\Teradici. Wenn ein Registrierungsschlüssel in beiden Verzeichnissen angegeben wurde, hat die Einstellung in HKLM\Software\Policies\Teradici Vorrang vor der Einstellung für den lokalen Computer.

Allgemeine PCoIP-Einstellungen

Die PCoIP-ADMX-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, mit denen allgemeine Einstellungen wie PCoIP-Bildqualität, USB-Geräte und Netzwerktops konfiguriert werden.

Alle diese Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Overridable Administrator Defaults** im Gruppenrichtlinienverwaltungs-Editor enthalten.

Alle diese Einstellungen sind auch im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Not Overridable Administrator Settings** im Gruppenrichtlinienverwaltungs-Editor gespeichert.

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen

Einstellung	Beschreibung
Configure PCoIP event log cleanup by size in MB	<p>Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Größe in MB.</p> <p>Wenn diese Richtlinie konfiguriert ist, wird mit dieser Einstellung gesteuert, wie groß eine Protokolldatei vor der Bereinigung werden kann. Protokolldateien größer als m MB werden für eine Einstellung von m ungleich null automatisch und unbeaufsichtigt gelöscht. Die Einstellung 0 gibt an, dass keine Datei-Bereinigung nach Größe durchgeführt wird.</p> <p>Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, beträgt die standardmäßige Ereignisprotokollbereinigung nach Größe 100 MB.</p> <p>Die Bereinigung der Protokolldatei wird einmal beim Sitzungsstart durchgeführt. Eine Änderung an der Einstellung wird erst bei der nächsten Sitzung angewendet.</p>
Configure PCoIP event log cleanup by time in days	<p>Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Zeit in Tagen.</p> <p>Wenn die Richtlinie konfiguriert ist, wird mit dieser Einstellung gesteuert, wie viele Tage vergehen können, bevor die Protokolldatei bereinigt wird. Protokolldateien älter als n Tage werden für eine Einstellung von n ungleich null automatisch und unbeaufsichtigt gelöscht. Die Einstellung 0 gibt an, dass keine Datei-Bereinigung nach Zeit durchgeführt wird.</p> <p>Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, beträgt die standardmäßige Ereignisprotokollbereinigung 7 Tage.</p> <p>Die Bereinigung der Protokolldatei wird einmal beim Sitzungsstart durchgeführt. Eine Änderung an der Einstellung wird erst bei der nächsten Sitzung angewendet.</p>
Configure PCoIP event log verbosity	<p>Legt die Ausführlichkeit der PCoIP-Ereignisprotokolle fest. Sie können einen Wert zwischen 0 (geringste Ausführlichkeit) und 3 (höchste Ausführlichkeit) festlegen.</p> <p>Bei Aktivierung dieser Einstellung können Sie einen Ausführlichkeitsgrad zwischen 0 und 3 festlegen. Wenn die Einstellung nicht konfiguriert oder deaktiviert ist, wird der standardmäßige Ausführlichkeitsgrad 2 verwendet.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure PCoIP image quality levels	<p data-bbox="676 268 1417 390">Steuert die PCoIP-Bilddarstellung während einer Netzwerküberlastung. Das Zusammenspiel der Werte Mindestqualität für Bilder, Maximale anfängliche Bildqualität und Maximale Frame-Rate ermöglicht eine genaue Steuerung in Umgebungen mit begrenzter Netzwerkbandbreite.</p> <p data-bbox="676 401 1417 680">Verwenden Sie den Wert Mindestqualität für Bilder zur Abstimmung von Bildqualität und Frame-Rate, wenn die Bandbreite begrenzt ist. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 40. Ein niedrigerer Wert ermöglicht höhere Frame-Rates, kann jedoch zu einer Beeinträchtigung der Anzeigequalität führen. Ein höherer Wert bietet eine höhere Bildqualität, unter Umständen jedoch niedrigere Frame-Rates, wenn die Netzwerkbandbreite begrenzt ist. Wenn die Netzwerkbandbreite keiner Einschränkung unterliegt, stellt PCoIP unabhängig von diesem Wert eine maximale Qualität sicher.</p> <p data-bbox="676 690 1417 1035">Verwenden Sie die Einstellung Maximale anfängliche Bildqualität, um Spitzen bei der Belegung von Netzwerkbandbreite durch PCoIP zu vermeiden. Beschränken Sie hierzu die anfängliche Qualität der geänderten Bereiche für die Bildanzeige. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 80. Ein niedrigerer Wert verringert die Bildqualität bei Inhaltsänderungen und verhindert Spitzen bei der Bandbreitenbelegung. Ein höherer Wert verbessert die Bildqualität bei Inhaltsänderungen und erhöht die Bandbreitenanforderungen. Die nicht geänderten Bildbereiche erreichen unabhängig von diesem Wert stufenweise eine verlustfreie (perfekte) Qualität. Zur optimalen Nutzung der verfügbaren Bandbreite empfiehlt sich ein Wert von 80 oder niedriger.</p> <p data-bbox="676 1045 1417 1104">Der Wert Mindestqualität für Bilder darf den Wert Maximale anfängliche Bildqualität nicht überschreiten.</p> <p data-bbox="676 1115 1417 1362">Verwenden Sie den Wert Maximale Frame-Rate zur Verwaltung der pro Benutzer durchschnittlich genutzten Bandbreite. Begrenzen Sie dazu die Anzahl der Bildschirmaktualisierungen pro Sekunde. Geben Sie einen Wert zwischen 1 und 120 Frames pro Sekunde an. Der Standardwert beträgt 30. Ein höherer Wert kann mehr Bandbreite belegen, jedoch weniger Jitter verursachen und so weichere Bildübergänge ermöglichen, z.B. bei einem Video. Bei einem geringeren Wert wird weniger Bandbreite belegt, allerdings mehr Jitter verursacht.</p> <p data-bbox="676 1373 1417 1432">Diese Werte für die Bildqualität gelten nur für den Softhost und haben auf einen Softclient keine Auswirkung.</p> <p data-bbox="676 1442 1417 1501">Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, werden die Standardwerte verwendet.</p> <p data-bbox="676 1512 1417 1570">Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure frame rate vs image quality preference	<p>Konfigurieren Sie die Einstellung für die Frame-Rate und die Bildqualität von 0 (höchste Frame-Rate) bis 100 (höchste Bildqualität). Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, beträgt die Standardeinstellung 50.</p> <p>Ein höherer Wert (maximal 100) bedeutet, dass die Bildqualität einen höheren Stellenwert bekommt, auch wenn die Frame-Rate zu einer abgehackten Darstellung führt. Bei einem geringeren Wert (mindestens 0) hat die flüssige Darstellung Vorrang vor der Bildqualität.</p> <p>Diese Einstellung kann in Verbindung mit der Configure PCoIP image quality levels-GPO verwendet werden, die die maximale anfängliche Bildqualität und die Mindestbildqualität festlegt. Mit Frame rate and image quality preference lässt sich die Bildqualität für jeden Frame anpassen. Allerdings sind die Einstellungsmöglichkeiten durch die mit der Configure PCoIP image quality levels-GPO konfigurierten Schwellenwerte für die maximale und Mindestbildqualität begrenzt.</p> <p>Wird diese Richtlinie während der Laufzeit geändert, wird dies sofort wirksam.</p>
Configure PCoIP session encryption algorithms	<p>Steuert die Verschlüsselungsalgorithmen, die vom PCoIP-Endpunkt während der Sitzungs-aushandlung angeboten werden.</p> <p>Durch Aktivierung eines Kontrollkästchens wird der entsprechende Verschlüsselungsalgorithmus deaktiviert. Sie müssen mindestens einen Algorithmus aktivieren.</p> <p>Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Die Endpunkte handeln den tatsächlich verwendeten Algorithmus für die Sitzungsverschlüsselung aus. Wenn der FIPS140-2-validierte Modus aktiviert ist, wird der Wert Disable AES-128-GCM encryption (AES-128-GCM-Verschlüsselung deaktivieren) immer außer Kraft gesetzt, sodass die AES-128-GCM-Verschlüsselung aktiviert wird.</p> <p>Unterstützte Verschlüsselungsalgorithmen sind in der bevorzugten Reihenfolge SALSA20/12-256, AES-GCM-128 und AES-GCM-256. Standardmäßig sind alle unterstützten Verschlüsselungsalgorithmen zur Aushandlung durch diesen Endpunkt verfügbar.</p> <p>Wenn beide Endpunkte für die Unterstützung aller drei Algorithmen konfiguriert sind und die Verbindung kein Sicherheits-Gateway (SG) verwendet, wird der Algorithmus SALSA20 ausgehandelt und verwendet. Wenn die Verbindung dennoch ein SG verwendet, wird SALSA20 automatisch deaktiviert und AES128 wird ausgehandelt und verwendet. Wenn der Endpunkt oder das SG entweder SALSA20 deaktiviert oder der Endpunkt AES128 deaktiviert, wird AES256 ausgehandelt und verwendet.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung								
Configure PCoIP USB allowed and unallowed device rules	<p>Legt fest, welche USB-Geräte für PCoIP-Sitzungen autorisiert oder nicht autorisiert sind, die einen Zero-Client verwenden, der Teradici-Firmware ausführt. In PCoIP-Sitzungen verwendete USB-Geräte müssen in der USB-Autorisierungstabelle aufgeführt sein. USB-Geräte, die in der USB-Ausschlussliste erscheinen, können in PCoIP-Sitzungen nicht verwendet werden.</p> <p>Sie können maximal 10 USB-Autorisierungsregeln und höchstens 10 USB-Ausschlussregeln definieren. Trennen Sie mehrere Regeln durch einen senkrechten Strich () voneinander.</p> <p>Jede Regel kann eine Kombination aus einer Anbieter-ID und einer Produkt-ID sein, oder die Regel beschreibt eine Klasse von USB-Geräten. Eine Klassenregel kann eine gesamte Geräteklasse, eine einzelne Unterklasse oder ein Protokoll innerhalb einer Unterklasse zulassen oder ausschließen.</p> <p>Das Format einer kombinierten Regel aus Anbieter- und Produkt-ID lautet 1xxxxyyy, wobei xxxx die Anbieter-ID im Hexadezimalformat und yyy die Produkt-ID im Hexadezimalformat darstellt. Die Regel zum Zulassen oder Sperren eines Geräts mit der Anbieter-ID 0x1a2b und Produkt-ID 0x3c4d würde beispielsweise 11a2b3c4d lauten.</p> <p>Für Klassenregeln stehen folgende Formate zur Auswahl:</p> <table> <tr> <td>Alle USB-Geräte zulassen</td><td>Format: 23XXXXXX Beispiel: 23XXXXXX</td></tr> <tr> <td>USB-Geräte mit einer bestimmten Klassen-ID zulassen</td><td>Format: 22KlasseXXXX. Beispiel: 22aaXXXX</td></tr> <tr> <td>Eine bestimmte Unterklasse zulassen</td><td>Format: 21Klasse-UnterklasseXX Beispiel: 21aabbXX</td></tr> <tr> <td>Ein bestimmtes Protokoll zulassen</td><td>Format: 20Klasse-Unterklasse-Protokoll Beispiel: 20aabbcc</td></tr> </table> <p>Die Zeichenfolge zur Autorisierung von USB-Eingabegeräten (Maus und Tastatur, Klassen-ID 0x03) und Webcams (Klassen-ID 0x0e) lautet beispielsweise 2203XXXX 220eXXXX. Die Zeichenfolge zum Ausschließen von USB-Massenspeichergeräten (Klassen-ID 0x08) lautet 2208XXXX.</p> <p>Eine leere Zeichenfolge für die USB-Autorisierung bedeutet, dass keine USB-Geräte zugelassen sind. Eine leere Zeichenfolge für den USB-Ausschluss bedeutet, dass für USB-Geräte keine Einschränkungen gelten.</p> <p>Diese Einstellung gilt ausschließlich für Horizon Agent und nur dann, wenn sich der Remote-Desktop in einer Sitzung mit einem Zero-Client befindet, der Teradici-Firmware ausführt. Die Geräteverwendung wird zwischen den Endpunkten ausgehandelt.</p> <p>Standardmäßig sind sämtliche Geräte zugelassen, und es sind keine Geräte ausgeschlossen.</p>	Alle USB-Geräte zulassen	Format: 23XXXXXX Beispiel: 23XXXXXX	USB-Geräte mit einer bestimmten Klassen-ID zulassen	Format: 22KlasseXXXX . Beispiel: 22aaXXXX	Eine bestimmte Unterklasse zulassen	Format: 21Klasse-UnterklasseXX Beispiel: 21aabbXX	Ein bestimmtes Protokoll zulassen	Format: 20Klasse-Unterklasse-Protokoll Beispiel: 20aabbcc
Alle USB-Geräte zulassen	Format: 23XXXXXX Beispiel: 23XXXXXX								
USB-Geräte mit einer bestimmten Klassen-ID zulassen	Format: 22KlasseXXXX . Beispiel: 22aaXXXX								
Eine bestimmte Unterklasse zulassen	Format: 21Klasse-UnterklasseXX Beispiel: 21aabbXX								
Ein bestimmtes Protokoll zulassen	Format: 20Klasse-Unterklasse-Protokoll Beispiel: 20aabbcc								

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure PCoIP virtual channels	<p data-bbox="676 268 1398 352">Gibt die virtuellen Kanäle an, die bei PCoIP-Sitzungen verwendet bzw. nicht verwendet werden können. Diese Einstellung legt auch fest, ob die Zwischenablageverarbeitung auf dem PCoIP-Host deaktiviert wird.</p> <p data-bbox="676 369 1422 489">Virtuelle Kanäle, die in PCoIP-Sitzungen verwendet werden, müssen in der Tabelle der autorisierten virtuellen Kanäle aufgeführt sein. Virtuelle Kanäle, die in der Ausschlussliste für virtuelle Kanäle erscheinen, können in PCoIP-Sitzungen nicht verwendet werden.</p> <p data-bbox="676 506 1406 558">Sie können maximal 15 virtuelle Kanäle zur Verwendung in PCoIP-Sitzungen angeben.</p> <p data-bbox="676 575 1406 659">Trennen Sie mehrere Kanäle durch einen senkrechten Strich () voneinander. Die Zeichenfolge zum Zulassen der virtuellen Kanäle „mksvchan“ und „vdp_rdpvcbridge“ lautet z.B. mksvchan vdp_rdpvcbridge.</p> <p data-bbox="676 676 1398 795">Wenn ein Kanalname einen senkrechten Strich oder einen umgekehrten Schrägstrich (\) enthält, fügen Sie vor dem Kanalnamen einen umgekehrten Schrägstrich ein. Der Kanalname „awk ward\channel“ wird beispielsweise folgendermaßen eingegeben: awk\ ward\channel.</p> <p data-bbox="676 812 1414 896">Ist die Tabelle der autorisierten virtuellen Kanäle leer, ist die Verwendung von virtuellen Kanälen nicht zulässig. Ist die Ausschlusstabelle für virtuelle Kanäle leer, sind alle virtuellen Kanäle zugelassen.</p> <p data-bbox="676 913 1406 997">Die Einstellung der virtuellen Kanäle gilt sowohl für den Agenten als auch für den Client. Zum Verwenden virtueller Kanäle müssen diese sowohl auf dem Agenten als auch auf dem Client aktiviert werden.</p> <p data-bbox="676 1014 1374 1098">Bei Festlegung der virtuellen Kanäle wird ein separates Kontrollkästchen angezeigt, mit dem Sie die Remote-Zwischenablageverarbeitung auf dem PCoIP-Host deaktivieren können. Dieser Wert gilt nur für den Agent.</p> <p data-bbox="676 1115 1334 1167">Standardmäßig sind alle virtuellen Kanäle aktiviert, einschließlich der Zwischenablageverarbeitung.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure the PCoIP transport header	<p data-bbox="676 268 1334 323">Konfiguriert den PCoIP-Übertragungsheader und legt die Priorität der Transportsitzung fest.</p> <p data-bbox="676 338 1406 520">Der PCoIP-Übertragungsheader ist ein 32-Bit-Header, der zu allen PCoIP-UDP-Paketen hinzugefügt wird (sofern der Übertragungsheader auf beiden Seiten aktiviert ist und unterstützt wird). Anhand des PCoIP-Übertragungsheaders können Netzwerkgeräte bei Netzwerkkonflikten eine bessere Priorisierung vornehmen bzw. bessere QoS-Entscheidungen treffen. Der Übertragungsheader ist standardmäßig aktiviert.</p> <p data-bbox="676 535 1406 653">Die Priorität einer Transportsitzung bestimmt die PCoIP-Sitzungspriorität, die im PCoIP-Übertragungsheader angegeben wird. Netzwerkgeräte können basierend auf der angegebenen Priorität einer Transportsitzung eine bessere Priorisierung vornehmen und bessere QoS-Entscheidungen treffen.</p> <p data-bbox="676 667 1406 722">Bei Aktivierung der Einstellung Configure the PCoIP transport header sind die folgenden Prioritäten für eine Transportsitzung verfügbar:</p> <ul style="list-style-type: none"> <li data-bbox="676 737 767 758">■ Hoch <li data-bbox="676 772 916 793">■ Mittel (Standardwert) <li data-bbox="676 808 788 829">■ Niedrig <li data-bbox="676 844 858 865">■ Nicht definiert <p data-bbox="676 879 1406 1129">Der Prioritätswert für die Transportsitzung wird vom PCoIP-Agent und -Client ausgehandelt. Wenn der PCoIP-Agent einen Prioritätswert für die Transportsitzung angibt, wird die vom Agent angegebene Sitzungspriorität für die Sitzung verwendet. Wenn nur auf dem Client eine Priorität für die Transportsitzung angegeben ist, wird die vom Client angegebene Priorität für die Sitzung verwendet. Wenn weder der Agent noch der Client eine Priorität für die Transportsitzung angibt oder der Wert Nicht definiert festgelegt wurde, wird der Standardwert (Mittel) für die Sitzung verwendet.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure the TCP port to which the PCoIP host binds and listens	<p>Gibt den TCP-Agenten-Port für Software-PCoIP-Hosts an.</p> <p>Der Wert des TCP-Ports gibt den TCP-Basisport für die Agentbindungen an. Der TCP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 1 und 10 liegen.</p> <p>Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182.</p> <p>Legen Sie die Größe des Wiederholungs-Portbereichs nicht auf 0 fest. Die Festlegung dieses Wertes auf 0 führt zu einem Verbindungsfehler, wenn sich Benutzer beim Desktop mit dem PCoIP-Anzeigeprotokoll anmelden. Horizon Client generiert die Fehlermeldung Das Anzeigeprotokoll für diesen Desktop steht zurzeit nicht zur Verfügung. Wenden Sie sich an Ihren Systemadministrator.</p> <p>Diese Einstellung gilt nur für Horizon Agent.</p> <p>Der standardmäßige TCP-Basisport auf einzelnen Benutzer-Computern ist 4172 in View 4.5 und höher. Der standardmäßige Basisport ist 50002 in View 4.0.x und früheren Versionen. Der Portbereich lautet standardmäßig 1.</p> <p>Der standardmäßige TCP-Basisport ist auf RDS-Hosts 4173. Wenn PCoIP mit RDS-Hosts verwendet wird, wird für jede Benutzerverbindung ein separater PCoIP-Port verwendet. Der standardmäßige Portbereich, der vom Remote-Desktop-Dienst festgelegt wird, ist groß genug, um die maximal erwartete Anzahl von parallelen Benutzerverbindungen unterzubringen.</p> <hr/> <p>Wichtig Es hat sich bewährt, diese Richtlinieneinstellung nicht zu verwenden, um den standardmäßigen Portbereich auf RDS-Hosts zu ändern, oder den TCP-Portwert vom Standardwert 4173 zu ändern. Vor allem ist der TCP-Portwert nicht auf 4172 festzulegen. Das Zurücksetzen dieses Wertes auf 4172 wirkt sich negativ auf die PCoIP-Leistung in RDS-Sitzungen aus.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure the UDP port to which the PCoIP host binds and listens	<p>Gibt den UDP-Agenten-Port für Software-PCoIP-Hosts an.</p> <p>Der Wert des UDP-Ports gibt den UDP-Basisport für die Agentbindung an. Der Wert für den UDP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 1 und 10 liegen.</p> <p>Legen Sie die Größe des Wiederholungs-Portbereichs nicht auf 0 fest. Die Festlegung dieses Wertes auf 0 führt zu einem Verbindungsfehler, wenn sich Benutzer beim Desktop mit dem PCoIP-Anzeigeprotokoll anmelden. Horizon Client generiert die Fehlermeldung Das Anzeigeprotokoll für diesen Desktop steht zurzeit nicht zur Verfügung. Wenden Sie sich an Ihren Systemadministrator.</p> <p>Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182. Diese Einstellung gilt nur für Horizon Agent.</p> <p>Der standardmäßige UDP-Basisport auf einzelnen Benutzer-Computern ist 4172 für View 4.5 und höher bzw. 50002 für View 4.0.x und früher. Der Portbereich lautet standardmäßig 10.</p> <p>Der standardmäßige UDP-Basisport ist auf RDS-Hosts 4173. Wenn PCoIP mit RDS-Hosts verwendet wird, wird für jede Benutzerverbindung ein separater PCoIP-Port verwendet. Der standardmäßige Portbereich, der vom Remote-Desktop-Dienst festgelegt wird, ist groß genug, um die maximal erwartete Anzahl von parallelen Benutzerverbindungen unterzubringen.</p> <hr/> <p>Wichtig Es hat sich bewährt, diese Richtlinieneinstellung nicht zu verwenden, um den standardmäßigen Portbereich auf RDS-Hosts zu ändern, oder den UDP-Portwert vom Standardwert 4173 zu ändern. Vor allem ist der UDP-Portwert nicht auf 4172 festzulegen. Das Zurücksetzen dieses Wertes auf 4172 wirkt sich negativ auf die PCoIP-Leistung in RDS-Sitzungen aus.</p>
Enable access to a PCoIP session from a vSphere console	<p>Legt fest, ob in einer vSphere Client-Konsole die Anzeige einer aktiven PCoIP-Sitzung und das Senden von Eingaben an den Desktop gestattet werden soll.</p> <p>Standardmäßig zeigt der Bildschirm der vSphere Client-Konsole nichts an, wenn ein Client über PCoIP verbunden ist, und die Konsole kann keine Eingaben senden. Diese Standardeinstellung verhindert, dass ein anderer Benutzer den Desktop des Benutzers anzeigen kann oder mit böswilligen Absichten lokal am Host Eingaben vornimmt, während eine PCoIP-Remote-Sitzung aktiv ist.</p> <p>Diese Einstellung gilt nur für Horizon Agent.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist ein Konsolenzugriff nicht zulässig. Wenn diese Einstellung aktiviert ist, zeigt die Konsole die PCoIP-Sitzung an und eine Konsoleneingabe ist zulässig.</p> <p>Wenn diese Einstellung aktiviert ist, kann die Konsole nur dann eine PCoIP-Sitzung anzeigen, die mit einem Windows 7-System ausgeführt wird, wenn die virtuelle Maschine für Windows 7 mit Hardware v8 arbeitet. Hardware v8 ist nur für ESXi 5.0 und neuere Versionen verfügbar. Im Gegensatz hierzu sind Konsoleneingaben in ein Windows 7-System für alle Hardwareversionen der virtuellen Maschinen zulässig.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Enable/disable audio in the PCoIP session	<p>Legt fest, ob die Audiofunktion während PCoIP-Sitzungen aktiviert ist. Die Audiofunktion muss für beide Endpunkte aktiviert sein. Ist diese Einstellung aktiviert, ist die Verwendung von PCoIP-Audio zulässig. Wurde diese Einstellung deaktiviert, kann die PCoIP-Audiofunktion nicht verwendet werden. Wurde diese Einstellung nicht konfiguriert, ist die Audiofunktion standardmäßig aktiviert.</p>
Enable/disable microphone noise and DC offset filter in PCoIP session	<p>Legt fest, ob Mikrofongeräusche und der Gleichstrom-Offset-Filter für die Mikrofoneingabe während der PCoIP-Sitzung aktiviert werden sollen. Diese Einstellung gilt nur für Horizon Agent und den Teradici-Audiotreiber. Wenn diese Einstellung nicht konfiguriert ist, verwendet der Teradici-Audiotreiber standardmäßig die Mikrofongeräusche und den Gleichstrom-Offset-Filter.</p>
Turn on PCoIP user default input language synchronization	<p>Legt fest, ob die Standardeingabesprache des Benutzers in der PCoIP-Sitzung mit der standardmäßigen Eingabesprache des PCoIP-Clientendpunktes synchronisiert wird. Wenn diese Einstellung aktiviert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung nicht erlaubt. Diese Einstellung gilt nur für Horizon Agent.</p>
Configure SSL Connections to satisfy Security Tools	<p>Legt fest, wie Verbindungen mit SSL-Sitzungsaushandlung aufgebaut werden. Um Port-Scanner korrekt verwenden zu können, aktivieren Sie diese Einstellung „SSL-Verbindungen konfigurieren“ und schließen Sie auf Horizon Agent die folgenden Aufgaben ab:</p> <ol style="list-style-type: none"> 1 Speichern Sie in Microsoft Management Console (MMC) ein korrekt benanntes und signiertes Zertifikat im persönlichen Informationsspeicher für das Computerkonto des lokalen Computers und stellen Sie sicher, dass es exportiert werden kann. 2 Speichern Sie das Zertifikat für die Zertifizierungsstelle, die es signiert hat, im Zertifikatspeicher für vertrauenswürdige Stammzertifikate. 3 Deaktivieren Sie Verbindungen mit VMware View 5.1 und früher. 4 Konfigurieren Sie Horizon Agent zum Laden von Zertifikaten aus dem Zertifikatspeicher. Wenn der persönliche Informationsspeicher für den lokalen Computer verwendet wird, belassen Sie die Namen der Zertifikatspeicher bei „MY“ und „ROOT“ (ohne Anführungszeichen), solange in Schritt 1 und 2 kein anderer Speicherort verwendet wurde. <p>Der sich daraus ergebende PCoIP-Server ermöglicht eine korrekte Verwendung von Security Tools wie z. B. Port-Scanner.</p>

Tabelle 5-23. Allgemeine PCoIP-Richtlinieneinstellungen (Fortsetzung)

Einstellung	Beschreibung
Configure SSL Protocols	<p>Konfiguriert das OpenSSL-Protokoll, um die Verwendung bestimmter Protokolle zu unterbinden, bevor eine verschlüsselte SSL-Verbindung hergestellt wird. Die Protokollliste besteht aus mindestens einer durch Doppelpunkte getrennten OpenSSL-Protokollzeichenfolge. Beachten Sie, dass für alle Verschlüsselungszeichenfolgen die Groß-/Kleinschreibung zu beachten ist.</p> <p>Der Standardwert lautet: „TLS1.1:TLS1.2“.</p> <p>Dies bedeutet, dass sowohl TLS v1.1 als auch TLS v1.2 aktiviert sind (SSL v2.0, SSLv3.0 und TLS v1.0 sind deaktiviert).</p> <p>Diese Einstellung gilt sowohl für Horizon Agent als auch für Horizon Client.</p> <p>Wenn dies auf beiden Seiten so festgelegt ist, wird die Regel für die OpenSSL-Protokollaushandlung angewendet.</p>
Configure SSL cipher list	<p>Konfiguriert die SSL-Verschlüsselungsliste, um die Verwendung der Verschlüsselungssammlungen zu beschränken, bevor eine verschlüsselte SSL-Verbindung hergestellt wird. Die Verschlüsselungsliste besteht aus einer oder mehreren Zeichenfolgen der Verschlüsselungs-Suite, die durch Doppelpunkte voneinander getrennt werden. Bei allen Zeichenfolgen der Verschlüsselungssammlung muss die Groß- und Kleinschreibung beachtet werden.</p> <p>Der Standardwert lautet: ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH.</p> <p>Wenn diese Einstellung konfiguriert ist, wird das Kontrollkästchen AES-256 oder stärkere Verschlüsselungen für die Aushandlung der SSL-Verbindung erzwingen in der Einstellung SSL-Verbindungen konfigurieren, um Security Tools korrekt zu verwenden zu können ignoriert.</p> <p>Diese Einstellung muss sowohl auf den PCoIP Server wie auf den PCoIP Client angewendet werden.</p>

PCoIP-Zwischenablagen- und Drag & Drop-Einstellungen

Die Horizon-PCoIP-ADMX-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, mit der die Zwischenablageeinstellungen für das Kopieren und Einfügen bzw. für das Ziehen und Ablegen mit der Maus konfiguriert werden.

Alle diese Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Overridable Administrator Defaults** im Gruppenrichtlinienverwaltungs-Editor enthalten.

Alle diese Einstellungen sind auch im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Not Overridable Administrator Settings** im Gruppenrichtlinienverwaltungs-Editor gespeichert.

Tabelle 5-24. PCoIP-Richtlinieneinstellungen für die Zwischenablage

Einstellung	Beschreibung
Configure clipboard audit	<p data-bbox="676 268 1423 352">Gibt an, ob die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer aktiviert ist. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> <li data-bbox="676 369 1230 426">■ In beiden Richtungen deaktiviert – Informationen zu Zwischenablagendaten werden nicht aufgezeichnet. <li data-bbox="676 438 1423 525">■ Aktiviert, nur Client zu Server – Informationen zu Zwischenablagendaten, die vom Client auf den Agent-Computer kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. <li data-bbox="676 537 1423 657">■ In beiden Richtungen aktiviert – Informationen zu Zwischenablagendaten, die vom Client auf den Agent-Computer und vom Agent-Computer auf den Client kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. <li data-bbox="676 669 1423 756">■ Aktiviert, nur Server zu Client – Informationen zu Zwischenablagendaten, die vom Agent-Computer auf den Client kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. <p data-bbox="676 770 1350 827">Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist standardmäßig der Wert In beiden Richtungen deaktiviert festgelegt.</p> <p data-bbox="676 840 1414 989">Sie können das Ereignisprotokoll mit der Windows-Ereignisanzeige auf dem Agent-Computer anzeigen. Der Protokollname ist „VMware Horizon RX-Überwachung“. Um das Ereignisprotokoll in einem zentralisierten Speicherort anzuzeigen, können Sie VMware Log Insight oder die Windows-Ereignissammlung konfigurieren.</p> <p data-bbox="676 1003 1401 1123">Bei Windows-Clients wird die Überwachung der Zwischenablage von Agent-Computer auf Client in Horizon Client 4.9 oder höher unterstützt. Bei allen Clients wird die Überwachung der Zwischenablage von Client Computer auf Agent-Computer in Horizon Client 4.10 oder höher unterstützt.</p> <hr/> <p data-bbox="676 1148 1318 1205">Hinweis Nur der Windows-Client unterstützt die Überwachung der Zwischenablage von Agent-Computer auf Client.</p>
Configure clipboard memory size on server	<p data-bbox="676 1239 1401 1325">Legt den Wert der Größe des Zwischenablagespeichers des Servers in Byte oder Kilobyte wie ausgewählt fest. Die Speichergröße wird in Kilobyte angegeben, wenn sie nicht konfiguriert ist.</p> <p data-bbox="676 1339 1423 1488">Der Client verfügt ebenfalls über einen Wert für die Größe des Zwischenablagespeichers, der immer in Kilobyte angegeben wird. Nach dem Einrichten der Sitzung sendet der Server seinen Zwischenspeichergrößenwert an den Client. Der effektive Zwischenspeichergrößenwert entspricht dem kleineren Wert des Zwischenablagespeichers von Client und Server.</p> <p data-bbox="676 1503 1423 1652">Diese Einstellung gilt nur für Windows-, Linux- und Mac-Clients, auf denen Horizon Client 4.1 oder höher installiert ist, und für iOS-Clients, auf denen Horizon Client 4.7 oder höher installiert ist. In früheren Versionen ist die Größe des Zwischenablagespeichers auf 1 MB festgelegt und kann nicht konfiguriert werden.</p> <hr/> <p data-bbox="676 1677 1401 1797">Hinweis Ein hoher Wert für die Größe des Zwischenablagespeichers kann sich je nach verwendetem Netzwerk negativ auf die Leistung auswirken. VMware empfiehlt für die maximale Größe des Zwischenablagespeichers einen Wert von 16 MB.</p>

Tabelle 5-24. PCoIP-Richtlinieneinstellungen für die Zwischenablage (Fortsetzung)

Einstellung	Beschreibung
Configure clipboard redirection	<p>Bestimmt die Richtung, in der die Zwischenablagenumleitung zulässig ist. Sie können einen der folgenden Werte auswählen:</p> <ul style="list-style-type: none"> ■ Nur Client zu Agent aktiviert ■ In beiden Richtungen deaktiviert ■ In beiden Richtungen aktiviert ■ Nur Agent zu Client aktiviert <p>Die Zwischenablagenumleitung wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert die Zwischenablagenumleitung nicht.</p> <p>Diese Einstellung gilt nur für Horizon Agent.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert Nur Client zu Agent aktiviert.</p>
Configure drag and drop direction	<p>Bestimmt die Richtung, in der „Drag & Drop“ zulässig ist. Bei Aktivierung sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ In beiden Richtungen deaktiviert ■ Nur Client zu Agent aktiviert. Ermöglicht Drag & Drop nur vom Clientsystem an den Agent. ■ Nur Agent zu Client aktiviert. Ermöglicht Drag & Drop nur vom Agent an das Clientsystem. ■ In beiden Richtungen aktiviert <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert Nur Client zu Agent aktiviert.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>
Configure drag and drop formats	<p>Legt fest, welche Drag & Drop-Richtung (In beiden Richtungen deaktiviert, Nur Agent zu Client aktiviert, Nur Client zu Agent aktiviert oder In beiden Richtungen aktiviert) für das jeweilige Datenformat zulässig ist. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ Option für Dateiformat ■ Option für Textformat ■ Option für Rich-Text-Format ■ Option für Image-Format ■ Option für HTML-Format ■ Option für Dateiinhaltsformat <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist standardmäßig der Wert In beiden Richtungen aktiviert für alle Formate festgelegt.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>

Tabelle 5-24. PCoIP-Richtlinieneinstellungen für die Zwischenablage (Fortsetzung)

Einstellung	Beschreibung
Configure drag and drop size threshold	<p>Bestimmt die Größenbeschränkung für das Ziehen allgemeiner Datentypen, die nicht Dateien oder Ordner sind.</p> <p>Wenn diese Einstellung aktiviert ist, wählen Sie die Einheit für die Größe der Daten zum Ziehen aus der aus. Wählen Sie die Einheit des Dropdown-Menüs für die Drag & Drop-Größe aus. Sie können Byte, Kilobyte oder Megabyte auswählen. Wählen Sie die Größe der Daten zum Ziehen im Textfeld Drag & Drop-Größenschwellenwert aus oder geben Sie diese ein. Der effektive Datenbereich für jede Einheit lautet wie folgt:</p> <ul style="list-style-type: none"> ■ Byte: 1 bis 1023 ■ Kilobyte: 1 bis 1023 ■ Megabyte: 1 bis 16 (maximale Datengröße für Drag & Drop beträgt 16 Megabyte) <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird der Schwellenwert von 1 Megabyte verwendet.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>
Filter text out of the incoming clipboard data	<p>Legt fest, ob Textdaten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>Legt fest, ob RTF-Daten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>
Filter images out of the incoming clipboard data	<p>Legt fest, ob Bilddaten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>Legt fest, ob Daten im Microsoft Office-Textformat (BIFF12-Format) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>Legt fest, ob Microsoft Office-Diagrammdaten und Smart Art-Daten (Art::GVML ClipFormat) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>Legt fest, ob Daten mit Microsoft Office-Texteffekten (HTML-Format) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.</p>

Tabelle 5-24. PCoIP-Richtlinieneinstellungen für die Zwischenablage (Fortsetzung)

Einstellung	Beschreibung
Filter text out of the outgoing clipboard data	Legt fest, ob Textdaten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Rich Text Format data out of the outgoing clipboard data	Legt fest, ob RTF-Daten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter images out of the outgoing clipboard data	Legt fest, ob Bilddaten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Office text data out of the outgoing clipboard data	Legt fest, ob Daten im Microsoft Office-Textformat (BIFF12-Format) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	Legt fest, ob Microsoft Office-Diagrammdaten und Smart Art-Daten (Art::GVML ClipFormat) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Text Effects data out of the outgoing clipboard data	Legt fest, ob Daten mit Microsoft Office-Texteffekten (HTML-Format) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Whether block clipboard redirection to client side when client doesn't support audit	<p>Legt fest, ob die Zwischenablagenumleitung zu Clients blockiert wird, wenn diese die Überwachungsfunktion für die Zwischenablage nicht unterstützen. Wenn diese Einstellung aktiviert ist, müssen Sie einen der folgenden Werte auswählen.</p> <ul style="list-style-type: none"> ■ Blockieren – Blockiert die Umleitung der Zwischenablage vom Agent zum Client, wenn die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer unterstützt wird, jedoch nicht auf dem Client-Computer. ■ Passthrough – Erlaubt die Umleitung der Zwischenablage vom Agent zum Client, wenn die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer unterstützt wird, jedoch nicht auf dem Client-Computer. <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird der Standardwert Blockieren verwendet.</p> <p>Damit diese Einstellung wirksam wird, müssen Sie die Gruppenrichtlinieneinstellung <code>Configure clipboard audit</code> aktivieren.</p>

Einstellungen für die PCoIP-Bandbreite

Die Horizon-PCoIP-ADMX-Vorlagendatei enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Bandbreitenmerkmalen.

Alle diese Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Overridable Administrator Defaults** im Gruppenrichtlinienverwaltungs-Editor enthalten.

Alle diese Einstellungen sind auch im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Not Overridable Administrator Settings** im Gruppenrichtlinienverwaltungs-Editor gespeichert.

Tabelle 5-25. Horizon-PCoIP-Sitzungsbandbreitenvariablen

Einstellung	Beschreibung
Configure the maximum PCoIP session bandwidth	<p>Legt die maximale Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und PCoIP-Steuerung eingeschlossen.</p> <p>Legen Sie diesen Wert auf die Gesamtkapazität der Verbindung fest, über die Ihr Endpunkt verbunden ist, und berücksichtigen Sie dabei die Anzahl der erwarteten gleichzeitigen PCoIP-Sitzungen. Beispiel: Legen Sie diesen Wert bei einer Einzelbenutzer-VDI-Konfiguration (eine einzelne PCoIP-Sitzung), die über eine Internetverbindung mit 4 MBit/s verbunden ist, auf 4 MBit oder auf 90 % dieses Werts fest, um etwas Spielraum für anderen Netzwerkdatenverkehr zu lassen. Wenn Sie erwarten, dass sich mehrere gleichzeitige PCoIP-Sitzungen, die entweder mehrere VDI-Benutzer oder eine RDS-Konfiguration umfassen, einen Link teilen, können Sie die Einstellung entsprechend anpassen. Durch eine Senkung dieses Werts wird jedoch die maximale Bandbreite für jede aktive Sitzung beschränkt.</p> <p>Durch eine Festlegung dieses Werts verhindern Sie, dass der Agent eine die Verbindungskapazität übersteigende Übertragungsrate wählt – was zu einem übermäßigen Paketverlust und einem schlechteren Benutzererlebnis führen würde. Dieser Wert ist symmetrisch. Client und Agent werden gezwungen, den niedrigeren der beiden Werte zu verwenden, die auf Client- und Agentseite festgelegt sind. Beispielsweise wird der Agent bei Festlegung einer maximalen Bandbreite von 4 MBit/s gezwungen, eine niedrigere Übertragungsrate zu verwenden – auch wenn die Einstellung auf dem Client konfiguriert ist.</p> <p>Wenn diese Einstellung deaktiviert wurde oder auf einem Endpunkt nicht konfiguriert ist, legt der Endpunkt keine Bandbreiteneinschränkungen fest. Wenn diese Einstellung konfiguriert ist, wird sie als maximale Bandbreiteneinschränkung des Endpunkts in KBit/s verwendet.</p> <p>Der Standardwert für die nicht konfigurierte Einstellung liegt bei 900000 KBit/s. Diese Einstellung gilt sowohl für Horizon Agent als auch für den Client. Haben die beiden Endpunkte unterschiedliche Einstellungen, wird der niedrigere Wert verwendet.</p>
Configure the PCoIP session bandwidth floor	<p>Legt die Mindestbandbreite in Kilobits pro Sekunde fest, die von der PCoIP-Sitzung reserviert wird.</p> <p>Mit dieser Einstellung wird die minimale erwartete Bandbreitenübertragungsrate für den Endpunkt konfiguriert. Wenn Sie diese Einstellung zum Reservieren der Bandbreite für einen Endpunkt verwenden, muss der Benutzer nicht warten, bis Bandbreite verfügbar ist, was die Reaktionszeit während der Sitzung verbessert.</p> <p>Achten Sie jedoch darauf, dass Sie allen Endpunkten gemeinsam nicht mehr Bandbreite zuweisen, als insgesamt zur Verfügung steht. Die Summe der Mindestbandbreitenwerte für alle Verbindungen in Ihrer Konfiguration darf die Netzwerkkapazität nicht überschreiten.</p> <p>Der Standardwert lautet 0, d.h. es wird keine Mindestbandbreite reserviert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird keine Mindestbandbreite reserviert.</p> <p>Diese Einstellung gilt sowohl für Horizon Agent als auch für den Client, wirkt sich allerdings nur auf den Endpunkt aus, für den sie konfiguriert wurde.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p>

Tabelle 5-25. Horizon-PCoIP-Sitzungsbandbreitenvariablen (Fortsetzung)

Einstellung	Beschreibung
Configure the PCoIP session MTU	<p>Legt die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung fest.</p> <p>Die MTU-Größe umfasst den IP- und UDP-Paketvorspann. TCP verwendet den standardmäßigen MTU-Ermittlungsmechanismus zum Festlegen der maximalen Übertragungseinheit und wird von dieser Einstellung nicht beeinflusst.</p> <p>Die maximale MTU-Größe beträgt 1.500 Byte. Die minimale MTU-Größe beträgt 500 Byte. Der Standardwert lautet 1.300 Byte.</p> <p>Normalerweise muss die MTU-Größe nicht geändert werden. Ändern Sie diesen Wert, wenn Sie in einer nicht standardmäßig eingerichteten Netzwerkumgebung arbeiten, die zu einer PCoIP-Paketfragmentierung führt.</p> <p>Diese Einstellung gilt sowohl für Horizon Agent als auch für den Client. Unterscheiden sich die MTU-Größeneinstellungen der beiden Endpunkte, wird der niedrigere Wert verwendet.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, verwendet der Client bei der Aushandlung mit Horizon Agent den Standardwert.</p>

Tabelle 5-25. Horizon-PCoIP-Sitzungsbandbreitenvariablen (Fortsetzung)

Einstellung	Beschreibung
Configure the PCoIP session audio bandwidth limit	<p>Legt die maximale Bandbreite fest, die in einer PCoIP-Sitzung für Audiodaten (Soundwiedergabe) verwendet werden kann.</p> <p>Der Audioprozessor überwacht die für Audiodaten verwendete Bandbreite. Er wählt auch den Algorithmus zur Audiokomprimierung, der bei der aktuellen Bandbreitennutzung die bestmögliche Audioqualität liefert. Wenn ein Bandbreitenlimit festgelegt wurde, reduziert der Audioprozessor durch einen Wechsel des Komprimierungsalgorithmus so lange die Qualität, bis das Bandbreitenlimit erreicht ist. Wenn die minimale Audioqualität mit dem festgelegten Bandbreitenlimit nicht erreicht werden kann, wird die Audiofunktion deaktiviert.</p> <p>Stellen Sie diesen Wert höher als 1.600 KBit/s ein, um Audiodaten nicht zu komprimieren und eine hohe Stereo-Qualität zu erzielen. Ein Wert ab 450 KBit/s bietet Stereo-Qualität mit komprimierten Audiodaten. Ein Wert zwischen 50 KBit/s und 450 KBit/s liefert eine Audioqualität, die zwischen einem UKW-Radio und einem Telefongespräch liegt. Bei einem Wert unter 50 KBit/s ist unter Umständen keine Audiowiedergabe mehr möglich.</p> <p>Diese Einstellung gilt nur für Horizon Agent. Diese Einstellung wird erst wirksam, wenn Sie die Audiofunktion an beiden Endpunkten aktivieren. Zudem hat diese Einstellung keinerlei Auswirkungen auf USB-Audio.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird standardmäßig ein Bandbreitenlimit von 500 KBit/s konfiguriert, um den ausgewählten Algorithmus für die Audiokomprimierung zu begrenzen. Bei Konfiguration dieser Einstellung wird der Wert in KBit/s gemessen, mit einem standardmäßigen Audiobandbreitenlimit von 500 KBit/s.</p> <p>Diese Einstellung gilt für View 4.6 und höhere Versionen. Bei früheren View-Versionen hat diese Einstellung keine Auswirkung.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p>
Turn off Build-to-Lossless feature	<p>Legt fest, ob die Build-to-Lossless-Funktion des PCoIP-Protokolls aktiviert oder deaktiviert werden soll. Diese Funktion ist standardmäßig deaktiviert.</p> <p>Wenn diese Einstellung aktiviert wurde oder nicht konfiguriert ist, ist die Build-to-Lossless-Funktion deaktiviert und Bilder sowie andere Desktop- und Anwendungsinhalte werden nie zu einem verlustfreien Anzeigestadium aufgebaut. In Netzwerkumgebungen mit begrenzter Bandbreite kann die Deaktivierung der Build-to-Lossless-Funktion Einsparungen bei der Bandbreite ermöglichen.</p> <p>Wenn diese Einstellung deaktiviert wurde, ist die Build-to-Lossless-Funktion aktiviert. Das Aktivieren dieser Funktion wird für Umgebungen, in denen ein Aufbau von Bildern und Desktop-Inhalten zu einem verlustfreien Anzeigestadium erforderlich ist, nicht empfohlen.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p> <p>Weitere Informationen über die PCoIP-Build-to-Lossless-Funktion finden Sie unter PCoIP Build-to-Lossless-Funktion.</p>

PCoIP-Tastatureinstellungen

Die View-PCoIP-ADMX-Vorlagendatei enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Einstellungen, die sich auf die Verwendung der Tastatur auswirken.

Alle diese Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Overridable Administrator Defaults** im Gruppenrichtlinienverwaltungs-Editor enthalten.

Alle diese Einstellungen sind auch im Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > PCoIP Session Variables > Not Overridable Administrator Settings** im Gruppenrichtlinienverwaltungs-Editor gespeichert.

Tabelle 5-26. Horizon-PCoIP-Sitzungsvariablen für die Tastatur

Einstellung	Beschreibung
Disable sending CAD when users press Ctrl+Alt+Del	<p>Wenn diese Richtlinie aktiviert ist, müssen Benutzer anstelle der Tastenkombination Strg+Alt+Entf die Tastenkombination Strg+Alt+Einfg drücken, um während einer PCoIP-Sitzung einen Sicherheitsaufruf (SAS) an den Remote-Desktop zu senden.</p> <p>Sie können diese Einstellung aktivieren, um eine Verwirrung der Benutzer zu vermeiden, wenn diese zum Sperren des Clientendpunktes Strg+Alt+Entf drücken, und sowohl an den Host als auch an den Gast ein Sicherheitsaufruf gesendet wird.</p> <p>Diese Einstellung gilt nur für Horizon Agent und hat keine Auswirkung auf einen Client.</p> <p>Wenn diese Richtlinie nicht konfiguriert ist oder deaktiviert wurde, können Benutzer die Tastenkombination Strg+Alt+Entf oder Strg+Alt+Einfg drücken, um einen Sicherheitsaufruf an den Remote-Desktop zu senden.</p>
Use alternate key for sending Secure Attention Sequence	<p>Gibt eine alternative Taste (anstelle der Einfg-Taste) zum Senden eines Sicherheitsaufrufs (Secure Attention Sequence, SAS) an.</p> <p>Sie können mit dieser Einstellung die Tastenkombination Strg+Alt+Einfg in virtuellen Maschinen beibehalten, die während einer PCoIP-Sitzung aus einem Remote-Desktop gestartet werden.</p> <p>Beispielsweise kann ein Benutzer eine vSphere Client-Instanz aus einem PCoIP-Desktop starten und auf einer virtuellen Maschine in vCenter Server eine Konsole öffnen. Wenn die Tastenkombination Strg+Alt+Einfg im Gastbetriebssystem auf der virtuellen vCenter Server-Maschine verwendet wird, wird ein Strg+Alt+Entf-Sicherheitsaufruf an die virtuelle Maschine gesendet. Diese Einstellung ermöglicht, dass mit der Tastenkombination Strg+Alt+<i>Alternative Taste</i> ein Strg+Alt+Entf-Sicherheitsaufruf an den PCoIP-Desktop gesendet wird.</p> <p>Wenn diese Einstellung aktiviert ist, müssen Sie eine alternative Taste aus einem Dropdown-Menü auswählen. Es ist nicht möglich, die Einstellung zu aktivieren und keinen Wert anzugeben.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird die Tastenkombination Strg+Alt+Einfg zum Senden eines Sicherheitsaufrufs verwendet.</p> <p>Diese Einstellung gilt nur für Horizon Agent und hat keine Auswirkung auf einen Client.</p>

PCoIP Build-to-Lossless-Funktion

Sie können das PCoIP-Anzeigeprotokoll so konfigurieren, dass es eine Kodierungsmethode namens „Progressive Build“ (Progressiver Aufbau oder Build-to-Lossless) verwendet, die auf die Gewährleistung einer optimalen allgemeinen Benutzerumgebung selbst unter eingeschränkten Netzwerkbedingungen abzielt. Diese Funktion ist standardmäßig deaktiviert.

Die Build-to-Lossless-Funktion bietet ein hochgradig komprimiertes Erstbild, auch „verlustbehaftetes Bild“ genannt, welches dann stufenweise zu einem vollständig verlustfreien Anzeigestadium erweitert wird. Unter einem „verlustfreien Stadium“ versteht man, dass das Bild mit der beabsichtigten Originaltreue angezeigt wird.

In einem LAN zeigt PCoIP Text immer unter Verwendung der verlustfreien Komprimierung an. Ist die Build-to-Lossless-Funktion aktiviert und sinkt die verfügbare Bandbreite pro Sitzung auf unter 1 MBit/s, zeigt PCoIP zuerst ein verlustbehaftetes Textbild an und baut das Bild dann innerhalb kürzester Zeit zu einem verlustfreien Anzeigestadium auf. Durch diese Vorgehensweise kann der Desktop weiterhin reagieren und auch bei wechselnden Netzwerkbedingungen das bestmögliche Bild anzeigen, was zu einer optimalen Benutzererfahrung führt.

Die Build-to-Lossless-Funktion verfügt über folgende Leistungsmerkmale:

- Dynamische Anpassung der Bildqualität
- Verringerung der Bildqualität in überlasteten Netzwerken
- Aufrechterhaltung der Reaktionsfähigkeit durch Minimierung der Wartezeiten bei der Bildschirmaktualisierung
- Wiederaufnahme der maximalen Bildqualität nach Beheben der Netzwerküberlastung

Sie können die Funktion „Build-to-Lossless“ aktivieren, indem Sie die Gruppenrichtlinieneinstellung Turn off Build-to-Lossless feature deaktivieren. Siehe [Einstellungen für die PCoIP-Bandbreite](#).

Richtlinieneinstellungen für VMware Blast

Die VMware Blast-ADMX-Vorlagendatei `vdm_blast.admx` enthält Richtlinieneinstellungen für das VMware Blast-Anzeigeprotokoll. Wenn die Richtlinie angewendet wird, werden die Einstellungen im Registrierungsschlüssel `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config` gespeichert.

Diese Einstellungen gelten für HTML Access und alle Horizon Client-Plattformen.

Tabelle 5-27. Richtlinieneinstellungen für VMware Blast

Einstellung	Beschreibung
Audio playback	Legt fest, ob die Audiowiedergabe für Remote-Desktops aktiviert ist. Mit dieser Einstellung kann die Audiowiedergabe aktiviert werden.
Clipboard memory size on server	<p>Legt den Wert der Größe des Zwischenablagenspeichers des Servers in Byte oder Kilobyte wie ausgewählt fest. Die Speichergröße wird in Kilobyte angegeben, wenn sie nicht konfiguriert ist. Der Client verfügt ebenfalls über einen Wert für die Größe des Zwischenablagenspeichers, der immer in Kilobyte angegeben wird. Nach dem Einrichten der Sitzung sendet der Server seinen Zwischenspeichergrößenwert an den Client. Der effektive Zwischenspeichergrößenwert entspricht dem kleineren Wert des Zwischenablagenspeichers von Client und Server.</p> <p>Bei Windows-Clients wird die Überwachung der Zwischenablage von Agent-Computer auf Client in Horizon Client 4.9 oder höher unterstützt. Bei allen Clients wird die Überwachung der Zwischenablage von Client Computer auf Agent-Computer in Horizon Client 4.10 oder höher unterstützt.</p> <p>Hinweis Nur der Windows-Client unterstützt die Überwachung der Zwischenablage von Agent-Computer auf Client.</p>
Configure clipboard audit	<p>Gibt an, ob die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer aktiviert ist. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ In beiden Richtungen deaktiviert – Informationen zu Zwischenablagendaten werden nicht aufgezeichnet. ■ Aktiviert, nur Client zu Server – Informationen zu Zwischenablagendaten, die vom Client auf den Agent-Computer kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. ■ In beiden Richtungen aktiviert – Informationen zu Zwischenablagendaten, die vom Client auf den Agent-Computer und vom Agent-Computer auf den Client kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. ■ Aktiviert, nur Server zu Client – Informationen zu Zwischenablagendaten, die vom Agent-Computer auf den Client kopiert werden, werden in einem Ereignisprotokoll auf dem Agent-Computer aufgezeichnet. <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist standardmäßig der Wert In beiden Richtungen deaktiviert festgelegt.</p> <p>Hinweis Nur der Windows-Client unterstützt die Überwachung der Zwischenablage von Agent-Computer auf Client Computer. Alle anderen Clients unterstützen nur die Überwachung der Zwischenablage von Client Computer auf Agent-Computer.</p> <p>Sie können das Ereignisprotokoll mit der Windows-Ereignisanzeige auf dem Agent-Computer anzeigen. Der Protokollname ist „VMware Horizon RX-Überwachung“. Um das Ereignisprotokoll in einem zentralisierten Speicherort anzuzeigen, können Sie VMware Log Insight oder die Windows-Ereignissammlung konfigurieren.</p>
Configure clipboard redirection	<p>Legt das zulässige Verhalten der Zwischenablageumleitung fest. Es stehen folgende Optionen zur Auswahl:</p> <ul style="list-style-type: none"> ■ In beiden Richtungen aktiviert ■ In beiden Richtungen deaktiviert ■ Aktiviert, nur Client zu Server ■ Aktiviert, nur Server zu Client <p>Standardmäßig ist Nur Client zu Server aktiviert eingestellt.</p>

Tabelle 5-27. Richtlinienereinstellungen für VMware Blast (Fortsetzung)

Einstellung	Beschreibung
Configure drag and drop direction	<p>Bestimmt die Richtung, in der „Drag & Drop“ zulässig ist. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ In beiden Richtungen deaktiviert ■ Nur Client zu Agent aktiviert. Ermöglicht Drag & Drop nur vom Clientsystem an den Agent. ■ Nur Agent zu Client aktiviert. Ermöglicht Drag & Drop nur vom Agent an das Clientsystem. ■ In beiden Richtungen aktiviert <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert Nur Client zu Agent aktiviert.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>
Configure drag and drop formats	<p>Legt fest, welche Drag & Drop-Richtung (In beiden Richtungen deaktiviert, Nur Agent zu Client aktiviert, Nur Client zu Agent aktiviert oder In beiden Richtungen aktiviert) für das jeweilige Datenformat zulässig ist. Wenn diese Einstellung aktiviert ist, sind die Optionen wie folgt:</p> <ul style="list-style-type: none"> ■ Option für Dateiformat ■ Option für Textformat ■ Option für Rich-Text-Format ■ Option für Image-Format ■ Option für HTML-Format ■ Option für Dateiinhaltsformat <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist standardmäßig der Wert In beiden Richtungen aktiviert für alle Formate festgelegt.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>
Configure drag and drop size threshold	<p>Bestimmt die Größenbeschränkung für das Ziehen allgemeiner Datentypen, die nicht Dateien oder Ordner sind.</p> <p>Wenn diese Einstellung aktiviert ist, wählen Sie die Einheit für die Größe der Daten zum Ziehen aus der aus. Wählen Sie die Einheit des Dropdown-Menüs für die Drag & Drop-Größe aus. Sie können Byte, Kilobyte oder Megabyte auswählen. Wählen Sie die Größe der Daten zum Ziehen im Textfeld Drag & Drop-Größenschwellenwert aus oder geben Sie diese ein. Der effektive Datenbereich für jede Einheit lautet wie folgt:</p> <ul style="list-style-type: none"> ■ Byte: 1 bis 1023 ■ Kilobyte: 1 bis 1023 ■ Megabyte: 1 bis 16 (maximale Datengröße für Drag & Drop beträgt 16 Megabyte) <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird der Schwellenwert von 1 Megabyte verwendet.</p> <p>Diese Einstellung gilt nur für den Agenten.</p>
Configure file transfer	<p>Legt das zulässige Verhalten für die Dateiübertragung zwischen einem Remote-Desktop und dem HTML Access-Client fest. Sie können einen der folgenden Werte auswählen:</p> <ul style="list-style-type: none"> ■ Upload und Download deaktiviert ■ Upload und Download aktiviert ■ Nur Dateiapload aktiviert (Benutzer können Dateien nur vom Clientsystem zum Remote-Desktop hochladen.) ■ Nur Dateidownload aktiviert (Benutzer können Dateien nur vom Remote-Desktop zum Clientsystem herunterladen.) <p>Die Standardeinstellung ist Nur Dateidownload aktiviert.</p> <p>Diese Einstellung gilt nur für HTML Access 4.1 und höher.</p>

Tabelle 5-27. Richtlinieneinstellungen für VMware Blast (Fortsetzung)

Einstellung	Beschreibung
Cookie Cleanup Interval	Legt in Millisekunden fest, wie oft Cookies, die mit der inaktiven Sitzung verbunden sind, gelöscht werden. Die Standardeinstellung beträgt 100 ms.
DSCP Marking	<p>Wenn diese Einstellung aktiviert oder nicht konfiguriert ist, wird die Angabe von Differentiated Services Code Point-(DSCP-)Werten im ausgehenden Netzwerkdatenverkehr von Blast ermöglicht, gemäß den verschiedenen individuellen Einstellungen für jeden Netzwerk-Hop. Wenn deaktiviert, werden keine DSCP-Werte im Blast-Netzwerkverkehr eingerichtet.</p> <p>Wenn aktiviert, können Sie für die folgenden Netzwerkverbindungen einen numerischen Wert zwischen 0 und 63 festlegen:</p> <ul style="list-style-type: none"> ■ DSCP from Agent, TCP/IPv4 ■ DSCP from Agent, TCP/IPv6 ■ DSCP from Agent, UDP/IPv4 ■ DSCP from Agent, UDP/IPv6 ■ DSCP from BSG to Client, TCP/IPv4 ■ DSCP from BSG to Client, TCP/IPv6 ■ DSCP from BSG to Client, UDP/IPv4 ■ DSCP from BSG to Client, UDP/IPv6 ■ DSCP from BSG to Agent, TCP/IPv4 ■ DSCP from BSG to Agent, TCP/IPv6 ■ DSCP from BSG to Agent, UDP/IPv4 ■ DSCP from BSG to Agent, UDP/IPv6 ■ DSCP from Client, TCP/IPv4 ■ DSCP from Client, TCP/IPv6 ■ DSCP from Client, UDP/IPv4 ■ DSCP from Client, UDP/IPv6
Filter images out of the incoming clipboard data	Legt fest, ob Bilddaten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter images out of the outgoing clipboard data	Legt fest, ob Bilddaten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	Legt fest, ob Microsoft Office-Diagrammdaten und Smart Art-Daten (Art::GVML ClipFormat) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	Legt fest, ob Microsoft Office-Diagrammdaten und Smart Art-Daten (Art::GVML ClipFormat) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.

Tabelle 5-27. Richtlinieneinstellungen für VMware Blast (Fortsetzung)

Einstellung	Beschreibung
Filter Microsoft Office text data out of the incoming clipboard data	Legt fest, ob Daten im Microsoft Office-Textformat (BIFF12-Format) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Office text data out of the outgoing clipboard data	Legt fest, ob Daten im Microsoft Office-Textformat (BIFF12-Format) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Text Effects data out of the incoming clipboard data	Legt fest, ob Daten mit Microsoft Office-Texteffekten (HTML-Format) aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Microsoft Text Effects data out of the outgoing clipboard data	Legt fest, ob Daten mit Microsoft Office-Texteffekten (HTML-Format) aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Rich Text Format data out of the incoming clipboard data	Legt fest, ob RTF-Daten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter Rich Text Format data out of the outgoing clipboard data	Legt fest, ob RTF-Daten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter text out of the incoming clipboard data	Legt fest, ob Textdaten aus den vom Client an den Agent übergebenen Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
Filter text out of the outgoing clipboard data	Legt fest, ob Textdaten aus den vom Agent an den Client gesendeten Zwischenablagendaten herausgefiltert werden. Wenn diese Einstellung aktiviert ist und das Kontrollkästchen aktiviert wird, werden die Daten herausgefiltert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, sind die Daten zulässig.
H264	Legt fest, ob die H.264- oder die JPEG/PNG-Codierung verwendet wird. Standardmäßig ist die H.264-Codierung eingestellt.
H264 High Color Accuracy	Erhöht die Farbgenauigkeit bei Verwendung der H.264-Codierung mithilfe des YUV-4:4:4-Farbraums anstelle von 4:2:0. Durch diese Einstellung kann die Leistung bei sehr hohen Auflösungen oder bei der Verwendung mehrerer Bildschirme absinken.

Tabelle 5-27. Richtlinieneinstellungen für VMware Blast (Fortsetzung)

Einstellung	Beschreibung
H.264 Quality	<p>Legt die Bildqualität fest, die für die Remote-Anzeige für die H.264-Codierung konfiguriert ist. Sie können Mindest- und Höchstwerte angeben, die festlegen, wie stark ein Bild für eine verlustfreie Komprimierung geregelt wird. Sie können einen Mindestwert für die beste Bildqualität angeben. Sie können einen Höchstwert für die geringste Bildqualität angeben. Sie können die folgenden Einstellungen festlegen:</p> <ul style="list-style-type: none"> ■ H264maxQP (verfügbarer Wertebereich: 0-51, Standard: 36) ■ H264minQP (verfügbarer Wertebereich: 0-51, Standard: 10) <p>Legen Sie für die beste Bildqualität für den Quantisierungsparameter (QP) Werte innerhalb von +5 oder -5 des verfügbaren Wertebereichs fest. Diese Parameter bestimmen den Umfang der Daten, die verworfen werden, weshalb ein niedrigerer Wert zu einer höheren Bildqualität führt.</p>
HEVC	Aktivieren Sie diese Einstellung oder konfigurieren Sie sie nicht, um die HEVC-Kodierung für das Remoting des Desktops zuzulassen. Deaktivieren Sie diese Einstellung, um H.264 oder JPEG/PNG für die Kodierung zu verwenden.
HTTP Service	Legt den Port für eine sichere Kommunikation (HTTPS) zwischen dem Sicherheitsserver oder der Access Point-Appliance und einem Desktop fest. In der Konfiguration der Firewall muss dieser Port geöffnet sein. Die Standardeinstellung ist 22443.
Image Quality	<p>Legt die Bildqualität für die Remote-Anzeige fest. Sie können zwei Einstellungen für eine niedrige Qualität, zwei für eine hohe Qualität und eine für eine mittlere Qualität angeben. Die Einstellungen für eine niedrige Bildqualität sind für Bereiche gedacht, die sich häufig ändern, z. B. durch einen Bildlauf. Die Einstellungen für eine hohe Bildqualität sind für eher statische Bereiche sinnvoll. Sie können die folgenden Einstellungen festlegen:</p> <ul style="list-style-type: none"> ■ Niedrige JPEG-Qualität (verfügbarer Wertebereich: 10–100, Standard: 25) ■ Mittlere JPEG-Qualität (verfügbarer Wertebereich: 10–100, Standard: 35) ■ Hohe JPEG-Qualität (verfügbarer Wertebereich: 10–100, Standard: 90)
Keyboard locale synchronization	<p>Gibt an, ob die Tastaturgebietsschemaliste eines Clients und ein standardmäßiges Gebietsschema mit dem Remote-Desktop oder der -Anwendung synchronisiert wird. Wenn diese Einstellung aktiviert ist, erfolgt die Synchronisierung. Diese Einstellung gilt nur für Horizon Agent.</p> <p>Hinweis Diese Funktion wird nur für Horizon Client für Windows unterstützt.</p>
Max Frame Rate	Legt die maximale Rate der Bildschirmaktualisierungen fest. Mit dieser Einstellung steuern Sie die durchschnittliche Bandbreite, die Benutzer in Anspruch nehmen. Die Standardeinstellung beträgt 30 Aktualisierungen pro Sekunde.
Max Session Bandwidth	Legt die maximale Bandbreite für eine VMware Blast-Sitzung in Kilobits pro Sekunde (KBit/s) fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und VMware Blast-Steuerung eingeschlossen. Die Standardeinstellung beträgt 1 GBit/s.
Max Session Bandwidth kbit/s Megapixel Slope	Legt in Kilobits pro Sekunde (KBit/s) die maximale Bandbreite fest, die für eine VMware Blast-Sitzung reserviert wird. Der Mindestwert ist 100. Der Maximalwert ist 100000. Der Standardwert ist 6200.
Min Session Bandwidth	Legt in Kilobits pro Sekunde (KBit/s) die Mindestbandbreite fest, die für eine VMware Blast-Sitzung reserviert wird. Die Standardeinstellung beträgt 256 KBit/s.
PNG	Wenn Sie diese Einstellung aktivieren oder nicht konfigurieren, ist die PNG-Codierung für Remotesitzungen verfügbar. Wenn Sie diese Einstellung deaktivieren, wird für eine Kodierung im JPEG/PNG-Modus nur die JPEG-Kodierung verwendet. Diese Richtlinie ist nicht gültig, wenn der H.264-Encoder aktiviert ist. Diese Einstellung ist standardmäßig nicht konfiguriert.

Tabelle 5-27. Richtlinieneinstellungen für VMware Blast (Fortsetzung)

Einstellung	Beschreibung
Screen Blanking	Legt fest, ob in der Konsole der Desktop-VM der jeweils vom Benutzer verwendete Desktop oder ein leerer Bildschirm angezeigt wird, wenn der Desktop über eine aktive Sitzung verfügt. Standardmäßig ist der Bildschirm leer.
UDP Protocol	Legt fest, ob das UDP- oder das TCP-Protokoll verwendet wird. Standardmäßig wird das UDP-Protokoll verwendet. Diese Einstellung erfordert einen Neustart der Horizon Agent-Maschine, auf der der registrierte Schlüssel vorhanden ist. Diese Einstellung gilt nicht für HTML Access. Hierfür wird immer das TCP-Protokoll verwendet.
Whether block clipboard redirection to client side when client doesn't support audit	<p>Legt fest, ob die Zwischenablagenumleitung zu Client-Computern blockiert wird, wenn diese die Überwachungsfunktion für die Zwischenablage nicht unterstützen.</p> <p>Wenn diese Einstellung aktiviert ist, müssen Sie einen der folgenden Werte auswählen.</p> <ul style="list-style-type: none"> ■ Blockieren – Blockiert die Umleitung der Zwischenablage vom Agent zum Client, wenn die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer unterstützt wird, jedoch nicht auf dem Client-Computer. ■ Passthrough – Erlaubt die Umleitung der Zwischenablage vom Agent zum Client, wenn die Überwachungsfunktion für die Zwischenablage auf dem Agent-Computer unterstützt wird, jedoch nicht auf dem Client-Computer. <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird der Standardwert Blockieren verwendet.</p> <p>Damit diese Einstellung wirksam wird, müssen Sie die Gruppenrichtlinieneinstellung <code>Configure clipboard audit</code> aktivieren.</p>

Anwenden von Richtlinieneinstellungen für VMware Blast

Wenn sich die folgenden VMware Blast-Richtlinien während einer Client-Sitzung ändern, ermittelt Horizon Client die Änderung und wendet sofort die neue Einstellung an.

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

Für alle anderen VMware Blast-Richtlinien gelten die Microsoft-GPO-Aktualisierungsregeln. GPOs können manuell oder durch das Neustarten der Horizon Agent-Maschine aktualisiert werden. Weitere Informationen dazu finden Sie in der Microsoft-Dokumentation.

Aktivieren der verlustfreien Komprimierung für VMware Blast

Sie können das VMware Blast-Anzeigeprotokoll aktivieren, um einen als „Progressive Build“ oder „Build-to-Lossless“ bezeichneten Codierungsansatz zu verwenden. Diese Funktion bietet ein hochgradig komprimiertes Erstbild, auch „verlustbehaftetes Bild“ genannt, welches dann stufenweise zu einem vollständig verlustfreien Anzeigestadium erweitert wird. Unter einem „verlustfreien Stadium“ versteht man, dass das Bild mit der beabsichtigten Originaltreue angezeigt wird.

Legen Sie zum Aktivieren der verlustfreien Komprimierung für VMware Blast den Schlüssel EncoderBuildToPNG auf 1 im Ordner HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config in der Windows-Registrierung auf dem Agentencomputer fest. Der Standardwert lautet 0 (deaktiviert). Der Codec wird demnach nicht als PNG erstellt, wobei es sich um ein verlustfreies Format handelt.

Konfigurationsänderungen am Schlüssel EncoderBuildToPNG erfolgen sofort.

Hinweis Durch die Aktivierung der verlustfreien Komprimierung für VMware Blast werden die Bandbreite und CPU-Auslastung erhöht. VMware empfiehlt die Verwendung des PCoIP-Anzeigeprotokolls anstelle von VMware Blast, wenn für Sie die verlustfreie Komprimierung erforderlich ist. Informationen über das Konfigurieren der verlustfreien Komprimierung für PCoIP finden Sie unter [PCoIP Build-to-Lossless-Funktion](#).

Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste

Sie können Gruppenrichtlinien für Remote-Desktop-Dienste (RDS) verwenden, um die Konfiguration und Leistung von RDS-Hosts sowie veröffentlichten Desktop- und Anwendungssitzungen zu steuern. Horizon 7 stellt eine ADMX-Datei bereit, die Microsoft-RDS-Gruppenrichtlinien enthält, die in Horizon 7 unterstützt werden.

Es hat sich bewährt, die Gruppenrichtlinien, die in der ADMX-Datei von Horizon 7 bereitgestellt werden, anstatt entsprechender Microsoft-Gruppenrichtlinien zu konfigurieren. Die Horizon 7-Gruppenrichtlinien sind für die Unterstützung Ihrer Horizon 7-Bereitstellung zertifiziert.

Kompatibilitätseinstellungen für Remote-Desktop-Dienstanwendungen

Die Gruppenrichtlinieneinstellungen zur Kompatibilität der RDS-Anwendung steuern die Kompatibilität des Windows-Installationsprogramms, die IP-Virtualisierung des Remote-Desktops, die Auswahl des Netzwerkadapters und die Verwendung der IP-Adresse des RDS-Hosts.

Tabelle 5-28. Gruppenrichtlinieneinstellungen zur Kompatibilität der RDS-Anwendung

Einstellung	Beschreibung
Turn off Windows Installer RDS Compatibility	<p>Die Richtlinieneinstellung legt fest, ob die RDS-Kompatibilität des Windows-Installationsprogramms für vollständig installierte Anwendungen auf Benutzerbasis ausgeführt wird. Das Windows-Installationsprogramm lässt das Ausführen von jeweils nur einer Instanz des <code>msiexec</code>-Prozesses zu. Standardmäßig ist die RDS-Kompatibilität des Windows-Installationsprogramms eingeschaltet. Wenn Sie diese Richtlinieneinstellung aktivieren, ist die RDS-Kompatibilität des Windows-Installationsprogramms ausgeschaltet. Zudem kann jeweils nur eine Instanz des <code>msiexec</code>-Prozesses ausgeführt werden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die RDS-Kompatibilität des Windows-Installationsprogramms eingeschaltet, und mehrere Anforderungen zur Anwendungsinstallation pro Benutzer werden in die Warteschlange eingereiht sowie vom <code>msiexec</code>-Prozess in der Reihenfolge des Erhalts behandelt.</p>
Turn on Remote Desktop IP Virtualization	<p>Diese Richtlinieneinstellung legt fest, ob die IP-Virtualisierung des Remote-Desktops eingeschaltet wird.</p> <p>Standardmäßig wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die IP-Virtualisierung des Remote-Desktops eingeschaltet. Sie können den Modus auswählen, in dem die Einstellung angewendet wird. Wenn Sie den Modus „Pro Programm“ verwenden, müssen Sie für die Verwendung virtueller IP-Adressen eine Liste von Programmen eingeben. Listen Sie jedes Programm in einer separaten Zeile auf (geben Sie keine leeren Zeilen zwischen Programmen ein). Beispiel:</p> <div data-bbox="794 1213 941 1266" style="background-color: #f0f0f0; padding: 5px;"> <pre>explorer.exe mstsc.exe</pre> </div> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet.</p>

Tabelle 5-28. Gruppenrichtlinieneinstellungen zur Kompatibilität der RDS-Anwendung (Fortsetzung)

Einstellung	Beschreibung
Select the network adapter to be used for Remote Desktop IP Virtualization	<p>Diese Richtlinieneinstellung legt die IP-Adress- und Netzwerkmaske fest, die dem Netzwerkadapter entspricht, der für die virtuellen IP-Adressen verwendet wird. Die IP-Adress- und Netzwerkmaske muss in der Notierung „Klassenloses domänenübergreifendes Routing“ eingegeben werden. Beispiel: 192.0.2.96/24.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die angegebene IP-Adress- und Netzwerkmaske verwendet, um den Netzwerkadapter für die virtuellen IP-Adressen auszuwählen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet. Ein Netzwerkadapter muss konfiguriert werden, damit die IP-Virtualisierung des Remote-Desktops funktioniert.</p>
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	<p>Die Richtlinieneinstellung legt fest, ob eine Sitzung die IP-Adresse des RDS-Hosts verwendet, wenn keine virtuelle IP-Adresse verfügbar ist.</p> <p>Wenn Sie die Richtlinieneinstellung aktivieren, wird die IP-Adresse des RDS-Hosts nicht verwendet, wenn keine virtuelle IP-Adresse verfügbar ist. Die Sitzung verfügt über keine Netzwerkverbindung.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Adresse des RDS-Hosts verwendet, wenn keine virtuelle IP-Adresse verfügbar ist.</p>

Einstellungen für Remote-Desktop-Dienstverbindungen

Mit Gruppenrichtlinieneinstellungen für RDS-Verbindungen können Benutzer Richtlinien für Verbindungen mit Sitzungen auf RDS-Hosts festlegen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Verbindungen** gespeichert.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind auch im Ordner **Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Verbindungen** gespeichert.

Tabelle 5-29. Gruppenrichtlinieneinstellungen für RDS-Verbindungen

Einstellung	Beschreibung
Automatic reconnection	<p>Legt fest, ob es für Remotedesktopverbindungs-Clients zulässig ist, automatisch eine erneute Verbindung mit Sitzungen auf einem RDS-Host herzustellen, wenn deren Netzwerkverbindung vorübergehend unterbrochen ist. Standardmäßig wird maximal 20-mal in Intervallen von fünf Sekunden versucht, erneut eine Verbindung herzustellen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird für alle Clients, die die Remotedesktopverbindung ausführen, automatisch versucht, erneut eine Verbindung herzustellen, wenn deren Netzwerkverbindung unterbrochen ist.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, wird die automatische Herstellung einer erneuten Verbindung verhindert.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird die automatische Herstellung einer erneuten Verbindung nicht auf Gruppenrichtlinienebene festgelegt. Benutzer können allerdings die automatische Herstellung einer erneuten Verbindung mithilfe des Kontrollkästchens Erneut verbinden bei unterbrochener Verbindung auf der Registerkarte Optionen der Remotedesktopverbindung konfigurieren.</p>
Allow users to connect remotely using Remote Desktop Services	<p>Diese Richtlinieneinstellung konfiguriert den Remotezugriff auf Computer mithilfe der Remotedesktopdienste (RDS, Remote Desktop Services).</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Benutzer, die Mitglieder der Gruppe der Remote-Desktop-Benutzer auf dem Zielcomputer sind, mithilfe der Remotedesktopdienste remote eine Verbindung mit dem Zielcomputer herstellen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, haben Benutzer nicht die Möglichkeit, mithilfe der Remotedesktopdienste remote eine Verbindung mit dem Zielcomputer herzustellen. Der Zielcomputer erhält dann alle aktuellen Verbindungen aufrecht, akzeptiert aber keine neuen eingehenden Verbindungen.</p>

Tabelle 5-29. Gruppenrichtlinieneinstellungen für RDS-Verbindungen (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, bestimmen die Remotedesktopdienste mit der Remote-Desktop-Einstellung auf dem Zielcomputer, ob eine Remoteverbindung zulässig ist. Diese Einstellung ist auf der Registerkarte Remote im Dialogfeld Systemeigenschaften enthalten. Standardmäßig ist keine Remoteverbindung zulässig.</p> <hr/> <p>Hinweis Sie können festlegen, welche Clients die Möglichkeit haben, mithilfe der Remotedesktopdienste remote eine Verbindung herzustellen. Dazu konfigurieren Sie die Richtlinieneinstellung „Benutzerauthentifizierung mit Authentifizierung auf Netzwerkebene ist für Remoteverbindungen erforderlich“ im Ordner Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sicherheit. Sie können die Anzahl der Benutzer begrenzen, die die Möglichkeit haben, gleichzeitig eine Verbindung herzustellen. Dazu konfigurieren Sie die Option „Maximale Anzahl an Verbindungen“ auf der Registerkarte Netzwerkadapter im Konfigurationstool für Remotedesktop-Sitzungshosts oder die Richtlinieneinstellung „Anzahl der Verbindungen einschränken“ im Ordner Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Verbindungen.</p>
Deny logoff of an administrator logged in to the console session	<p>Diese Richtlinieneinstellung legt fest, ob ein Administrator, der versucht, eine Remoteverbindung mit der Konsole eines Servers herzustellen, einen Administrator abmelden kann, der aktuell bei der Konsole angemeldet ist.</p> <p>Diese Richtlinie ist hilfreich, wenn der aktuell verbundene Administrator nicht möchte, dass er von einem anderen Administrator abgemeldet wird. Wenn der aktuell verbundene Administrator abgemeldet wird, gehen alle zuvor nicht gespeicherten Daten verloren.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist das Abmelden des verbundenen Administrators nicht zulässig.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist das Abmelden des verbundenen Administrators erlaubt.</p> <hr/> <p>Hinweis Die Konsolensitzung wird auch als „Sitzung 0“ bezeichnet. Der Konsolenzugriff kann mithilfe des <code>/console</code>-Switch von der Remotedesktopverbindung im Feld „Computername“ oder von der Befehlszeile aus durchgeführt werden.</p>

Tabelle 5-29. Gruppenrichtlinieneinstellungen für RDS-Verbindungen (Fortsetzung)

Einstellung	Beschreibung
Configure keep-alive connection interval	<p>Diese Richtlinieneinstellung ermöglicht Ihnen die Eingabe eines Keep-alive-Intervalls, um sicherzustellen, dass der Sitzungsstatus auf dem RDS-Host dem Clientstatus entspricht.</p> <p>Wenn die Verbindung eines Clients mit einem RDS-Host unterbrochen ist, bleibt die Sitzung auf dem RDS-Host eventuell aktiv und wechselt nicht in den Status „Getrennt“, auch wenn der Client physisch vom RDS-Host getrennt wurde. Wenn sich der Client wieder beim selben RDS-Host anmeldet, wird eventuell eine neue Sitzung eingerichtet (wenn der RDS-Host für mehrere Sitzungen konfiguriert ist), und die ursprüngliche Sitzung ist eventuell weiterhin aktiv.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie ein Keep-alive-Intervall eingeben. Das Keep-alive-Intervall legt in Minuten fest, wie oft der Server den Sitzungsstatus prüft. Es können Werte von 1 bis 999.999 eingegeben werden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird kein Keep-alive-Intervall festgelegt, und der Server prüft den Sitzungsstatus nicht.</p>
Limit number of connections	<p>Legt fest, ob für Remotedesktopdienste (RDS, Remote Desktop Services) die Anzahl der gleichzeitigen Verbindungen mit dem Server beschränkt ist.</p> <p>Sie haben mit dieser Einstellung die Möglichkeit, die Anzahl der Remotedesktopdienste-Sitzungen zu begrenzen, die auf einem Server aktiv sein können. Wird dieser Wert überschritten, erhalten weitere Benutzer, die versuchen, eine Verbindung herzustellen, die Fehlermeldung, dass der Server beschäftigt ist und sie es später noch einmal versuchen sollen. Durch Begrenzung der Anzahl der Sitzungen lässt sich die Leistung verbessern, da weniger Sitzungen weniger Systemressourcen in Anspruch nehmen. Standardmäßig ist für RDS-Hosts eine unbegrenzte Anzahl an Remotedesktopdienste-Sitzungen zulässig. Mit „Remote Desktop for Administration“ sind zwei Remotedesktopdienste-Sitzungen möglich.</p> <p>Wenn Sie diese Einstellung verwenden, geben Sie die Anzahl an Verbindungen ein, die maximal für den Server zulässig sein sollen. Wenn die Anzahl an Verbindungen nicht beschränkt werden soll, geben Sie 999999 ein.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die maximale Anzahl an Verbindungen auf den angegebenen Wert begrenzt, der der Windows-Version und dem Modus der Remotedesktopdienste (RDS, Remote Desktop Services), die auf dem Server ausgeführt werden, entspricht.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Anzahl der Verbindungen nicht auf Gruppenrichtlinienebene verbindlich festgelegt.</p> <p>Hinweis Diese Einstellung ist für die Verwendung auf RDS-Hosts vorgesehen. Dabei handelt es sich um Server mit dem Windows-Betriebssystem und installiertem Remotedesktop-Sitzungshost-Rollendienst.</p>

Tabelle 5-29. Gruppenrichtlinieneinstellungen für RDS-Verbindungen (Fortsetzung)

Einstellung	Beschreibung
Set rules for remote control of Remote Desktop Services user sessions	<p>Mit dieser Richtlinieneinstellung können Sie die Ebene der Remotesteuerung festlegen, die in einer Remotedesktopdienstesitzung zulässig ist.</p> <p>Mit dieser Richtlinieneinstellung lassen sich zwei Ebenen der Remotesteuerung festlegen: „Sitzung anzeigen“ oder „Vollzugriff“. „Sitzung anzeigen“ ermöglicht dem Benutzer der Remotesteuerung das Beobachten einer Sitzung. Mit „Vollzugriff“ kann der Administrator interaktiv bei der Sitzung eingreifen. Die Remotesteuerung kann mit oder ohne Benutzerberechtigung eingerichtet werden.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Administratoren remote interaktiv auf die Remotedesktopdienstesitzung eines Benutzers den festgelegten Regeln entsprechend zugreifen. Zur Festlegung dieser Regeln wählen Sie die gewünschte Ebene der Steuerung und der Berechtigung in der Liste „Optionen“ aus. Um die Remotesteuerung zu deaktivieren, wählen Sie „Keine Remotesteuerung zulässig“ aus.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden die Regeln für die Remotesteuerung durch die Einstellung auf der Registerkarte Remotesteuerung im Konfigurationstool für Remotedesktop-Sitzungshosts festgelegt. Standardmäßig verfügen Benutzer der Remotesteuerung über einen kompletten Zugriff auf die Sitzung entsprechend der Benutzerberechtigung.</p> <p>Hinweis Diese Richtlinieneinstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Richtlinieneinstellungen konfiguriert sind, hat die Richtlinie der Computerkonfiguration Vorrang.</p>
Restrict Remote Desktop Services users to a single Remote Desktop Services session	<p>Mit dieser Richtlinieneinstellung können Sie Benutzer auf eine einzelne Remotedesktopdienstesitzung beschränken.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird der Zugriff von Benutzern, die sich remote mithilfe der Remotedesktopdienste anmelden, auf eine einzige Sitzung (aktiv oder getrennt) auf diesem Server beschränkt. Wenn der Benutzer die Sitzung in einem getrennten Status verlässt, wird der Benutzer bei der nächsten Anmeldung automatisch erneut mit dieser Sitzung verbunden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, können Benutzer unbegrenzt gleichzeitige Remoteverbindungen mithilfe der Remotedesktopdienste herstellen.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, legt die Einstellung „Nur eine Sitzung pro Benutzer zulassen“ im Konfigurationstool für Remotedesktop-Sitzungshosts fest, ob Benutzer auf nur auf eine Remotedesktopdienstesitzung beschränkt werden sollen.</p>

Tabelle 5-29. Gruppenrichtlinieneinstellungen für RDS-Verbindungen (Fortsetzung)

Einstellung	Beschreibung
Allow remote start of unlisted programs	<p>Diese Richtlinieneinstellung bietet Ihnen die Möglichkeit, festzulegen, ob Remotebenutzer beliebige Programme auf einem RDS-Host aufrufen können, wenn sie eine Remotedesktopdienste-Sitzung starten, oder ob sie nur Programme aufrufen können, die in der Liste „RemoteApp-Programme“ aufgeführt sind.</p> <p>Sie können steuern, welche Programme auf einem RDS-Host sich remote starten lassen, indem Sie mithilfe des Tools „RemoteApp Manager“ eine entsprechende Liste von RemoteApp-Programmen erstellen. Standardmäßig können nur Programme aus der Liste „RemoteApp-Programme“ aufgerufen werden, wenn ein Benutzer eine Remotedesktopdienste-Sitzung startet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Remotebenutzer beliebige Programme auf einem RDS-Host aufrufen, wenn sie eine Remotedesktopdienste-Sitzung starten. Ein Benutzer kann beispielsweise durch Angabe des Ausführungspaths des Programms ein beliebiges Programm zum Zeitpunkt der Verbindung mithilfe des Remotedesktopverbindungs-Clients aufrufen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Remotebenutzer nur Programme aufrufen, in der Liste „RemoteApp-Programme“ im RemoteApp Manager aufgeführt sind, wenn sie eine Remotedesktopdienste-Sitzung starten.</p>
Turn off Fair Share CPU Scheduling	<p>Die gleichmäßige CPU-Planung verteilt die Prozessorzeit dynamisch auf alle Remotedesktopdienste-Sitzungen auf dem RDS-Host, basierend auf der Anzahl der Sitzungen und ihrem jeweiligen Bedarf an Prozessorzeit.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die gleichmäßige CPU-Planung deaktiviert.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist die gleichmäßige CPU-Planung aktiviert.</p>

Einstellungen zur Umleitung von RDS-Geräten und Ressourcen

Die Gruppenrichtlinieneinstellungen zur Umleitung von Remote-Desktop-Dienste-Geräten und Ressourcen steuern die Geräte und Ressourcen auf einem Clientcomputer in RDS-Sitzungen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Geräte- und Ressourcenumleitung** gespeichert.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind auch im Ordner **Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Geräte- und Ressourcenumleitung** gespeichert.

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen

Einstellung	Beschreibung
Allow audio and video playback redirection	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob Benutzer die Audio- und Videoausgabe eines Remotecomputers in einer Remotedesktopdienste-Sitzung weiterleiten können.</p> <p>Benutzer haben die Möglichkeit, festzulegen, wo die Audioausgabe des Remotecomputers wiedergegeben wird. Dazu müssen sie die Remoteaudioeinstellungen auf der Registerkarte „Lokale Ressourcen“ in der Remotedesktopverbindung (Remote Desktop Connection, RDC) konfigurieren. Benutzer können wählen, ob das Remoteaudio auf dem Remotecomputer oder auf dem lokalen Computer ausgeführt werden soll. Außerdem haben Benutzer die Möglichkeit, auszuwählen, dass das Audio nicht wiedergegeben wird. Die Videowiedergabe kann mithilfe der Einstellung „videoplayback“ in einer RDP-Datei (Remotedesktopprotokoll) konfiguriert werden. Standardmäßig ist die Videowiedergabe aktiviert.</p> <p>Standardmäßig ist eine Umleitung der Audio- und Videowiedergabe nicht zulässig, wenn eine Verbindung mit einem Computer hergestellt wird, auf dem Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003 ausgeführt wird. Die Umleitung der Audio- und Videowiedergabe ist standardmäßig zulässig, wenn eine Verbindung mit einem Computer hergestellt wird, auf dem Windows 7, Windows Vista oder Windows XP Professional ausgeführt wird.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die Umleitung der Audio- und Videowiedergabe zulässig.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, ist die Umleitung der Audio- und Videowiedergabe nicht zulässig, auch wenn die Audiowiedergabe in RDC oder die Videowiedergabe in der RDP-Datei festgelegt ist.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird durch die Einstellung für die Audio- und Videowiedergabe auf der Registerkarte „Clienteneinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts bestimmt, ob die Audio- und Videowiedergabe zulässig ist.</p>
Allow audio recording redirection	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob Benutzer die Möglichkeit haben sollen, Audio auf dem Remotecomputer in einer Remotedesktopdienste-Sitzung aufzunehmen.</p> <p>Benutzer können festlegen, ob die Audioaufnahme auf dem Remotecomputer möglich ist. Dazu müssen Sie die Remoteaudioeinstellungen auf der Registerkarte „Lokale Ressourcen“ in der Remotedesktopverbindung (Remote Desktop Connection, RDC) konfigurieren. Benutzer haben die Möglichkeit, Audio mithilfe eines Audioeingabegeräts auf dem lokalen Computer aufzunehmen (z. B. durch ein integriertes Mikrofon).</p>

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen (Fortsetzung)

Einstellung	Beschreibung
	<p>Standardmäßig ist die Umleitung der Audioaufnahme nicht zulässig, wenn eine Verbindung mit einem Computer hergestellt wird, auf dem Windows Server 2008 R2 ausgeführt wird. Die Umleitung der Audioaufnahme ist standardmäßig bei der Herstellung einer Verbindung mit einem Windows 7-Computer zulässig.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die Umleitung der Audioaufnahme zulässig.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, ist die Umleitung der Audioaufnahme nicht zulässig, auch wenn die Audioaufnahme in RDC festgelegt ist.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird durch die Einstellung für die Audioaufnahme auf der Registerkarte „Clienteneinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts bestimmt, ob die Audioaufnahme zulässig ist.</p>
Limit audio playback quality	<p>Mit dieser Richtlinieneinstellung können Sie die Qualität der Audiowiedergabe für eine Remotedesktopdienste-Sitzung beschränken. Die Beschränkung der Qualität der Audiowiedergabe kann die Verbindungsleistung verbessern, speziell bei langsamen Verbindungen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie eine der folgenden Optionen auswählen: Hoch, Mittel oder Dynamisch. Bei der Auswahl von „Hoch“ werden die Audiotöne unkomprimiert und ohne Mindestlatenz gesendet. Dafür ist Bandbreite in größerem Umfang erforderlich. Bei der Auswahl von „Mittel“ werden die Audiotöne mit geringer Komprimierung und mit der vom verwendeten Codec vorgegebenen Mindestlatenz gesendet. Bei der Auswahl von „Dynamisch“ werden die Audiotöne mit der durch die Bandbreite der Remoteverbindung notwendigen Komprimierung gesendet.</p> <p>Die Qualität der Audiowiedergabe, die Sie mithilfe dieser Richtlinieneinstellung auf dem Remotecomputer festlegen, ist die für eine Remotedesktopdienste-Sitzung maximal mögliche Qualität, unabhängig von der auf dem Clientcomputer konfigurierten Audiowiedergabequalität. Wenn beispielsweise die auf dem Clientcomputer konfigurierte Qualität der Audiowiedergabe höher ist als die auf dem Remotecomputer konfigurierte Qualität, wird für die Audiowiedergabe die geringere Qualität verwendet.</p> <p>Die Qualität der Audiowiedergabe kann auf dem Clientcomputer mithilfe der Einstellung „audioqualitymode“ in einer RDP-Datei (Remote-Desktop-Protokoll) konfiguriert werden. Standardmäßig ist für die Audiowiedergabequalität die Option „Dynamisch“ festgelegt.</p>

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen (Fortsetzung)

Einstellung	Beschreibung
Do not allow clipboard redirection	<p>Legt fest, ob die gemeinsame Nutzung von Zwischenablageinhalten (Zwischenablagenumleitung) von einem Remotecomputer und einem Clientcomputer in einer Remotedesktopdienste-Sitzung verhindert wird.</p> <p>Sie können mithilfe dieser Einstellung die Weiterleitung von Zwischenablagendaten von Remotecomputer zu lokalem Computer und umgekehrt durch Benutzer unterbinden. Standardmäßig ist die Zwischenablagenumleitung bei Remotedesktopdiensten zulässig.</p> <p>Wenn Sie diese Einstellung aktivieren, können Benutzer keine Zwischenablagendaten umleiten.</p> <p>Wenn Sie diese Einstellung deaktivieren, ist die Zwischenablagenumleitung bei Remotedesktopdiensten immer zulässig.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird die Zwischenablagenumleitung nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die Zwischenablagenumleitung mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu deaktivieren.</p>
Do not allow COM port redirection	<p>Legt fest, ob die Umleitung von Daten vom Remotecomputer zu Client-COM-Ports in einer Remotedesktopdienste-Sitzung unterbunden wird.</p> <p>Sie können mithilfe dieser Einstellung verhindern, dass Benutzer Daten zu COM-Port-Peripheriegeräten umleiten oder lokale COM-Ports zuordnen, wenn sie bei einer Remotedesktopdienste-Sitzung angemeldet sind. Standardmäßig ist diese COM-Port-Umleitung bei Remotedesktopdiensten zulässig.</p> <p>Wenn Sie diese Einstellung aktivieren, haben Benutzer nicht die Möglichkeit, Serverdaten zum lokalen COM-Port umzuleiten.</p> <p>Wenn Sie diese Einstellung deaktivieren, ist die COM-Port-Umleitung bei Remotedesktopdiensten immer zulässig.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird die COM-Port-Umleitung nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die COM-Port-Umleitung mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu deaktivieren.</p>

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen (Fortsetzung)

Einstellung	Beschreibung
Do not allow drive redirection	<p>Legt fest, ob die Zuordnung von Clientlaufwerken (Laufwerksumleitung) in einer Remotedesktopdienste-Sitzung verhindert wird.</p> <p>Standardmäßig ordnet ein RD-Sitzungshostserver Clientlaufwerke automatisch bei der Herstellung einer Verbindung zu. Zugeordnete Laufwerke werden in der Ordnerstruktur der Sitzung in Windows Explorer oder im Computer im Format <Laufwerksbuchstabe> auf <Computername> angezeigt. Sie können dieses Verhalten mit dieser Einstellung ändern.</p> <p>Wenn Sie diese Einstellung aktivieren, ist die Clientlaufwerksumleitung in Remotedesktopdienste-Sitzungen nicht zulässig.</p> <p>Wenn Sie diese Einstellung deaktivieren, ist die Clientlaufwerksumleitung immer zulässig.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird die Clientlaufwerksumleitung nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die Clientlaufwerksumleitung mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu deaktivieren.</p>
Do not allow LTP Port redirection	<p>Legt fest, ob die Umleitung von Daten zu Client-LPT-Ports in einer Remotedesktopdienste-Sitzung unterbunden wird.</p> <p>Sie können mit dieser Einstellung verhindern, dass Benutzer lokale LPT-Ports zuordnen und Daten vom Remotecomputer zu lokalen LPT-Port-Peripheriegeräten umleiten. Standardmäßig ist diese LPT-Port-Umleitung bei Remotedesktopdiensten zulässig.</p> <p>Wenn Sie diese Einstellung aktivieren, haben Benutzer in einer Remotedesktopdienste-Sitzung nicht die Möglichkeit, Serverdaten zum lokalen LPT-Port umzuleiten.</p> <p>Wenn Sie diese Einstellung deaktivieren, ist die LPT-Port-Umleitung immer zulässig.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird die LPT-Port-Umleitung nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die lokale LPT-Port-Umleitung mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu deaktivieren.</p>

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen (Fortsetzung)

Einstellung	Beschreibung
Do not allow supported Plug and Play device redirection	<p>Mithilfe dieser Richtlinieneinstellung können Sie die Umleitung der unterstützten „Plug-and-Play“-Geräte (z. B. tragbare Windows-Geräte) zum Remotecomputer in einer Remotedesktopdienst-Sitzung steuern.</p> <p>Standardmäßig ist die Umleitung unterstützter Plug-and-Play-Geräte bei Remotedesktopdiensten zulässig. Benutzer haben die Möglichkeit, mit der Option „Mehr“ auf der Registerkarte „Lokale Ressourcen“ in der Remotedesktopverbindung die unterstützten Plug-and-Play-Geräte für die Umleitung zum Remotecomputer auszuwählen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, haben Benutzer nicht die Möglichkeit, ihre unterstützten Plug-and-Play-Geräte zum Remotecomputer umzuleiten.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer ihre unterstützten Plug-and-Play-Geräte zum Remotecomputer umleiten.</p> <p>Hinweis Sie können die Umleitung unterstützter Plug-and-Play-Geräte auch auf der Registerkarte „Clienteneinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts ausschließen. Sie haben die Möglichkeit, die Umleitung bestimmter Typen von unterstützten Plug-and-Play-Geräten mithilfe der Richtlinieneinstellungen im Ordner Computerkonfiguration > Administrative Vorlagen > System > Geräteinstallation > Einschränkungen bei der Geräteinstallation auszuschließen.</p>

Tabelle 5-30. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen (Fortsetzung)

Einstellung	Beschreibung
Do not allow smart card device redirection	<p>Mit dieser Richtlinieneinstellung können Sie die Umleitung von Smartcard-Geräten in einer Remotedesktopdienste-Sitzung steuern.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können sich Benutzer der Remotedesktopdienste nicht mithilfe einer Smartcard bei einer Remotedesktopdienste-Sitzung anmelden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist die Smartcard-Geräteumleitung erlaubt. Standardmäßig leiten die Remotedesktopdienste Smartcard-Geräte automatisch bei der Herstellung einer Verbindung um.</p> <p>Hinweis Auf dem Clientcomputer muss mindestens Microsoft Windows 2000 Server oder mindestens Microsoft Windows XP Professional ausgeführt werden. Der Zielservers muss außerdem einer Domäne beigetreten sein.</p>
Allow time zone redirection	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob der Clientcomputer seine Zeitzoneneinstellungen an die Remote-Desktop-Dienste-Sitzung umleitet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, senden Clients, die eine Zeitzonenumleitung durchführen können, ihre Zeitzoneneinstellungen an den Server. Über die Basiszeit des Servers wird die aktuelle Sitzungszeit berechnet (aktuelle Sitzungszeit = Serverbasiszeit + Clientzeitzone).</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, leitet der Clientcomputer seine Zeitzoneneinstellungen nicht um, und die Sitzungszeitzone entspricht der Serverzeitzone.</p>

Einstellungen für die Remote-Desktop-Dienstlizenzierung

Die Gruppenrichtlinieneinstellungen für RDS-Lizenzierung steuern die Reihenfolge, in der RDS-Lizenzserver positioniert werden, ob Problembenachrichtigungen angezeigt werden und ob für RDS-CALs (Client Access Licenses) eine Lizenzierung auf Benutzer- oder Gerätebasis verwendet wird.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Lizenzierung** gespeichert.

Tabelle 5-31. Gruppenrichtlinieneinstellungen für RDS-Lizenzierung

Einstellung	Beschreibung
Use the specified Remote Desktop license servers	<p>Diese Richtlinieneinstellung ermöglicht Ihnen, die Reihenfolge anzugeben, in der ein RDS-Hostserver versucht, Remote-Desktop-Lizenzserver zu finden.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, versucht ein RDS-Hostserver zunächst, die von Ihnen angegebenen Lizenzserver zu finden. Wenn die angegebenen Lizenzserver nicht gefunden werden können, versucht der RDS-Hostserver eine automatische Lizenzservererkennung durchzuführen.</p> <p>Bei der automatischen Lizenzservererkennung versucht ein RDS-Hostserver in einer Domäne auf Windows Server-Basis, in der folgenden Reihenfolge einen Lizenzserver zu finden:</p> <ol style="list-style-type: none"> 1 Lizenzserver, die im Tool für die Konfiguration des Remotedesktop-Sitzungshosts angegeben sind. 2 Lizenzserver, die in den Active Directory-Domänendiensten veröffentlicht sind. 3 Lizenzserver, die auf Domänencontrollern in derselben Domäne wie der RDS-Host installiert sind. <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, verwendet der RDS-Host den Lizenzservererkennungsmodus, der im Tool für die Konfiguration des Remotedesktop-Sitzungshosts angegeben ist.</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>Diese Richtlinieneinstellung legt fest, ob Benachrichtigungen auf einem RDS-Host angezeigt werden, wenn Probleme bei der RD-Lizenzierung auftreten, die den RD-Host betreffen.</p> <p>Standardmäßig werden Benachrichtigungen auf einem RDS-Host angezeigt, nachdem Sie sich als lokaler Administrator angemeldet haben, falls Probleme bei der RD-Lizenzierung auftreten, die den RDS-Host betreffen. Wenn zutreffend, wird auch eine Benachrichtigung angezeigt, die die Anzahl von Tagen bis zum Ablauf der Lizenzfrist für den RDS-Host angibt.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, werden diese Benachrichtigungen auf dem RDS-Host nicht angezeigt.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden diese Benachrichtigungen auf dem RDS-Host nach der Anmeldung als lokaler Administrator angezeigt.</p>
Set the Remote Desktop licensing mode	<p>Diese Richtlinieneinstellung ermöglicht Ihnen, den Typ der Clientzugriffslizenz für Remotedesktopdienste (RDS-CAL) anzugeben, der für die Verbindung mit diesem RDS-Host erforderlich ist.</p> <p>Sie können mit dieser Richtlinieneinstellung einen von zwei Lizenzierungsmodi auswählen: pro Benutzer oder pro Gerät.</p> <p>Beim benutzerbasierten Lizenzierungsmodus muss jedes Benutzerkonto, das eine Verbindung mit diesem RDS-Host herstellt, über eine benutzerbasierte RDS-CAL verfügen.</p> <p>Beim gerätebasierten Lizenzierungsmodus muss jedes Gerät, das eine Verbindung mit diesem RDS-Host herstellt, über eine gerätebasierte RDS-CAL verfügen.</p>

Tabelle 5-31. Gruppenrichtlinieneinstellungen für RDS-Lizenzierung (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie diese Richtlinieneinstellung aktivieren, hat der angegebene Lizenzierungsmodus Vorrang vor dem Lizenzierungsmodus, der während der Installation des Remote-Desktop-Sitzungshosts oder im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts angegeben ist.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird der Lizenzierungsmodus verwendet, der während der Installation des Diensts der Remote-Desktop-Sitzungshost-Rolle oder im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts angegeben ist.</p>

Einstellungen für die Druckerumleitung für Remote-Desktop-Dienste

Mit den Richtlinieneinstellungen der RDS-Druckerumleitung können Benutzer Richtlinien für die RDS-Druckerumleitung konfigurieren.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Druckerumleitung** gespeichert.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind auch im Ordner **Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Druckerumleitung** gespeichert.

Tabelle 5-32. Gruppenrichtlinieneinstellungen für die RDS-Druckerumleitung

Einstellung	Beschreibung
Do not set default client printer to be default printer in a session	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob der Standardclientdrucker automatisch als Standarddrucker in einer Sitzung auf einem RDS-Host vorgesehen ist.</p> <p>Standardmäßig weisen die Remotedesktopdienste automatisch den Standardclientdrucker als Standarddrucker in einer Sitzung auf einem RDS-Host zu. Sie können dieses Verhalten mit dieser Richtlinieneinstellung ändern.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird der auf dem Remotecomputer festgelegte Drucker als Standarddrucker verwendet.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, ordnet der RDS-Host automatisch den Standardclientdrucker zu und legt diesen als Standarddrucker bei der Herstellung einer Verbindung fest.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird der Standarddrucker nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, den Standarddrucker für Clientsitzungen mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu konfigurieren.</p>
Do not allow client printer redirection	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob die Zuordnung von Clientdruckern in Remotedesktopdienste-Sitzungen unterbunden werden soll.</p> <p>Mit dieser Richtlinieneinstellung können Sie verhindern, dass Benutzer Druckaufträge vom Remotecomputer zu an einem an ihren lokalen Clientcomputer angeschlossenen Drucker umleiten. Standardmäßig ist diese Clientdruckerzuordnung für die Remotedesktopdienste zulässig.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Benutzer keine Druckaufträge vom Remotecomputer zu einem lokalen Clientdrucker in Remotedesktopdienste-Sitzungen umleiten.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, haben Benutzer die Möglichkeit, Druckaufträge durch Zuordnung des Clientdruckers umzuleiten.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird die Zuordnung des Clientdruckers nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die Zuordnung des Clientdruckers mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu deaktivieren.</p>

Tabelle 5-32. Gruppenrichtlinieneinstellungen für die RDS-Druckerumleitung (Fortsetzung)

Einstellung	Beschreibung
Use Remote Desktop Easy Print printer driver first	<p data-bbox="810 268 1422 352">Mit dieser Richtlinieneinstellung können Sie festlegen, ob der Druckertreiber „Easy Print für Remotedesktop“ als Erstes für die Installation aller Clientdrucker verwendet wird.</p> <p data-bbox="810 369 1422 678">Wenn diese Richtlinieneinstellung aktiviert oder nicht konfiguriert ist, versucht der RDS-Host zuerst, den Druckertreiber „Remote Desktop Easy Print“ zur Installation aller Clientdrucker zu verwenden. Wenn der Druckertreiber „Easy Print für Remotedesktop“ aus irgendeinem Grund nicht verwendet werden kann, wird ein Druckertreiber auf dem RDS-Host verwendet, der den Clientdrucker unterstützt. Wenn der RDS-Host über keinen Druckertreiber für den Clientdrucker verfügt, ist der Clientdrucker für die Remotedesktopdienste-Sitzung nicht verfügbar.</p> <p data-bbox="810 695 1422 968">Wenn Sie diese Richtlinieneinstellung deaktivieren, versucht der RDS-Host einen geeigneten Druckertreiber für die Installation des Clientdruckers zu ermitteln. Wenn der RDS-Host über keinen Druckertreiber für den Clientdrucker verfügt, versucht der RDS-Host den Druckertreiber „Easy Print für Remotedesktop“ zur Installation des Clientdruckers zu verwenden. Wenn der Druckertreiber „Easy Print für Remotedesktop“ aus irgendeinem Grund nicht verwendet werden kann, ist der Clientdrucker für die Remotedesktopdienste-Sitzung nicht verfügbar.</p> <p data-bbox="810 995 1382 1115">Hinweis Wenn die Richtlinieneinstellung „Clientdruckerumleitung nicht zulassen“ aktiviert ist, wird die Richtlinieneinstellung „Zuerst Easy Print-Druckertreiber für Remotedesktop verwenden“ ignoriert.</p>

Tabelle 5-32. Gruppenrichtlinieneinstellungen für die RDS-Druckerumleitung (Fortsetzung)

Einstellung	Beschreibung
Specify RD Session Host Server fallback printer driver behavior	<p>Mit dieser Richtlinieneinstellung können Sie das Verhalten des Fallback-Druckertreibers für den RDS-Host festlegen.</p> <p>Standardmäßig ist der Fallback-Druckertreiber für den RDS-Host deaktiviert. Wenn der RDS-Host über keinen Druckertreiber für den Clientdrucker verfügt, ist kein Drucker für die Remotedesktopdienste-Sitzung verfügbar.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird der Fallback-Druckertreiber aktiviert. Der RDS-Host versucht dann standardmäßig einen geeigneten Druckertreiber zu ermitteln. Wird kein anwendbarer Druckertreiber gefunden, ist der Clientdrucker nicht verfügbar. Sie können dieses Standardverhalten ändern. Folgende Optionen stehen zur Verfügung:</p> <ul style="list-style-type: none"> ■ Do nothing if one is not found. Wenn kein passender Druckertreiber vorhanden ist, versucht der RDS-Host einen geeigneten Druckertreiber zu ermitteln. Wird keiner gefunden, ist der Clientdrucker nicht verfügbar. Dies ist das Standardverhalten. ■ Default to PCL if one is not found. Wenn kein geeigneter Druckertreiber gefunden wird, wird standardmäßig der PCL-Fallback-Druckertreiber (Printer Control Language) verwendet. ■ Default to PS if one is not found. Wenn kein geeigneter Druckertreiber gefunden wird, wird standardmäßig der PS-Fallback-Druckertreiber (PostScript) verwendet. ■ Show both PCL and PS if one is not found. Wenn kein geeigneter Druckertreiber gefunden wird, werden sowohl der PS- als auch der PCL-Fallback-Druckertreiber angezeigt. <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, wird der Fallback-Druckertreiber für den RDS-Host deaktiviert, sodass der RDS-Host nicht versucht, den Fallback-Druckertreiber zu verwenden.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird das Verhalten des Fallback-Druckertreibers standardmäßig deaktiviert.</p> <p>Hinweis Wenn die Einstellung „Clientdruckerumleitung nicht zulassen“ aktiviert ist, wird diese Richtlinieneinstellung ignoriert und der Fallback-Druckertreiber deaktiviert.</p>
Redirect only the default client printer	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob der Standardclientdrucker als einziger Drucker in Remotedesktopdienste-Sitzungen umgeleitet wird.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird nur der Standardclientdrucker in Remotedesktopdienste-Sitzungen umgeleitet.</p>

Tabelle 5-32. Gruppenrichtlinieneinstellungen für die RDS-Druckerumleitung (Fortsetzung)

Einstellung	Beschreibung
	Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden alle Clientdrucker in Remotedesktopdienste-Sitzungen umgeleitet.

Einstellungen zu RDS-Profilen

Die Gruppenrichtlinieneinstellungen für RDS-Profile steuern die Einstellungen für servergespeicherte Profile und das Basisverzeichnis bei Sitzungen der Remote-Desktop-Dienste.

Tabelle 5-33. Gruppenrichtlinieneinstellungen für RDS-Profile

Einstellung	Beschreibung
Limit the size of the entire roaming user profile cache	<p>Mithilfe dieser Richtlinieneinstellung können Sie die Größe des gesamten servergespeicherten Benutzerprofil-Caches auf dem lokalen Laufwerk begrenzen. Diese Richtlinieneinstellung gilt nur für Computer, auf denen der Remote-Desktop-Sitzungshost-Rollendienst installiert ist.</p> <hr/> <p>Hinweis Wenn Sie die Größe eines einzelnen Benutzerprofils begrenzen möchten, verwenden Sie die Richtlinieneinstellung <code>Limit profile size</code> unter Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\System\Benutzerprofile.</p> <hr/> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie ein Überwachungsintervall (in Minuten) und eine maximale Größe (in Gigabyte) für den gesamten servergespeicherten Benutzerprofil-Cache angeben. Das Überwachungsintervall bestimmt, wie oft die Größe des gesamten servergespeicherten Benutzerprofil-Caches überprüft wird. Wenn die Größe des gesamten servergespeicherten Benutzerprofil-Caches die von Ihnen angegebene Maximalgröße übersteigt, werden die ältesten servergespeicherten Benutzerprofile (deren Verwendung am längsten zurückliegt) gelöscht, bis die Größe des gesamten servergespeicherten Benutzerprofil-Caches geringer ist als die angegebene Maximalgröße.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Größe des gesamten servergespeicherten Benutzerprofil-Caches auf dem lokalen Laufwerk nicht begrenzt.</p> <p>Hinweis: Diese Richtlinieneinstellung wird ignoriert, wenn die Richtlinieneinstellung <code>Prevent Roaming Profile changes from propagating to the server</code> unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Benutzerprofile aktiviert ist.</p>
Set Remote Desktop Services User Home Directory	<p>Gibt an, ob die Remote-Desktop-Dienste die angegebene Netzwerkfreigabe oder den lokalen Verzeichnispfad als Stamm für das Basisverzeichnis des Benutzers für eine RDS-Sitzung verwenden.</p> <p>Um diese Einstellung zu verwenden, wählen Sie den Speicherort für das Basisverzeichnis (Netzwerk oder lokal) aus der Dropdown-Liste für den Speicherort. Wenn Sie das Verzeichnis auf einer Netzwerkfreigabe anlegen, geben Sie den Stammpfad für das Basisverzeichnis in der Form <code>\\Computername\Freigabename</code> an und wählen Sie dann den Laufwerksbuchstaben aus, dem Sie die Netzwerkfreigabe zuordnen möchten.</p>

Tabelle 5-33. Gruppenrichtlinieneinstellungen für RDS-Profil (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie das Basisverzeichnis auf dem lokalen Computer anlegen möchten, geben Sie den Stammpfad für das Basisverzeichnis in der Form Laufwerk:\Pfad an, ohne Umgebungsvariablen oder Auslassungszeichen (drei Punkte). Geben Sie keinen Platzhalter für einen Benutzer-Alias an, da die Remotedesktopdienste diesen bei der Anmeldung automatisch anhängt.</p> <hr/> <p>Hinweis Das Feld für den Laufwerkbuchstaben wird ignoriert, wenn Sie einen lokalen Pfad angeben. Wenn Sie einen lokalen Pfad angeben, aber im Stammpfad für das Basisverzeichnis den Namen einer Netzwerkfreigabe eingeben, legen die Remotedesktopdienste die Basisverzeichnisse für die Benutzer im Netzwerk-Speicherort an.</p> <hr/> <p>Wenn der Status auf „Aktiviert“ gesetzt ist, erstellen die Remotedesktopdienste das Basisverzeichnis für den betreffenden Benutzer in dem angegebenen Speicherort auf dem lokalen Computer oder im Netzwerk. Der Basisverzeichnispfad für jeden Benutzer entspricht dem angegebenen Stammpfad für das Basisverzeichnis und dem Alias des Benutzers.</p> <p>Wenn der Status auf „Deaktiviert“ oder „Nicht konfiguriert“ gesetzt ist, wird das Basisverzeichnis für den betreffenden Benutzer wie angegeben auf dem Server angelegt.</p>

Tabelle 5-33. Gruppenrichtlinieneinstellungen für RDS-Profile (Fortsetzung)

Einstellung	Beschreibung
Use mandatory profiles on the RD Session Host server	<p>Mithilfe dieser Richtlinieneinstellung können Sie festlegen, ob die Remotedesktopdienste ein obligatorisches Profil für alle Benutzer verwenden sollen, die eine Remoteverbindung zum RDS-Host herstellen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, verwenden die Remotedesktopdienste den in der Richtlinieneinstellung <code>Set path for Remote Desktop Services Roaming User Profile</code> angegebenen Pfad als Stammordner für das obligatorische Benutzerprofil. Alle Benutzer, die eine Remoteverbindung zum RDS-Host herstellen, verwenden das gleiche Benutzerprofil.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden obligatorische Benutzerprofile nicht von Benutzern verwendet, die eine Remoteverbindung zum RDS-Host herstellen.</p> <p>Hinweis Damit diese Einstellung übernommen wird, müssen Sie auch die Richtlinieneinstellung <code>Set path for Remote Desktop Services Roaming User Profile</code> aktivieren und konfigurieren.</p>
Set path for Remote Desktop Services Roaming User Profile	<p>Mithilfe dieser Richtlinieneinstellung können Sie den Netzwerkpfad angeben, den die Remotedesktopdienste für servergespeicherte Benutzerprofile verwenden.</p> <p>Remotedesktopdienste speichern standardmäßig sämtliche Benutzerprofile lokal auf dem RDS-Host. Sie können diese Richtlinieneinstellung verwenden, um eine Netzwerkfreigabe anzugeben, in der Benutzerprofile zentral gespeichert werden können, sodass ein Benutzer für Sitzungen auf allen RDS-Hosts, die für die Verwendung dieser Netzwerkfreigabe für Benutzerprofile konfiguriert sind, auf das gleiche Benutzerprofil zugreifen kann.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, verwenden die Remotedesktopdienste den angegebenen Pfad als Stammverzeichnis für alle Benutzerprofile. Die Profile befinden sich in Unterordnern, die nach dem Kontonamen des jeweiligen Benutzers benannt sind.</p> <p>Um diese Richtlinieneinstellung zu konfigurieren, geben Sie den Pfad zu der Netzwerkfreigabe in der Form <code>\\Computername\Freigabename</code> an. Geben Sie keinen Platzhalter für den Benutzerkontonamen an, da die Remotedesktopdienste diesen automatisch hinzufügen, wenn der Benutzer sich anmeldet und das Profil erstellt wird. Wenn die angegebene Netzwerkfreigabe nicht vorhanden ist, zeigen die Remotedesktopdienste eine Fehlermeldung auf dem RDS-Host an und speichern die Benutzerprofile lokal auf dem RDS-Host.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden die Benutzerprofile lokal auf dem RDS-Host gespeichert. Sie können den Profilpfad eines Benutzers auf der Registerkarte „Remote-Desktop-Dienste-Profil“ im Dialogfeld „Eigenschaften“ des Benutzerkontos konfigurieren.</p> <p>Anmerkungen:</p> <ol style="list-style-type: none"> Die durch diese Richtlinieneinstellung aktivierten, servergespeicherten Benutzerprofile gelten nur für RDS-

Tabelle 5-33. Gruppenrichtlinieneinstellungen für RDS-Profile (Fortsetzung)

Einstellung	Beschreibung
	Verbindungen. Es kann vorkommen, dass ein Benutzer außerdem ein servergespeichertes Windows-Benutzerprofil konfiguriert hat. Ein servergespeichertes Remote-Desktop-Dienste-Benutzerprofil hat immer Vorrang in einer RDS-Sitzung.
2	Verwenden Sie diese Richtlinieneinstellung zusammen mit der Richtlinieneinstellung <i>Use mandatory profiles on the RD Session Host server</i> unter Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > RD-Sitzungshost > Profile , um ein obligatorisches servergespeichertes Remotedesktopdienste-Benutzerprofil für alle Benutzer zu konfigurieren, die eine Remoteverbindung zum RDS-Host herstellen. Der Pfad, der in der Richtlinieneinstellung <i>Set path for Remote Desktop Services Roaming User Profile</i> festgelegt wird, muss das obligatorische Profil enthalten.

Einstellungen für den RDS-Verbindungsserver

Mit den Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver können Benutzer Richtlinien für den Verbindungsserver festlegen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > RD-Verbindungsbroker** gespeichert.

Tabelle 5-34. Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver

Einstellung	Beschreibung
Join RD Connection Broker	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob der RDS-Host einer Farm im Verbindungsserver hinzugefügt werden soll, der auf einem RDS-Host installiert ist. Der Verbindungsserver auf einem RDS-Host erfasst Benutzersitzungen und ermöglicht einem Benutzer die erneute Herstellung einer Verbindung mit seiner bestehenden Sitzung in einer RDS-Farm mit Lastausgleich. Um den Verbindungsserver auf einem RDS-Host nutzen zu können, muss der Remotedesktop-Sitzungshost-Rollendienst auf dem Host installiert sein.</p> <p>Wenn die Richtlinieneinstellung aktiviert ist, wird der RDS-Host der Farm hinzugefügt, die mit der Einstellung „Namen der Remotedesktop-Verbindungsbrokerfarm konfigurieren“ festgelegt wurde. Die Farm befindet sich auf dem Verbindungsserver, der in der Richtlinieneinstellung „Namen des Remotedesktop-Verbindungsbrokerservers konfigurieren“ angegeben ist.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, wird der RDS-Host keiner Farm im Verbindungsserver hinzugefügt, und es wird keine Erfassung von Benutzersitzungen durchgeführt. Wenn die Einstellung deaktiviert ist, können Sie den RDS-Host weder mit dem Konfigurationstool für Remotedesktop-Sitzungshosts noch mit dem Anbieter für Terminaldienste-WMI (Windows Management Instrumentation) dem Verbindungsserver hinzufügen.</p> <p>Wenn die Richtlinieneinstellung nicht konfiguriert ist, wird die Einstellung nicht auf Gruppenrichtlinienebene festgelegt. In diesem Fall können Sie das Hinzufügen des RDS-Hosts zum Verbindungsserver mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI auf dem RDS-Host konfigurieren.</p>
Hinweis	
<ol style="list-style-type: none"> 1 Wenn Sie diese Einstellung aktivieren, müssen Sie auch die Richtlinieneinstellungen „Namen der Remotedesktop-Verbindungsbrokerfarm konfigurieren“ und „Namen des Remotedesktop-Verbindungsbrokerservers konfigurieren“ aktivieren oder diese Einstellungen mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI konfigurieren. 2 Für Windows Server 2008 wird diese Richtlinieneinstellung mindestens für Windows Server 2008 Standard unterstützt. 	
Configure RD Connection Broker farm name	<p>Mit dieser Richtlinieneinstellung können Sie den Namen einer Farm festlegen, die im Verbindungsserver für einen RDS-Host hinzugefügt werden soll. Der Verbindungsserver bestimmt auf der Basis des Farmnamens, welche RDS-Hosts in einer RDS-Farm enthalten sind. Deshalb müssen Sie für alle RDS-Hosts in einer Farm mit Lastausgleich denselben Farmnamen verwenden. Der Farmname muss keinem Namen in den Active Directory-Domänendiensten entsprechen.</p>

Tabelle 5-34. Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie einen neuen Farmnamen angeben, wird im Verbindungsserver für den RDS-Host eine neue Farm erstellt. Wenn Sie einen vorhandenen Farmnamen angeben, wird der RDS-Host dieser Farm im Verbindungsserver auf dem RDS-Host hinzugefügt.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie den Namen einer Farm im Verbindungsserver auf dem RDS-Host angeben.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird der Farmname nicht durch eine Gruppenrichtlinie festgelegt. In diesem Fall können Sie den Farmnamen mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI anpassen.</p> <hr/> <p>Hinweis Für Windows Server 2008 wird diese Richtlinieneinstellung mindestens für Windows Server 2008 Standard unterstützt. Diese Einstellung ist nicht wirksam, solange nicht sowohl die Einstellung „Remotedesktop-Verbindungsbroker beitreten“ als auch die Einstellung „Namen des Remotedesktop-Verbindungsbrokerservers konfigurieren“ aktiviert und mithilfe einer Gruppenrichtlinie, des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI konfiguriert wurde.</p>

Tabelle 5-34. Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver (Fortsetzung)

Einstellung	Beschreibung
Use IP Address Redirection	<p>Mit dieser Richtlinieneinstellung legen Sie die Umleitungsmethode für den Fall fest, dass ein Clientgerät erneut eine Verbindung mit einer bestehenden Remotedesktopdienst-Sitzung in einer Farm mit Lastausgleich herstellt. Diese Einstellung wird für einen RDS-Host angewendet, der für die Verwendung des Verbindungsservers auf einem RDS-Host und nicht für die Verwendung des Verbindungsservers auf einem Remote-Desktop konfiguriert ist.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, führt der Remotedesktopdienste-Client eine Abfrage für den Verbindungsserver auf dem RDS-Host durch und wird zu einer bestehenden Sitzung mithilfe der IP-Adresse des RDS-Hosts, auf dem die Sitzung aktiv ist, umgeleitet. Um diese Umleitungsmethode verwenden zu können, müssen Clientcomputer in der Lage sein, mithilfe der IP-Adresse direkt eine Verbindung mit dem RDS-Host in der Farm herzustellen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, wird die IP-Adresse des RDS-Hosts nicht zum Client gesendet. Stattdessen wird die IP-Adresse in einen Token eingebettet. Wenn ein Client erneut eine Verbindung mit dem Lastausgleichsdienst herstellt, wird er mit dem Routing-Token zur bestehenden Sitzung auf dem korrekten RDS-Host in der Farm umgeleitet. Deaktivieren Sie diese Einstellung nur, wenn Ihre Lösung zum Netzwerklastausgleich die Verwendung von Routing-Token für RDS-Host-Verbindungsserver unterstützt und wenn Clients mithilfe der IP-Adresse nicht direkt eine Verbindung mit dem RDS-Host in der Farm mit Lastausgleich herstellen sollen.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, wird die Einstellung „IP-Adressumleitung verwenden“ im Konfigurationstool für Remotedesktop-Sitzungshosts verwendet. Standardmäßig ist diese Einstellung im Konfigurationstool für Remotedesktop-Sitzungshosts aktiviert.</p> <p>Hinweis Für Windows Server 2008 wird diese Richtlinieneinstellung mindestens für Windows Server 2008 Standard unterstützt.</p>

Tabelle 5-34. Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver (Fortsetzung)

Einstellung	Beschreibung
Configure RD Connection Broker Server name	<p data-bbox="810 268 1414 485">Mit dieser Richtlinieneinstellung können Sie den Verbindungsserver festlegen, den der RDS-Host für die Erfassung und Umleitung von Benutzersitzungen für eine Farm mit Lastausgleich verwendet. Der angegebene RDS-Host muss den Verbindungsserver-Dienst ausführen. Alle RDS-Hosts in einer Farm mit Lastausgleich müssen denselben Verbindungsserver verwenden.</p> <p data-bbox="810 495 1414 711">Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie den Verbindungsserver für den RDS-Host mithilfe seines Hostnamens, der IP-Adresse oder des vollqualifizierten Domännennamens angeben. Wenn Sie einen ungültigen Namen oder eine ungültige Adresse für den Verbindungsserver angeben, wird eine Fehlermeldung in der Ereignisanzeige auf dem RDS-Host protokolliert.</p> <p data-bbox="810 722 1414 873">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Sie den Namen des RDS-Host-Verbindungsservers oder die IP-Adresse mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI anpassen.</p> <p data-bbox="810 898 890 919">Hinweis</p> <ul data-bbox="810 936 1414 1383" style="list-style-type: none"> ■ Für Windows Server 2008 wird diese Richtlinieneinstellung für Windows Server 2008 Standard unterstützt. ■ Diese Richtlinieneinstellung ist erst wirksam, wenn die Einstellung „Remotedesktop-Verbindungsbroker beitreten“ aktiviert und oder das Hinzufügen des RDS-Hosts zum Verbindungsserver auf dem RDS-Host mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI konfiguriert wurde. ■ Um als aktives Mitglied an einer vom Verbindungsserver aktivierten Sitzung in einer RDS-Farm teilnehmen zu können, muss das Computerkonto jedes RDS-Hosts in der Farm zur lokalen Gruppe „Sitzungsverzeichnis Computer“ auf dem Verbindungsserver für den RDS-Host gehören.
Use RD Connection Broker load balancing	<p data-bbox="810 1423 1414 1539">Mit dieser Richtlinieneinstellung legen Sie fest, ob der Lastausgleichsdienst im Verbindungsserver auf einem RDS-Host zum Lastausgleich zwischen Servern in einer RDS-Farm verwendet wird.</p> <p data-bbox="810 1549 1414 1831">Wenn Sie diese Richtlinieneinstellung aktivieren, leitet der Verbindungsserver auf einem RDS-Host Benutzer, die über keine bestehende Sitzung verfügen, auf den RDS-Host in der Farm mit den wenigsten Sitzungen um. Das Umleitungsverhalten für Benutzer mit bestehenden Sitzungen ist davon nicht betroffen. Wenn der Server für die Verwendung des Verbindungsservers auf einem RDS-Host konfiguriert ist, werden Benutzer, die über eine bestehende Sitzung verfügen, zu dem RDS-Host ihrer Sitzungen umgeleitet.</p>

Tabelle 5-34. Gruppenrichtlinieneinstellungen für den RDS-Verbindungsserver (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie diese Richtlinieneinstellung deaktivieren, melden sich Benutzer, die über keine bestehende Sitzung verfügen, beim ersten RDS-Host an, mit dem sie eine Verbindung herstellen.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können Sie den RDS-Host zur Teilnahme am Lastausgleich des Verbindungsservers für den RDS-Host mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts oder mit dem Anbieter für Terminaldienste-WMI konfigurieren.</p> <hr/> <p>Hinweis Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie auch die Richtlinieneinstellungen „Remotedesktop-Verbindungsbroker beitreten“, „Namen der Remotedesktop-Verbindungsbrokerfarm konfigurieren“ und „Namen des Remotedesktop-Verbindungsbrokerservers konfigurieren“ aktivieren.</p>

Umgebungseinstellungen zur RDS-Remote-Sitzung

Die Gruppenrichtlinieneinstellungen der RDS-Remotesitzungsumgebung steuern die Konfiguration der Benutzerschnittstelle in Remotedesktopdienste-Sitzungen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung** gespeichert.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind auch im Ordner **Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung** gespeichert.

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung

Einstellung	Beschreibung
Limit maximum color depth	<p data-bbox="778 268 1342 323">Mit dieser Richtlinieneinstellung können Sie die maximale Farbauflösung (Farbtiefe) für RDS-Verbindungen festlegen.</p> <p data-bbox="778 338 1422 487">Sie haben mit dieser Richtlinieneinstellung die Möglichkeit, eine Beschränkung für die Farbtiefe jeder Verbindung festzulegen, die das RDP-Protokoll verwendet. Eine Beschränkung der Farbtiefe kann speziell bei langsamen Verbindungen die Verbindungsleistung verbessern und die Serverarbeitslast reduzieren.</p> <p data-bbox="778 501 1406 714">Wenn Sie diese Richtlinieneinstellung aktivieren, stellt die von Ihnen festgelegte Farbtiefe die maximal mögliche Farbtiefe für die Verbindung eines Benutzers über RDP dar. Die tatsächliche Farbtiefe der Verbindung wird durch die auf dem Clientcomputer verfügbare Farbunterstützung bestimmt. Wenn Sie „Clientkompatibel“ auswählen, wird die vom Client maximal unterstützte Farbtiefe verwendet.</p> <hr/> <p data-bbox="778 741 1358 795">Hinweis Eine Farbtiefe von 24 Bit wird nur auf Windows XP Professional und Windows Server 2003 unterstützt.</p> <hr/> <p data-bbox="778 823 1398 1035">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Farbtiefe für Verbindungen durch die Einstellung „Maximale Farbtiefe einschränken“ auf der Registerkarte „Clienteneinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festgelegt, solange vom Benutzer zum Zeitpunkt der Herstellung einer Verbindung kein niedrigerer Wert festgelegt wird.</p>
Enforce Removal of Remote Desktop Wallpaper	<p data-bbox="778 1062 1350 1148">Legt fest, ob ein Desktop-Hintergrundbild auf Remoteclients angezeigt wird, die eine Verbindung über die Remotedesktopdienste herstellen.</p> <p data-bbox="778 1163 1422 1472">Sie haben mit dieser Einstellung die Möglichkeit, das Entfernen eines Hintergrundbildes in einer Remotedesktopdienste-Sitzung zu erzwingen. Standardmäßig wird in Windows XP Professional je nach Clientkonfiguration ein Hintergrundbild für Remoteclients angezeigt, die eine Verbindung über Remotedesktopdienste herstellen. Weitere Informationen erhalten Sie auf der Registerkarte „Erweitert“ der Optionen der Remotedesktopverbindung. Standardmäßig wird auf Servern, auf denen Windows Server 2003 ausgeführt wird, kein Hintergrundbild für Remotedesktopdienste-Sitzungen angezeigt.</p> <p data-bbox="778 1486 1410 1541">Wenn Sie diese Einstellung aktivieren, wird kein Hintergrundbild in einer Remotedesktopdienste-Sitzung angezeigt.</p> <p data-bbox="778 1556 1294 1642">Wenn Sie diese Einstellung deaktivieren, kann je nach Clientkonfiguration ein Hintergrundbild in einer Remotedesktopdienste-Sitzung eingeblendet werden.</p> <p data-bbox="778 1656 1302 1711">Wenn Sie diese Einstellung nicht konfigurieren, gilt das Standardverhalten.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Configure RemoteFX	<p>Mit dieser Richtlinieneinstellung können Sie die Verfügbarkeit von RemoteFX sowohl auf einem Remotedesktop-Virtualisierungshost als auch auf einem RDS-Host steuern.</p> <p>Wenn RemoteFX auf einem Remotedesktop-Virtualisierungshost bereitgestellt wird, bietet es ein umfassendes Benutzererlebnis durch das Rendern von Inhalten auf dem Server mithilfe von GPUs (Grafikprozessoren) oder der Hardware. Standardmäßig verwendet RemoteFX für den Remotedesktop-Virtualisierungshost serverseitige GPUs oder die entsprechende Hardware, um ein umfassendes Benutzererlebnis über LAN-Verbindungen und RDP 7.1 zu gewährleisten.</p> <p>Wenn RemoteFX auf einem RDS-Host bereitgestellt wird, ermöglicht es ein umfassendes Benutzererlebnis durch Verwendung eines Hardware-beschleunigten Komprimierungsschemas.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird mit RemoteFX ein umfassendes Benutzererlebnis über LAN-Verbindungen und RDP 7.1 ermöglicht.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren, wird RemoteFX deaktiviert.</p> <p>Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, gilt das Standardverhalten. Standardmäßig ist RemoteFX für den Remotedesktop-Virtualisierungshost aktiviert und RemoteFX für RDS-Hosts deaktiviert.</p>
Limit maximum display resolution	<p>Mit dieser Richtlinieneinstellung können Sie die maximale Anzeigeauflösung festlegen, die von jedem Monitor zur Anzeige einer Remotedesktopdienste-Sitzung verwendet werden kann. Eine Beschränkung der Auflösung für die Anzeige einer Remotesitzung kann speziell bei langsamen Verbindungen die Verbindungsleistung verbessern und die Serverarbeitslast reduzieren.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie die Breite und die Höhe der Auflösung angeben. Die festgelegte Auflösung stellt die maximale Anzeigeauflösung dar, die von jedem Monitor zur Anzeige einer Remotedesktopdienste-Sitzung verwendet werden kann.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die maximale Auflösung, die von jedem Monitor zur Anzeige einer Remotedesktopdienste-Sitzung verwendet werden kann, von den Werten auf der Registerkarte „Anzeigeeinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festgelegt.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Limit maximum number of monitors	<p>Mit dieser Richtlinieneinstellung können Sie die Anzahl der Monitore beschränken, die ein Benutzer zur Anzeige einer Remotedesktopdienste-Sitzung verwenden kann. Eine Beschränkung der Anzahl der Monitore für die Anzeige einer Remotedesktopdienste-Sitzung kann speziell bei langsamen Verbindungen die Verbindungsleistung verbessern und die Serverarbeitslast reduzieren.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie die Anzahl der Monitore festlegen, die einem Benutzer zur Anzeige einer Remotedesktopdienste-Sitzung zur Verfügung stehen. Es kann eine Zahl von 1 bis 10 angegeben werden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Anzahl der Monitore, die für die Anzeige einer Remotedesktopdienste-Sitzung verwendet werden können, vom im Feld „Maximale Anzahl der Bildschirme pro Sitzung begrenzen“ angegebenen Wert auf der Registerkarte „Anzeigeeinstellungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festgelegt.</p>
Remove "Disconnect" option from Shut Down dialog	<p>Mit dieser Richtlinieneinstellung können Sie die Option „Trennen“ aus dem Dialogfeld „Windows herunterfahren“ in Remotedesktopdienste-Sitzungen entfernen.</p> <p>Mit dieser Richtlinieneinstellung können Sie verhindern, dass Benutzer mit dieser gewohnten Methode die Verbindung von ihrem Client zum RDS-Host trennen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die Option „Trennen“ nicht mehr in der Dropdown-Liste im Dialogfeld „Windows herunterfahren“ enthalten.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Option „Trennen“ nicht aus der Liste im Dialogfeld „Windows herunterfahren“ entfernt.</p> <p>Hinweis Diese Richtlinieneinstellung betrifft nur das Dialogfeld „Windows herunterfahren“. Damit wird nicht verhindert, dass Benutzer mit anderen Methoden die Verbindung mit einer Remotedesktopdienste-Sitzung trennen. Diese Richtlinieneinstellung unterbindet auch nicht die Trennung von Sitzungen auf dem Server. Sie können festlegen, wie lange eine getrennte Sitzung auf dem Server noch aktiv ist. Dazu konfigurieren Sie die Richtlinieneinstellung „Zeitlimit für getrennte Sitzungen festlegen“ im Ordner Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sitzungszeitlimits.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Optimize visual experience when using RemoteFX	<p>Mit dieser Richtlinieneinstellung können Sie das visuelle Erlebnis von Remotebenutzern in RDC-Verbindungen (Remote Desktop Connection, Remotedesktopverbindung) festlegen, die RemoteFX verwenden. Mit dieser Richtlinieneinstellung können Sie die Nutzung der Netzwerkbandbreite auf die Art des bereitgestellten grafischen Erlebnisses abstimmen.</p> <p>Abhängig von den Anforderungen Ihrer Benutzer können Sie die Nutzung der Netzwerkbandbreite durch Reduzierung der Rate der Bildschirmfassung vermindern. Sie haben auch die Möglichkeit, die Nutzung der Netzwerkbandbreite durch Reduzierung der Bildqualität (d. h. durch Erhöhung der durchgeführten Bildkomprimierung) zu vermindern.</p> <p>Wenn Sie über ein Netzwerk verfügen, dessen Bandbreite über dem Durchschnitt liegt, können Sie die Nutzung der Bandbreite durch Auswahl der höchsten Einstellungen für die Rate der Bildschirmfassung und für die Bildqualität maximieren.</p> <p>Standardmäßig sind Remotedesktopverbindungen, die RemoteFX verwenden, für ein abgestimmtes Benutzererlebnis unter LAN-Bedingungen optimiert. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, gelten für Remotedesktopverbindungen, die RemoteFX verwenden, die Bedingungen einer mittleren Rate der Bildschirmfassung und einer mittleren Bildkomprimierung (Standardverhalten).</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Set compression algorithm for RDP data	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, welcher Komprimierungsalgorithmus für das Remotedesktopprotokoll (RDP) verwendet wird.</p> <p>Standardmäßig verwenden Server den RDP-Komprimierungsalgorithmus der Hardwarekonfiguration des Servers.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie festlegen, welcher RDP-Komprimierungsalgorithmus verwendet wird. Wenn Sie den für die Verwendung von weniger Arbeitsspeicher optimierten Algorithmus verwenden, wird mit dieser Option weniger Arbeitsspeicher, aber mehr Netzwerkbandbreite in Anspruch genommen. Wenn Sie den für die Verwendung von weniger Netzwerkbandbreite optimierten Algorithmus verwenden, wird mit dieser Option umgekehrt weniger Netzwerkbandbreite, aber mehr Arbeitsspeicher in Anspruch genommen. Darüber hinaus ist eine dritte Option verfügbar, die Netzwerkbandbreite und Arbeitsspeicher gleichmäßig aufeinander abstimmt.</p> <p>Sie können auch festlegen, dass der RDP-Komprimierungsalgorithmus nicht verwendet wird. Wenn Sie keinen RDP-Komprimierungsalgorithmus verwenden, wird mehr Netzwerkbandbreite verwendet. Dies ist nur empfehlenswert, wenn Sie eine Hardware verwenden, die für die Optimierung des Netzwerkdatenverkehrs optimiert ist. Beachten Sie, dass auch bei Verzicht auf den RDP-Komprimierungsalgorithmus einige Grafikdaten weiter komprimiert werden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird der standardmäßige RDP-Komprimierungsalgorithmus verwendet.</p>
Optimize visual experience for Remote Desktop Services sessions	<p>Mit dieser Richtlinieneinstellung können Sie das visuelle Erlebnis von Remotebenutzern in Remotedesktopdienste-Sitzungen festlegen. Die Remotesitzungen auf dem Remotecomputer werden dabei zur Unterstützung dieses visuellen Erlebnisses optimiert.</p> <p>Standardmäßig werden Remotedesktopdienste-Sitzungen für reichhaltige Multimediainhalte optimiert, z. B. für Anwendungen, die Silverlight oder Windows Presentation Foundation verwenden.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie die Art des visuellen Erlebnisses auswählen, für das die Remotedesktopdienste-Sitzungen optimiert werden sollen. Sie können zwischen „Reichhaltige Multimediainhalte“ und „Text“ wählen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden Remotedesktopdienste-Sitzungen für reichhaltige Multimediainhalte optimiert.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Start a program on connection	<p>Konfiguriert Remotedesktopdienste für die automatische Ausführung eines angegebenen Programms bei der Herstellung einer Verbindung.</p> <p>Sie haben mit dieser Einstellung die Möglichkeit, ein Programm automatisch ausführen zu lassen, wenn sich ein Benutzer bei einem Remotecomputer anmeldet.</p> <p>Standardmäßig bieten Remotedesktopdienste-Sitzungen einen Zugriff auf den kompletten Windows-Desktop, solange mit dieser Einstellung bei der Konfiguration der Clientverbindung durch den Serveradministrator oder durch den Benutzer nichts anderes festgelegt wurde. Durch Aktivierung dieser Einstellung werden die vom Serveradministrator oder vom Benutzer festgelegten Einstellungen für „Programm starten“ außer Kraft gesetzt. Das Startmenü und der Windows-Desktop werden nicht angezeigt. Wenn der Benutzer das Programm beendet, wird die Sitzung automatisch abgemeldet.</p> <p>Geben Sie zur Verwendung dieser Einstellung den vollqualifizierten Pfad und Dateinamen der ausführbaren Datei, die bei der Anmeldung des Benutzers ausgeführt werden soll, in das Feld „Programmpfad und Dateiname“ ein. Wenn erforderlich, geben Sie unter „Arbeitsverzeichnis“ den vollqualifizierten Pfad zum Startverzeichnis des Programms ein. Wenn für „Arbeitsverzeichnis“ nichts festgelegt ist, wird das Programm mit seinem standardmäßigen Arbeitsverzeichnis ausgeführt. Wenn der angegebene Programmpfad, der angegebene Dateiname oder das angegebene Arbeitsverzeichnis keinem gültigen Verzeichnis entspricht, kann keine RDS-Hostverbindung hergestellt werden. Es wird dann eine Fehlermeldung angezeigt.</p> <p>Wenn die Einstellung aktiviert ist, wird in den Remotedesktopdienste-Sitzungen automatisch das angegebene Programm ausgeführt und das angegebene Arbeitsverzeichnis (oder das standardmäßige Programmverzeichnis, falls kein Arbeitsverzeichnis angegeben wurde) als Arbeitsverzeichnis für das Programm verwendet.</p> <p>Wenn die Einstellung deaktiviert oder nicht konfiguriert ist, starten Remotedesktopdienste-Sitzungen mit der Anzeige des vollständigen Desktops, sofern vom Serveradministrator oder Benutzer nicht anders festgelegt ist. Weitere Informationen finden Sie unter „Diese Programme bei der Benutzeranmeldung ausführen: Richtlinieneinstellung“ im Ordner Computerkonfiguration > Administrative Vorlagen > System > Anmeldung.</p> <p>Hinweis Diese Einstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Einstellungen konfiguriert sind, hat die Einstellung der Computerkonfiguration Vorrang vor jener der Benutzerkonfiguration.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Always show desktop on connection	<p data-bbox="778 300 1422 575">Diese Richtlinieneinstellung legt fest, ob der Desktop immer angezeigt wird, wenn ein Client eine Verbindung mit einem Remotecomputer herstellt, oder ob ein Startprogramm ausgeführt wird. Mit dieser Einstellung können Sie festlegen, dass der Desktop angezeigt wird, wenn ein Client eine Verbindung mit einem Remotecomputer herstellt, auch wenn bereits ein Startprogramm im standardmäßigen Benutzerprofil, in der Remotedesktopverbindung, im Remotedesktopdienste-Client oder über die Gruppenrichtlinie festgelegt ist.</p> <p data-bbox="778 592 1409 709">Wenn Sie diese Richtlinieneinstellung aktivieren, wird der Desktop immer angezeigt, wenn ein Client eine Verbindung mit einem Remotecomputer herstellt. Diese Richtlinieneinstellung setzt alle Startprogramm-Richtlinieneinstellungen außer Kraft.</p> <p data-bbox="778 726 1406 936">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, kann ein Startprogramm festgelegt werden, das auf dem Remotecomputer ausgeführt wird, wenn der Client eine Verbindung mit einem Remotecomputer herstellt. Wenn kein Startprogramm festgelegt wird, wird immer der Desktop auf dem Remotecomputer angezeigt, wenn der Client eine Verbindung mit einem Remotecomputer herstellt.</p> <p data-bbox="778 961 1394 1050">Hinweis Wenn diese Richtlinieneinstellung aktiviert ist, wird die Richtlinieneinstellung „Ein Programm beim Herstellen der Verbindung ausführen“ ignoriert.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Allow desktop composition for remote desktop sessions	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob die Desktopgestaltung für Remote-Desktop-Sitzungen zulässig ist. Diese Einstellung gilt nicht für RemoteApp-Sitzungen.</p> <p>Die Desktopgestaltung stellt die Benutzeroberflächenelemente von Windows Aero, wie durchscheinende Fenster, für Remote-Desktop-Sitzungen bereit. Da Windows Aero zusätzliche System- und Bandbreitenressourcen erfordert, kann das Zulassen der Desktopgestaltung insbesondere bei langsamen Verbindungen die Verbindungsleistung beeinträchtigen und die Arbeitslast auf dem Remotecomputer erhöhen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die Desktopgestaltung für Remote-Desktop-Sitzungen zulässig. Auf dem Clientcomputer können Sie die Desktopgestaltung auf der Registerkarte „Erweitert“ in der Remotedesktopverbindung oder in einer Remotedesktopprotokoll-Datei (RDP) mithilfe der Einstellung „allow desktop composition“ konfigurieren. Darüber hinaus muss der Clientcomputer über die entsprechende Hardware zur Unterstützung von Windows Aero-Funktionen verfügen.</p> <hr/> <p>Hinweis Damit Windows Aero-Funktionen für Remote-Desktop-Sitzungen verfügbar sind, ist möglicherweise eine zusätzliche Konfiguration des Remotecomputers erforderlich. Beispielsweise muss die Funktion der Desktop-Darstellung auf dem Remotecomputer installiert sein, und die maximale Farbtiefe auf dem Remotecomputer muss auf 32 Bits pro Pixel festgelegt sein. Außerdem muss der Designdienst auf dem Remotecomputer gestartet werden.</p> <hr/> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist die Desktopgestaltung für Remote-Desktop-Sitzungen nicht zulässig, auch wenn die Desktopgestaltung in der Remotedesktopverbindung oder in der RDP-Datei aktiviert ist.</p>

Tabelle 5-35. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung (Fortsetzung)

Einstellung	Beschreibung
Do not allow font smoothing	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob die Schriftartglättung für Remoteverbindungen zulässig ist.</p> <p>Die Schriftartglättung bietet eine ClearType-Funktionalität für eine Remoteverbindung. ClearType ist eine Technologie zur Darstellung von Computerschriftarten in klarer und geglätteter Form, speziell, wenn Sie einen LCD-Monitor verwenden. Da für die Schriftartglättung zusätzliche Bandbreitenressourcen erforderlich sind, kann die Deaktivierung der Schriftartglättung für Remoteverbindungen die Verbindungsleistung verbessern, speziell bei langsamen Verbindungen.</p> <p>Standardmäßig ist die Schriftartglättung für Remoteverbindungen zulässig. Sie können die Schriftartglättung auf der Registerkarte „Erweitert“ in der Remotedesktopverbindung oder in einer Remotedesktopprotokoll-Datei (RDP) mithilfe der Einstellung „allow font smoothing“ konfigurieren.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die Schriftartglättung für Remotedesktopverbindungen nicht zulässig, auch wenn die Schriftartglättung in der Remotedesktopverbindung oder in der RDP-Datei aktiviert ist.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist die Schriftartglättung für Remoteverbindungen zulässig.</p>
Remove Windows Security item from Start menu	<p>Gibt an, ob der Eintrag „Windows-Sicherheit“ aus dem Einstellungsmenü auf Remote-Desktop-Clients entfernt werden soll. Sie können diese Einstellung verwenden, um unerfahrene Benutzer davon abzuhalten, sich unbeabsichtigt von Remote-Desktop-Diensten abzumelden.</p> <p>Wenn der Status auf Aktiviert gesetzt ist, wird Windows-Sicherheit nicht in den Einstellungen im Start-Menü angezeigt. In der Folge müssen Benutzer eine Sicherheitssequenz wie beispielsweise STRG+ALT+Ende eingeben, um das Dialogfeld „Windows-Sicherheit“ auf dem Clientcomputer zu öffnen.</p> <p>Wenn der Status auf Deaktiviert oder Nicht konfiguriert gesetzt ist, bleibt Windows-Sicherheit im Einstellungsmenü.</p>

Sicherheitseinstellungen für Remote-Desktop-Dienste

Die Gruppenrichtlinieneinstellung zur RDS-Sicherheit steuert, ob lokale Administratoren Berechtigungen anpassen dürfen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sicherheit** gespeichert.

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe

Einstellung	Beschreibung
Server Authentication Certificate Template	<p data-bbox="778 266 1414 384">Mit dieser Richtlinieneinstellung können Sie den Namen der Zertifikatvorlage angeben, die festlegt, welches Zertifikat automatisch für die Authentifizierung eines RDS-Hosts ausgewählt wird.</p> <p data-bbox="778 401 1425 518">Für die Authentifizierung eines RDS-Hosts ist ein Zertifikat erforderlich, wenn SSL (TLS 1.0) zur Gewährleistung einer sicheren Kommunikation zwischen einem Client und einem RDS-Host bei RDP-Verbindungen verwendet wird.</p> <p data-bbox="778 533 1422 745">Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie den Namen einer Zertifikatvorlage angeben. Bei der automatischen Auswahl eines Zertifikats für die Authentifizierung eines RDS-Hosts werden nur Zertifikate berücksichtigt, die mit der angegebenen Zertifikatvorlage erstellt wurden. Die automatische Zertifikatauswahl wird nur durchgeführt, wenn kein spezielles Zertifikat ausgewählt wurde.</p> <p data-bbox="778 760 1406 1005">Wenn kein Zertifikat vorhanden ist, das mit der angegebenen Zertifikatvorlage erstellt wurde, wird vom RDS-Host eine Anforderung für eine Zertifikatregistrierung ausgegeben. Solange diese Anforderung nicht erfüllt wird, wird weiter das aktuelle Zertifikat verwendet. Wenn mehr als ein Zertifikat vorhanden ist, das mit der angegebenen Zertifikatvorlage erstellt wurde, wird das Zertifikat mit dem spätesten Ablaufdatum ausgewählt, das dem aktuellen Namen des RDS-Hosts entspricht.</p> <p data-bbox="778 1020 1418 1232">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird standardmäßig ein selbstsigniertes Zertifikat zur Authentifizierung des RDS-Hosts verwendet. Sie haben die Möglichkeit, ein bestimmtes Zertifikat für die Authentifizierung des RDS-Hosts auf der Registerkarte „Allgemein“ des Konfigurationstools für Remotedesktop-Sitzungshosts auszuwählen.</p> <p data-bbox="778 1257 1402 1346">Hinweis Wenn Sie ein bestimmtes Zertifikat für die Authentifizierung des RDS-Hosts auswählen, hat dieses Zertifikat Vorrang vor dieser Richtlinieneinstellung.</p>
Set client connection encryption level	<p data-bbox="778 1381 1390 1470">Legt fest, ob eine bestimmte Verschlüsselungsstufe zur Gewährleistung einer sicheren Kommunikation zwischen Clients und RDS-Hosts bei RDP-Verbindungen erforderlich ist.</p> <p data-bbox="778 1484 1406 1665">Wenn Sie diese Einstellung aktivieren, muss für die gesamte Kommunikation zwischen Clients und RDS-Hosts bei Remoteverbindungen die mit dieser Einstellung festgelegte Verschlüsselungsmethode verwendet werden. Standardmäßig gilt für die Verschlüsselungsstufe der Wert „Hoch“. Es sind folgende Verschlüsselungsmethoden verfügbar:</p> <ul style="list-style-type: none"> <li data-bbox="778 1680 1393 1797">■ High. Mit der Einstellung „Hoch“ werden die zwischen Client und Server gesendeten Daten mithilfe der starken 128-Bit-Verschlüsselung verschlüsselt. Diese Verschlüsselungsstufe sollte in Umgebungen verwendet werden, die ausschließlich

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe (Fortsetzung)

Einstellung	Beschreibung
	<p>128-Bit-Clients enthalten (z. B. Clients, die die Remotedesktopverbindung ausführen). Clients, die diese Verschlüsselungsstufe nicht unterstützen, können keine Verbindung mit RDS-Hostservern herstellen.</p> <ul style="list-style-type: none"> ■ Client Compatible. Mit der Einstellung „Clientkompatibel“ werden zwischen Client und Server gesendete Daten mit der vom Client unterstützten maximalen Schlüsselstärke verschlüsselt. Verwenden Sie diese Verschlüsselungsstufe für Umgebungen mit Clients, die keine 128-Bit-Verschlüsselung unterstützen. ■ Low. Mit der Einstellung „Niedrig“ werden nur vom Client zum Server gesendete Daten mithilfe der 56-Bit-Verschlüsselung verschlüsselt. <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die für Remoteverbindungen zum RDS-Host verwendete Verschlüsselungsstufe nicht über Gruppenrichtlinien festgelegt. Sie haben aber die Möglichkeit, die erforderliche Verschlüsselungsstufe für diese Verbindungen mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu konfigurieren.</p> <hr/> <p>Wichtig Die FIPS-Kompatibilität kann mithilfe der Richtlinieneinstellung „Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden“ im Ordner Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen oder über die Einstellung „FIPS-konform“ im Konfigurationstool für Remotedesktop-Sitzungshosts konfiguriert werden. Die Einstellung „FIPS-konform“ verschlüsselt und entschlüsselt zwischen Client und Server gesendete Daten unter Verwendung der kryptografischen Microsoft-Module mit dem FIPS-140-1-Verschlüsselungsalgorithmus (Federal Information Processing Standard). Verwenden Sie diese Verschlüsselungsstufe, wenn für die Kommunikation zwischen Clients und RDS-Hosts die höchste Verschlüsselungsstufe erforderlich ist. Wenn die FIPS-Kompatibilität bereits über die Gruppenrichtlinieneinstellung „Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden“ aktiviert ist, hat diese Einstellung Vorrang vor der in dieser Gruppenrichtlinieneinstellung oder im Konfigurationstool für Remotedesktop-Sitzungshosts festgelegten Verschlüsselungsstufe.</p>

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe (Fortsetzung)

Einstellung	Beschreibung
Always prompt for password upon connection	<p>Legt fest, ob Remotedesktopdienste den Client bei der Herstellung einer Verbindung immer zur Eingabe eines Kennworts auffordern.</p> <p>Sie haben mit dieser Einstellung die Möglichkeit, die Kennworteingabe für Benutzer anzufordern, die sich bei den Remotedesktopdiensten anmelden, auch wenn diese bereits im Remotedesktopverbindungs-Client ein Kennwort angegeben haben.</p> <p>Standardmäßig ermöglichen die Remotedesktopdienste Benutzern die automatische Anmeldung durch Eingabe eines Kennworts im Remotedesktopverbindungs-Client.</p> <p>Wenn Sie diese Einstellung aktivieren, haben Benutzer nicht die Möglichkeit, sich automatisch bei den Remotedesktopdiensten durch Eingabe des Kennworts im Remotedesktopverbindungs-Client anzumelden. Die Benutzer werden dann zur Eingabe eines Kennworts für die Anmeldung aufgefordert.</p> <p>Wenn Sie diese Einstellung deaktivieren, können sich Benutzer immer automatisch bei den Remotedesktopdiensten durch Eingabe des Kennworts im Remotedesktopverbindungs-Client anmelden.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird automatische Anmeldung nicht auf Gruppenrichtlinienebene festgelegt. Ein Administrator hat aber weiterhin die Möglichkeit, die Kennworteingabe mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts anzufordern.</p>
Require secure RPC communication	<p>Legt fest, ob ein RDS-Host eine sichere RPC-Kommunikation mit allen Clients erfordert oder ob eine unsichere Kommunikation zulässig ist.</p> <p>Sie haben mit dieser Einstellung die Möglichkeit, die Sicherheit der RPC-Kommunikation mit Clients zu erhöhen, indem Sie nur authentifizierte und verschlüsselte Anforderungen zulassen.</p> <p>Wenn Sie diese Einstellung aktivieren, akzeptieren die Remotedesktopdienste Anforderungen von RPC-Clients, die sichere Anforderungen unterstützen, und unterbinden eine unsichere Kommunikation mit nicht vertrauenswürdigen Clients.</p> <p>Wenn Sie diese Einstellung deaktivieren, muss der gesamte RPC-Datenverkehr für Remotedesktopdienste immer sicher sein. Allerdings ist eine unsichere Kommunikation für RPC-Clients erlaubt, die nicht auf die Anforderung reagieren.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, ist eine unsichere Kommunikation zulässig.</p> <p>Hinweis Die RPC-Schnittstelle wird für die Verwaltung und Konfiguration der Remotedesktopdienste verwendet.</p>

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe (Fortsetzung)

Einstellung	Beschreibung
Require use of specific security layer for remote (RDP) connections	<p data-bbox="778 268 1425 352">Legt fest, ob eine bestimmte Sicherheitsebene zur Gewährleistung einer sicheren Kommunikation zwischen Clients und RDS-Hosts bei RDP-Verbindungen erforderlich ist.</p> <p data-bbox="778 369 1425 520">Wenn Sie diese Einstellung aktivieren, muss für die gesamte Kommunikation zwischen Clients und RDS-Hosts bei Remoteverbindungen die mit dieser Einstellung festgelegte Sicherheitsmethode verwendet werden. Es sind folgende Sicherheitsmethoden verfügbar:</p> <ul data-bbox="778 533 1425 1045" style="list-style-type: none"> <li data-bbox="778 533 1425 781">■ Negotiate. Mit der Methode „Aushandeln“ wird die sicherste Methode, die vom Client unterstützt wird, erzwungen. Wird Transport Layer Security (TLS) Version 1.0 unterstützt, wird diese Methode zur Authentifizierung des RDS-Hosts verwendet. Wird TLS nicht unterstützt, wird die native RDP-Verschlüsselung (Remotedesktopprotokoll) für die Gewährleistung einer sicheren Kommunikation verwendet. Der RDS-Host wird jedoch nicht authentifiziert. <li data-bbox="778 793 1425 911">■ RDP. Die RDP-Methode verwendet eine native RDP-Verschlüsselung für eine sichere Kommunikation zwischen Client und RDS-Host. Wenn Sie diese Einstellung auswählen, wird der RDS-Host nicht authentifiziert. <li data-bbox="778 924 1425 1045">■ SSL (TLS 1.0). Die SSL-Methode erfordert die Verwendung von TLS 1.0 zur Authentifizierung des RDS-Hosts. Wenn TLS nicht unterstützt wird, kann keine Verbindung hergestellt werden. <p data-bbox="778 1058 1425 1268">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die für Remoteverbindungen zum RDS-Host verwendete Sicherheitsmethode nicht über Gruppenrichtlinien festgelegt. Sie haben aber die Möglichkeit, die erforderliche Sicherheitsmethode für diese Verbindungen mithilfe des Konfigurationstools für Remotedesktop-Sitzungshosts zu konfigurieren.</p>

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe (Fortsetzung)

Einstellung	Beschreibung
Require user authentication for remote connections by using Network	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob eine Benutzerauthentifizierung für Remoteverbindungen zum RDS-Host mithilfe der Authentifizierung auf Netzwerkebene (Network Level Authentication, NLA) erforderlich ist. Diese Richtlinieneinstellung erhöht die Sicherheit, da die Benutzerauthentifizierung bereits früher im Prozess der Herstellung der Remoteverbindung stattfindet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, können nur Computer, die die NLA-Authentifizierung unterstützen, eine Verbindung mit RDS-Hosts herstellen.</p> <p>Um festzustellen, ob ein Clientcomputer die NLA-Authentifizierung unterstützt, starten Sie die Remotedesktopverbindung auf dem Clientcomputer, klicken Sie auf das Symbol links oben im Dialogfeld „Remotedesktopverbindung“ und dann auf „Info“. Suchen Sie im Dialogfeld „Info“ der Remotedesktopverbindung nach dem Ausdruck „Authentifizierung auf Netzwerkebene wird unterstützt“.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist keine Authentifizierung auf Netzwerkebene für die Benutzerauthentifizierung erforderlich, um eine Remoteverbindung mit dem RDS-Host herzustellen.</p> <p>Sie können mit dem Konfigurationstool für Remotedesktop-Sitzungshosts oder mit der Registerkarte „Remote“ in den Systemeigenschaften festlegen, dass die Authentifizierung auf Netzwerkebene für die Benutzerauthentifizierung erforderlich ist.</p> <hr/> <p>Wichtig Die Deaktivierung oder fehlende Konfiguration dieser Richtlinieneinstellung vermindert die Sicherheit, da die Benutzerauthentifizierung erst später im Prozess der Herstellung der Remoteverbindung vorgenommen wird.</p>
Do not allow local administrators to customize permissions	<p>Gibt an, ob die Administratorrechte zum Anpassen der Sicherheitsberechtigungen im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts deaktiviert werden.</p> <p>Sie können diese Einstellung verwenden, um Administratoren daran zu hindern, im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts auf der Registerkarte „Berechtigungen“ Änderungen an den Benutzergruppen vorzunehmen.</p> <p>Administratoren sind standardmäßig in der Lage, derartige Änderungen vorzunehmen.</p> <p>Wenn der Status auf „Aktiviert“ gesetzt ist, kann die Registerkarte „Berechtigungen“ im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts nicht verwendet werden, um die Sicherheitsbeschreibungen für jede Verbindung anzupassen oder um die Standard-Sicherheitsbeschreibungen für eine bestehende Gruppe zu verändern. Sämtliche Sicherheitsbeschreibungen sind schreibgeschützt.</p>

Tabelle 5-36. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn der Status auf „Deaktiviert“ oder „Nicht konfiguriert“ gesetzt ist, haben Server-Administratoren auf der Registerkarte „Berechtigungen“ im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts vollen Lese-/Schreibzugriff auf die Sicherheitsbeschreibungen für Benutzer.</p> <hr/> <p>Hinweis Die bevorzugte Methode zur Verwaltung des Benutzerzugriffs besteht darin, einen Benutzer zu der Gruppe der Remote-Desktop-Benutzer hinzuzufügen.</p>

Zeitbeschränkung von RDS-Sitzungen

Mit Gruppenrichtlinieneinstellungen für die Zeitbeschränkung von RDS-Sitzungen können Benutzer Richtlinien für die Zeitbeschränkung von Sitzungen auf RDS-Hosts festlegen.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sitzungszeitlimits** gespeichert.

Die Gruppenrichtlinieneinstellungen für Horizon 7-RDS sind auch im Ordner **Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sitzungszeitlimits** gespeichert.

Tabelle 5-37. Gruppenrichtlinieneinstellungen für die Zeitbeschränkung von RDS-Sitzungen

Einstellung	Beschreibung
Set time limit for disconnected sessions	<p data-bbox="810 268 1342 352">Sie können mit dieser Richtlinieneinstellung eine Zeitbeschränkung für getrennte Remotedesktopdienste-Sitzungen konfigurieren.</p> <p data-bbox="810 369 1422 552">Mit dieser Richtlinieneinstellung haben Sie die Möglichkeit, den maximalen Zeitraum festzulegen, in dem eine getrennte Sitzung noch auf dem Server aktiv bleibt. Standardmäßig ist für die Remotedesktopdienste eine Trennung der Benutzer von einer Remotedesktopdienste-Sitzung ohne Abmeldung und Beendigung der Sitzung zulässig.</p> <p data-bbox="810 569 1422 684">Wenn sich eine Sitzung in einem getrennten Zustand befindet, bleiben die ausgeführten Programme aktiviert, auch wenn der Benutzer nicht mehr aktiv verbunden ist. Standardmäßig bleiben getrennte Sitzungen auf dem Server unbegrenzt erhalten.</p> <p data-bbox="810 701 1410 911">Wenn Sie diese Richtlinieneinstellung aktivieren, werden getrennte Sitzungen nach Ablauf des festgelegten Zeitraums vom Server gelöscht. Wenn das Standardverhalten einer unbegrenzten Aktivierung getrennter Sitzungen gelten soll, wählen Sie „Nie“ aus. Wenn Sie über eine Konsolensitzung verfügen, wird keine Zeitbeschränkung für getrennte Sitzungen angewendet.</p> <p data-bbox="810 928 1422 1110">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, bleiben getrennte Sitzungen unbegrenzt erhalten. Sie haben die Möglichkeit, Zeitbeschränkungen für getrennte Sitzungen auf der Registerkarte „Sitzungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festzulegen.</p> <hr/> <p data-bbox="810 1136 1422 1251">Hinweis Diese Richtlinieneinstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Richtlinieneinstellungen konfiguriert sind, hat die Richtlinie der Computerkonfiguration Vorrang.</p>
Set time limit for active but idle Remote Desktop Services sessions	<p data-bbox="810 1287 1378 1436">Mit dieser Richtlinieneinstellung können Sie den maximalen Zeitraum festlegen, in dem sich eine aktive Remotedesktopdienste-Sitzung im Leerlauf (d. h. ohne Benutzereingabe) befinden kann, bevor sie automatisch getrennt wird.</p> <p data-bbox="810 1453 1426 1791">Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie den gewünschten Zeitraum in der Dropdown-Liste „Leerlaufsitzungslimit“ auswählen. In den Remotedesktopdiensten werden aktive Sitzungen im Leerlauf nach Ablauf des angegebenen Zeitraums automatisch getrennt. Der Benutzer erhält zwei Minuten vor der Trennung der Sitzung eine entsprechende Warnung. Er hat dann die Möglichkeit, eine Taste zu drücken oder die Maus zu bewegen, um die Trennung der Sitzung zu verhindern. Wenn Sie über eine Konsolensitzung verfügen, wird keine Zeitbeschränkung für Sitzungen im Leerlauf angewendet.</p>

Tabelle 5-37. Gruppenrichtlinieneinstellungen für die Zeitbeschränkung von RDS-Sitzungen (Fortsetzung)

Einstellung	Beschreibung
	<p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, sind in den Remotedesktopdiensten Sitzungen im Leerlauf unbegrenzt aktiv. Sie haben die Möglichkeit, Zeitbeschränkungen für aktive Sitzungen im Leerlauf auf der Registerkarte „Sitzungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festzulegen.</p> <p>Wenn in den Remotedesktopdiensten eine Sitzung nach einem bestimmten Zeitraum nicht nur getrennt, sondern beendet werden soll, konfigurieren Sie dafür die Richtlinieneinstellung „Sitzung abbrechen, wenn Zeitlimit erreicht wird“ im Ordner Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sitzungszeitlimits.</p> <hr/> <p>Hinweis Diese Richtlinieneinstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Richtlinieneinstellungen konfiguriert sind, hat die Richtlinie der Computerkonfiguration Vorrang.</p>
Set time limit for active Remote Desktop Services sessions	<p>Mit dieser Richtlinieneinstellung können Sie den maximalen Zeitraum festlegen, nach dem eine aktive Remotedesktopdienste-Sitzung automatisch getrennt wird.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie den gewünschten Zeitraum in der Dropdown-Liste „Zeitlimit für aktive Sitzungen“ auswählen. In den Remotedesktopdiensten werden aktive Sitzungen nach Ablauf des angegebenen Zeitraums automatisch getrennt. Der Benutzer erhält zwei Minuten vor der Trennung der Remotedesktopdienste-Sitzung eine entsprechende Warnung. Er hat dann die Möglichkeit, geöffnete Dateien zu speichern und Programme zu beenden. Wenn Sie über eine Konsolensitzung verfügen, wird keine Zeitbeschränkung für aktive Sitzungen angewendet.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, sind Sitzungen in den Remotedesktopdiensten unbegrenzt aktiv. Sie haben die Möglichkeit, Zeitbeschränkungen für aktive Sitzungen auf der Registerkarte „Sitzungen“ im Konfigurationstool für Remotedesktop-Sitzungshosts festzulegen.</p> <p>Wenn in den Remotedesktopdiensten eine Sitzung nach einem bestimmten Zeitraum nicht nur getrennt, sondern beendet werden soll, konfigurieren Sie dafür die Richtlinieneinstellung „Sitzung abbrechen, wenn Zeitlimit erreicht wird“ im Ordner Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Sitzungszeitlimits.</p> <hr/> <p>Hinweis Diese Richtlinieneinstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Richtlinieneinstellungen konfiguriert sind, hat die Richtlinie der Computerkonfiguration Vorrang.</p>

Tabelle 5-37. Gruppenrichtlinieneinstellungen für die Zeitbeschränkung von RDS-Sitzungen (Fortsetzung)

Einstellung	Beschreibung
<p>Terminate session when time limits are reached</p>	<p>Legt fest, ob eine Remotedesktopdienste-Sitzung, für die die Zeit überschritten ist, nicht getrennt, sondern beendet wird.</p> <p>Sie haben mit dieser Einstellung die Möglichkeit festzulegen, dass Remotedesktopdienste eine Sitzung beenden, wenn ein bestimmter Zeitraum für aktive Sitzungen oder für Sitzungen im Leerlauf überschritten ist. Der Benutzer wird dann abgemeldet, und die Sitzung wird vom Server gelöscht. Standardmäßig werden in den Remotedesktopdiensten Sitzungen nach einem bestimmten Zeitraum getrennt.</p> <p>Der entsprechende Zeitraum wird lokal vom Serveradministrator oder über eine Gruppenrichtlinie festgelegt. Siehe die Einstellungen für „Zeitlimit für aktive Remotedesktopdienste-Sitzungen festlegen“ und „Zeitlimit für aktive, aber im Leerlauf befindliche Remotedesktopdienste-Sitzungen festlegen“.</p> <p>Wenn Sie diese Einstellung aktivieren, werden in den Remotedesktopdiensten alle Sitzungen nach Ablauf dieses Zeitraums beendet.</p> <p>Wenn Sie diese Einstellung deaktivieren, werden in den Remotedesktopdiensten alle Sitzungen immer nach Ablauf des angegebenen Zeitraums getrennt, auch wenn dies vom Serveradministrator anders festgelegt ist.</p> <p>Wenn Sie diese Einstellung nicht konfigurieren, wird in den Remotedesktopdiensten jede Sitzung mit Zeitüberschreitung getrennt, solange in den lokalen Einstellungen nichts anderes festgelegt ist.</p> <p>Hinweis Diese Einstellung gilt nur für Zeitbeschränkungen, die gezielt im Konfigurationstool für Remotedesktop-Sitzungshosts oder in der Verwaltungskonsole für Gruppenrichtlinien festgelegt wurden. Sie wird nicht auf Zeitüberschreitungen angewendet, die aufgrund von Konnektivitätsproblemen oder von Netzwerkbedingungen auftreten. Beachten Sie, dass diese Einstellung sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar ist. Wenn beide Einstellungen konfiguriert sind, hat die Einstellung der Computerkonfiguration Vorrang.</p>
<p>Set time limit for logoff of RemoteApp sessions</p>	<p>Mit dieser Richtlinieneinstellung können Sie festlegen, wie lange die Remoteanwendungssitzung eines Benutzers im getrennten Status verbleibt, bevor die Sitzung vom RDS-Host abgemeldet wird.</p> <p>Standardmäßig wird die Sitzung vom RDS-Host getrennt, wenn der Benutzer eine Remoteanwendung beendet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, verbleibt die Remoteanwendungssitzung im getrennten Status, wenn der Benutzer eine Remoteanwendung beendet, bis der von Ihnen festgelegte Zeitraum abgelaufen ist. Wenn der festgelegte Zeitraum abgelaufen ist, wird die Remoteanwendungssitzung</p>

Tabelle 5-37. Gruppenrichtlinieneinstellungen für die Zeitbeschränkung von RDS-Sitzungen (Fortsetzung)

Einstellung	Beschreibung
	<p>vom RDS-Host abgemeldet. Wenn der Benutzer eine Remoteanwendung startet, bevor das Ende des Zeitlimits erreicht ist, stellt der Benutzer erneut eine Verbindung mit der getrennten Sitzung auf dem RDS-Host her.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Sitzung vom RDS-Host getrennt, wenn der Benutzer eine Remoteanwendung beendet.</p> <hr/> <p>Hinweis Diese Richtlinieneinstellung ist sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration verfügbar. Wenn beide Richtlinieneinstellungen konfiguriert sind, hat die Richtlinie der Computerkonfiguration Vorrang.</p>

Einstellungen zu temporären RDS-Ordern

Die Gruppenrichtlinieneinstellungen von RDS-Verbindungen steuern das Erstellen und Löschen temporärer Ordner für RDS-Sitzungen.

Tabelle 5-38. Gruppenrichtlinieneinstellungen zu temporären RDS-Ordern

Einstellung	Beschreibung
<code>Do not delete temp folder upon exit</code>	<p data-bbox="778 268 1358 323">Legt fest, ob Remote-Desktop-Dienste temporäre Ordner pro Sitzung eines Benutzers beim Abmelden beibehalten.</p> <p data-bbox="778 338 1410 518">Sie können diese Einstellung verwenden, um die sitzungsspezifischen, temporären Ordner eines Benutzers auf einem Remote-Computer beizubehalten, auch wenn der Benutzer sich von einer Sitzung abmeldet. Standardmäßig löschen die Remote-Desktop-Dienste die temporären Ordner eines Benutzers, wenn sich der Benutzer abmeldet.</p> <p data-bbox="778 533 1418 619">Wenn der Status auf „Aktiviert“ festgelegt ist, werden die temporären Ordner pro Sitzung eines Benutzers beibehalten, wenn sich der Benutzer von einer Sitzung abmeldet.</p> <p data-bbox="778 634 1401 751">Wenn der Status auf „Deaktiviert“ festgelegt ist, werden die temporären Ordner gelöscht, wenn sich ein Benutzer abmeldet, auch wenn der Administrator Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts angibt.</p> <p data-bbox="778 766 1426 884">Wenn der Status auf „Nicht konfiguriert“ festgelegt ist, löschen die Remote-Desktop-Dienste die temporären Ordner beim Abmelden aus dem Remote-Computer – es sei denn, der Server-Administrator hat Anderweitiges festgelegt.</p> <hr/> <p data-bbox="778 911 1418 1058">Hinweis Diese Einstellung wird nur wirksam, wenn die temporären Ordner pro Sitzung auf dem Server verwendet werden. Dies bedeutet, dass die Einstellung keine Auswirkung hat, wenn Sie die Einstellung „Temporäre Ordner pro Sitzung nicht verwenden“ aktivieren.</p>
<code>Do not use temporary folders per session</code>	<p data-bbox="778 1098 1390 1184">Durch diese Richtlinieneinstellung können Sie verhindern, dass Remote-Desktop-Dienste sitzungsspezifische temporäre Ordner erstellen.</p> <p data-bbox="778 1199 1422 1442">Sie können diese Richtlinieneinstellung verwenden, um das Erstellen separater temporärer Ordner auf einem Remote-Computer für jede Sitzung zu deaktivieren. Standardmäßig erstellen die Remote-Desktop-Dienste einen separaten temporären Ordner für jede aktive Sitzung, die ein Benutzer auf einem Remote-Computer beibehält. Diese temporären Ordner werden auf dem Remote-Computer in einem temporären Ordner unter dem Profilordner des Benutzers erstellt und <code>sessionid</code> benannt.</p> <p data-bbox="778 1457 1422 1638">Wenn Sie diese Richtlinieneinstellung aktivieren, werden die temporären Ordner pro Sitzung nicht erstellt. Stattdessen werden die temporären Dateien eines Benutzers für alle Sitzungen auf dem Remote-Computer in einem gemeinsamen temporären Ordner unter dem Profilordner des Benutzers auf dem Remote-Computer gespeichert.</p> <p data-bbox="778 1652 1410 1770">Wenn Sie diese Richtlinieneinstellung deaktivieren, werden immer temporäre Ordner pro Sitzung erstellt; selbst wenn Sie Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts angeben.</p>

Tabelle 5-38. Gruppenrichtlinieneinstellungen zu temporären RDS-Ordern (Fortsetzung)

Einstellung	Beschreibung
	Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, werden temporäre Ordner pro Sitzung erstellt; es sei denn, Sie geben Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts an.

Filtern von Druckern für den virtuellen Druck

Wenn die virtuelle Druckfunktion aktiviert ist, können Benutzer von ihren Remote-Desktops und -Anwendungen aus mit einem beliebigen auf ihren Clientsystemen verfügbaren Drucker drucken. Sie können die Agent-Gruppenrichtlinieneinstellung **Geben Sie beim Umleiten von Client-Druckern einen Filter an** verwenden, um die virtuelle Druckfunktion daran zu hindern, bestimmte Clientdrucker an Remote-Desktops und -Anwendungen umzuleiten.

Die Gruppenrichtlinieneinstellung **Geben Sie beim Umleiten von Client-Druckern einen Filter an** befindet sich in der ADMX-Vorlagendatei für VMware Horizon-Druckerumleitung (`vdm_agent_printing.admx`), die im Dateipaket `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` enthalten ist. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).

Wenn Sie die Gruppenrichtlinieneinstellung **Geben Sie beim Umleiten von Client-Druckern einen Filter an** aktivieren, müssen Sie eine Filterregel in das Textfeld **Name des Registrierungswerts: PrinterFilterString** eingeben. Bei der Filterregel handelt es sich um einen regulären Ausdruck, der angibt, dass der Drucker nicht umgeleitet werden soll (Schwarze Liste). Jeder Drucker, der nicht mit den Druckern in der Filterregel übereinstimmt, wird umgeleitet. Standardmäßig ist die Filterregel leer, was bedeutet, dass alle Clientdrucker umgeleitet werden.

Die folgende Tabelle enthält die Attribute, Operatoren und Platzhalter, die Sie in Filterregeln verwenden können.

Tabelle 5-39. Unterstützte Attribute, Operatoren und Platzhalter für Filterregeln

Attribute	Operatoren	Platzhalter
DriverName, VendorName und PrinterName	UND, ODER und NICHT	* und ?

Nachfolgend sehen Sie einige Beispiele für Filterregeln.

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"

PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"

PrinterName!=".*PDFCreator.*"
```

Aktivieren Sie die virtuelle Druckfunktion, wenn Sie Horizon Agent auf einem virtuellen Desktop oder RDS-Host installieren. Anweisungen zur Installation finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon 7* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Einrichten des standortbasierten Drucks

Die standortbasierte Druckfunktion ordnet Drucker, die sich physisch in der Nähe von Clientsystemen befinden, Remote-Desktops zu. Auf diese Weise können Benutzer von ihren Remote-Desktops über ihre lokalen Drucker oder Netzwerkdrucker drucken.

Das standortbasierte Drucken ermöglicht es IT-Organisationen, Remote-Desktops dem Drucker zuzuordnen, der sich am nächsten am Endpunkt-Clientgerät befindet. Wenn ein Arzt im Krankenhaus sich beispielsweise von Raum zu Raum bewegt, wird der Druckauftrag bei jedem Ausdrucken eines Dokuments an den nächstgelegenen Drucker gesendet.

Die standortbasierte Druckfunktion ist für Windows, Mac, Linux und Mobil-Clientgeräte verfügbar. Sie steht auch für browserbasierte Clients zur Verfügung.

Hinweis Die Richtlinien für das standortbasierte Drucken, die die MAC-Adresse oder den Client-Namen verwenden, werden nicht unterstützt, wenn Sie HTML Access verwenden, um sich mit Remote-Desktops und veröffentlichten Anwendungen zu verbinden.

Das standortbasierte Drucken wird auf folgenden Remote-Desktops und -Anwendungen unterstützt:

- Desktops, die auf Computern für Einzelbenutzer bereitgestellt werden, z. B. Windows Desktop- und Windows Server-Maschinen
- Veröffentlichte Desktops und veröffentlichte Anwendungen, die auf RDS-Hosts bereitgestellt werden, wobei die RDS-Hosts virtuelle Maschinen oder physische Computer sind
- Veröffentlichte Anwendungen, die von Horizon Client innerhalb von Remote-Desktops gestartet werden

Um die standortbasierte Druckfunktion zu verwenden, müssen Sie die Setup-Optionen für den virtuellen Druck mit Horizon Agent sowie die korrekten Druckertreiber auf dem Desktop installieren.

Sie richten den standortbasierten Druck ein, indem Sie die Active Directory-Gruppenrichtlinieneinstellung **AutoConnect Map Additional Printers for VMware View** konfigurieren, die sich im Gruppenrichtlinienobjekt-Editor von Microsoft im Ordner **Softwareeinstellungen** unter **Computerkonfiguration** befindet.

Hinweis AutoConnect Map Additional Printers for VMware View ist eine computerspezifische Richtlinie. Computerspezifische Richtlinien gelten für alle Remote-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.

AutoConnect Map Additional Printers for VMware View ist als eine Tabelle für die Namensübersetzung implementiert. Sie verwenden jede Zeile in der Tabelle, um einen bestimmten Drucker zu identifizieren und einen Satz an Übersetzungsregeln für diesen Drucker zu definieren. Die Übersetzungsregeln legen fest, ob der Drucker zum Remote-Desktop für ein bestimmtes Clientsystem zugeordnet wird.

Wenn sich ein Benutzer mit einem Remote-Desktop verbindet, vergleicht Horizon 7 das Clientsystem mit den Übersetzungsregeln, die mit jedem Drucker in der Tabelle verknüpft sind. Wenn das Clientsystem allen Übersetzungsregeln für einen Drucker entspricht, oder wenn mit einem Drucker keine Übersetzungsregeln verknüpft sind, ordnet Horizon 7 den Drucker während der Benutzersitzung dem Remote-Desktop zu.

Sie können Übersetzungsregeln basierend auf der IP-Adresse, dem Namen und der MAC-Adresse des Clientsystems sowie basierend auf dem Benutzernamen und der Benutzergruppe definieren. Sie können für einen bestimmten Drucker eine Übersetzungsregel oder eine Kombination aus mehreren Übersetzungsregeln festlegen.

Die Informationen für die Zuordnung des Druckers zum Remote-Desktop werden in einem Eintrag im Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect auf dem Remote-Desktop gespeichert.

Druckereinstellungen für standortbasiertes Drucken

– Die Druckereinstellungen für standortbasierte Drucker bleiben auch dann erhalten, wenn der Benutzer sich abmeldet oder die Verbindung mit dem Desktop beendet. Beispiel: Ein Benutzer konfiguriert einen standortbasierten Drucker für die Verwendung des Schwarzweißmodus. Nachdem der Benutzer sich vom Desktop abgemeldet und erneut bei ihm angemeldet hat, verwendet der standortbasierte Drucker weiterhin den Scharzweißmodus.

Um Druckereinstellungen sitzungsübergreifend in einer veröffentlichten Anwendung zu speichern, muss der Benutzer im Dialogfeld „Drucken“ der Anwendung einen standortbasierten Drucker auswählen, mit der rechten Maustaste auf den ausgewählten Drucker klicken und anschließend **Druckereinstellungen** auswählen. Druckereinstellungen werden nicht gespeichert, wenn der Benutzer im Dialogfeld „Drucken“ der Anwendung einen Drucker auswählt und auf die Schaltfläche **Einstellungen** klickt.

Dauerhafte Einstellungen für standortbasierte Drucker werden nicht unterstützt, wenn die Einstellungen im „private space“ (geräteabhängigen Teil) des Druckertreibers statt, wie von Microsoft empfohlen, im erweiterten (geräteunabhängigen) DEVMODE-Teil des Druckertreibers gespeichert werden. Um dauerhafte Einstellungen zu unterstützen, sollen Sie Drucker bereitstellen, die ihre Einstellungen im DEVMODE-Teil des Druckertreibers speichern lassen.

Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck

Um die Gruppenrichtlinieneinstellung für den standortbasierten Druck konfigurieren zu können, muss die DLL-Datei TPVMGPoACmap.dll registriert werden.

Die 32- und 64-Bit-Versionen von TPVMGPoACmap.dll stehen in einer mitgelieferten .zip-Datei namens VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip zur Verfügung, wobei x.x.x die Version und yyyyyy die Build-Nummer ist. Sie können die Datei von der VMware-Download-Site unter <http://www.vmware.com/go/downloadview> herunterladen.

Verfahren

- 1 Kopieren Sie die geeignete Version der DLL-Datei TPVMGPoACmap.dll auf Ihren Active Directory-Server oder den Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.
- 2 Verwenden Sie das Dienstprogramm regsvr32, um die Datei TPVMGPoACmap.dll zu registrieren.
Zum Beispiel: `regsvr32 "C:\TPVMGPoACmap.dll"`

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellung für den standortbasierten Druck.

Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck

Um den standortbasierten Druck einzurichten, konfigurieren Sie die Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View`. Die Gruppenrichtlinieneinstellung ist eine Tabelle mit Namensübersetzungen, die Drucker zu Horizon-Desktops zuordnet.

Voraussetzungen

- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server oder dem Domänencomputer zur Verfügung stehen, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.
- Registrieren Sie die DLL-Datei TPVMGPoACmap.dll auf Ihrem Active Directory-Server oder dem Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden. Siehe [Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck](#).
- Machen Sie sich mit der Syntax der Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View` vertraut. Siehe [Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck](#).
- Erstellen Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für die Gruppenrichtlinieneinstellung für den standortbasierten Druck und verknüpfen Sie es mit der Organisationseinheit (Organizational Unit, OU), die Ihre Horizon-Desktops enthält. Unter [Erstellen von GPOs für Horizon 7-Gruppenrichtlinien](#) finden Sie ein Beispiel für die Erstellung von GPOs für Horizon-Gruppenrichtlinien.
- Überprüfen Sie, ob die Setuption „Virtueller Druck“ mit Horizon Agent auf Ihren Desktops installiert wurde. Überprüfen Sie dazu, ob die Dienste „TP AutoConnect Service“ und „TP VC Gateway Service“ auf dem Desktop-Betriebssystem installiert sind.
- Da Druckaufträge direkt vom Horizon-Desktop zum Drucker gesendet werden, müssen Sie sicherstellen, dass die erforderlichen Druckertreiber auf Ihren Desktops installiert sind.

Verfahren

- 1 Bearbeiten Sie das GPO auf dem Active Directory-Server.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf die OU, die Ihre Horizon-Desktops enthält, und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellung für den standortbasierten Druck erstellt haben, und wählen Sie Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die standortbasierte Druckgruppenrichtlinieneinstellung erstellt haben, und wählen Sie Bearbeiten aus.

Das Fenster **Gruppenrichtlinienobjekt-Editor** wird angezeigt.

- 2 Erweitern Sie die Ansicht **Computerkonfiguration**, öffnen Sie den Ordner **Softwareeinstellungen** und wählen Sie **Automatische Zuordnung zusätzlicher Drucker für VMware View** aus.
- 3 Doppelklicken Sie im Fensterbereich „Richtlinie“ auf **Automatische Zuordnung zusätzlicher Drucker konfigurieren**.

Das Fenster **Automatische Zuordnung zusätzlicher Drucker für VMware View** wird angezeigt.

- 4 Wählen Sie die Option **Aktiviert**, um die Gruppenrichtlinieneinstellung zu aktivieren.

Im Gruppenrichtlinienfenster werden die Überschriften und Schaltflächen der Übersetzungstabelle angezeigt.

Wichtig Durch Klicken auf **Deaktiviert** werden alle Tabelleneinträge gelöscht. Als Vorsichtsmaßnahme sollten Sie Ihre Konfiguration speichern, um sie später importieren zu können.

- 5 Fügen Sie alle Drucker hinzu, die Sie Horizon-Desktops zuordnen möchten, und definieren Sie die zugehörigen Übersetzungsregeln.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck

Sie verwenden die Gruppenrichtlinieneinstellung AutoConnect Map Additional Printers for VMware View, um Drucker zu Remote-Desktops zuzuordnen.

AutoConnect Map Additional Printers for VMware View ist eine Tabelle für die Namensübersetzung, die Drucker identifiziert und verknüpfte Übersetzungsregeln definiert. [Tabelle 5-40. Spalten und Werte in der Übersetzungstabelle](#) beschreibt die Syntax der Übersetzungstabelle.

Standortbasiertes Drucken weist lokalen Druckern Remote-Desktops zu, unterstützt jedoch nicht die Zuweisung von Netzwerkdruckern, die durch Verwendung von UNC-Pfaden konfiguriert wurden.

Tabelle 5-40. Spalten und Werte in der Übersetzungstabelle

Spalte	Beschreibung
IP Range	<p>Eine Übersetzungsregel, die einen Bereich mit IP-Adressen für Clientsysteme angibt.</p> <p>Verwenden Sie die folgende Notierung, um IP-Adressen in einem bestimmten Bereich anzugeben:</p> <p><i>IP-Adresse–IP-Adresse</i></p> <p>Beispiel: 10.112.116.0–10.112.119.255</p> <p>Verwenden Sie die folgende Notierung, um alle IP-Adressen in einem bestimmten Subnetz anzugeben:</p> <p><i>ip_adresse/subnetz_masken_bits</i></p> <p>Beispiel: 10.112.4.0/22</p> <p>Diese Notierung gibt die verwendbaren IPv4-Adressen von 10.112.4.1 bis 10.112.7.254 an.</p> <p>Geben Sie für eine beliebige IP-Adresse ein Sternchen (*) ein.</p> <p>Wichtig Fügen Sie in einer IPv6-Umgebung im gemischten Modus zwei IP-Adressbereiche für einen Drucker hinzu (einen Bereich für IPv4-Adressen und einen weiteren Bereich für IPv6-Adressen), um sicherzustellen, dass der Drucker in Remote-Sitzungen unabhängig von dem von Horizon Client für die Verbindung verwendeten Protokoll angezeigt wird.</p>
Client Name	<p>Eine Übersetzungsregeln, die einen Computernamen angibt.</p> <p>Beispiel: Marias Computer</p> <p>Geben Sie für einen beliebigen Computernamen ein Sternchen (*) ein.</p>
Mac Address	<p>Eine Übersetzungsregeln, die eine MAC-Adresse angibt. Im GPO-Editor muss dasselbe Format wie im Clientsystem verwendet werden. Beispiel:</p> <ul style="list-style-type: none"> ■ Windows-Clients verwenden Bindestriche: 01–23–45–67–89–ab ■ Linux-Clients verwenden Doppelpunkte: 01:23:45:67:89:ab <p>Geben Sie für eine beliebige MAC-Adresse ein Sternchen (*) ein.</p>
User/Group	<p>Eine Übersetzungsregeln, die einen Benutzer oder eine Benutzergruppe angibt.</p> <p>Um einen bestimmten Benutzer oder eine bestimmte Gruppe anzugeben, verwenden Sie die folgende Notierung:</p> <p><i>\\Domäne\Benutzer_oder_Gruppe</i></p> <p>Beispiel: \\meineDomäne\Marie</p> <p>Der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) wird für den Domänennamen nicht unterstützt. Geben Sie für einen beliebigen Benutzernamen bzw. eine beliebige Benutzergruppe ein Sternchen (*) ein.</p>
Printer Name	<p>Der Name des Druckers bei der Zuweisung zum Remote-Desktop.</p> <p>Beispiel: DRUCKER–2–CLR</p> <p>Der zugewiesene Name muss nicht dem Druckernamen auf dem Clientsystem entsprechen.</p> <p>Der Drucker muss lokal am Clientgerät angeschlossen sein. Die Zuweisung eines Netzwerkdruckers in einem UNC-Pfad wird nicht unterstützt.</p>

Tabelle 5-40. Spalten und Werte in der Übersetzungstabelle (Fortsetzung)

Spalte	Beschreibung
Printer Driver	<p>Der Name des Treibers, den der Drucker verwendet.</p> <p>Beispiel: HP Color LaserJet 4700 PS</p> <p>Wichtig Da Druckaufträge direkt vom Remote-Desktop zum Drucker gesendet werden, muss der Druckertreiber auf dem Remote-Desktop installiert sein.</p>
IP Port/ThinPrint Port	<p>Für Netzwerkdrucker wird der IP-Adresse des Druckers das Präfix IP_ vorangestellt.</p> <p>Beispiel: IP_10.114.24.1</p> <p>Der Standardport lautet 9100. Sie können einen nicht standardmäßigen Port durch Anhängen der Portnummer an die IP-Adresse angeben.</p> <p>Beispiel: IP_10.114.24.1:9104</p>
Default	Gibt an, ob es sich bei dem Drucker um den Standarddrucker handelt.

Sie verwenden die Schaltflächen, die oberhalb der Spaltenüberschriften angezeigt werden, um Tabelleneinträge hinzuzufügen, zu löschen, Zeilen zu verschieben und zu importieren. Jede Schaltfläche verfügt über eine äquivalente Tastaturkombination. Bewegen Sie die Maus über jede Schaltfläche, um eine Beschreibung der Schaltfläche und die zugehörige Tastaturkombination anzuzeigen. Um beispielsweise eine Zeile am Ende der Tabelle einzufügen, klicken Sie auf die erste Tabellenschaltfläche und drücken Alt+A. Klicken Sie auf die letzten zwei Schaltflächen, um Tabelleneinträge zu importieren und zu speichern.

[Tabelle 5-41. Gruppenrichtlinieneinstellung für den standortbasierten Druck – Beispiel](#) zeigt ein Beispiel für zwei Zeilen einer Übersetzungstabelle.

Tabelle 5-41. Gruppenrichtlinieneinstellung für den standortbasierten Druck – Beispiel

IP-Bereich	Clientname	Mac-Adresse	Benutzer / Gruppe	Druckername	Druckertreiber	IP Port/ThinPrint Port (IP-Port/ThinPrint-Port)	Standard
*	*	*	*	DRUCKER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	DRUCKER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

Der in der ersten Zeile angegebene Netzwerkdrucker wird einem Remote-Desktop für ein beliebiges Clientsystem zugeordnet, da in allen Spalten für die Übersetzungsregeln Sternchen angezeigt werden. Der in der zweiten Zeile angegebene Netzwerkdrucker wird nur dann einem Remote-Desktop zugeordnet, wenn sich die IP-Adresse des Clientsystems im Bereich 10.112.116.140 bis 10.112.116.145 befindet.

Verwalten von speziellen Unity-Fenstern

Sie können die Agent-Gruppenrichtlinieneinstellung **Liste mit Unity-Filterregeln** verwenden, um Unity-Fenster herauszufiltern oder Unity-Fenster einem bestimmten Typ zuzuordnen, wenn Sie veröffentlichte Anwendungen verwenden. Diese Funktion ist nützlich, wenn Sie ein Fensteranzeigeproblem, beispielsweise ein Fenster mit einem schwarzen Hintergrund, oder ein Dropdown-Fenster mit falscher Größe haben.

Die Gruppenrichtlinieneinstellung **Liste mit Unity-Filterregeln** ist in der ADMX-Vorlagendatei zur Konfiguration von VMware View Agent (`vdm_agent.admx`) verfügbar, die in die Datei `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` gepackt ist. Weitere Installationsanweisungen finden Sie unter [Hinzufügen der ADMX-Vorlagendateien in Active Directory](#).

Wenn Sie die Gruppenrichtlinieneinstellung **Liste mit Unity-Filterregeln** aktivieren, klicken Sie auf **Anzeigen**, und geben Sie eine Filterregel in das Textfeld **Wert** ein. Eine Filterregel besteht aus Merkmalen und Aktionen. Wenn Sie die Aktion Zuordnen angeben, müssen Sie auch einen Typ angeben. Die folgende Tabelle enthält die Merkmale, Aktionen und Typen, die Sie in Filterregeln verwenden können.

Tabelle 5-42. Merkmale, Aktionen und Typen der Unity-Filterregeln

Merkmale	Aktionen	Typen
classname, company, product, major, minor, build, revision	block, map	normal, panel, dialog, tooltip, splash, toolbar, dock, desktop, widget, combobox, startscreen, sidepanel, taskbar, metrofullscreen, metrodocked

Der Windows-Klassenname in der Regel ist das bevorzugte Merkmal, z. B.

`classname=CustomClassName`. Die Merkmale `company`, `product`, `major`, `minor`, `build` und `revision` werden bereitgestellt, für den Fall, dass Sie Regeln auf ein bestimmtes Produkt beschränken müssen. Sie finden die Werte für diese Merkmale im Fenster **Eigenschaften** einer ausführbaren Datei. Die Werte für diese Merkmale müssen in der Groß-/Kleinschreibung (einschließlich Sonderzeichen) genau übereinstimmen. Wenn Sie mehrere Merkmale angeben, müssen alle Werte übereinstimmen, damit die Regel für das Fenster gilt.

Um eine Aktion zu festzulegen, geben Sie `action=wert`, z. B. `action=block` ein. Die Aktion `block` weist Horizon Agent an, das Fenster nicht auf dem Client anzuzeigen. Verwenden Sie die Aktion `block`, wenn ein Fenster zu groß angezeigt wird oder mit normalem Fensterfokusverhalten auf dem Client in Konflikt steht.

Die Aktion `map`, z. B. `action=map`, weist Horizon Agent an, das Fenster als einen bestimmten hartcodierten Typ zu behandeln. Um den Typ anzugeben, müssen Sie `type=wert` in der Regel angeben, z. B. `type=normal`. Da es schwierig ist, festzustellen, ob ein Fenster dem falschen Typ zugeordnet ist, ist die Zuordnung eines Fensters zu einem Typ nur notwendig, wenn der VMware-Support Sie dazu anweist.

Beispiele für Filterregeln

Die folgende Filterregel blockiert alle Fenster, die den Klassennamen „MyClassName“ haben.

```
classname=MyClassName;action=block
```

Die folgende Filterregel blockiert alle Fenster des Produkts „MyProduct“.

```
product=MyProduct;action=block
```

Die folgende Filterregel ordnet eine benutzerdefinierte Klasse dem Typ der Combobox zu.

```
classname=MyClassName;action=map;type=combobox
```

Hinweis Die Gruppenrichtlinieneinstellung **Liste mit Unity-Filterregeln** hat eine niedrigere Priorität als Filterregeln, die im Verzeichnis %ProgramData%\VMware\RdeServer\Unity Filters einer Datei auf dem RDS-Host angegeben werden.

Beispiel einer Active Directory-Gruppenrichtlinie

Eine Möglichkeit zur Implementierung von Active Directory-Gruppenrichtlinien in Horizon 7 besteht darin, eine Organisationseinheit (OU) für Computer zu erstellen, die Remote-Desktop-Sitzungen übermitteln, und mindestens ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) mit dieser OU zu verknüpfen. Sie können diese GPOs verwenden, um Gruppenrichtlinieneinstellungen auf Ihre Horizon 7-Computer anzuwenden.

GPOs können direkt mit einer Domäne verbunden werden, wenn die Gruppenrichtlinieneinstellungen für alle Computer in dieser Domäne gelten. Es hat sich jedoch bewährt, die GPOs in den meisten Bereitstellungen mit einzelnen OUs zu verbinden, um zu vermeiden, dass Richtlinien auf allen Computern in der Domäne verarbeitet werden.

Sie können Richtlinien auf Ihrem Active Directory-Server oder einem beliebigen anderen Computer in Ihrer Domäne konfigurieren. Dieses Beispiel zeigt, wie Sie Richtlinien direkt auf Ihrem Active Directory-Server konfigurieren.

Hinweis Da jede Horizon 7-Umgebung anders ist, müssen Sie möglicherweise unterschiedliche Schritte ausführen, um die Anforderungen der jeweiligen Organisation zu erfüllen.

Erstellen einer OU für Horizon 7-Computer

Um Gruppenrichtlinien auf Computer anzuwenden, die Remote-Desktop-Sitzungen bereitstellen, ohne dass sich dies auf andere Windows-Computer in derselben Active Directory-Domäne auswirkt, erstellen Sie eine Organisationseinheit (OU) speziell für Ihre Horizon 7-Computer. Möglicherweise erstellen Sie eine Organisationseinheit für Ihre gesamte Horizon 7-Bereitstellung oder separate Organisationseinheiten für einzelne virtuelle Desktop-Maschinen und RDS-Hosts.

Verfahren

- 1 Wählen Sie auf Ihrem Active Directory-Server **Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer** aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Domäne, die Ihre Horizon 7-Computer enthält, und wählen Sie **Neu > Organisationseinheit** aus.
- 3 Geben Sie einen Namen für die OU ein und klicken Sie auf **OK**.
Die neue OU wird im linken Fensterbereich angezeigt.
- 4 Fügen Sie der neuen OU Horizon 7-Computer hinzu.
 - a Klicken Sie im linken Fensterbereich auf **Computer**.
Alle Computerobjekte in der Domäne werden im rechten Fensterbereich angezeigt.
 - b Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Computerobjekt, das den Horizon 7-Computer repräsentiert, und wählen Sie **Verschieben** aus.
 - c Wählen Sie die OU und klicken Sie auf **OK**.
Der Horizon 7-Computer wird im rechten Fensterbereich angezeigt, wenn Sie die OU auswählen.

Nächste Schritte

Erstellen Sie GPOs für Horizon 7-Gruppenrichtlinien.

Erstellen von GPOs für Horizon 7-Gruppenrichtlinien

Erstellen Sie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) für Gruppenrichtlinien, die Sie für Horizon 7-Komponenten und den standortbasierten Druck konfigurieren, und verknüpfen Sie diese GPOs anschließend mit der Organisationseinheit (Organizational Unit, OU) für Ihre Horizon 7-Computer.

Voraussetzungen

- Erstellen Sie eine OU für Ihre Horizon 7-Computer.
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.
- 2 Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf die OU, die Ihre Horizon 7-Computer enthält, und wählen Sie **GPO in dieser Domäne erstellen und hier verknüpfen**.
- 3 Geben Sie einen Namen für das GPO ein und klicken Sie auf **OK**.
Das neue GPO wird im linken Fensterbereich unterhalb der OU angezeigt.

4 (Optional) Wenden Sie das GPO auf bestimmte Horizon 7-Computer in der OU an.

- a Wählen Sie das GPO im linken Fensterbereich aus.
- b Wählen Sie **Sicherheitsfilterung > Hinzufügen** aus.
- c Geben Sie die Computernamen der Horizon 7-Computer ein und klicken Sie auf **OK**.

Die Horizon 7-Computer werden im Fensterbereich „Sicherheitsfilterung“ angezeigt. Die Einstellungen im GPO werden nur auf diese Computer angewendet.

Nächste Schritte

Fügen Sie die Horizon-ADMX-Vorlagen zum GPO hinzu.

Hinzufügen einer Horizon 7-ADMX-Vorlagendatei zu einem GPO

Um Gruppenrichtlinieneinstellungen für Horizon 7-Komponenten auf Ihre Desktops und Anwendungen anzuwenden, fügen Sie den GPOs die zugehörigen ADMX-Vorlagendateien hinzu.

Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für Horizon 7-Komponenten und verknüpfen Sie sie mit der Organisationseinheit, die Ihre Horizon 7-Computer enthält.
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- 1 Laden Sie die Horizon 7-GPO-Bundle-.zip-Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die GPO-Bundle-Datei enthält.

Der Dateiname ist VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip und kopieren Sie die ADMX-Dateien auf Ihren Active Directory-Server.
 - a Kopieren Sie die .admx-Dateien und den Ordner en-US in den Ordner %systemroot%\PolicyDefinitions auf Ihrem Active Directory-Server.
 - b Kopieren Sie die Sprachressourcendateien (.adml) in den entsprechenden Unterordner des Ordners %systemroot%\PolicyDefinitions\ auf Ihrem Active Directory-Server.

- Öffnen Sie auf dem Active Directory-Server den Gruppenrichtlinienverwaltungs-Editor und geben Sie den Pfad zu den Vorlagendateien an der Stelle ein, an der diese im Editor nach der Installation angezeigt werden.

Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen und aktivieren Sie die Loopbackverarbeitung für Ihre Horizon 7-Computer.

Aktivieren der Loopback-Verarbeitung für Remote-Desktops

Um Benutzerkonfigurationseinstellungen, die normalerweise für einen Computer gelten, auf alle Benutzer anzuwenden, die sich an diesem Computer anmelden, aktivieren Sie die Loopback-Verarbeitung.

Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für Horizon 7-Komponenten und verknüpfen Sie sie mit der Organisationseinheit, die Ihre Horizon 7-Computer enthält.
- Stellen Sie sicher, dass Sie sich als Administratordomänenbenutzer auf dem Computer anmelden können, auf dem Ihr Active Directory-Server gehostet wird.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server installiert sind.

Verfahren

- Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsolle für Gruppenrichtlinien.
- Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- Navigieren Sie im Gruppenrichtlinienverwaltungs-Editor zu **Computerkonfiguration > Richtlinien > Administrative Vorlagen: Richtliniendefinitionen > System > Gruppenrichtlinie**.
- Doppelklicken Sie im rechten Bereich auf **Loopback-Verarbeitungsmodus für Benutzergruppenrichtlinie**.
- Wählen Sie **Aktiviert** und danach einen Loopback-Verarbeitungsmodus im Dropdown-Menü **Modus** aus.

Option	Aktion
Merge (Zusammenführen)	Die angewendeten Benutzerrichtlinieneinstellungen sind eine Kombination der Richtlinien in den Computer- und Benutzer-GPOs. Bei Konflikten haben die Computer-GPOs Vorrang.
Replace (Ersetzen)	Die Benutzerrichtlinie wird ausschließlich anhand der mit dem Computer verknüpften GPOs definiert. Mit dem Benutzer verknüpfte GPOs werden ignoriert.

- Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.