

Horizon Client und Agent-Sicherheit

Horizon Client 3.x/4.x/5.x und View Agent 6.2.x/Horizon Agent 7.x

14. MÄRZ 2019

VMware Horizon 7 7.8



vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Inhalt

Horizon Client- und Agent-Sicherheit 5

1 Externe Ports 7

Grundlegendes zu Kommunikationsprotokollen 7

Firewall-Regeln für View Agent oder Horizon Agent 8

Von Clients und Agents verwendete TCP- und UDP-Ports 9

2 Installierte Dienste, Deamons und Prozesse 14

Durch das View Agent- oder Horizon Agent -Installationsprogramm auf Windows-Maschinen installierte Dienste 14

Auf dem Windows-Client installierte Dienste 15

In anderen Clients und dem Linux-Desktop installierte Daemons 16

3 Zu sichernde Ressourcen 17

Implementieren von Best Practices zum Sichern von Clientsystemen 17

Konfigurationsdateispeicherorte 17

Konten 18

4 Sicherheitseinstellungen für Client und Agent 20

Konfigurieren der Zertifikatsprüfung 20

Sicherheitsbezogene Einstellungen in den View Agent- und Horizon Agent -Konfigurationsvorlagen 21

Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop 23

Gruppenrichtlinieneinstellungen für HTML Access 34

Sicherheitseinstellungen in den Horizon Client -Konfigurationsvorlagen 36

Konfigurieren des Horizon Client -Zertifikatüberprüfungsmodus 40

Konfigurieren des Schutzes durch die lokale Sicherheitsautorität 41

5 Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen 42

Standardmäßige Richtlinien für Sicherheitsprotokolle und Verschlüsselungssammlungen 42

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für spezielle Clienttypen 51

Deaktivieren von schwachen Verschlüsselungen in SSL/TLS 52

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für HTML Access-Agent 53

Konfigurieren von Vorschlagsrichtlinien auf Remote-Desktops 54

6 Client- und Agent-Protokolldateispeicherorte 55

Horizon Client für Windows-Protokolle 55

[Horizon Client für Mac-Protokolle](#) 58

[Horizon Client für Linux-Protokolle](#) 59

[Horizon Client-Protokolle auf mobilen Geräten](#) 60

[Horizon Agent -Protokolle von Windows-Computern](#) 61

[Linux-Desktop-Protokolle](#) 62

7 Anwenden von Sicherheits-Patches 65

[Anwenden eines Patches für View Agent oder Horizon Agent](#) 65

[Anwenden eines Patches für Horizon Client](#) 66

Horizon Client- und Agent-Sicherheit

Horizon Client und Agent-Sicherheit bietet eine kurze Referenz für die Sicherheitsfunktionen von VMware Horizon® Client™ und Horizon Agent (für Horizon 7) oder VMware View Agent® (für Horizon 6). Dieses Handbuch ist als Ergänzung für das Handbuch *Horizon 7-Sicherheit* vorgesehen, das für jede Haupt- und Nebenversion von VMware Horizon™ 6 und Horizon 7 hergestellt wird. Das Handbuch *Horizon Client und Agent-Sicherheit* wird vierteljährlich aktualisiert – zusammen mit den vierteljährlich erscheinenden Versionen der Client- und Agent-Software.

Horizon Client ist die Anwendung, die von Endbenutzern auf ihren Clientgeräten gestartet wird, um die Verbindung zu einer Remoteanwendung oder zum Remote-Desktop herzustellen. View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7) ist die Agent-Software, die im Betriebssystem des Remote-Desktops oder des Microsoft RDS-Hosts ausgeführt wird, der die Remoteanwendungen bereitstellt. Dieses Handbuch enthält die folgenden Informationen:

- Erforderliche Anmeldekonto für das System. Die bei der Systeminstallation/beim Bootstrap erstellte Anmelde-ID von Konten sowie Anweisungen dazu, wie Standardwerte geändert werden.
- Sicherheitsrelevante Konfigurationsoptionen und Einstellungen.
- Zu schützende Ressourcen, z. B. sicherheitsrelevante Konfigurationsdateien und Kennwörter, sowie die empfohlenen Zugriffskontrollen für sicheren Betrieb.
- Speicherort von Protokolldateien und deren Zweck.
- Die „Dienst“-Benutzern zugewiesenen Berechtigungen.
- Externe Schnittstellen, Ports und Dienste, die für den ordnungsgemäßen Betrieb des Client und Agent geöffnet oder aktiviert sein müssen.
- Informationen dazu, wie Kunden die neuesten Sicherheits-Updates/-Patches erhalten und installieren können.

Zielgruppe

Diese Informationen richten sich an IT-Entscheider, -Architekten, -Administratoren und andere Personen, die sich mit den Sicherheitskomponenten von Horizon 6 oder Horizon 7, einschließlich Client und Agent, vertraut machen möchten.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Externe Ports

Zum ordnungsgemäßen Betrieb des Produkts und in Abhängigkeit der Funktionen, die Sie nutzen möchten, müssen bestimmte Ports geöffnet sein, damit die Clients und der Agent auf Remote-Desktops miteinander kommunizieren können.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu Kommunikationsprotokollen](#)
- [Firewall-Regeln für View Agent oder Horizon Agent](#)
- [Von Clients und Agents verwendete TCP- und UDP-Ports](#)

Grundlegendes zu Kommunikationsprotokollen

Horizon 6- und Horizon 7-Komponenten tauschen Meldungen mithilfe mehrerer unterschiedlicher Protokolle aus.

[Tabelle 1-1](#) zeigt die Standardports, die von den einzelnen Protokollen verwendet werden. Um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern, können die verwendeten Portnummern bei Bedarf geändert werden.

Tabelle 1-1. Standardports

| Protokoll | Port |
|-------------------------|--|
| JMS | TCP-Port 4001 TCP-Port 4002 |
| HTTP | TCP-Port 80 |
| HTTPS | TCP-Port 443 |
| MMR/CDR | Für Multimedia-Umleitung und Clientlaufwerksumleitung, TCP-Port 9427 |
| RDP- | TCP-Port 3389 |
| PCoIP | TCP-Port 4172 UDP-Ports 4172, 50002, 55000 |
| USB-Umleitung | TCP-Port 32111. Dieser Port wird auch zur Zeitzonensynchronisierung verwendet. |
| VMware Blast Extreme | TCP-Ports 8443, 22443 UDP-Ports 443, 8443, 22443 |
| HTML Access | TCP-Ports 8443, 22443 |

Firewall-Regeln für View Agent oder Horizon Agent

Mit den Installationsprogrammen für View Agent und Horizon Agent lassen sich optional Windows-Firewallregeln auf Remote-Desktops und RDS-Hosts für das Öffnen der standardmäßigen Netzwerkports konfigurieren. Wenn nicht anders angegeben, handelt es sich hierbei um eingehende Ports.

Die Installationsprogramme für View Agent und Horizon Agent konfigurieren die lokale Firewallregel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389).

Wenn Sie im Installationsprogramm für View Agent oder Horizon Agent angeben, dass die Remote-Desktop-Unterstützung nicht aktiviert werden soll, werden die Ports 3389 und 32111 nicht geöffnet. Sie müssen diese Ports dann manuell öffnen.

Wenn Sie die RDP-Portnummer nach der Installation ändern, müssen Sie die dazugehörigen Firewall-Regeln ändern. Wenn Sie den Standard-Port nach der Installation ändern, müssen Sie die Windows-Firewall-Regeln manuell neu konfigurieren, um den Zugriff auf den aktualisierten Port zu erlauben. Weitere Informationen finden Sie unter „Ersetzen von Standardports für View-Dienste“ im Dokument *Horizon 7-Installation*.

Die Windows-Firewallregeln für View Agent oder Horizon Agent auf RDS-Hosts zeigen an, dass ein Block von 256 zusammenhängenden UDP-Ports für den eingehenden Datenverkehr geöffnet ist. Dieser Portblock ist für die interne Verwendung von VMware Blast in View Agent oder Horizon Agent vorgesehen. Ein spezieller Microsoft-signierter Treiber auf RDS-Hosts blockiert den eingehenden Datenverkehr zu diesen Ports von externen Quellen. Aufgrund dieses Treibers behandelt die Windows-Firewall die Ports als geschlossen.

Bei Verwendung einer Vorlage einer virtuellen Maschine als Desktop-Quelle werden Firewall-Ausnahmen auf bereitgestellten Desktops nur dann übernommen, wenn die Vorlage eine virtuelle Maschine der Desktop-Domäne ist. Sie können Microsoft-Gruppenrichtlinieneinstellungen verwenden, um lokale Firewall-Ausnahmen zu verwalten. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 875357.

Tabelle 1-2. Während der View Agent- oder Horizon Agent -Installation geöffnete TCP- und UDP-Ports

| Protokoll | Ports |
|---|----------------|
| RDP- | TCP-Port 3389 |
| USB-Umleitung und Zeitzonensynchronisierung | TCP-Port 32111 |
| MMR (Multimedia-Umleitung) und CDR (Clientlaufwerksumleitung) | TCP-Port 9427 |

Tabelle 1-2. Während der View Agent- oder Horizon Agent -Installation geöffnete TCP- und UDP-Ports (Fortsetzung)

| Protokoll | Ports |
|--------------|--|
| PCoIP | <p>Für RDS-Hosts verwendet PCoIP die folgenden Portnummern: TCP-Port 4172 und UDP-Port 4172 (bidirektional).</p> <p>Für Desktops verwendet PCoIP Portnummern aus einem konfigurierbaren Bereich. Standardmäßig verbindet TCP 4172 mit 4173 und UDP verbindet 4172 mit 4182. Die Firewall-Regeln hierfür legen keine Portnummern fest, sondern folgen dynamisch den Ports, die von jedem PCoIP-Server geöffnet werden. Die ausgewählten Portnummern werden über den Verbindungsserver an den Client übertragen.</p> |
| VMware Blast | <p>TCP-Port 22443</p> <p>UDP-Port 22443 (bidirektional)</p> <p>Hinweis UDP wird auf Linux-Desktops nicht verwendet.</p> |
| HTML Access | TCP-Port 22443 |
| XDMCP | <p>UDP 177</p> <p>Hinweis Dieser Port ist nur auf Linux-Desktops mit Ubuntu 18.04 für den XDMCP-Zugriff geöffnet. Firewallregeln blockieren den gesamten externen Hostzugriff auf diesen Port.</p> |
| X11 | <p>TCP 6100</p> <p>Hinweis Dieser Port ist nur auf Linux-Desktops mit Ubuntu 18.04 für den XServer-Zugriff geöffnet. Firewallregeln blockieren den gesamten externen Hostzugriff auf diesen Port.</p> |

Von Clients und Agents verwendete TCP- und UDP-Ports

View Agent (für Horizon 6), Horizon Agent (für Horizon 7) und Horizon Client verwenden TCP- und UDP-Ports für den Netzwerkzugriff untereinander und zwischen den verschiedenen Serverkomponenten.

Tabelle 1-3. Von View Agent oder Horizon Agent verwendete TCP- und UDP-Ports

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|----------------|------|--------------------------|-------|-----------|--|
| Horizon Client | * | View Agent/Horizon Agent | 3389 | TCP | Microsoft RDP-Datenverkehr zu Remote-Desktops, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |
| Horizon Client | * | View Agent/Horizon Agent | 9427 | TCP | <p>Windows Media MMR-Umleitung und Clientlaufwerksumleitung, wenn anstelle von Tunnelverbindungen direkte Verbindungen verwendet werden.</p> <p>Hinweis Wird nicht für die Clientlaufwerksumleitung benötigt, wenn VMware Blast verwendet wird.</p> |
| Horizon Client | * | View Agent/Horizon Agent | 32111 | TCP | USB-Umleitung und Zeitzonensynchronisierung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |

Tabelle 1-3. Von View Agent oder Horizon Agent verwendete TCP- und UDP-Ports (Fortsetzung)

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|--|-------|--------------------------|-------|-------------|--|
| Horizon Client | * | View Agent/Horizon Agent | 4172 | TCP und UDP | PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird. Hinweis Da es verschiedene Quellports gibt, siehe den Hinweis unter dieser Tabelle. |
| Horizon Client | * | Horizon Agent | 22443 | TCP und UDP | VMware Blast, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. Hinweis UDP wird auf Linux-Desktops nicht verwendet. |
| Browser | * | View Agent/Horizon Agent | 22443 | TCP | HTML Access, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | View Agent/Horizon Agent | 3389 | TCP | Microsoft RDP-Datenverkehr zu Remote-Desktops, wenn Tunnelverbindungen verwendet werden. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | View Agent/Horizon Agent | 9427 | TCP | Windows Media-MMR-Umleitung und Clientlaufwerksumleitung, wenn Tunnelverbindungen verwendet werden. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | View Agent/Horizon Agent | 32111 | TCP | USB-Umleitung und Zeitzonensynchronisierung, wenn Tunnelverbindungen verwendet werden. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | 55000 | View Agent/Horizon Agent | 4172 | UDP | PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | View Agent/Horizon Agent | 4172 | TCP | PCoIP, wenn PCoIP Secure Gateway verwendet wird. |
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | Horizon Agent | 22443 | TCP und UDP | VMware Blast, wenn das Blast Secure Gateway verwendet wird. Hinweis UDP wird auf Linux-Desktops nicht verwendet. |

Tabelle 1-3. Von View Agent oder Horizon Agent verwendete TCP- und UDP-Ports (Fortsetzung)

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|--|------|--|------------|-----------|--|
| Sicherheitsserver, Verbindungsserver oder Unified Access Gateway-Appliance | * | View Agent/Horizon Agent | 22443 | TCP | HTML Access, wenn Blast Secure Gateway verwendet wird. |
| View Agent/Horizon Agent | * | Verbindungsserver | 4001, 4002 | TCP | JMS-SSL-Datenverkehr. |
| View Agent/Horizon Agent | 4172 | Horizon Client | * | UDP | PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird. Hinweis Da es verschiedene Zielpoints gibt, siehe den Hinweis unter dieser Tabelle. |
| View Agent/Horizon Agent | 4172 | Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance | 55000 | UDP | PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird. |

Hinweis Die UDP-Portnummer, die von Agents für PCoIP verwendet wird, kann sich ändern. Wenn Port 50002 verwendet wird, verwendet der Agent 50003. Wenn Port 50003 verwendet wird, verwendet der Agent 50004, usw. Sie müssen die Firewalls mit ANY konfigurieren, wo ein Sternchen (*) in der Tabelle aufgelistet ist.

Tabelle 1-4. Von Horizon Client verwendete TCP- und UDP-Ports

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|---|------|--|------|-----------|--|
| Horizon Client | * | Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance | 443 | TCP | HTTPS für die Anmeldung bei Horizon 6 oder Horizon 7. (Dieser Port wird auch zur Tunnelung verwendet, wenn Tunnelverbindungen verwendet werden.) Hinweis Horizon Client 4.4 und höher unterstützt den UDP-Port 443 (siehe im Folgenden). |
| Horizon Client 4.4 oder höher | * | Unified Access Gateway-Appliance 2.9 oder höher | 443 | UDP | HTTPS für die Anmeldung bei Horizon 6 oder Horizon 7, wenn das Blast Secure Gateway verwendet wird und der UDP-Tunnel-Server aktiviert ist. (Dieser Port wird auch zur Tunnelung verwendet, wenn Tunnelverbindungen verwendet werden.) |
| Unified Access Gateway-Appliance 2.9 oder höher | 443 | Horizon Client 4.4 oder höher | * | UDP | HTTPS für die Anmeldung bei Horizon 6 oder Horizon 7, wenn das Blast-Sicherheitsgateway verwendet wird und der UDP-Tunnel-Server aktiviert ist. (Dieser Port wird auch zur Tunnelung verwendet, wenn Tunnelverbindungen verwendet werden.) |

Tabelle 1-4. Von Horizon Client verwendete TCP- und UDP-Ports (Fortsetzung)

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|---|-------|--|-------|-------------|---|
| Horizon Client | * | View Agent/Horizon Agent | 22443 | TCP | HTML Access und VMware Blast, wenn das Blast-Sicherheitsgateway nicht verwendet wird. |
| Horizon Client | * | Horizon Agent | 22443 | UDP | VMware Blast, wenn das Blast Secure Gateway nicht verwendet wird. Hinweis Wird nicht für Verbindungen mit Linux-Desktops verwendet. |
| Horizon Agent | 22443 | Horizon Client | * | UDP | VMware Blast, wenn das Blast-Sicherheitsgateway nicht verwendet wird. Hinweis Wird nicht für Verbindungen mit Linux-Desktops verwendet. |
| Horizon Client | * | View Agent/Horizon Agent | 3389 | TCP | Microsoft RDP-Datenverkehr zu Remote-Desktops, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |
| Horizon Client | * | View Agent/Horizon Agent | 9427 | TCP | Windows Media MMR-Umleitung und Clientlaufwerksumleitung, wenn anstelle von Tunnelverbindungen direkte Verbindungen verwendet werden. Hinweis Wird nicht für die Clientlaufwerksumleitung benötigt, wenn VMware Blast verwendet wird. |
| Horizon Client | * | View Agent/Horizon Agent | 32111 | TCP | USB-Umleitung und Zeitzonensynchronisierung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |
| Horizon Client | * | View Agent/Horizon Agent | 4172 | TCP und UDP | PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird. Hinweis Da es verschiedene Quellports gibt, siehe den Hinweis unter dieser Tabelle. |
| Horizon Client | * | Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance | 4172 | TCP und UDP | PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird. Hinweis Da es verschiedene Quellports gibt, siehe den Hinweis unter dieser Tabelle. |
| View Agent/Horizon Agent | 4172 | Horizon Client | * | UDP | PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird. Hinweis Da es verschiedene Zielports gibt, siehe den Hinweis unter dieser Tabelle. |
| Sicherheitsserver, View-Verbindungsserver oder Unified Access Gateway-Appliance | 4172 | Horizon Client | * | UDP | PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird. Hinweis Da es verschiedene Zielports gibt, siehe den Hinweis unter dieser Tabelle. |

Tabelle 1-4. Von Horizon Client verwendete TCP- und UDP-Ports (Fortsetzung)

| Quelle | Port | Ziel | Port | Protokoll | Beschreibung |
|--|------|--|------|-----------|--|
| Horizon Client | * | Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance | 8443 | TCP | HTML Access und VMware Blast, wenn das Blast-Sicherheitsgateway verwendet wird. |
| Horizon Client | * | Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance | 8443 | UDP | VMware Blast, wenn das Blast-Sicherheitsgateway verwendet wird. Hinweis Wird nicht für Verbindungen mit einem Linux-Desktop verwendet. |
| View-Verbindungs- server, Sicherheits- server oder Unified Access Gateway-Appliance | 8443 | Horizon Client | * | UDP | VMware Blast, wenn das Blast Secure Gateway verwendet wird. Hinweis Wird nicht für Verbindungen mit einem Linux-Desktop verwendet. |

Hinweis Die UDP-Portnummer, die Clients für PCoIP und VMware Blast verwenden, kann sich ändern. Wenn Port 50002 verwendet wird, verwendet der Client 50003. Wenn Port 50003 verwendet wird, verwendet der Client 50004, usw. Sie müssen die Firewalls mit ANY konfigurieren, wo ein Sternchen (*) in der Tabelle aufgelistet ist.

Installierte Dienste, Deamons und Prozesse

2

Wenn Sie das Client- oder Agent-Installationsprogramm ausführen, werden verschiedene Komponenten installiert.

Dieses Kapitel enthält die folgenden Themen:

- [Durch das View Agent- oder Horizon Agent-Installationsprogramm auf Windows-Maschinen installierte Dienste](#)
- [Auf dem Windows-Client installierte Dienste](#)
- [In anderen Clients und dem Linux-Desktop installierte Daemons](#)

Durch das View Agent- oder Horizon Agent - Installationsprogramm auf Windows-Maschinen installierte Dienste

Der Betrieb von Remote-Desktops und Remoteanwendungen hängt von mehreren Windows-Diensten ab.

Tabelle 2-1. View Agent-Dienste (für Horizon 6) oder Horizon Agent -Dienste (für Horizon 7)

| Dienstname | Starttyp | Beschreibung |
|---|---|---|
| VMware Blast | Automatisch | Stellt Dienste für HTML Access und für die Verwendung des VMware Blast Extreme-Protokolls zur Herstellung einer Verbindung mit nativen Clients bereit. |
| VMware Horizon View Agent | Automatisch | Stellt Dienste für View Agent/Horizon Agent bereit. |
| VMware Horizon View Composer Guest Agent Server | Automatisch | Stellt Dienste bereit, wenn diese virtuelle Maschine Bestandteil eines Linked-Clone-Desktop-Pools von View Composer ist. |
| VMware Horizon View Persona Management | Automatisch, wenn die Funktion aktiviert ist; ansonsten deaktiviert | Stellt Dienste für die VMware Persona Management-Funktion bereit. |
| VMware Horizon View Script Host | Deaktiviert | Bietet Unterstützung für die Ausführung von Sitzungsstart-Skripts, sofern diese vorhanden sind, um die Desktop-Sicherheitsrichtlinien zu konfigurieren, bevor eine Desktop-Sitzung beginnt. Die Richtlinien basieren auf dem Client-Gerät und der Position des Benutzers. |

Tabelle 2-1. View Agent-Dienste (für Horizon 6) oder Horizon Agent -Dienste (für Horizon 7) (Fortsetzung)

| Dienstname | Starttyp | Beschreibung |
|---|-------------|---|
| VMware Netlink Supervisor Service | Automatisch | Unterstützt die Funktion zur Scannerumleitung und die Funktion zur Umleitung serieller Ports, stellt Überwachungsdienste zur Übertragung von Informationen zwischen Kernel- und Benutzerraumprozessen bereit. |
| VMware Scanner Redirection Client Service | Automatisch | (View Agent 6.0.2 und höher) Stellt Dienste für die Funktion zur Scannerumleitung bereit. |
| VMware Serial Com Client Service | Automatisch | (View Agent 6.1.1 und höher) Stellt Dienste für die Funktion zur Umleitung serieller Ports bereit. |
| VMware Snapshot Provider | Manuell | Stellt Dienste für Snapshots von virtuellen Maschinen bereit, die zum Klonen verwendet werden. |
| VMware Tools | Automatisch | Bietet Unterstützung für Synchronisierungsobjekte zwischen den Host- und Gastbetriebssystemen, wodurch sich die Leistung des Gastbetriebssystems der virtuellen Maschinen verbessert und die Verwaltung der virtuellen Maschine erleichtert wird. |
| VMware USB Arbitration Service | Automatisch | Listet die verschiedenen USB-Geräte auf, die an den Client angeschlossen sind, und ermittelt, welche Geräte mit dem Client und welche mit dem Remote-Desktop verbunden werden müssen. |
| VMware View USB | Automatisch | Stellt Dienste für die Funktion zur USB-Umleitung bereit. |

Auf dem Windows-Client installierte Dienste

Der Betrieb von Horizon Client hängt von mehreren Windows-Diensten ab.

Tabelle 2-2. Horizon Client-Dienste

| Dienstname | Starttyp | Beschreibung |
|---|-------------|---|
| VMware Horizon Client | Automatisch | Stellt Horizon Client-Dienste bereit. |
| VMware Netlink Supervisor Service | Automatisch | Unterstützt die Funktion zur Scannerumleitung und die Funktion zur Umleitung serieller Ports, stellt Überwachungsdienste zur Übertragung von Informationen zwischen Kernel- und Benutzerraumprozessen bereit. |
| VMware Scanner Redirection Client Service | Automatisch | (Horizon Client 3.2 und höher) Stellt Dienste für die Funktion zur Scannerumleitung bereit. |
| VMware Serial Com Client Service | Automatisch | (Horizon Client 3.4 und höher) Stellt Dienste für die Funktion zur Umleitung für serielle Ports bereit. |
| VMware USB Arbitration Service | Automatisch | Listet die verschiedenen USB-Geräte auf, die an den Client angeschlossen sind, und ermittelt, welche Geräte mit dem Client und welche mit dem Remote-Desktop verbunden werden müssen. |
| VMware View USB | Automatisch | (Horizon Client 4.3 und früher) Stellt Dienste für die Funktion zur USB-Umleitung bereit. |
| Hinweis In Horizon Client 4.4 und höher wurde dieser Dienst entfernt und der USB-Dienst zum <code>vmware-remotemks.exe</code> -Vorgang übertragen. | | |

In anderen Clients und dem Linux-Desktop installierte Daemons

Aus Sicherheitsgründen ist es wichtig zu wissen, ob durch Horizon Client irgendwelche Daemons oder Prozesse installiert werden.

Tabelle 2-3. Durch Horizon Client installierte Dienste, Prozesse oder Daemons nach Clienttyp

| Typ | Dienst, Prozess oder Daemon |
|-----------------------|--|
| Linux-Client | <ul style="list-style-type: none"> ■ <code>vmware-usbarbitrator</code>: Listet die verschiedenen USB-Geräte auf, die an den Client angeschlossen sind, und ermittelt, welche Geräte mit dem Client und welche mit dem Remote-Desktop verbunden werden müssen. ■ <code>vmware-view-used</code>: Stellt Dienste für die Funktion zur USB-Umleitung bereit. <p>Hinweis Diese Daemons werden automatisch gestartet, wenn Sie bei der Installation das Kontrollkästchen Dienst(e) nach der Installation registrieren und starten aktivieren. Diese Prozesse werden als Root ausgeführt.</p> |
| Mac-Client | Horizon Client erstellt keine Daemons. |
| Chrome OS-Client | Horizon Client wird in einem einzigen Android-Prozess ausgeführt. Horizon Client erstellt keine Daemons. |
| iOS-Client | Horizon Client erstellt keine Daemons. |
| Android-Client | Horizon Client wird in einem einzigen Android-Prozess ausgeführt. Horizon Client erstellt keinerlei Daemons. |
| Windows 10 UWP-Client | Horizon Client erstellt keinerlei Systemdienste und löst auch keine aus. |
| Windows Store-Client | Horizon Client erstellt keinerlei Systemdienste und löst auch keine aus. |
| Linux-Desktop | <ul style="list-style-type: none"> ■ <code>StandaloneAgent</code>: Wird mit Root-Rechten ausgeführt und gestartet, wenn das Linux-System betriebsbereit ist. <code>StandaloneAgent</code> kommuniziert mit dem Verbindungsserver, um die Remote-Desktop-Sitzungsverwaltung durchzuführen (richtet die Sitzung ein und baut sie wieder ab, wobei der Remote-Desktop-Status gegenüber dem Broker im Verbindungsserver aktualisiert wird). ■ <code>VMwareBlastServer</code>: Wird vom <code>StandaloneAgent</code> gestartet, wenn eine <code>StartSession</code>-Anforderung vom Verbindungsserver empfangen wird. Der <code>VMwareBlastServer</code>-Daemon wird mit den Rechten von <code>vmwblast</code> (ein bei der Installation von Linux Agent erstelltes Systemkonto) ausgeführt. Er kommuniziert mit dem <code>StandaloneAgent</code> über einen internen <code>MKSControl</code>-Kanal und mit Horizon Client mithilfe des VMware Blast-Anzeigeprotokolls. |

Zu sichernde Ressourcen

Zu diesen Ressourcen zählen die relevanten Konfigurationsdateien, Kennwörter und Zugriffskontrollen.

Dieses Kapitel enthält die folgenden Themen:

- [Implementieren von Best Practices zum Sichern von Clientsystemen](#)
- [Konfigurationsdateispeicherorte](#)
- [Konten](#)

Implementieren von Best Practices zum Sichern von Clientsystemen

Implementieren Sie diese Best Practices, um Clientsysteme zu sichern.

- Stellen Sie sicher, dass Clientsysteme so konfiguriert sind, dass sie nach einer bestimmten Leerlaufzeit in den Energiesparmodus wechseln. Benutzer müssen somit ein Kennwort eingeben, um den Computer wieder zu aktivieren.
- Verlangen Sie von Benutzern beim Starten von Clientsystemen die Eingabe eines Benutzernamens und eines Kennworts. Konfigurieren Sie Clientsysteme nicht so, dass automatische Anmeldungen zulässig sind.
- Für Mac-Clientsysteme sollten Sie erwägen, verschiedene Kennwörter für den Schlüsselbund und das Benutzerkonto festzulegen. Wenn die Kennwörter sich unterscheiden, werden Benutzer abgefragt, bevor das System Kennwörter in ihrem Namen eingibt. Ziehen Sie außerdem die Aktivierung des FileVault-Schutzes in Betracht.

Konfigurationsdateispeicherorte

Zu den Ressourcen, die geschützt werden müssen, zählen die sicherheitsrelevanten Konfigurationsdateien.

Tabelle 3-1. Speicherort der Konfigurationsdateien, nach Clienttyp

| Typ | Verzeichnispfad |
|---|--|
| Linux-Client | <p>Beim Start von Horizon Client werden die Konfigurationseinstellungen aus mehreren Speicherorten in der folgenden Reihenfolge verarbeitet:</p> <ol style="list-style-type: none"> 1 /etc/vmware/view-default-config 2 ~/.vmware/view-preferences 3 /etc/vmware/view-mandatory-config <p>Ist eine Einstellung in verschiedenen Speicherorten konfiguriert, entspricht der verwendete Wert dem Wert aus dem letzten Lesevorgang der Datei oder Befehlszeilenoption.</p> |
| Windows-Client | <p>Die Benutzereinstellungen, die einige private Informationen enthalten könnten, befinden sich in folgender Datei:</p> <p>C:\Benutzer\Benutzername\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt</p> |
| Mac-Client | <p>Einige Konfigurationsdateien werden nach dem Starten des Mac-Clients erzeugt.</p> <ul style="list-style-type: none"> ■ \$HOME/Library/Preferences/com.vmware.horizon.plist ■ \$HOME/Library/Preferences/com.vmware.vmr.plist ■ \$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist ■ /Library/Preferences/com.vmware.horizon.plist |
| Chrome OS-Client | <p>Die sicherheitsbezogenen Einstellungen erscheinen in der Benutzeroberfläche anstatt in Konfigurationsdateien. Für keinen Benutzer sind irgendwelche Konfigurationsdateien sichtbar.</p> |
| iOS-Client | <p>Die sicherheitsbezogenen Einstellungen erscheinen in der Benutzeroberfläche anstatt in Konfigurationsdateien. Für keinen Benutzer sind irgendwelche Konfigurationsdateien sichtbar.</p> |
| Android-Client | <p>Die sicherheitsbezogenen Einstellungen erscheinen in der Benutzeroberfläche anstatt in Konfigurationsdateien. Für keinen Benutzer sind irgendwelche Konfigurationsdateien sichtbar.</p> |
| Windows 10 UWP-Client | <p>Die sicherheitsbezogenen Einstellungen erscheinen in der Benutzeroberfläche anstatt in Konfigurationsdateien. Für keinen Benutzer sind irgendwelche Konfigurationsdateien sichtbar.</p> |
| Windows Store-Client | <p>Die sicherheitsbezogenen Einstellungen erscheinen in der Benutzeroberfläche anstatt in Konfigurationsdateien. Für keinen Benutzer sind irgendwelche Konfigurationsdateien sichtbar.</p> |
| View Agent oder Horizon Agent (Remote-Desktop mit Windows-Betriebssystem) | <p>Die sicherheitsbezogenen Einstellungen erscheinen nur in der Windows-Registrierung.</p> |
| Linux-Desktop | <p>Sie können einen Texteditor verwenden, um die folgende Konfigurationsdatei zu öffnen und die SSL-bezogenen Einstellungen anzugeben.</p> <p>/etc/vmware/viewagent-custom.conf</p> |

Konten

Client-Benutzer müssen über Konten in Active Directory verfügen.

Horizon Client -Benutzerkonten

Konfigurieren Sie in Active Directory Benutzerkonten für die Benutzer, die Zugriff auf Remote-Desktops und -Anwendungen haben. Die Benutzerkonten müssen Mitglieder der Gruppe „Remote-Desktop-Benutzer“ sein, falls Sie vorhaben, das RDP-Protokoll zu verwenden.

Endbenutzer sollten im Normalfall keine Horizon-Administratoren sein. Wenn ein Horizon-Administrator die Benutzererfahrung überprüfen muss, erstellen Sie ein getrenntes Testkonto mit entsprechenden Rechten. Auf dem Desktop sollten Horizon-Endbenutzer keine Mitglieder von privilegierten Gruppen wie z. B. „Administratoren“ sein, weil sie sonst in der Lage sind, gesperrte Konfigurationsdateien und die Windows-Registrierung zu ändern.

Bei der Installation erstellte Systemkonten

Durch die Horizon Client-Anwendung werden auf keinem Clienttyp Dienstbenutzerkonten erstellt. Für die von Horizon Client für Windows erstellten Dienste lautet die Anmelde-ID „Local System“.

Auf dem Mac-Client muss der Benutzer beim erstmaligen Start den Local Admin-Zugriff gewähren, um die Dienste für USB und virtuellen Druck (ThinPrint) zu starten. Nachdem diese Dienste erstmalig gestartet wurden, verfügt der Standardbenutzer über die entsprechenden Ausführungszugriffsrechte. In gleicher Weise werden auf dem Linux-Client automatisch die Daemons `vmware-usbarbitrator` und `vmware-view-used` gestartet, wenn Sie bei der Installation das Kontrollkästchen **Dienst(e) nach der Installation registrieren und starten** aktivieren. Diese Prozesse werden als Root ausgeführt.

Auf Windows-Desktops werden von View Agent oder Horizon Agent keine Dienstbenutzerkonten erstellt. Auf Linux-Desktops wird das Systemkonto `vmwblast` erstellt. Auf Linux-Desktops wird der Daemon `StandaloneAgent` mit Root-Rechten ausgeführt, und der Daemon `VmwareBlastServer` wird mit `vmwblast`-Rechten ausgeführt.

Sicherheitseinstellungen für Client und Agent

4

Es stehen verschiedene Client- und Agent-Einstellungen zur Verfügung, mit denen sich die Sicherheit der Konfiguration anpassen lässt. Sie können auf die Einstellungen für den Remote-Desktop und die Windows-Clients zugreifen, indem Sie Gruppenrichtlinienobjekte verwenden oder die Windows-Registrierungseinstellungen bearbeiten.

Informationen zu den Konfigurationseinstellungen zur Protokollsammlung finden Sie unter [Kapitel 6 Client- und Agent-Protokolldateispeicherorte](#). Informationen zu den Konfigurationseinstellungen zu den Sicherheitsprotokollen und Verschlüsselungssammlungen finden Sie unter [Kapitel 5 Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen](#).

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren der Zertifikatsprüfung](#)
- [Sicherheitsbezogene Einstellungen in den View Agent- und Horizon Agent-Konfigurationsvorlagen](#)
- [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#)
- [Gruppenrichtlinieneinstellungen für HTML Access](#)
- [Sicherheitseinstellungen in den Horizon Client-Konfigurationsvorlagen](#)
- [Konfigurieren des Horizon Client-Zertifikatüberprüfungsmodus](#)
- [Konfigurieren des Schutzes durch die lokale Sicherheitsautorität](#)

Konfigurieren der Zertifikatsprüfung

Administratoren können den Zertifikatüberprüfungsmodus so konfigurieren, dass beispielsweise immer die vollständige Überprüfung durchgeführt wird. Administratoren können über eine Konfiguration festlegen, ob Clientverbindungen abgelehnt werden sollen, wenn bei Zertifikatsüberprüfungen Fehler auftreten.

Die Zertifikatsprüfung wird für SSL-/TLS-Verbindungen zwischen Verbindungsserver-Instanzen und Horizon Client durchgeführt. Die Administratoren können den Überprüfungsmodus so konfigurieren, dass eine der folgenden Strategien verwendet wird:

- Die Endbenutzer wählen selbst den Überprüfungsmodus. In der restlichen Liste werden die drei Überprüfungsmodi beschrieben.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.

- (Warnen) Die Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat vorlegt. Die Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Die Zertifikatsüberprüfung umfasst die folgenden Checks:

- Wurde das Zertifikat widerrufen?
- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?
- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

Um diese Prüfung zu bestehen, muss sich das Stammzertifikat für die Zertifikatvertrauenskette im lokalen Zertifikatspeicher des Geräts befinden.

Informationen zum Konfigurieren der Zertifikatsprüfung für einen bestimmten Clienttyp finden Sie im Dokument Horizon Client für den jeweiligen Clienttyp. Diese Dokumente enthalten auch Informationen zur Verwendung von selbstsignierten Zertifikaten.

Sicherheitsbezogene Einstellungen in den View Agent- und Horizon Agent -Konfigurationsvorlagen

Sicherheitsbezogene Einstellungen werden in den ADM- und ADMX-Vorlagendateien für View Agent und Horizon Agent bereitgestellt. Die Namen der ADM- und ADMX-Vorlagendateien lauten `vdm_agent.adm` und `vdm_agent.admx`. Falls nicht anders angegeben, enthalten die Einstellungen nur eine Einstellung „Computerkonfiguration“.

Sicherheitseinstellungen werden in der Registrierung auf dem Gastcomputer unter `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration` gespeichert.

Tabelle 4-1. Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage (für Horizon 6) oder Horizon Agent -Konfigurationsvorlage (für Horizon 7)

| Einstellung | Beschreibung |
|---------------------------|---|
| AllowDirectRDP | <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 <code>Access is denied</code> (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> <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> <p>Diese Einstellung ist standardmäßig aktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet AllowDirectRDP.</p> |
| AllowSingleSignon | <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> <p>Der entsprechende Wert in der Windows-Registrierung lautet AllowSingleSignon.</p> |
| CommandsToRunOnConnect | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die bei der ersten Verbindungsherstellung ausgeführt werden.</p> <p>Standardmäßig ist keine Liste angegeben.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet CommandsToRunOnConnect.</p> |
| CommandsToRunOnDisconnect | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung getrennt wird.</p> <p>Standardmäßig ist keine Liste angegeben.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet CommandsToRunOnReconnect.</p> |
| CommandsToRunOnReconnect | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird.</p> <p>Standardmäßig ist keine Liste angegeben.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet CommandsToRunOnDisconnect.</p> |

Tabelle 4-1. Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage (für Horizon 6) oder Horizon Agent -Konfigurationsvorlage (für Horizon 7) (Fortsetzung)

| Einstellung | Beschreibung |
|----------------------------|--|
| ConnectionTicketTimeout | <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> <p>Der entsprechende Wert in der Windows-Registrierung lautet VdmConnectionTicketTimeout.</p> |
| CredentialFilterExceptions | <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> <p>Standardmäßig ist keine Liste angegeben.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet CredentialFilterExceptions.</p> |

Weitere Informationen zu diesen Einstellungen und ihren Auswirkungen auf die Sicherheit finden Sie im Dokument *Administration von View*.

Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop

Sie können verschiedene Optionen konfigurieren, indem Sie der Datei `/etc/vmware/config` oder `/etc/vmware/viewagent-custom.conf` Einträge hinzufügen.

Bei der Installation von Horizon Agent kopiert das Installationsprogramm die beiden Konfigurationsvorlagendateien `config.template` und `viewagent-custom.conf.template` in `/etc/vmware`. Außerdem kopiert das Installationsprogramm, wenn `/etc/vmware/config` und `/etc/vmware/viewagent-custom.conf` nicht vorhanden sind, `config.template` nach `config` und `viewagent-custom.conf.template` nach `viewagent-custom.conf`. In den Vorlagendateien sind alle Konfigurationsoptionen aufgelistet und dokumentiert. Um eine Option einzustellen, entfernen Sie einfach den Kommentar und ändern Sie den Wert wie gewünscht.

So aktiviert beispielsweise die folgende Zeile in `/etc/vmware/config` den Build-to-Lossless-PNG-Modus.

```
RemoteDisplay.buildToPNG=TRUE
```

Nachdem Sie Ihre Änderungen vorgenommen haben, müssen Sie Linux neu starten, damit die Änderungen wirksam werden.

Konfigurationsoptionen in /etc/vmware/config

VMwareBlastServer und seine zugehörigen Plug-ins verwenden die Konfigurationsdatei /etc/vmware/config.

Hinweis Die folgende Tabelle enthält Beschreibungen für alle von Agent erzwungenen Richtlinieneinstellungen für USB in der Horizon Agent-Konfigurationsdatei. Horizon Agent verwendet die Einstellungen, um zu entscheiden, ob der USB-Anschluss zur Host-Maschine umgeleitet werden kann. Horizon Agent übergibt diese Einstellungen außerdem an Horizon Client zur Interpretation und Erzwingung. Die Erzwingung hängt davon ab, ob Sie den merge (m)-Modifizierer zur Anwendung der Horizon Agent-Filterrichtlinieneinstellung zusätzlich zur Horizon Client-Filterrichtlinieneinstellung festlegen oder den (o)-Modifizierer zur Verwendung der Horizon Agent-Filterrichtlinieneinstellung anstelle der Horizon Client-Filterrichtlinieneinstellung überschreiben.

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config

| Option | Wert/Format | Standard | Beschreibung |
|--|-----------------|----------|--|
| Clipboard.Direction | 0, 1, 2, oder 3 | 2 | Verwenden Sie diese Option zur Festlegung der Richtlinie für die Zwischenablagenumleitung. Folgende Werte sind gültig: <ul style="list-style-type: none"> ■ 0 - Zwischenablagenumleitung deaktivieren. ■ 1 - Zwischenablagenumleitung in beide Richtungen aktivieren. ■ 2 - Zwischenablagenumleitung nur vom Client zum Remote-Desktop aktivieren. ■ 3 - Zwischenablagenumleitung nur vom Remote-Desktop zum Client aktivieren. |
| RemoteDisplay.allowAudio | true oder false | true | Legen Sie diese Option fest, um die Audio-Ausgabe zu aktivieren/deaktivieren. |
| RemoteDisplay.allowH264 | true oder false | true | Legen Sie diese Option zum Aktivieren oder Deaktivieren der H.264-Codierung fest. |
| RemoteDisplay.buildToPNG | true oder false | false | Grafische Anwendungen und insbesondere grafische Anwendungen zur Bildbearbeitung erfordern ein pixelgenaues Rendering von Bildern in der Clientanzeige eines Linux-Desktops. Sie haben die Möglichkeit, einen speziellen Build-to-Lossless-PNG-Modus für Bilder und die Videowiedergabe zu konfigurieren, die auf einem Linux-Desktop generiert und auf dem Clientgerät gerendert werden. Diese Funktion verwendet zusätzliche Bandbreite zwischen dem Client und dem ESXi-Host. Bei Aktivierung dieser Option wird die H.264-Codierung deaktiviert. |
| RemoteDisplay.enableNetwork-Continuity | true oder false | true | Legen Sie diese Option fest, um die Funktion für durchgängige Netzwerke in Horizon Agent für Linux zu aktivieren oder zu deaktivieren. |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|---|--|----------|--|
| RemoteDisplay.enableNetworkIntelligence | true oder false | true | Legen Sie diese Option fest, um die Funktion für intelligente Netzwerke in Horizon Agent für Linux zu aktivieren oder zu deaktivieren. |
| RemoteDisplay.enableStats | true oder false | false | Aktivieren oder deaktivieren Sie die VMware Blast-Anzeigeprotokollstatistik im MKS-Protokoll, beispielsweise Bandbreite, FPS, RTT usw. |
| RemoteDisplay.enableUDP | true oder false | true | Legen Sie diese Option fest, um die Unterstützung für das UDP-Protokoll in Horizon Agent für Linux zu aktivieren oder zu deaktivieren. |
| RemoteDisplay.maxBandwidthKbps | Eine Ganzzahl | 4096000 | 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 und VMware Blast-Steuerung eingeschlossen. Der maximale Wert lautet 4 GBit/s (4096000). |
| RemoteDisplay.maxFPS | Eine Ganzzahl | 60 | Legt die maximale Rate der Bildschirmaktualisierungen fest. Mit dieser Einstellung steuern Sie die durchschnittliche Bandbreite, die Benutzer in Anspruch nehmen. Der gültige Wert muss zwischen 3 und 60 liegen. Die Standardeinstellung beträgt 60 Aktualisierungen pro Sekunde. |
| RemoteDisplay.maxQualityJPEG | Verfügbarer Wertebereich: 1–100 | 90 | Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Die Einstellungen für eine hohe Bildqualität sind für eher statische Bereiche sinnvoll. |
| RemoteDisplay.midQualityJPEG | Verfügbarer Wertebereich: 1–100 | 35 | Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Legt die Einstellungen für die mittlere Qualität der Desktop-Anzeige fest. |
| RemoteDisplay.minQualityJPEG | Verfügbarer Wertebereich: 1–100 | 25 | Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Die Einstellungen für eine niedrige Bildqualität sind für Bereiche gedacht, die sich häufig ändern, z. B. durch einen Bildlauf. |
| RemoteDisplay.qpmaxH264 | Verfügbarer Wertebereich: 0–51 | 36 | Verwenden Sie diese Option, um den Quantisierungsparameter „H264minQP“ festzulegen, der die für die H.264-Codierung konfigurierte beste Bildqualität angibt. Geben Sie einen Wert an, der größer ist als der für „RemoteDisplay.qpminH264“ festgelegte Wert. |
| RemoteDisplay.qpminH264 | Verfügbarer Wertebereich: 0–51 | 10 | Verwenden Sie diese Option, um den Quantisierungsparameter „H264maxQP“ festzulegen, der die für die H.264-Codierung konfigurierte geringste Bildqualität angibt. Geben Sie einen Wert an, der kleiner ist als der für „RemoteDisplay.qpmaxH264“ festgelegte Wert. |
| UsbRedirPlugin.log.logLevel | error, warn, info, debug, trace oder verbose | info | Verwenden Sie diese Option zur Festlegung der Protokollebene des USB-Umleitungs-Plug-Ins. |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|------------------------------|--|----------|---|
| UsbRedirServer.log.logLevel | error, warn, info, debug, trace oder verbose | info | Verwenden Sie diese Option zur Festlegung der Protokollebene des USB-Umleitungsservers. |
| VMWPKcs11Plugin.log.enable | true oder false | false | Legen Sie diese Option fest, um den Protokollierungsmodus für die True SSO-Funktion zu aktivieren oder zu deaktivieren. |
| VMWPKcs11Plugin.log.logLevel | error, warn, info, debug, trace oder verbose | info | Verwenden Sie diese Option, um die Protokollebene für die True SSO-Funktion festzulegen. |
| VVC.RTAV.Enable | true oder false | true | Legen Sie diese Option fest, um die Audio-Eingabe zu aktivieren/deaktivieren. |
| VVC.ScRedir.Enable | true oder false | true | Legen Sie diese Option fest, um die Smartcard-Umleitung zu aktivieren/deaktivieren. |
| VVC.logLevel | fatal error, warn, info, debug oder trace | info | Verwenden Sie diese Option zur Festlegung der Protokollebene des VVC-Proxy-Knotens. |
| cdrserver.cacheEnable | true oder false | true | Legen Sie diese Option fest, um die Funktion des Schreibcache von der Agentseite zur Clientseite zu aktivieren oder zu deaktivieren. |
| cdrserver.forcedByAdmin | true oder false | false | Legen Sie mit dieser Option fest, ob der Client zusätzliche Ordner gemeinsam nutzen kann, die nicht mit der Option cdrserver.shareFolders angegeben wurden. |
| cdrserver.logLevel | error, warn, info, debug, trace oder verbose | info | Verwenden Sie diese Option zur Festlegung der Protokollebene für die Datei vmware-CDRserver.log. |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|----------------------------|---|-----------------|---|
| cdserver.permissions | R | RW | <p>Verwenden Sie diese Option zur Anwendung zusätzlicher Lese/Schreib-Berechtigungen, über die Horizon Agent für die von Horizon Client freigegebenen Ordner verfügt. Beispiel:</p> <ul style="list-style-type: none"> ■ Wenn der von Horizon Client freigegebene Ordner über die Berechtigungen <code>read</code> und <code>write</code> verfügt und Sie cdserver.permissions=R festlegen, verfügt Horizon Agent nur über <code>read</code>-Zugriffsberechtigungen. ■ Wenn der von Horizon Client freigegebene Ordner nur über <code>read</code>-Berechtigungen verfügt und Sie cdserver.permissions=RW festlegen, verfügt Horizon Agent weiterhin nur über <code>read</code>-Zugriffsrechte. Horizon Agent kann nicht das Schreibschutzattribut „read only“ ändern, das von Horizon Client festgelegt wurde. Mit Horizon Agent lassen sich nur die Schreibzugriffsrechte entfernen. <p>Eine typische Verwendung lautet:</p> <ul style="list-style-type: none"> ■ cdserver.permissions=R ■ #cdserver.permissions=R (z. B., um den Eintrag auszukommentieren oder zu löschen) |
| cdserver.sharedFolders | <i>file_path1,R;file_path2,;file_path3,R; . .</i> | Nicht definiert | <p>Geben Sie einen oder mehrere Dateipfade zu den Ordnern an, die der Client mit dem Linux-Desktop gemeinsam nutzen kann. Beispiel:</p> <ul style="list-style-type: none"> ■ Für einen Windows-Client: C:\spreadsheets,;D:\ebooks,R ■ Für einen Nicht-Windows-Client: /tmp/spreadsheets;/tmp/ebooks,;/home/finance,R |
| collaboration.logLevel | error, info oder debug | info | Verwenden Sie diese Option zur Festlegung der Protokollebene für die Zusammenarbeitssitzung. Wenn die Protokollebene <code>debug</code> ausgewählt ist, werden alle Aufrufe von <code>collabui</code> -Funktionen sowie die Inhalte der <code>collabor</code> -Liste protokolliert. |
| collaboration.maxCollabors | Eine Ganzzahl kleiner 10 | 5 | Legt die maximale Anzahl der Benutzer fest, die Sie zur Teilnahme an einer Sitzung einladen können. |
| collaboration.enableEmail | true oder false | true | Legen Sie diese Option zum Aktivieren oder Deaktivieren der Einladungen zur Zusammenarbeit mithilfe einer installierten E-Mail-Anwendung fest. Ist diese Option deaktiviert, können Sie keine Einladungen zur Zusammenarbeit mit E-Mails versenden, auch wenn eine E-Mail-Anwendung installiert ist. |
| collaboration.serverUrl | [URL] | Nicht definiert | Spezifiziert die Server-URLs, die in Einladungen zur Zusammenarbeit enthalten sein sollen. |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|--|---|---|---|
| collaboration.enableControlPas- sing | true oder false | true | Legen Sie diese Option fest, um die Kontrolle der Teilnehmer über die Linux-Desktops zuzulassen oder einzuschränken. Um für die Zusammenarbeitssitzung einen reinen Lesezugriff festzulegen, setzen Sie diese Option auf false . |
| mksVNCServer.useUInputBut- tonMapping | true oder false | false | Legen Sie diese Option fest, um die Unterstützung einer linkshändigen Maus auf Ubuntu oder RHEL 7 zu aktivieren. CentOS und RHEL 6 unterstützen eine linkshändige Maus, und Sie müssen diese Option nicht festlegen. |
| mksVNCServer.useXExtButton- Mapping | true oder false | false | Legen Sie diese Option fest, um die Unterstützung einer linkshändigen Maus auf SLED 11 SP3 zu aktivieren oder zu deaktivieren. |
| mksvhan.clipboardSize | Eine Ganzzahl | 1024 | Verwenden Sie diese Option, um die maximale Größe der Zwischenablage für das Kopieren und Einfügen anzugeben. |
| vdpservice.log.logLevel | fatal error, warn, info, debug oder trace | info | Verwenden Sie diese Option zum Festlegen der Protokollebene des vdp-service. |
| viewusb.AllowAudioIn | {m o}: {true false} | Nicht defi- niert, ent- spricht true | Verwenden Sie diese Option, um die Umleitung für Audio-Eingabe-Geräte zuzulassen oder auszuschließen. Beispiel: o: false |
| viewusb.AllowAudioOut | {m o}: {true false} | Nicht defi- niert, ent- spricht false | Legen Sie diese Option fest, um die Umleitung für Audio-Ausgabe-Geräte zuzulassen oder auszuschließen. |
| viewusb.AllowAutoDeviceSplit- ting | {m o}: {true false} | Nicht defi- niert, ent- spricht false | Legen Sie diese Option fest, um das automatische Splitten von Composite USB-Geräten zuzulassen oder auszuschließen. Beispiel: m: true |
| viewusb.AllowDevDescFailsafe | {m o}: {true false} | Nicht defi- niert, ent- spricht false | Legen Sie diese Option fest, um die Umleitung für Geräte zuzulassen oder auszuschließen, auch wenn Horizon Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät auch beim Scheitern des Abrufs der Konfigurations-/Gerätebeschreibungen zuzulassen, muss dieses in „Include“-Filter wie z. B. IncludeVidPid oder IncludePath eingeschlossen werden. |
| viewusb.AllowHIDBootable | {m o}: {true false} | Nicht defi- niert, ent- spricht true | Verwenden Sie diese Option, um die Umleitung anderer Eingabegeräte neben Tastatur und Maus, die zur Startzeit verfügbar sind (auch als „startfähige Eingabegeräte“ bezeichnet), zuzulassen oder auszuschließen. |
| viewusb.AllowKeyboardMouse | {m o}: {true false} | Nicht defi- niert, ent- spricht false | Verwenden Sie diese Option, um die Umleitung von Tastaturen mit eingebauten Zeigegegeräten (Maus, Trackball oder Touchpad) zuzulassen oder auszuschließen. |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|-----------------------------|--|--|--|
| viewusb.AllowSmartcard | <code>{m o}:</code> <code>{true false}</code> | Nicht definiert, entspricht <code>false</code> | Legen Sie diese Option fest, um die Umleitung für Smartcard-Geräte zuzulassen oder auszuschließen. |
| viewusb.AllowVideo | <code>{m o}:</code> <code>{true false}</code> | Nicht definiert, entspricht <code>true</code> | Verwenden Sie diese Option, um die Umleitung für Videogeräte zuzulassen oder auszuschließen. |
| viewusb.DisableRemoteConfig | <code>{m o}:</code> <code>{true false}</code> | Nicht definiert, entspricht <code>false</code> | Legen Sie diese Option fest, um die Verwendung von Horizon Agent-Einstellungen zuzulassen oder auszuschließen, wenn eine USB-Gerätefilterung durchgeführt wird. |
| viewusb.ExcludeAllDevices | <code>{true false}</code> | Nicht definiert, entspricht <code>false</code> | Verwenden Sie diese Option, um alle USB-Geräte von der Umleitung auszuschließen oder in die Umleitung einzubeziehen. 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. Wenn Sie den Wert von ExcludeAllDevices in Horizon Agent auf true setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die Horizon Agent-Einstellung die Horizon Client-Einstellung. |
| viewusb.ExcludeFamily | <code>{m o}:family_name_1[;family_name_2;...]</code> | Nicht definiert | Verwenden Sie diese Option, um Gerätefamilien von der Umleitung auszuschließen oder in die Umleitung einzubeziehen. Beispiel: m:bluetooth;smart-card Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden muss. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon die Gerätefamilie des gesamten Composite USB-Gerätes. Hinweis Maus und Tastatur sind standardmäßig von der Umleitung ausgeschlossen und müssen deshalb nicht mit dieser Einstellung ausgeschlossen werden. |
| viewusb.ExcludePath | <code>{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2;...]</code> | Nicht definiert | Verwenden Sie diese Option, um Geräte an bestimmten Hub- oder Portpfaden von der Umleitung auszuschließen. Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: m:bus-1/2/3_port-02;bus-1/1/1/4_port-ff |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|-----------------------|--|-----------------|--|
| viewusb.ExcludeVidPid | <code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code> | Nicht definiert | Legen Sie diese Option fest, um Geräte mit einer bestimmten Anbieter- oder Produkt-ID von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: o:vid-0781_pid-****;vid-0561_pid-554c |
| viewusb.IncludeFamily | <code>{m o}:family_name_1[;family_name_2]...</code> | Nicht definiert | Legen Sie diese Option fest, um Gerätefamilien in die Umleitung einzubeziehen. Beispiel: o:storage; smart-card |
| viewusb.IncludePath | <code>{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2;...]</code> | Nicht definiert | Verwenden Sie diese Option, um Geräte an bestimmten Hub- oder Portpfaden in die Umleitung einzubeziehen. Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: m:bus-1/2_port-02;bus-1/7/1/4_port-0f |
| viewusb.IncludeVidPid | <code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code> | Nicht definiert | Legen Sie diese Option fest, um Geräte mit bestimmten Anbieter- oder Produkt-IDs in die Umleitung einzubeziehen. Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: o:vid-***_pid-0001;vid-0561_pid-554c |

Tabelle 4-2. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)

| Option | Wert/Format | Standard | Beschreibung |
|----------------------------|---|-----------------|--|
| viewusb.SplitExcludeVidPid | {m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...] | Nicht definiert | <p>Verwenden Sie diese Option, um ein bestimmtes Composite USB-Gerät für das Splitten nach Anbieter- und Produkt-IDs auszuschließen oder einzubeziehen. Das Format dieser Einstellung lautet vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]. ID-Nummern müssen in hexadezimaler Schreibweise angegeben werden. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.</p> <p>Beispiel: m:vid-0f0f_pid-55**</p> |
| viewusb.SplitVidPid | {m o}: vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[;...] | Nicht definiert | <p>Legen Sie diese Option fest, um die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte zu behandeln. Das Format dieser Einstellung lautet vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]). Sie können mit dem Stichwort exintf Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung ausschließen. 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.</p> <p>Beispiel: o:vid-0f0f_pid-*** (exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</p> <p>Hinweis Horizon schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. Include VidPid Device (VidPid-Gerät einbeziehen) angeben, um diese Komponenten einzubeziehen.</p> |

Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf

Java Standalone Agent verwendet die Konfigurationsdatei /etc/vmware/viewagent-custom.conf.

Tabelle 4-3. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf

| Option | Wert | Standard | Beschreibung |
|---------------------|-----------------------|----------|---|
| CDREnable | true oder false | true | Verwenden Sie diese Option, um die Funktion der Clientlaufwerkumleitung (Client Drive Redirection, CDR) zu aktivieren oder zu deaktivieren. |
| CollaborationEnable | true oder false | true | Legen Sie diese Option fest, um die Funktion „Session Collaboration“ in Linux Desktop zu aktivieren oder zu deaktivieren. |

Tabelle 4-3. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)

| Option | Wert | Standard | Beschreibung |
|---------------------|--|----------|--|
| EndpointVPNEnable | true oder false | false | Legen Sie diese Option fest, um anzugeben, ob die IP-Adresse der physischen Client-Netzwerkkarte oder die VPN-IP-Adresse zur Überprüfung der IP-Adresse des Endpunkts anhand des Bereichs der in der User Environment Manager-Konsole verwendeten Endpunkt-IP-Adressen verwendet werden soll. Wenn die Option auf <code>false</code> festgelegt ist, wird die IP-Adresse der physischen Client-Netzwerkkarte verwendet. Andernfalls wird die VPN-IP-Adresse verwendet. |
| HelpDeskEnable | true oder false | true | Legen Sie diese Option fest, um die Helpdesk-Tool-Funktion zu aktivieren oder zu deaktivieren. |
| KeyboardLayout-Sync | true oder false | true | <p>Verwenden Sie diese Option, um festzulegen, ob das Systemgebietsschema und das aktuelle Tastaturlayout eines Clients mit Horizon Agent for Linux-Desktops synchronisiert werden sollen.</p> <p>Wenn diese Einstellung aktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert ist, ist eine Synchronisierung nicht erlaubt.</p> <p>Diese Funktion wird nur für Horizon Client für Windows und nur für die Gebietsschemas Englisch, Französisch, Deutsch, Japanisch, Koreanisch, Spanisch, Chinesisch (vereinfacht) und Chinesisch (traditionell) unterstützt.</p> |
| LogCnt | Eine Ganzzahl | -1 | <p>Verwenden Sie diese Option zur Festlegung der Anzahl der reservierten Protokolle in <code>/tmp/vmware-root</code>.</p> <ul style="list-style-type: none"> ■ -1 - alle beibehalten ■ 0 - alle löschen ■ > 0 - Anzahl der reservierten Protokolle. |
| NetbiosDomain | Eine Textzei- chenfolge in Groß- buchsta- ben | | Verwenden Sie diese Option bei der Konfiguration von True SSO, um den NetBIOS-Namen der Domäne Ihrer Organisation festzulegen. |
| OfflineJoinDomain | pbis oder samba | pbis | Mit dieser Option wird der Instant-Clone-Offline-Domänenbeitritt festgelegt. Die verfügbaren Methoden zum Durchführen eines Offline-Domänenbeitritts sind die PowerBroker Identity Services Open(PBISO)-Authentifizierung und der Samba-Offline-Domänenbeitritt. Wenn für diese Eigenschaft ein anderer Wert als <code>pbis</code> oder <code>samba</code> festgelegt ist, wird der Offline-Domänenbeitritt ignoriert. |

Tabelle 4-3. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)

| Option | Wert | Standard | Beschreibung |
|----------------------|---|---|---|
| RunOnceScript | | | <p>Mit dieser Option kann die geklonte virtuelle Maschine Active Directory erneut beitreten.</p> <p>Legen Sie das RunOnceScript fest, nachdem der Hostname geändert wurde. Das angegebene Skript wird nur einmal nach der ersten Änderung des Hostnamens ausgeführt. Das Skript wird mit der Stammberechtigung ausgeführt, wenn der Agentendienst gestartet wird und sich der Hostname seit der Agenteninstallation geändert hat.</p> <p>Zum Beispiel müssen Sie für die winbind-Lösung die virtuelle Basis-Maschine Active Directory mit winbind beitreten lassen und diese Option auf einen Skriptpfad festlegen. Diese muss den Befehl für den erneuten Beitritt zur Domäne <code>/usr/bin/net ads join -U <ADUserName>%<ADUserPassword></code> enthalten. Nach dem VM-Klon ändert die Betriebssystemanpassung den Hostnamen. Wenn der Agentendienst gestartet wird, wird das Skript ausgeführt, damit die geklonte virtuelle Maschine Active Directory beitrifft.</p> |
| RunOnceScriptTimeout | | 120 | <p>Verwenden Sie diese Option, um die Zeit bis zur Zeitüberschreitung in Sekunden für die Option „RunOnceScript“ festzulegen.</p> <p>Legen Sie z. B. <code>RunOnceScriptTimeout=120</code> fest</p> |
| SSLCiphers | Eine Textzeichenfolge | !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES | <p>Verwenden Sie diese Option zum Festlegen der Liste der Verschlüsselungen. Sie müssen das Format verwenden, das in https://www.openssl.org/docs/manmaster/man1/ciphers.html definiert ist.</p> |
| SSLProtocols | Eine Textzeichenfolge | TLSv1_1:TLSv1_2 | <p>Verwenden Sie diese Option zum Festlegen der Sicherheitsprotokolle. Die unterstützten Protokolle sind TLSv1.0, TLSv1.1 und TLSv1.2.</p> |
| SSODesktopType | UseGnomeClassic oder UseGnomeFlashback oder UseGnomeUbuntu oder UseMATE oder UseKdePlasma oder | | <p>Über diese Option wird die Desktop-Umgebung festgelegt, die bei aktivierter SSO-Funktion anstelle der Standard-Desktop-Umgebung verwendet wird.</p> <p>Sie müssen zuerst sicherstellen, dass die ausgewählte Desktop-Umgebung auf Ihrem Desktop installiert ist, bevor Sie sie zur Verwendung auswählen. Nachdem Sie diese Option auf einem Ubuntu 14.04/16.04/18.04-Desktop festgelegt haben, wird diese Option unabhängig davon, ob die SSO-Funktion aktiviert ist oder nicht, angewendet. Wenn diese Option auf einem RHEL/CentOS 7.x-Desktop festgelegt wird, wird die ausgewählte Desktop-Umgebung nur dann verwendet, wenn die SSO-Funktion aktiviert ist.</p> <p>Hinweis Diese Option wird auf RHEL/CentOS 6- und SLED 11-Desktops nicht unterstützt. Weitere Informationen zur Einrichtung von KDE als Standard-Desktop-Umgebung, wenn die SSO-Funktion auf diesen Desktops aktiviert ist, finden Sie im Dokument <i>Einrichten von Horizon 7 for Linux-Desktops</i>.</p> |

Tabelle 4-3. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)

| Option | Wert | Standard | Beschreibung |
|----------------|---|----------------|--|
| SSOEnable | true oder false | true | Legen Sie diese Option fest, um Single Sign-On (SSO) zu aktivieren/deaktivieren. |
| SSOUserFormat | Eine Textzei- chenfolge | [Benutzername] | Verwenden Sie diese Option, um das Format des Anmel- denamens für das Single Sign-On anzugeben. Der Standard ist lediglich der Benutzername. Legen Sie diese Option fest, wenn auch der Domänenname erforderlich ist. Meist ist der Anmeldename der Domänenname plus einem Sonderzei- chen, gefolgt vom Benutzernamen. Wenn das Sonderzei- chen ein Rückschrägstrich ist, muss ein weiterer Rück- schrägstrich als Escape-Zeichen verwendet werden. Bei- spiele für Formate von Anmeldennamen: <ul style="list-style-type: none"> ■ SSOUserFormat=[Domäne]\\[Benutzername] ■ SSOUserFormat=[Domäne]+[Benutzername] ■ SSOUserFormat=[Benutzername]@[Domäne] |
| Subnet | Ein Wert im CIDR- IP-Adres- senfor- mat | [Subnetz] | Legen Sie diese Option auf ein Subnetz fest, das andere Maschinen zur Verbindungsherstellung mit Horizon Agent für Linux verwenden können. Wenn mehr als eine lokale IP- Adresse mit unterschiedlichen Subnetzen vorhanden ist, wird die lokale IP-Adresse im konfigurierten Subnetz ver- wendet, um eine Verbindung mit Horizon Agent für Linux herzustellen. Sie müssen den Wert im CIDR-IP-Adressfor- mat angeben. Beispielsweise Subnetz=123.456.7.8/24. |
| UEMEnable | true oder false | false | Legen Sie diese Option zum Aktivieren oder Deaktivieren der intelligenten User Environment Manager-Richtlinien fest. Wenn die Option zum Aktivieren festgelegt ist und die Bedin- gung in der intelligenten User Environment Manager-Richtli- nie erfüllt ist, werden die Richtlinien erzwungen. |
| UEMNetworkPath | Eine Textzei- chenfolge | | Diese Option muss auf denselben Netzwerkpfad festgelegt werden, der auch in der User Environment Manager-Konso- le festgelegt ist. Der Pfad muss dem For- mat //10.111.22.333/view/LinuxAgent/UEMConfig ent- sprechen. |

Hinweis Die drei Sicherheitsoptionen SSLCiphers, SSLProtocols und SSLCipherServerPreference gel-
ten für den VMwareBlastServer-Prozess. Beim Start des VMwareBlastServer-Prozesses durchläuft der
Java Standalone Agent diese Optionen als Parameter. Wenn Blast Secure Gateway (BSG) aktiviert ist,
wirken sich diese Optionen auf die Verbindung zwischen BSG und dem Linux-Desktop aus. Wenn BSG
deaktiviert ist, wirken sich diese Optionen auf die Verbindung zwischen dem Client und dem Linux-Desk-
top aus.

Gruppenrichtlinieneinstellungen für HTML Access

Gruppenrichtlinieneinstellungen für HTML Access werden in den ADM- und ADMX-Vorlagendateien na-
mens vdm_blast.adm und vdm_blast.admx angegeben. Diese Vorlagen sind für das VMware Blast-An-
zeigeprotokoll vorgesehen, das einzige von HTML Access verwendete Anzeigeprotokoll.

Die VMware Blast-Richtlinieneinstellungen für HTML Access 4.0 und höher sowie für Horizon 7 Version 7.x werden unter „Richtlinieneinstellungen für VMware Blast“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7* beschrieben.

Für HTML Access 3.5 oder früher und Horizon 6 Version 6.2.x oder höher finden Sie in der nachfolgenden Tabelle eine Beschreibung der für HTML Access gültigen Gruppenrichtlinieneinstellungen. In Horizon 7 Version 7.x und höher sind weitere VMware Blast-Gruppenrichtlinieneinstellungen verfügbar.

Tabelle 4-4. Gruppenrichtlinieneinstellungen für HTML Access 3.5 oder früher und Horizon 6 Version 6.2.x oder früher

| Einstellung | Beschreibung |
|--|--|
| Löschen des Bildschirms | <p>Legt fest, ob die virtuelle Remote-Maschine während einer HTML Access-Sitzung außerhalb von Horizon 6 angezeigt wird. Beispielsweise kann ein Administrator vSphere Web Client verwenden, um auf der virtuellen Maschine eine Konsole zu öffnen, während ein Benutzer über HTML Access mit dem Desktop verbunden ist.</p> <p>Wenn diese Einstellung aktiviert oder nicht konfiguriert ist und ein Benutzer versucht, während einer HTML Access-Sitzung außerhalb von Horizon 6 auf die virtuelle Remote-Maschine zuzugreifen, zeigt die virtuelle Remote-Maschine einen leeren Bildschirm an.</p> |
| Sitzungsspeicherbereinigung | <p>Steuert die Speicherbereinigung für abgebrochene Remotesitzungen. Wenn diese Einstellung aktiviert ist, können Sie Intervall und Schwellenwert für die Speicherbereinigung konfigurieren.</p> <p>Das Intervall steuert, wie häufig die Speicherbereinigung durchgeführt wird. Sie legen das Intervall in Millisekunden fest.</p> <p>Der Schwellenwert gibt an, wie viel Zeit nach dem Abbruch einer Sitzung verstreichen muss, damit diese zum Löschen markiert wird. Sie legen den Schwellenwert in Sekunden fest.</p> |
| Zwischenablagenumleitung konfigurieren | <p>Bestimmt die Richtung, in der die Zwischenablagenumleitung zulässig ist. Es kann nur Text kopiert und eingefügt werden. Sie können einen der folgenden Werte auswählen:</p> <ul style="list-style-type: none"> ■ Nur Client zu Server aktiviert (Dadurch ist der Kopier- und Einfügevorgang nur vom Clientsystem zum Remote-Desktop zulässig.) ■ In beide Richtungen deaktiviert ■ In beide Richtungen aktiviert ■ Nur Server zu Client aktiviert (Dadurch ist der Kopier- und Einfügevorgang nur vom Remote-Desktop zum Clientsystem zulässig.) <p>Diese Einstellung gilt nur für View Agent oder Horizon Agent.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert Nur Client zu Server aktiviert.</p> |
| HTTP-Dienst | <p>Ermöglicht es Ihnen, den sicheren TCP-Port (HTTPS) für den Blast Agent-Dienst zu ändern. Der Standardport ist 22443.</p> <p>Aktivieren Sie diese Einstellung, um die Portnummer zu ändern. Wenn Sie diese Einstellung ändern, müssen Sie auch Einstellungen für die Firewall auf den betroffenen Remote-Desktops (auf denen View Agent oder Horizon Agent installiert ist) aktualisieren.</p> |

Sicherheitseinstellungen in den Horizon Client - Konfigurationsvorlagen

Sicherheitsbezogene Einstellungen werden in den Abschnitten „Security“ (Sicherheit) und „Scripting Definitions“ (Skriptdefinitionen) der ADM- und ADMX-Vorlagendateien für Horizon Client bereitgestellt. Der Name der ADM-Vorlagendatei lautet `vdm_client.adm` und der der ADMX-Vorlagendatei `vdm_client.admx`. Falls nicht anders angegeben, enthalten die Einstellungen nur eine Einstellung „Computerkonfiguration“. Wenn eine Benutzerkonfigurationseinstellung verfügbar ist und Sie einen Wert dafür definieren, setzt diese die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

In der folgenden Tabelle werden die Einstellungen im Abschnitt „Security“ (Sicherheit) der ADM- und ADMX-Vorlagendateien beschrieben.

Tabelle 4-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen

| Einstellung | Beschreibung |
|---|--|
| Allow command line credentials (Einstellung für die Computerkonfiguration) | <p>Legt fest, ob Benutzeranmeldedaten mit Horizon Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung deaktiviert ist, stehen die Optionen <code>smartCardPIN</code> und <code>password</code> nicht zur Verfügung, wenn Benutzer Horizon Client über die Befehlszeile ausführen.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet <code>AllowCmdLineCredentials</code>.</p> |
| Servers Trusted For Delegation (Einstellung für die Computerkonfiguration) | <p>Gibt die Verbindungsserver-Instanzen an, die die Benutzeridentitäts- und Anmeldedaten akzeptieren, die bei Aktivierung des Kontrollkästchens Als aktueller Benutzer anmelden übergeben werden. Wenn Sie keine Verbindungsserver-Instanzen angeben, akzeptieren alle Verbindungsserver-Instanzen diese Informationen.</p> <p>Verwenden Sie zum Hinzufügen einer Verbindungsserverinstanz eines der folgenden Formate:</p> <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ Service Principal Name (SPN) des Verbindungsserver-Dienstes <p>Der entsprechende Wert in der Windows-Registrierung lautet <code>BrokersTrustedForDelegation</code>.</p> |

Tabelle 4-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

| Einstellung | Beschreibung |
|---|--|
| Certificate verification mode (Einstellung für die Computerkonfiguration) | <p>Konfiguriert die Ebene der Zertifikatsprüfung, die durch Horizon Client durchgeführt wird. Es stehen folgende Modi zur Auswahl:</p> <ul style="list-style-type: none"> ■ No Security. Keine Zertifikatsprüfung. ■ Warn But Allow. Es wird eine Warnung eingeblendet, wenn der Verbindungsserver-Host ein selbstsigniertes Zertifikat anzeigt. Der Benutzer kann jedoch weiterhin mit dem Verbindungsserver eine Verbindung herstellen. Der Zertifikatsname muss nicht mit dem durch den Benutzer in Horizon Client angegebenen Verbindungsserver-Namen übereinstimmen. Wenn andere Zertifikatsfehlerbedingungen vorliegen, wird ein Fehlerdialogfeld angezeigt, und es wird verhindert, dass der Benutzer eine Verbindung zum Verbindungsserver herstellt. Warn But Allow ist der Standardwert. ■ Full Security. Wenn ein beliebiger Zertifikatsfehler auftritt, kann der Benutzer keine Verbindung mit dem Verbindungsserver herstellen. Es werden Zertifikatsfehler angezeigt. <p>Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatsprüfung in Horizon Client anzeigen, ihn aber nicht konfigurieren. Das Dialogfeld für die SSL-Konfiguration informiert die Benutzer darüber, dass der Administrator die Einstellung gesperrt hat.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können Horizon Client-Benutzer einen Zertifikatsprüfungsmodus auswählen.</p> <p>Wenn Sie die Zertifikatsüberprüfungseinstellung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatsüberprüfung auch aktivieren, indem Sie Windows-Registrierungseinstellungen ändern.</p> |
| Default value of the 'Log in as current user' checkbox (Einstellung für die Computer- und Benutzerkonfiguration) | <p>Gibt den Standardwert des Kontrollkästchens Als aktueller Benutzer anmelden im Dialogfeld für die Horizon Client-Verbindung an.</p> <p>Diese Einstellung setzt den Standardwert außer Kraft, der während der Horizon Client-Installation angegeben wurde.</p> <p>Wenn ein Benutzer Horizon Client über die Befehlszeile ausführt und die Option <code>LogInAsCurrentUser</code> angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben.</p> <p>Wenn das Kontrollkästchen Als aktueller Benutzer anmelden aktiviert ist, werden die Identität und die Anmeldedaten des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die Verbindungsserverinstanz und schließlich an den Remote-Desktop übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor sie auf einen Remote-Desktop zugreifen können.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet <code>LogInAsCurrentUser</code>.</p> |

Tabelle 4-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

| Einstellung | Beschreibung |
|---|--|
| Display option to Log in as current user (Einstellung für die Computer- und Benutzerkonfiguration) | <p>Legt fest, ob das Kontrollkästchen Als aktueller Benutzer anmelden im Dialogfeld für die Horizon Client-Verbindung angezeigt wird.</p> <p>Bei Anzeige des Kontrollkästchens können Benutzer die Option aktivieren oder deaktivieren oder den zugehörigen Standardwert außer Kraft setzen. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die Horizon Client-Verbindung nicht ändern.</p> <p>Sie können den Standardwert für Als aktueller Benutzer anmelden über die Richtlinieneinstellung Default value of the 'Log in as current user' checkbox festlegen.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet LogInAsCurrentUser_Display.</p> |
| Enable jump list integration (Einstellung für die Computerkonfiguration) | <p>Legt fest, ob eine Sprungliste im Horizon Client icon on the taskbar of Windows 7 and later systems. Über die Sprungliste können Benutzer eine Verbindung zu zuletzt verwendeten Verbindungsserver-Instanzen und Remote-Desktops herstellen.</p> <p>Wenn Horizon Client gemeinsam verwendet wird, sollen Benutzer möglicherweise nicht die Namen der zuletzt verwendeten Desktops sehen. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet EnableJumplist.</p> |
| Enable SSL encrypted framework channel (Einstellung für die Computer- und Benutzerkonfiguration) | <p>Legt fest, ob der SSL-verschlüsselte Framework-Kanal aktiviert wird.</p> <ul style="list-style-type: none"> ■ Aktivieren: Aktiviert SSL, aber ermöglicht das Zurücksetzen auf die vorherige unverschlüsselte Verbindung, falls der Remote-Desktop SSL nicht unterstützt. ■ Deaktivieren: Deaktiviert SSL. Diese Einstellung wird nicht empfohlen. Sie kann aber hilfreich sein für das Debugging oder wenn der Kanal nicht getunnelt wird und deshalb möglicherweise durch ein Produkt zur WAN-Beschleunigung optimiert werden könnte. ■ Erzwingen: Aktiviert SSL und verweigert das Herstellen einer Verbindung zu Desktops ohne SSL-Unterstützung. <p>Der entsprechende Wert in der Windows-Registrierung lautet EnableTicketSSLAuth.</p> |

Tabelle 4-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

| Einstellung | Beschreibung |
|--|--|
| Configures SSL protocols and cryptographic algorithms (Einstellung für die Computer- und Benutzerkonfiguration) | <p>Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden.</p> <hr/> <p>Hinweis Für alle Verschlüsselungszeichenfolgen wird die Groß-/Kleinschreibung berücksichtigt.</p> <ul style="list-style-type: none"> ■ Der Standardwert für Horizon Client 4.10 und höher ist TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. ■ Der Standardwert für Horizon Client 4.2 und höher ist TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. ■ Der Standardwert für Horizon Client 4.0.1 und 4.1 ist TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ Der Standardwert für Horizon Client 4.0 lautet TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ Der Standardwert für Horizon Client 3.5 lautet TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ Die Standardeinstellung für Horizon Client 3.3 und 3.4 lautet TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ Der Wert für Horizon Client 3.2 und niedriger lautet SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. <hr/> <p>Ab Horizon Client 4.10 ist TLS v1.0 dauerhaft deaktiviert, sodass es nicht mehr unterstützt wird.</p> <p>In Horizon Client 4.0.1 bis 4.9 sind standardmäßig TLS v1.0, TLS v1.1 und TLS v1.2 aktiviert. (SSL v2.0 und v3.0 wurden entfernt.) Sie können TLS v1.0 deaktivieren, sofern die TLS v1.0-Kompatibilität mit dem Server nicht erforderlich ist.</p> <p>In Horizon Client 4.0 sind TLS v1.1 und TLS v1.2 aktiviert. (TLS v1.0 ist deaktiviert. SSL v2.0 und v3.0 wurden entfernt.)</p> <p>In Horizon Client 3.5 sind TLS v1.0, TLS v1.1 und TLS v1.2 aktiviert. (SSL v2.0 und v3.0 sind deaktiviert.) In Horizon Client 3.3 und 3.4 sind TLS v1.0 und TLS v1.1 aktiviert. (SSL v2.0 und v3.0 sowie TLS v1.2 sind deaktiviert.)</p> <p>In Horizon Client 3.2 und niedriger ist SSL v3.0 ebenfalls aktiviert. (SSL v2.0 und TLS v1.2 sind deaktiviert.)</p> <p>Verschlüsselungssammlungen verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus.</p> <p>Referenz-Link für die Konfiguration: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet SSLCipherList.</p> <p>Wenn Sie diese Einstellung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie sie auch aktivieren, indem Sie den Wertnamen SSLCipherList zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer hinzufügen:</p> <ul style="list-style-type: none"> ■ Für 32-Bit-Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security |

Tabelle 4-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

| Einstellung | Beschreibung |
|--|---|
| | <ul style="list-style-type: none"> Für 64-Bit-Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security |
| Enable Single Sign-On for smart card authentication (Einstellung für die Computerkonfiguration) | <p>Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist ein Single Sign-On aktiviert, speichert Horizon Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an den Verbindungsserver gesendet wird. Ist SSO deaktiviert, zeigt Horizon Client kein benutzerdefiniertes PIN-Dialogfeld an.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet EnableSmartCardSSO.</p> |

In der folgenden Tabelle werden die Einstellungen im Abschnitt „Scripting Definitions“ (Skriptdefinitionen) der ADM- und ADMX-Vorlagendateien beschrieben.

Tabelle 4-6. Sicherheitsbezogene Einstellungen im Abschnitt „Skriptdefinitionen“

| Einstellung | Beschreibung |
|---|--|
| Connect all USB devices to the desktop on launch | <p>Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet connectUSBOnStartup.</p> |
| Connect all USB devices to the desktop when they are plugged in | <p>Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet connectUSBOnInsert.</p> |
| Logon Password | <p>Legt das von Horizon Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.</p> <p>Diese Einstellung ist standardmäßig nicht definiert.</p> <p>Der entsprechende Wert in der Windows-Registrierung lautet Password.</p> |

Weitere Informationen zu diesen Einstellungen und ihren Auswirkungen auf die Sicherheit finden Sie in der Horizon Client für Windows-Dokumentation.

Konfigurieren des Horizon Client - Zertifikatüberprüfungsmodus

Sie können den Horizon Client-Zertifikatüberprüfungsmodus konfigurieren, indem Sie einem Registrierungsschlüssel auf dem Windows-Clientcomputer den Wertnamen CertCheckMode hinzufügen.

Auf 32-Bit-Windows-Systemen lautet der Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security. Auf 64-Bit-Windows-Systemen lautet der Registrierungsschlüssel HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security.

Verwenden Sie einen der folgenden Werte im Registrierungsschlüssel:

- 0: Implementiert die Option **Serveridentitätszertifikate nicht überprüfen**.

- 1: Implementiert die Option **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**.
- 2: Implementiert die Option **Nie mit nicht vertrauenswürdigen Servern verbinden**.

Sie können den Horizon Client-Zertifikatüberprüfungsmodus auch konfigurieren, indem Sie die Gruppenrichtlinieneinstellung Zertifikatüberprüfungsmodus konfigurieren. Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung CertCheckMode im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

Wenn die Gruppenrichtlinieneinstellung oder die Registrierungseinstellung konfiguriert ist, können Benutzer den ausgewählten Zertifikatsüberprüfungsmodus in Horizon Client anzeigen, sie können die Einstellung jedoch nicht konfigurieren.

Informationen über das Konfigurieren der Gruppenrichtlinieneinstellung Zertifikatsüberprüfungsmodus finden Sie unter [Sicherheitseinstellungen in den Horizon Client-Konfigurationsvorlagen](#).

Konfigurieren des Schutzes durch die lokale Sicherheitsautorität

Horizon Client und Horizon Agent unterstützen den Schutz durch die lokale Sicherheitsautorität (Local Security Authority, LSA). Der LSA-Schutz verhindert, dass Benutzer mit nicht geschützten Anmeldedaten den Arbeitsspeicher auslesen und Programmcode einfügen können.

Weitere Informationen zum Konfigurieren des LSA-Schutzes finden Sie in der Dokumentation zu Microsoft Windows Server.

Die folgende Funktion schlägt fehl, wenn der LSA-Schutz für Horizon Client 4.4 und früher konfiguriert ist:

- Als aktueller Benutzer anmelden

Die folgenden Funktionen schlagen fehl, wenn der LSA-Schutz für Horizon Agent-Versionen vor Horizon 7 Version 7.2 konfiguriert ist:

- Smartcard-Authentifizierung
- True SSO

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen

5

Sie können die Sicherheitsprotokolle und Verschlüsselungssammlungen konfigurieren, die von den Horizon Client-, View Agent/Horizon Agent- und Serverkomponenten akzeptiert und untereinander vorge schlagen werden.

Dieses Kapitel enthält die folgenden Themen:

- [Standardmäßige Richtlinien für Sicherheitsprotokolle und Verschlüsselungssammlungen](#)
- [Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für spezielle Clienttypen](#)
- [Deaktivieren von schwachen Verschlüsselungen in SSL/TLS](#)
- [Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für HTML Access-Agent](#)
- [Konfigurieren von Vorschlagsrichtlinien auf Remote-Desktops](#)

Standardmäßige Richtlinien für Sicherheitsprotokolle und Verschlüsselungssammlungen

Globale Akzeptanz- und Vorschlagsrichtlinien ermöglichen die standardmäßige Verwendung bestimmter Sicherheitsprotokolle und Verschlüsselungssammlungen.

Die folgenden Tabellen stellen die Protokolle und Verschlüsselungssammlungen dar, die standardmäßig für Horizon Client aktiviert sind. In Horizon Client 3.1 und höher für Windows, Linux und Mac werden diese Verschlüsselungssammlungen und Protokolle auch zur Verschlüsselung des USB-Kanals (Kommunikation zwischen dem USB-Dienst-Daemon und View Agent oder Horizon Agent) verwendet. Für Horizon Client-Versionen vor Version 4.0 fügt der USB-Dienst-Daemon RC4 (:RC4-SHA: +RC4) am Ende der Schlüsselsteuerzeichenfolge hinzu, wenn eine Verbindung zu einem Remote-Desktop hergestellt wird. RC4 wird ab der Version 4.0 von Horizon Client nicht mehr hinzugefügt.

Horizon Client 4.2 und höher

Tabelle 5-1. Auf Horizon Client 4.2 und höher standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--|--|
| TLS 1.2 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |
| <ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) |

Hinweis Ab Horizon Client 4.10 ist TLS v1.0 dauerhaft deaktiviert, sodass es nicht mehr unterstützt wird.

Tabelle 5-1. Auf Horizon Client 4.2 und höher standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen (Fortsetzung)

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--------------------------------------|---|
| | <ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

Ab Horizon Client 4.10 ist TLS v1.0 dauerhaft deaktiviert, sodass es nicht mehr unterstützt wird.

In Horizon Client 4.2 bis 4.9 ist TLS v1.0 standardmäßig aktiviert, um sicherzustellen, dass Horizon Client standardmäßig eine Verbindung mit Horizon Cloud für gehostete Infrastrukturserver herstellen kann. Die standardmäßige Verschlüsselungszeichenfolge lautet laNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. Sie können TLS v1.0 deaktivieren, sofern die TLS v1.0-Kompatibilität mit dem Server nicht erforderlich ist.

Horizon Client 4.0.1 und 4.1

Tabelle 5-2. Auf Horizon Client 4.0.1 und 4.1 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--|--|
| TLS 1.2 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |
| <ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) |

Tabelle 5-2. Auf Horizon Client 4.0.1 und 4.1 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen (Fortsetzung)

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--------------------------------------|---|
| | <ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

TLS 1.0 ist standardmäßig aktiviert, um sicherzustellen, dass Horizon Client standardmäßig eine Verbindung mit Horizon Cloud für gehostete Infrastrukturserver herstellen kann. Die standardmäßige Verschlüsselungszeichenfolge lautet: TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. Sie können TLS 1.0 deaktivieren, sofern die TLS 1.0-Kompatibilität mit dem Server nicht erforderlich ist.

Horizon Client 4.0

Tabelle 5-3. Auf Horizon Client 4.0 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--------------------------------------|--|
| TLS 1.2 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |
| ■ TLS 1.1 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) |

Tabelle 5-3. Auf Horizon Client 4.0 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen (Fortsetzung)

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--------------------------------------|--|
| | <ul style="list-style-type: none">■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

Wichtig TLS 1.0 ist standardmäßig deaktiviert. SSL 3.0 wurde entfernt.

Horizon Client 3.5

Tabelle 5-4. Auf Horizon Client 3.5 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--|--|
| TLS 1.2 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |
| <ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) |

Tabelle 5-4. Auf Horizon Client 3.5 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen (Fortsetzung)

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--------------------------------------|---|
| | <ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

Horizon Client 3.3 und 3.4

Tabelle 5-5. Auf Horizon Client 3.3 und 3.4 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|--|--|
| <ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 | <ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

Hinweis TLS 1.2 wird ebenfalls unterstützt, ist jedoch nicht standardmäßig aktiviert. Zum Aktivieren von TLS 1.2 folgen Sie den Anweisungen in [VMware KB 2121183](#), wonach die in [Tabelle 5-4](#) aufgelisteten Verschlüsselungssammlungen unterstützt werden.

Horizon Client 3.0, 3.1 und 3.2

Tabelle 5-6. Auf Horizon Client 3.0, 3.1 und 3.2 standardmäßig aktivierte Sicherheitsprotokolle und Verschlüsselungssammlungen

| Standardmäßige Sicherheitsprotokolle | Standardmäßige Verschlüsselungssammlungen |
|---|--|
| <ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (nur auf Windows-Clients aktiviert) | <ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff) |

Hinweis TLS 1.2 wird ebenfalls unterstützt, ist jedoch nicht standardmäßig aktiviert. Zum Aktivieren von TLS 1.2 folgen Sie den Anweisungen in [VMware KB 2121183](#), wonach die in [Tabelle 5-4](#) aufgelisteten Verschlüsselungssammlungen unterstützt werden.

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für spezielle Clienttypen

Jeder Clienttyp verfügt über seine eigene Methode zum Konfigurieren der verwendeten Protokolle und Verschlüsselungssammlungen.

Sie sollten die Sicherheitsprotokolle in Horizon Client nur dann ändern, wenn der View Server die aktuellen Einstellungen nicht unterstützt. Wenn Sie ein Sicherheitsprotokoll für Horizon Client konfigurieren, das auf dem View Server, mit dem sich der Client verbindet, nicht aktiviert ist, tritt ein TLS-/SSL-Fehler auf und die Verbindung schlägt fehl.

Zum Ändern der Protokolle und Verschlüsselungen gegenüber ihren Standardwerten verwenden Sie den clientspezifischen Mechanismus:

- Auf Windows-Clientsystemen können Sie entweder eine Gruppenrichtlinieneinstellung oder eine Windows-Registrierungseinstellung verwenden.
- Auf Windows 10 UWP-Clientsystemen können Sie die Einstellung für die SSL-Optionen in den Horizon Client-Optionen verwenden.
- Auf Linux-Clientsystemen können Sie entweder Konfigurationsdateieigenschaften oder Befehlszeilenooptionen verwenden.

- Auf Mac-Clientsystemen können Sie eine Einstellung in Horizon Client verwenden.
- Auf iOS-, Android- und Chrome OS-Clientsystemen können Sie eine Einstellung der erweiterten SSL-Optionen in den Horizon Client-Einstellungen verwenden.

Weitere Informationen finden Sie in der Dokumentation Horizon Client.

Deaktivieren von schwachen Verschlüsselungen in SSL/TLS

Zur Erhöhung der Sicherheit können Sie das Domänenrichtlinien-GPO (Group Policy Object, Gruppenrichtlinienobjekt) so konfigurieren, dass Windows-basierte Maschinen, die View Agent oder Horizon Agent ausführen, keine schwachen Verschlüsselungen für die Kommunikation mithilfe des SSL/TLS-Protokolls verwenden.

Verfahren

- 1 Bearbeiten Sie auf dem Active Directory-Server das GPO, indem Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung** wählen, mit der rechten Maustaste auf das GPO klicken und **Bearbeiten** auswählen.
- 2 Im Editor der Gruppenrichtlinienverwaltung wechseln Sie zu **Computerkonfiguration > Richtlinien > Administratorvorlagen > Netzwerk > SSL-Konfigurationseinstellungen**.
- 3 Doppelklicken Sie auf **Reihenfolge der SSL-Verschlüsselungssammlungen**.
- 4 Im Fenster „Reihenfolge der SSL-Verschlüsselungssammlungen“ klicken Sie auf **Aktiviert**.
- 5 Im Bereich „Optionen“ ersetzen Sie den gesamten Inhalt des Textfeldes „SSL-Verschlüsselungssammlungen“ mit der folgenden Verschlüsselungsliste:

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

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

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

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für HTML Access-Agent

Ab View Agent 6.2 können Sie die Verschlüsselungssammlungen konfigurieren, die HTML Access Agent verwendet, indem Sie die Windows-Registrierung bearbeiten. Ab View Agent 6.2.1 können Sie auch die verwendeten Sicherheitsprotokolle konfigurieren. Sie können die Konfigurationen auch in einem Gruppenrichtlinienobjekt (GPO) festlegen.

Ab View Agent 6.2.1 und in späteren Versionen verwendet der HTML Access Agent nur TLS 1.1 und TLS 1.2. Die zulässigen Protokolle sind (mit steigender Sicherheit) TLS 1.0, TLS 1.1 und TLS 1.2. Ältere Protokolle wie z. B. SSLv3 und frühere Versionen sind niemals zulässig. Zwei Registrierungswerte, `SslProtocolLow` und `SslProtocolHigh`, legen den Protokollbereich fest, den HTML Access Agent akzeptiert. Zum Beispiel bewirken die Einstellungen `SslProtocolLow=tls_1.0` und `SslProtocolHigh=tls_1.2`, dass HTML Access Agent TLS 1.0, TLS 1.1 und TLS 1.2 akzeptiert. Die Standardeinstellungen sind `SslProtocolLow=tls_1.1` und `SslProtocolHigh=tls_1.2`.

Sie müssen die Liste der Verschlüsselungen festlegen, und zwar mit dem Format, das in <https://www.openssl.org/docs/manmaster/man1/ciphers.html> im Abschnitt FORMAT DER VERSCHLÜSSLUNGSLISTE definiert ist. Die folgende Verschlüsselungsliste wird standardmäßig verwendet:

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor.
- 2 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.
- 3 Fügen Sie zwei neue Zeichenfolgenwerte (REG_SZ), `SslProtocolLow` und `SslProtocolHigh`, hinzu, um den Protokollbereich anzugeben.

Die Daten für die Registrierungswerte müssen `tls_1.0`, `tls_1.1` oder `tls_1.2` sein. Um nur ein Protokoll zu aktivieren, geben Sie dasselbe Protokoll für beide Registrierungswerte an. Wenn einer der beiden Registrierungswerte nicht vorhanden ist oder wenn seine Daten nicht auf eines der drei Protokolle festgelegt sind, werden die Standardprotokolle verwendet.

- 4 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ), `SslCiphers`, hinzu, um eine Liste von Verschlüsselungssammlungen anzugeben.

Geben Sie die Liste von Verschlüsselungssammlungen in das Datenfeld des Registrierungswerts ein oder fügen Sie sie ein. Beispiel:

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

- 5 Führen Sie einen Neustart des Windows-Dienstes VMware Blast durch.

Um zur Nutzung der standardmäßigen Verschlüsselungsliste zurückzukehren, löschen Sie den `SslCiphers`-Registrierungswert und starten Sie den Windows-Dienst VMware Blast neu. Löschen Sie nicht einfach den Datenteil des Werts, sonst behandelt der HTML Access-Agent alle Verschlüsselungsverfahren entsprechend der Formatdefinition für die OpenSSL-Verschlüsselungsliste als inakzeptabel.

Wenn der HTML Access Agent startet, schreibt er die Protokoll- und Verschlüsselungsinformationen in seine Protokolldatei. Sie können die Protokolldatei überprüfen, um festzustellen, welche Werte in Kraft sind.

Die Standardprotokolle und Verschlüsselungssammlungen können sich auf der Grundlage der von VMware empfohlenen und ständig weiterentwickelten Vorgehensweisen für die Netzwerksicherheit zukünftig ändern.

Konfigurieren von Vorschlagsrichtlinien auf Remote-Desktops

Durch das Konfigurieren von Vorschlagsrichtlinien auf Remote-Desktops, auf denen Windows ausgeführt wird, steuern Sie die Sicherheit der Message Bus-Verbindungen zum Verbindungsserver.

Stellen Sie sicher, dass der Verbindungsserver so konfiguriert ist, dass er die gleichen Richtlinien akzeptiert. Andernfalls kann es zu Verbindungsfehlern kommen.

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem Remote-Desktop.
- 2 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.
- 3 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ), `ClientSSLSecureProtocols`, hinzu.
- 4 Setzen Sie den Wert auf eine Liste von Verschlüsselungssammlungen im Format: **\LISTE:Protokoll_1,Protokoll_2,...**

Geben Sie das neueste Protokoll zuerst in der Liste an. Beispiel:

```
\LIST:TLSv1.2,TLSv1.1,TLSv1
```

- 5 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ), `ClientSSLCipherSuites`, hinzu.
- 6 Setzen Sie den Wert auf eine Liste von Verschlüsselungssammlungen im Format: **\LISTE:Verschlüsselungssammlung_1,Verschlüsselungssammlung_2,...**

Die Liste sollte in der Form einer Prioritätenliste angelegt sein, d. h. die am meisten bevorzugte Verschlüsselungssammlung sollte zuerst aufgeführt sein. Beispiel:

```
\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Client- und Agent-Protokolldateispeicherorte

6

Die Clients und der Agent erzeugen Protokolldateien, in denen die Installation und die Vorgänge ihrer Komponenten aufgezeichnet werden.

Dieses Kapitel enthält die folgenden Themen:

- [Horizon Client für Windows-Protokolle](#)
- [Horizon Client für Mac-Protokolle](#)
- [Horizon Client für Linux-Protokolle](#)
- [Horizon Client-Protokolle auf mobilen Geräten](#)
- [Horizon Agent-Protokolle von Windows-Computern](#)
- [Linux-Desktop-Protokolle](#)

Horizon Client für Windows-Protokolle

Protokolldateien können dabei helfen, Probleme bei der Installation, dem Anzeigeprotokoll und verschiedenen Funktionskomponenten zu beheben. Sie können Gruppenrichtlinieneinstellungen verwenden, um den Speicherort, die Ausführlichkeit und den Aufbewahrungszeitraum einiger Protokolldateien zu konfigurieren.

Protokollspeicherort

Bei den Dateinamen in der folgenden Tabelle steht *YYYY* für das Jahr, *MM* für den Monat, *DD* für den Tag, und *XXXXXX* ist eine Nummer.

Tabelle 6-1. Horizon Client für Windows-Protokolldateien

| Protokolltyp | Verzeichnispfad | Dateiname |
|--|--|---|
| Installation | C:\Benutzer\%Benutzername%\AppData\Local\Temp | vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt |
| PCoIP-Client Vom vmware-remotemks.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp | pcoip_client_YYYY_MM_DD_XXXXXX.txt Hinweis Mithilfe einer GPO können Sie die Protokollebene von 0 bis 3 (höchste Ausführlichkeit) konfigurieren. Verwenden Sie die ADMX-Vorlagendatei pcoip.admx für View-PCoIP-Client-Sitzungsvariablen. Die Einstellung heißt Ausführlichkeit der PCoIP-Ereignisprotokolle konfigurieren . |
| Horizon Client-Benutzeroberfläche Vom vmware-view.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\VMware\VDM\Logs | vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt Hinweis Sie können ein GPO verwenden, um den Protokollspeicherort zu konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration. |
| Horizon Client-Protokolle Vom vmware-view.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp\vmware-Benutzername-XXXXXX | vmware-crtbora-XXXXXX.log |
| Nachrichten-Framework | C:\Benutzer\%Benutzername%\AppData\Local\VMware\VDM\Logs | log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt |
| Remote MKS (Mouse-Key-board-Screen)-Protokolle Vom vmware-remotemks.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp\vmware-Benutzername | ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-rdeSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log |
| Tsdr-Client Vom vmware-remotemks.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp\vmware-Benutzername | vmware-ViewTsdr-Client-XXXXXX.log |
| Tsmmr-Client Vom vmware-remotemks.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp\vmware-Benutzername | vmware-ViewTsmmr-Client-XXXXXX.log |
| VdpService-Client Vom vmware-remotemks.exe-Prozess | C:\Benutzer\%Benutzername%\AppData\Local\Temp\vmware-Benutzername | vmware-vdpServiceClient-XXXXXX.log |
| WSNM-Dienst Vom wsnm.exe-Prozess | C:\ProgramData\VMware\VDM\logs | debug-yyyy-mm-dd-XXXXXX.txt Hinweis Sie können ein GPO verwenden, um den Protokollspeicherort zu konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration. |

Tabelle 6-1. Horizon Client für Windows-Protokolldateien (Fortsetzung)

| Protokolltyp | Verzeichnispfad | Dateiname |
|--|--------------------------------|---|
| USB-Umleitung Vom vmware-view- usbd.exe- oder vmware- remotemks.exe-Vorgang | C:\ProgramData\VMware\VDM\logs | debug-yyyy-mm-dd-XXXXXX.txt In Horizon Client 4.4 und höher wurde der vmware-view-usbd.exe-Vorgang entfernt und der USB-D-Vorgang zum vmware-remotemks.exe-Vorgang übertragen. Hinweis Sie können ein GPO verwenden, um den Protokollspeicherort zu konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration. |
| Umleitung serieller Ports Vom vmwsprrdpwks.exe- Prozess | C:\ProgramData\VMware\VDM\Logs | Serial*.txt Netlink*.txt |
| Scannerumleitung Vom ftscanmgr.exe-Pro- zess | C:\ProgramData\VMware\VDM\Logs | Scanner*.txt Netlink*.txt |

Protokollkonfiguration

Sie können Gruppenrichtlinieneinstellungen verwenden, um einige Konfigurationsänderungen vorzunehmen.

- Für PCoIP-Client-Protokolle können Sie die Protokollebene von 0 bis 3 (höchste Ausführlichkeit) konfigurieren. Verwenden Sie die ADMX-Vorlagendatei pcoip.admx für View-PCoIP-Client-Sitzungsvariablen. Die Einstellung heißt **Ausführlichkeit der PCoIP-Ereignisprotokolle konfigurieren**.
- Für Protokolle der Client-Benutzeroberfläche können Sie den Protokollspeicherort, die Ausführlichkeit und den Aufbewahrungszeitraum konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration.
- Für Protokolle der USB-Umleitung können Sie den Protokollspeicherort, die Ausführlichkeit und den Aufbewahrungszeitraum konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration.
- Für Protokolle des WSNM-Diensts können Sie den Protokollspeicherort, die Ausführlichkeit und den Aufbewahrungszeitraum konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration.

Sie können auch einen Befehlszeilenbefehl verwenden, um einen Ausführlichkeitsgrad festzulegen.

Wechseln Sie in das Verzeichnis C:\Programme (x86)\VMware\VMware Horizon View Client\DCI und geben Sie folgenden Befehl ein:

```
support.bat loglevels
```

Es wird eine Eingabeaufforderung geöffnet, und Sie werden zur Auswahl eines Ausführlichkeitsgrads aufgefordert.

Sammeln eines Protokollpakets

Sie können entweder die Client-Benutzeroberfläche oder einen Befehlszeilenbefehl verwenden, um Protokolle in einer ZIP-Datei zu erfassen, die Sie an den technischen Support von VMware senden können.

- Wählen Sie im **Horizon Client**-Fenster aus dem Menü „Optionen“ die Option **Support-Informationen** aus und klicken Sie im angezeigten Dialogfeld auf **Support-Daten sammeln**.
- Wechseln Sie von der Befehlszeile in das Verzeichnis `c:\Programme (x86)\VMware\VMware Horizon View Client\DCT` und geben Sie folgenden Befehl ein: `support.bat`.

Horizon Client für Mac-Protokolle

Protokolldateien können dabei helfen, Probleme bei der Installation, dem Anzeigeprotokoll und verschiedenen Funktionskomponenten zu beheben. Sie können eine Konfigurationsdatei erstellen, um den Ausführlichkeitsgrad zu konfigurieren.

Protokollspeicherort

Tabelle 6-2. Horizon Client für Mac-Protokolldateien

| Protokolltyp | Verzeichnispfad | Dateiname |
|---|--------------------------------------|---------------------|
| Horizon Client-Benutzeroberfläche | ~/Library/Logs/VMware Horizon Client | |
| PCoIP-Client | ~/Library/Logs/VMware Horizon Client | |
| Echtzeit-Audio/Video | ~/Library/Logs/VMware | vmware-RTAV-pid.log |
| USB-Umleitung | ~/Library/Logs/VMware | |
| VChan | ~/Library/Logs/VMware Horizon Client | |
| Remote MKS (Mouse-Keyboard-Screen)-Protokolle | ~/Library/Logs/VMware | |
| Crtbora | ~/Library/Logs/VMware | |

Protokollkonfiguration

In Horizon Client 3.1 und höher generiert Horizon Client Protokolldateien im Verzeichnis `~/Library/Logs/VMware Horizon Client` auf dem Mac-Client. Administratoren können auf einem Mac-Client die maximale Anzahl an Protokolldateien sowie die maximale Anzahl an Tagen konfigurieren, die Protokolldateien aufbewahrt werden sollen: Dazu werden in der Datei `/Library/Preferences/com.vmware.re.horizon.plist` Schlüssel festgelegt.

Tabelle 6-3. plist-Schlüssel für das Erfassen von Protokolldateien

| Schlüssel | Beschreibung |
|-------------------|---|
| MaxDebugLogs | Die maximale Anzahl von Protokolldateien. Der Maximalwert ist 100. |
| MaxDaysToKeepLogs | Die maximale Anzahl von Tagen, die Protokolldateien aufbewahrt werden sollen. Für diesen Wert gibt es keinen Grenzwert. |

Dateien, die diesen Kriterien nicht entsprechen, werden gelöscht, wenn Sie Horizon Client starten.

Wenn der Schlüssel MaxDebugLogs bzw. MaxDaysToKeepLogs in der Datei `com.vmware.horizon.plist` nicht festgelegt ist, beträgt die Standardanzahl der Protokolldateien 5 und die Standardanzahl an Tagen zum Beibehalten der Protokolldateien 7.

Horizon Client für Linux-Protokolle

Protokolldateien können dabei helfen, Probleme bei der Installation, dem Anzeigeprotokoll und verschiedenen Funktionskomponenten zu beheben. Sie können eine Konfigurationsdatei erstellen, um den Ausführlichkeitsgrad zu konfigurieren.

Protokollspeicherort

Tabelle 6-4. Horizon Client für Linux-Protokolldateien

| Protokolltyp | Verzeichnispfad | Dateiname |
|---|-----------------------------|---|
| Installation | /tmp/vmware-root/ | .vmware-installer-pid.log vmware-vmis-pid.log |
| Horizon Client-Benutzer- oberfläche | /tmp/vmware-Benutzername/ | vmware-horizon-client-pid.log |
| PCoIP-Client | /tmp/teradici-Benutzername/ | pcoip_client_YYYY_MM_DD_XXXXXX.log |
| Echtzeit-Audio/Video | /tmp/vmware-Benutzername/ | vmware-RTAV-pid.log |
| USB-Umleitung | /tmp/vmware-root/ | vmware-usbarb-pid.log vmware-view-usbd-pid.log |
| VChan | /tmp/vmware-Benutzername/ | VChan-Client.log Hinweis Dieses Protokoll wird erstellt, wenn Sie RDPVCBridge-Protokolle aktivieren, indem Sie „export VMW_RDPVC_BRIDGE_LOG_ENABLED=1“ festlegen. |
| Remote MKS (Mouse- Keyboard-Screen)- Protokolle | /tmp/vmware-Benutzername/ | vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log |
| VdpService-Client | /tmp/vmware-Benutzername/ | vmware-vdpServiceClient-pid.log |
| Tsdr-Client | /tmp/vmware-Benutzername/ | vmware-ViewTsdr-Client-pid.log |

Protokollkonfiguration

Sie können eine Konfigurationseigenschaft (`view.defaultLogLevel`) verwenden, um den Ausführlichkeitsgrad der Client-Protokolle von 0 (alle Ereignisse sammeln) bis 6 (nur schwerwiegende Ereignisse sammeln) festzulegen.

Für USB-spezifische Protokolle können Sie die folgenden Befehlszeilenbefehle verwenden:

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

Sammeln eines Protokollpakets

Das Protokollsammelmodul befindet sich in `/usr/bin/vmware-view-log-collector`. Zur Verwendung des Protokollsammelmoduls müssen Sie über Ausführungsberechtigungen verfügen. Sie können die Berechtigungen an der Linux-Befehlszeile festlegen, indem Sie den folgenden Befehl eingeben:

```
chmod +x /usr/bin/vmware-view-log-collector
```

Sie können das Protokollsammelmodul einer Linux-Befehlszeile ausführen, indem Sie den folgenden Befehl eingeben:

```
/usr/bin/vmware-view-log-collector
```

Horizon Client-Protokolle auf mobilen Geräten

Auf mobilen Geräten müssen Sie eventuell ein Drittanbieterprogramm installieren, um zum Verzeichnis navigieren zu können, in dem sich die Protokolldateien befinden. Mobile Clients verfügen über Konfigurationseinstellungen zum Senden von Protokollpaketen an VMware. Da sich die Protokollierung negativ auf die Leistung auswirken kann, sollten Sie die Protokollierung nur aktivieren, wenn Sie ein Problem beheben müssen.

iOS-Client-Protokolle

Für iOS-Clients befinden sich die Protokolldateien in den Verzeichnissen `tmp` und `Documents` unter `User Programs/Horizon/`. Um zu diesen Verzeichnissen navigieren zu können, müssen Sie zunächst eine Drittanbieter-App wie zum Beispiel `iFunbox` installieren.

Sie können die Protokollierung aktivieren, indem Sie die Einstellung **Protokollierung** in den Horizon Client-Einstellungen aktivieren. Wenn diese Einstellung aktiviert ist und der Client unerwartet beendet wird oder Sie den Client beenden und ihn erneut starten, werden die Protokolldateien zu einer einzelnen GZ-Datei zusammengeführt und komprimiert. Sie können das Paket dann per E-Mail an VMware senden. Wenn Ihr Gerät mit einem PC oder Mac verbunden ist, können Sie die Protokolldateien auch mit iTunes abrufen.

Android-Client-Protokolle

Für Android-Clients befinden sich die Protokolldateien im Verzeichnis `Android/data/com.vmware-re.view.client.android/files/`. Um zu diesem Verzeichnis navigieren zu können, müssen Sie zunächst eine Drittanbieter-App wie zum Beispiel File Explorer oder My Files installieren.

Standardmäßig werden Protokolle nur erstellt, nachdem die Anwendung unerwartet beendet wird. Sie können diese Standardeinstellung ändern, indem Sie die Einstellung **Protokoll aktivieren** in den Horizon Client-Einstellungen aktivieren. Um ein Protokollpaket per E-Mail an VMware zu schicken, können Sie die Einstellung **Protokoll senden** in den Allgemeinen Einstellungen des Clients verwenden.

Chrome OS-Clientprotokolle

Für Chrome OS-Clients sind die Protokolle ausschließlich über die JavaScript-Konsole verfügbar.

Windows 10 UWP-Clientprotokolle

Für Windows 10 UWP-Clients befinden sich die Protokolle im Verzeichnis `C:\Windows\Users\%Benutzername%\AppData\Local\VMware\VDM\logs`.

Sie können die Protokollierung aktivieren, indem Sie die Option **Erweiterte Protokollierung aktivieren** im Abschnitt „Protokollierung“ der Horizon Client-Optionen aktivieren und dann auf die Schaltfläche **Support-Informationen einholen** klicken. Sie werden aufgefordert, einen Ordner für die Protokolle auszuwählen, und Sie können den Ordner wie jeden Ordner in eine ZIP-Datei komprimieren.

Windows Store-Client-Protokolle

Für Windows Store-Clients, auf denen Horizon Client für Windows Store anstatt Horizon Client für Windows installiert ist, befinden sich die Protokolldateien im Verzeichnis `C:\Benutzer\%Benutzername%\AppData\Local\Packages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs`.

Sie können die Protokollierung aktivieren, indem Sie die Option **Erweiterte Protokollierung aktivieren** in den allgemeinen Einstellungen für Horizon Client aktivieren und dann auf die Schaltfläche **Support-Informationen einholen** klicken. Sie werden aufgefordert, einen Ordner für die Protokolle auszuwählen, und Sie können den Ordner wie jeden Ordner in eine ZIP-Datei komprimieren.

Horizon Agent -Protokolle von Windows-Computern

Protokolldateien können dabei helfen, Probleme bei der Installation, dem Anzeigeprotokoll und verschiedenen Funktionskomponenten zu beheben. Sie können Gruppenrichtlinieneinstellungen verwenden, um den Speicherort, die Ausführlichkeit und den Aufbewahrungszeitraum einiger Protokolldateien zu konfigurieren.

Protokollspeicherort

Bei den Dateinamen in der folgenden Tabelle steht *YYYY* für das Jahr, *MM* für den Monat, *DD* für den Tag, und *XXXXXX* ist eine Nummer.

Tabelle 6-5. Horizon Client für Windows-Protokolldateien

| Protokolltyp | Verzeichnispfad | Dateiname |
|---|--|--|
| Installation | C:\Benutzer\%Benutzername%\AppData\Local\Temp | vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt |
| View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7) | <Laufwerksbuchstabe>:\ProgramData\VMware\re\VDM\logs | pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt |
| | | Hinweis Sie können ein GPO verwenden, um den Protokollspeicherort zu konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration. |

Protokollkonfiguration

Es gibt mehrere Methoden, um die Protokollierungsoptionen zu konfigurieren.

- Sie können Gruppenrichtlinieneinstellungen verwenden, um den Speicherort, die Ausführlichkeit und den Aufbewahrungszeitraum zu konfigurieren. Verwenden Sie die ADMX-Vorlagendatei vdm_common.admx für die allgemeine View-Konfiguration.
- Sie können einen Befehlszeilenbefehl verwenden, um einen Ausführlichkeitsgrad festzulegen. Wechseln Sie in das Verzeichnis c:\Programme\VMware\VMware View\Agent\DCT und geben Sie folgenden Befehl ein: support.bat loglevels. Es wird eine Eingabeaufforderung geöffnet, und Sie werden zur Auswahl eines Ausführlichkeitsgrads aufgefordert.
- Sie können den Befehl vdmadmin mit der Option -A verwenden, um die Protokollierung in View Agent oder Horizon Agent zu konfigurieren. Die Anweisungen dazu finden Sie im *Horizon 7-Verwaltungs-Dokument*.

Sammeln eines Protokollpakets

Sie können einen Befehlszeilenbefehl verwenden, um Protokolle in einer ZIP-Datei zu erfassen, die Sie an den technischen Support von VMware senden können. Wechseln Sie von der Befehlszeile in das Verzeichnis c:\Programme\VMware\VMware View\Agent\DCT und geben Sie folgenden Befehl ein: support.bat.

Linux-Desktop-Protokolle

Protokolldateien können dabei helfen, Probleme bei der Installation, dem Anzeigeprotokoll und verschiedenen Funktionskomponenten zu beheben. Sie können eine Konfigurationsdatei erstellen, um den Ausführlichkeitsgrad zu konfigurieren.

Protokollspeicherort

Tabelle 6-6. Linux-Desktop-Protokolldateien

| Protokolltyp | Verzeichnispfad |
|--|---|
| Installation | /tmp/vmware-root |
| View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7) | /var/log/vmware |
| View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7) | /usr/lib/vmware/viewagent/viewagent-debug.log |

Protokollkonfiguration

Bearbeiten Sie die Datei `/etc/vmware/config`, um die Protokollierung zu konfigurieren.

Sammeln eines Protokollpakets

Dazu können Sie ein DCT-Bundle (Data Collection Tool, Datenerfassungstool) erstellen, in dem die Informationen zur Konfiguration der Maschine zusammengestellt und in einem komprimierten TAR-Archiv protokolliert werden. Öffnen Sie auf dem Linux-Desktop eine Eingabeaufforderung und führen Sie das Skript `dct-debug.sh` aus.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

Das TAR-Archiv wird in dem Verzeichnis generiert, in dem das Skript ausgeführt wurde (das aktuelle Arbeitsverzeichnis). Der Dateiname enthält das Betriebssystem, einen Zeitstempel sowie andere Informationen, zum Beispiel: `ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`.

Dieser Befehl sammelt Protokolldateien aus dem Verzeichnis `/tmp/vmware-root` und dem Verzeichnis `/var/log/vmware` und sammelt außerdem das folgende Systemprotokoll und die folgenden Konfigurationsdateien:

- `/var/log/messages*`
- `/var/log/syslog*`
- `/var/log/boot*.log`
- `/proc/cpuinfo`, `/proc/meminfo`, `/proc/vmstat`, `/proc/loadavg`
- `/var/log/audit/auth.log*`
- `/etc/hosts`
- `/etc/resolv.conf`
- `/etc/nsswitch.conf`
- `/var/log/Xorg*`
- `/etc/X11/xorg.conf`

- Kerndateien in `/usr/lib/vmware/viewagent`
- Alle Absturzprotokolldateien in `/var/crash/_usr_lib_vmware_viewagent*`

Anwenden von Sicherheits-Patches

7

Patch-Versionen können Installationsdateien für die folgenden Horizon 6- oder Horizon 7-Komponenten enthalten: View Composer, Verbindungsserver, View Agent oder Horizon Agent und verschiedene Clients. Welche Patch-Komponenten Sie installieren müssen, hängt von den Fehlerbehebungsmaßnahmen ab, die für Ihre Bereitstellung erforderlich sind.

Je nachdem, welche Fehlerbehebungen Sie benötigen, installieren Sie die entsprechenden Horizon 6- oder Horizon 7-Komponenten in der folgenden Reihenfolge:

- 1 View Composer
- 2 Verbindungsserver
- 3 View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7)
- 4 Horizon Client

Anweisungen zum Anwenden von Patches für die Serverkomponenten finden Sie im Dokument *Horizon 7-Upgrades*.

Dieses Kapitel enthält die folgenden Themen:

- [Anwenden eines Patches für View Agent oder Horizon Agent](#)
- [Anwenden eines Patches für Horizon Client](#)

Anwenden eines Patches für View Agent oder Horizon Agent

Für die Anwendung eines Patches müssen Sie das Installationsprogramm für die Patch-Version herunterladen und ausführen.

Die folgenden Schritte müssen auf der übergeordneten virtuellen Maschine für Linked-Clone-Desktop-Pools, auf jedem Desktop einer virtuellen Maschine in einem Full-Clone-Pool oder auf einzelnen Desktops auf virtuellen Maschinen für Pools, die nur einen Desktop auf einer virtuellen Maschine enthalten, durchgeführt werden.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Patch-Installationsprogramm ausführen möchten.

Verfahren

- 1 Laden Sie für alle übergeordneten virtuellen Maschinen, für alle für Vorlagen vollständiger Klone verwendeten virtuellen Maschinen, für alle vollständigen Klone in einem Pool und für alle manuell hinzugefügten einzelnen virtuellen Maschinen die Installationsdatei für die Patch-Version von View Agent (für Horizon 6) oder Horizon Agent (für Horizon 7) herunter.

Ihr Ansprechpartner bei VMware unterstützt Sie beim Download dieser Datei.

- 2 Führen Sie das Installationsprogramm aus, das Sie für die Patch-Version von View Agent oder Horizon Agent heruntergeladen haben.

Hinweis In Horizon 6 Version 6.2 und höheren Versionen müssen Sie die vorherige Version nicht deinstallieren, bevor Sie den Patch installieren.

- 3 Wenn Sie die Bereitstellung neuer virtueller Maschinen bei der Vorbereitung auf die Anwendung eines Patches für View Composer deaktiviert haben, aktivieren Sie die Bereitstellungsoption wieder.
- 4 Erstellen Sie für übergeordnete virtuelle Maschinen, die zur Erstellung von Linked-Clone-Desktop-Pools verwendet werden, einen Snapshot der virtuellen Maschine.

Informationen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client.
- 5 Verwenden Sie für Linked-Clone-Desktop-Pools den Snapshot, den Sie für die Neuzusammenstellung der Desktop-Pools erstellt haben.
- 6 Stellen Sie sicher, dass Sie sich mit Horizon Client bei den gepatchten Desktop-Pools anmelden können.
- 7 Wenn Sie Aktualisierungs- oder Neuzusammenstellungsvorgänge für Linked-Clone-Desktop-Pools abgebrochen haben, planen Sie die Aufgaben erneut.

Anwenden eines Patches für Horizon Client

Für die Anwendung eines Patches auf Desktop-Clientgeräten müssen Sie das Installationsprogramm für die Patch-Version herunterladen und ausführen. Auf mobilen Clients müssen Sie zum Anwenden eines Patches einfach die neue Version von der Website, die die App verkauft (wie Google Play, Windows Store oder Apple App Store), herunterladen und installieren.

Verfahren

- 1 Laden Sie auf jedem Clientsystem die Installationsdatei für die Patch-Version von Horizon Client herunter.

Ihr Ansprechpartner bei VMware unterstützt Sie beim Download dieser Datei. Sie können alternativ zur Client-Downloadseite unter <http://www.vmware.com/go/viewclients> gehen. Wie bereits erwähnt können Sie die Patch-Version für einige Clients von einem App Store herunterladen.

- 2 Wenn es sich beim Clientgerät um einen Mac- oder Linux-Desktop oder -Laptop handelt, entfernen Sie die aktuelle Version der Client-Software von dem Gerät.

Verwenden Sie die gebräuchliche und gerätespezifische Methode zur Entfernung von Anwendungen.

Hinweis Mit Horizon Client 3.5 für Windows und höheren Versionen müssen Sie die vorherige Version nicht deinstallieren, bevor Sie den Patch auf Windows-Clients installieren. Mit Horizon Client 4.1 für Windows und höheren Versionen können Sie die Funktion „Horizon Client Online aktualisieren“ aktivieren, um Horizon Client online auf Windows-Clients zu aktualisieren. Mit Horizon Client für Mac 4.4 und höher können Sie die Funktion „Horizon Client Online aktualisieren“ aktivieren, um Horizon Client online auf Mac-Clients zu aktualisieren.

- 3 Führen Sie gegebenenfalls das heruntergeladene Installationsprogramm für die Patch-Version von Horizon Client aus.

Wenn Sie den Patch vom Apple App Store oder Google Play bezogen haben, ist die Anwendung meist schon beim Download installiert, und Sie benötigen kein Installationsprogramm.

- 4 Stellen Sie sicher, dass Sie sich bei den gepatchten Desktop-Pools mit dem neu gepatchten Horizon Client anmelden können.