

View-Sicherheit

VMware Horizon 7 7.2



vmware®

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

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

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

docfeedback@vmware.com

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

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

Copyright © 2009-2017 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

View-Sicherheit 5

1 Horizon 7-Konten, -Ressourcen und -Protokolldateien 6

Horizon 7-Konten 6

Horizon 7-Ressourcen 7

Horizon 7-Protokolldateien 8

2 View-Sicherheitseinstellungen 10

Sicherheitsbezogene globale Einstellungen in View Administrator 10

Sicherheitsbezogene Servereinstellungen in View Administrator 13

Sicherheitsbezogene Einstellungen in View LDAP 14

3 Ports und Dienste 15

View-TCP- und UDP-Ports 15

HTTP-Umleitung in View 19

Dienste auf einem View-Verbindungsserver-Host 20

Dienste auf einem Sicherheitsserver 21

4 Konfigurieren von Sicherheitsprotokollen und Cipher Suites auf einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver 22

Standardmäßige globale Richtlinien für Sicherheitsprotokolle und Cipher Suites 23

Konfigurieren globaler Akzeptanz- und Vorschlagsrichtlinien 23

In View LDAP definierte globale Akzeptanz- und Vorschlagsrichtlinien 23

Ändern der globalen Akzeptanz- und Vorschlagsrichtlinien 24

Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern 25

Konfigurieren von Vorschlagsrichtlinien auf View-Desktops 26

Ältere Protokolle und in View deaktivierte Verschlüsselungen 27

5 Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway 30

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway (BSG) 30

6 Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung 32

Deaktivieren der USB-Umleitung für alle Gerätetypen 32

Deaktivieren der USB-Umleitung für bestimmte Geräte 34

7 HTTP-Schutzmaßnahmen auf Verbindungsservern und Sicherheitsservern 36

IETF-Standards 36

Standards des World Wide Web Consortium	37
Ressourcenfreigabe zwischen verschiedenen Ursprüngen	37
Richtlinie zur Inhaltssicherheit	39
Weitere Schutzmaßnahmen	40
Reduzieren von Sicherheitsrisiken von MIME-Typen	40
Abwenden von Site-übergreifenden Skriptangriffen	41
Überprüfen der Inhaltstypen	41
Positivliste für Benutzeragenten	42
Konfigurieren von HTTP-Schutzmaßnahmen	42

View-Sicherheit

View-Sicherheit enthält eine übersichtliche Referenz für die Sicherheitsfunktionen von VMware Horizon 7.

- Erforderliche Anmeldekonto für das System und die Datenbank.
- 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.
- Externe Schnittstellen, Ports und Dienste, die für den ordnungsgemäßen Betrieb von View geöffnet oder aktiviert sein müssen.

Zielgruppe

Diese Informationen richten sich an IT-Entscheidungsträger, -Architekten, -Administratoren und andere Benutzer, die sich mit den Sicherheitskomponenten von View vertraut machen möchten.

Horizon 7-Konten, -Ressourcen und -Protokolldateien

1

Durch unterschiedliche Konten für bestimmte Komponenten müssen Einzelpersonen nicht mehr Zugriffsrechte und Genehmigungen erteilt werden als sie benötigen. Die Kenntnis der Speicherorte der Konfigurationsdateien und anderer Dateien mit sensiblen Daten trägt zur Sicherheit der verschiedenen Hostsysteme bei.

Hinweis Ab Horizon 7.0 wird View Agent in Horizon Agent umbenannt.

Dieses Kapitel enthält die folgenden Themen:

- [Horizon 7-Konten](#)
- [Horizon 7-Ressourcen](#)
- [Horizon 7-Protokolldateien](#)

Horizon 7-Konten

Sie müssen System- und Datenbankkonten einrichten, um die Horizon 7-Komponenten zu verwalten.

Tabelle 1-1. Horizon 7-Systemkonten

Horizon-Komponente	Erforderliche Konten
Horizon Client	Konfigurieren Sie in Active Directory Benutzerkonten für die Benutzer, die Zugriff auf Remote-Desktops und -Anwendungen haben. Die Benutzerkonten müssen Mitglieder der Gruppe der Remote-Desktop-Benutzer sein, aber die Konten erfordern keine Horizon Administrator-Berechtigungen.
vCenter Server	Konfigurieren Sie in Active Directory ein Benutzerkonto, das über die Berechtigung verfügt, die Vorgänge in vCenter Server auszuführen, die erforderlich sind, um Horizon 7 zu unterstützen. Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument <i>View-Installation</i> .

Horizon-Komponente	Erforderliche Konten
View Composer	<p>Erstellen Sie in Active Directory ein Benutzerkonto, das mit View Composer verwendet werden soll. Dieses Konto ist für View Composer erforderlich, um Linked-Clone-Desktops zur Active Directory-Domäne hinzuzufügen.</p> <p>Das Benutzerkonto sollte kein Horizon-Administratorkonto sein. Erteilen Sie diesem Konto die Mindestberechtigungen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind die Berechtigungen eines Domänenadministrators nicht für das Konto erforderlich.</p> <p>Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument <i>View-Installation</i>.</p>
Verbindungsserver	<p>Bei der Installation von Horizon 7 können Sie einen bestimmten Domänenbenutzer, die lokale Administratorgruppe oder eine bestimmte Domänenbenutzergruppe als Horizon-Administratoren festlegen. Es wird empfohlen, eine dedizierte Domänenbenutzergruppe von Horizon-Administratoren zu erstellen. Standardmäßig wird der aktuell angemeldete Domänenbenutzer verwendet.</p> <p>In Horizon Administrator können Sie mit View-Konfiguration > Administratoren die Liste der Horizon-Administratoren ändern.</p> <p>Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Dokument <i>Administration von View</i>.</p>

Tabelle 1-2. Horizon-Datenbankkonten

Horizon-Komponente	Erforderliche Konten
View Composer-Datenbank	<p>Eine SQL Server- oder Oracle-Datenbank speichert die View Composer-Daten. Sie können ein Administratorkonto für die Datenbank erstellen, die Sie dem View Composer-Benutzerkonto zuweisen können.</p> <p>Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument <i>View-Installation</i>.</p>
Vom Horizon-Verbindungsserver verwendete Ereignisdatenbank	<p>Eine SQL Server- oder Oracle-Datenbank speichert die Horizon-Ereignisdaten. Sie erstellen ein Administratorkonto für die Datenbank, das Horizon Administrator zum Zugriff auf die Ereignisdaten verwenden kann.</p> <p>Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument <i>View-Installation</i>.</p>

Um das Risiko von Sicherheitsgefährdungen zu mindern, unternehmen Sie Folgendes:

- Konfigurieren Sie Horizon 7-Datenbanken auf Servern, die von anderen von Ihrem Unternehmen verwendeten Datenbankservern getrennt sind.
- Gewähren Sie einem einzelnen Benutzerkonto nicht das Recht, auf mehrere Datenbanken zuzugreifen.
- Konfigurieren Sie separate Konten für den Zugriff auf die View Composer- und Ereignisdatenbanken.

Horizon 7-Ressourcen

Horizon 7 enthält verschiedene Konfigurationsdateien und ähnliche Ressourcen, die geschützt werden müssen.

Tabelle 1-3. Horizon-Verbindungsserver- und Sicherheitsserver-Ressourcen

Ressource	Speicherort	Schutz
LDAP-Einstellungen	Nicht anwendbar.	LDAP-Daten werden automatisch als Teil der rollenbasierten Zugriffskontrolle geschützt.
LDAP-Sicherungsdateien	%ProgramData%\VMware\VDM\backups	Geschützt durch die Zugriffskontrolle.
locked.properties (Secure Gateway-Konfigurationsdatei)	<i>Installationsverzeichnis</i> \VMware\VMware View\Server\sslgateway\conf	Stellen Sie sicher, dass die Datei vor dem Zugriff durch Benutzer geschützt ist, die nicht zu den Horizon-Administratoren gehören.
absg.properties (Blast-Sicherheitsgateway-Konfigurationsdatei)	<i>Installationsverzeichnis</i> \VMware\VMware View\Server\appblastgateway	Stellen Sie sicher, dass die Datei vor dem Zugriff durch Benutzer geschützt ist, die nicht zu den Horizon-Administratoren gehören.
Protokolldateien	Siehe Horizon 7-Protokolldateien .	Geschützt durch die Zugriffskontrolle.
web.xml (Tomcat-Konfigurationsdatei)	<i>Installationsverzeichnis</i> \VMware View\Server\broker\web apps\ROOT\Web INF	Geschützt durch die Zugriffskontrolle.

Horizon 7-Protokolldateien

Horizon 7 erstellt Protokolldateien, mit denen die Installation und der Betrieb der View-Komponenten aufgezeichnet werden.

Hinweis Horizon 7-Protokolldateien sind für die Verwendung durch den VMware Support bestimmt. VMware empfiehlt das Konfigurieren und Verwenden der Ereignisdatenbank zur Überwachung von Horizon 7. Weitere Informationen hierzu finden Sie in den Dokumenten *Installation von View* und *Integration von View*.

Tabelle 1-4. Horizon 7-Protokolldateien

Horizon-Komponente	Dateipfad und andere Informationen
Alle Komponenten (Installationsprotokolldateien)	%TEMP%\vminst.log_ Datum _ Zeitstempel %TEMP%\vmmsi.log_ Datum _ Zeitstempel
Horizon Agent	<p><Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs</p> <p>Um auf Horizon 7-Protokolldateien zugreifen zu können, die unter <Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs gespeichert sind, müssen Sie die Protokolle aus einem Programm mit erweiterten Administratorberechtigungen öffnen. Klicken Sie mit der rechten Maustaste auf die Programmdatei und wählen Sie Als Administrator ausführen.</p> <p>Wenn eine Benutzerdaten-Festplatte (User Data Disk, UDD) konfiguriert ist, stimmt der <Laufwerksbuchstabe> möglicherweise mit der UDD überein.</p> <p>Die Protokolle für PCoIP heißen pcoip_agent*.log und pcoip_server*.log.</p>

Horizon-Komponente	Dateipfad und andere Informationen
Veröffentlichte Anwendungen	View Event Database, konfiguriert auf einem SQL Server- oder Oracle-Datenbankserver. Windows-Anwendungsereignisprotokolle. Standardmäßig deaktiviert.
View Composer	<i>%Systemlaufwerk%</i> \Windows\Temp\vmware-viewcomposer-ga-new.log auf dem Linked-Clone-Desktop. Das View Composer-Protokoll enthält Informationen über die Ausführung von QuickPrep- und Sysprep-Skripts. Das Protokoll zeichnet den Start und das Ende der Skriptausführung sowie Ausgabe- oder Fehlermeldungen auf.
Verbindungsserver oder Sicherheitsserver	<i><Laufwerksbuchstabe></i> :\ProgramData\VMware\VDM\logs. Das Protokollverzeichnis ist in den Protokollkonfigurationseinstellungen der ADMX-Vorlagendatei für die allgemeine View-Konfiguration (vdm_common.admx) konfigurierbar. PCoIP Secure Gateway-Protokolle werden in Dateien namens SecurityGateway_*.log im Unterverzeichnis PCoIP Secure Gateway geschrieben. Blast-Sicherheitsgateway-Protokolle werden in Dateien namens absq*.log im Unterverzeichnis Blast Secure Gateway geschrieben.
Horizon-Dienste	Horizon-Ereignisdatenbank, konfiguriert auf einem SQL Server- oder einem Oracle-Datenbankserver. Windows-Systemereignisprotokolle.

View-Sicherheitseinstellungen

View enthält verschiedene Einstellungen, die Sie verwenden können, um die Sicherheit der Konfiguration anzupassen. Sie können mit View Administrator, bzw. indem Sie das Dienstprogramm „ADSI Edit“ verwenden, auf diese Einstellungen zugreifen.

Hinweis Informationen zu Sicherheitseinstellungen für Horizon Client und Horizon Agent finden Sie im Dokument *Horizon Client und Agent-Sicherheit*.

Dieses Kapitel enthält die folgenden Themen:

- [Sicherheitsbezogene globale Einstellungen in View Administrator](#)
- [Sicherheitsbezogene Servereinstellungen in View Administrator](#)
- [Sicherheitsbezogene Einstellungen in View LDAP](#)

Sicherheitsbezogene globale Einstellungen in View Administrator

Sicherheitsbezogene globale Einstellungen für Clientsitzungen und -verbindungen sind in View Administrator unter **View-Konfiguration > Globale Einstellungen** verfügbar.

Tabelle 2-1. Sicherheitsbezogene globale Einstellungen

Einstellung	Beschreibung
Kennwort für die Datenwiederherstellung ändern	<p>Das Kennwort ist erforderlich, wenn Sie die View LDAP-Konfiguration aus einem verschlüsselten Backup wiederherstellen.</p> <p>Wenn Sie View-Verbindungsserver Version 5.1 oder höher installieren, geben Sie ein Kennwort für die Datenwiederherstellung an. Nach der Installation können Sie dieses Kennwort in View Administrator ändern.</p> <p>Wenn Sie View-Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Sie müssen das Kennwort für die Datenwiederherstellung angeben, um das verschlüsselte Backup mit dem Dienstprogramm <code>vdmimport</code> wiederherzustellen. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.</p>
Sicherheitsmodus für Nachrichten	<p>Bestimmt den Sicherheitsmechanismus, der bei der Übertragung von JMS-Nachrichten zwischen View-Komponenten verwendet wird.</p> <ul style="list-style-type: none"> ■ Wenn für diese Einstellung Deaktiviert festgelegt ist, ist der Sicherheitsmodus für Nachrichten deaktiviert. ■ Wenn Sie Aktiviert festlegen, werden ältere JMS-Nachrichten signiert und überprüft. Nicht signierte Nachrichten werden von View-Komponenten abgelehnt. Dieser Modus unterstützt eine Mischung aus SSL und einfachen JMS-Verbindungen. ■ Wenn Sie Erweitert festlegen, wird SSL für alle JMS-Verbindungen zum Verschlüsseln aller Nachrichten verwendet. Die Zugriffssteuerung wird ebenfalls aktiviert, um die JMS-Themen zu beschränken, für die View-Komponenten Nachrichten senden und empfangen können. ■ Wenn für diese Einstellung Gemischt festgelegt ist, ist der Sicherheitsmodus für Nachrichten aktiviert, wird aber für View-Komponenten, die älter als View Manager 3.0 sind, nicht erzwungen. <p>Die Standardeinstellung für Neuinstallationen lautet Erweitert. Bei einem Upgrade von einer vorherigen Version wird die in der vorherigen Version verwendete Einstellung beibehalten.</p> <p>Wichtig VMware empfiehlt dringend, den Sicherheitsmodus für Nachrichten auf Erweitert festzulegen, nachdem Sie das Upgrade für alle View-Verbindungsserver-Instanzen, Sicherheitsserver und View-Desktops auf diese Version durchgeführt haben. Die Einstellung Erweitert bietet viele wichtige Sicherheitsverbesserungen und Aktualisierungen bei der Nachrichtenwarteschlange.</p>
Erweiterter Sicherheitsstatus (schreibgeschützt)	<p>Schreibgeschütztes Feld, das angezeigt wird, wenn Sicherheitsmodus für Meldungen von Aktiviert in Erweitert geändert wird. Da die Änderung phasenweise erfolgt, wird in diesem Feld der Fortschritt für die verschiedenen Phasen angezeigt:</p> <ul style="list-style-type: none"> ■ Warten auf Nachrichtenbus-Neustart ist die erste Phase. Dieser Zustand wird angezeigt, bis Sie entweder alle Verbindungsserver-Instanzen im Pod oder den VMware Horizon View Message Bus-Komponenten-Dienst auf allen Verbindungsserver-Hosts im Pod manuell neu starten. ■ Erweiterter Modus wird aktiviert ist der nächste Status. Nachdem alle View Message Bus-Komponenten-Dienste neu gestartet wurden, beginnt das System damit, den Sicherheitsmodus für Nachrichten für alle Desktops und Sicherheitsserver in Erweitert zu ändern. ■ Erweitert ist der endgültige Status und gibt an, dass alle Komponenten nun Erweitert als Sicherheitsmodus für Nachrichten verwenden.

Einstellung	Beschreibung
Sichere Tunnelverbindungen nach Netzwerkunterbrechung neu authentifizieren	<p>Legt fest, ob die Anmeldedaten nach einer Netzwerkunterbrechung neu authentifiziert werden müssen, wenn Horizon Clients sichere Tunnelverbindungen zu View-Desktops und -Anwendungen verwenden.</p> <p>Diese Einstellung bietet erhöhte Sicherheit. Wenn beispielsweise ein Laptop gestohlen und in ein anderes Netzwerk bewegt wurde, kann der Benutzer nicht automatisch Zugang zu View-Desktops und -Anwendungen erlangen, da die Netzwerkverbindung vorübergehend unterbrochen wurde. Diese Einstellung ist standardmäßig deaktiviert.</p>
Trennung der Benutzer erzwingen	<p>Trennt alle Desktops und Anwendungen, nachdem die angegebene Anzahl von Minuten seit der Anmeldung des Benutzers bei View vergangen ist. Alle Desktops und Anwendungen werden gleichzeitig getrennt, unabhängig davon, wann der Benutzer sie geöffnet hat.</p> <p>Der Standardwert lautet 600 Minuten.</p>
Für Clients, die Anwendungen unterstützen. Verbindungen zu Anwendungen trennen und SSO-Anmeldeinformationen verwerfen, sobald der Benutzer nicht mehr mit Tastatur und Maus arbeitet	<p>Schützt Anwendungssitzungen, wenn auf dem Client-Gerät keine Tastatur- oder Mausaktivitäten stattfinden. Bei Festlegung auf Nach ... Minuten trennt View nach Ablauf der angegebenen Anzahl von Minuten ohne Benutzeraktivität sämtliche Anwendungssitzungen und verwirft die SSO-Anmeldeinformationen. Desktop-Sitzungen werden getrennt. Benutzer müssen sich erneut anmelden, um eine Verbindung zu den getrennten Anwendungen wiederherzustellen, oder einen neuen Desktop bzw. eine neue Anwendung starten.</p> <p>Bei der Einstellung Nie trennt View in keinem Fall Anwendungen oder verwirft SSO-Anmeldeinformationen aufgrund von Benutzerinaktivität.</p> <p>Die Standardeinstellung ist Nie.</p>
Andere Clients. SSO-Anmeldeinformationen verwerfen	<p>Verwirft die SSO-Anmeldeinformationen nach einem bestimmten Zeitraum. Diese Einstellung gilt für Clients, die die Remote-Ausführung von Anwendungen nicht unterstützen. Bei Festlegung von Nach ... Minuten müssen sich die Benutzer nach Ablauf der angegebenen Anzahl von Minuten nach der Anmeldung bei View erneut anmelden, um eine Verbindung zu einem Desktop herzustellen, unabhängig von den Benutzeraktivitäten auf dem Client-Gerät.</p> <p>Die Standardeinstellung ist Nach 15 Minuten.</p>
IPSec für Sicherheitsserver-Kombination aktivieren	<p>Bestimmt, ob Internet Protocol Security (IPSec) für Verbindungen zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen verwendet wird. Diese Einstellung muss deaktiviert sein, ehe Sie einen Sicherheitsserver im FIPS-Modus installieren, andernfalls schlägt die Kopplung fehl.</p> <p>Standardmäßig ist IPSec für Sicherheitsserver-Verbindungen aktiviert.</p>
Zeitüberschreitung für View Administrator-Sitzung	<p>Bestimmt, wie lange eine View Administrator-Sitzung im Leerlauf bleibt, bevor die Sitzung abläuft.</p> <p>Wichtig Wenn Sie den Zeitüberschreitungswert für die View Administrator-Sitzung auf eine hohe Minutenzahl einstellen, steigt das Risiko, dass View Administrator unautorisiert genutzt werden könnte. Seien Sie vorsichtig, wenn Sie zulassen, dass eine Sitzung lange Zeit im Leerlauf bleibt.</p> <p>Standardmäßig beträgt die Zeitüberschreitung für die View Administrator-Sitzung 30 Minuten. Sie können eine Sitzungszeitüberschreitung von 1 bis 4.320 Minuten festlegen.</p>

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

Hinweis Für alle Horizon Client-Verbindungen und View Administrator-Verbindungen mit View ist SSL erforderlich. Wenn Ihre View-Bereitstellung Lastausgleichsmodule oder andere Zwischenserver mit Client-Verbindung verwendet, können Sie SSL darauf verlagern und dann Nicht-SSL-Verbindungen auf einzelnen View-Verbindungsserver-Instanzen und Sicherheitsservern konfigurieren. Weitere Informationen finden Sie unter „Verschieben von SSL-Verbindungen auf Zwischenserver“ im Dokument *Administration von View*.

Sicherheitsbezogene Servereinstellungen in View Administrator

Sicherheitsbezogene Servereinstellungen sind in View Administrator unter **View-Konfiguration > Server** verfügbar.

Tabelle 2-2. Sicherheitsbezogene Servereinstellungen

Einstellung	Beschreibung
PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden	<p>Bestimmt, ob Horizon Client eine weitere sichere Verbindung zum View-Verbindungsserver- oder Sicherheitsserverhost herstellt, wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit View-Desktops und -Anwendungen verbinden.</p> <p>Wenn diese Einstellung deaktiviert ist, wird die Desktop- bzw. Anwendungssitzung direkt zwischen dem Client und dem View-Desktop oder Remote-Desktop-Dienste-Hosts unter Umgehung des View-Verbindungsserver- bzw. Sicherheitsserverhosts aufgebaut.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Sichere Tunnelverbindung zum Computer verwenden	<p>Bestimmt, ob Horizon Client eine zweite HTTPS-Verbindung mit dem View-Verbindungsserver- oder Sicherheitsserverhost aufbaut, wenn Benutzer sich mit einem View-Desktop bzw. mit einer View-Anwendung verbinden.</p> <p>Wenn diese Einstellung deaktiviert ist, wird die Desktop- bzw. Anwendungssitzung direkt zwischen dem Client und dem View-Desktop oder Remote-Desktop-Dienste-Hosts unter Umgehung des View-Verbindungsserver- bzw. Sicherheitsserverhosts aufgebaut.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Blast Secure Gateway für Blast-Verbindungen mit dem Computer verwenden	<p>Legt fest, ob Clients, die einen Webbrowser oder das Blast Extreme-Anzeigeprotokoll für den Zugriff auf Desktops verwenden, Blast Secure Gateway zum Herstellen einer sicheren Tunnelverbindung zum View-Verbindungsserver verwenden.</p> <p>Ist diese Option nicht aktiviert, stellen Benutzer mit einer Blast Extreme-Sitzung und Webbrowsern direkte Verbindungen zu View-Desktops her, unter Umgehung des View-Verbindungservers.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>

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

Sicherheitsbezogene Einstellungen in View LDAP

Sicherheitsbezogene Einstellungen werden in View LDAP im Objektpfad `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` bereitgestellt. Sie können das Dienstprogramm „ADSI Edit“ zum Ändern des Wertes dieser Einstellungen auf einer View-Verbindungsserver-Instanz verwenden. Die Änderung wird automatisch auf alle anderen View-Verbindungsserver-Instanzen in einer Gruppe übernommen.

Tabelle 2-3. Sicherheitsbezogene Einstellungen in View LDAP

Name/Wert-Paar	Beschreibung
cs-allowunencryptedstartsession	<p>Das Attribut ist <code>pae-NameValuePair</code>.</p> <p>Dieses Attribut steuert, ob eine sichere Verbindung zwischen einer View-Verbindungsserver-Instanz und einem Desktop notwendig ist, wenn eine Remotebenutzer-Sitzung gestartet wird. Wenn View Agent 5.1 oder höher oder Horizon Agent 7.0 oder höher auf einem Desktop-Computer installiert ist, hat dieses Attribut keine Auswirkung, und es ist immer eine sichere Verbindung erforderlich. Wenn ein View Agent installiert ist, der älter als View 5.1 ist, kann keine sichere Verbindung hergestellt werden, sofern der Desktop-Computer nicht einer Domäne mit einer bidirektionalen Vertrauensbeziehung zur Domäne der View-Verbindungsserver-Instanz angehört. In diesem Fall ist das Attribut wichtig, um zu bestimmen, ob eine Remotebenutzer-Sitzung ohne eine sichere Verbindung gestartet werden kann. In allen Fällen werden Anmeldedaten und Autorisierungstickets durch einen statischen Schlüssel geschützt. Eine sichere Verbindung bietet einen weiteren Vertrauensschutz durch Verwendung dynamischer Schlüssel.</p> <p>Bei der Einstellung 0 wird keine Remotebenutzer-Sitzung gestartet, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung eignet sich, wenn sich alle Desktops in vertrauenswürdigen Domänen befinden oder wenn auf allen Desktops View Agent 5.1 oder höher installiert ist.</p> <p>Bei der Einstellung 1 kann eine Remotebenutzer-Sitzung auch dann gestartet werden, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung eignet sich, wenn auf einigen Desktops ältere View Agents installiert sind und sich diese nicht in vertrauenswürdigen Domänen befinden.</p> <p>Die Standardeinstellung ist</p> <p>1.</p>

Ports und Dienste

Bestimmte UDP- und TCP-Ports müssen offen sein, damit die View-Komponenten miteinander kommunizieren können. Die Kenntnis, welche Windows-Dienste auf jedem Typ von View Server ausgeführt werden, hilft bei der Identifizierung der Dienste, die nicht zum Server gehören.

Dieses Kapitel enthält die folgenden Themen:

- [View-TCP- und UDP-Ports](#)
- [Dienste auf einem View-Verbindungsserver-Host](#)
- [Dienste auf einem Sicherheitsserver](#)

View-TCP- und UDP-Ports

View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten.

Während der Installation kann View optional Windows-Firewall-Regeln konfigurieren, um die Ports zu öffnen, die standardmäßig verwendet werden. Wenn Sie die Standard-Ports nach der Installation ändern, müssen Sie die Windows-Firewall-Regeln manuell neu konfigurieren, um Zugriff auf die aktualisierten Ports zu erlauben. Weitere Informationen finden Sie unter „Ersetzen von Standard-Ports für View-Dienste“ im Dokument *Installation von View*.

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

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Sicherheitsserver, View-Verbindungsserver oder Unified Access Gateway-Appliance	55000	Horizon Agent	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
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.
Sicherheitsserver	500	View-Verbindungsserver	500	UDP	IPsec-Aushandlungsverkehr.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Sicherheitsserver	*	View-Verbindungsserver	4001	TCP	JMS-Datenverkehr.
Sicherheitsserver	*	View-Verbindungsserver	4002	TCP	JMS-SSL-Datenverkehr.
Sicherheitsserver	*	View-Verbindungsserver	8009	TCP	AJP13-weitergeleiteter Webdatenverkehr, falls nicht IPsec verwendet wird.
Sicherheitsserver	*	View-Verbindungsserver	*	ESP	AJP13-weitergeleiteter Webdatenverkehr, wenn IPsec ohne NAT verwendet wird.
Sicherheitsserver	4500	View-Verbindungsserver	4500	UDP	AJP13-weitergeleiteter Webdatenverkehr, wenn IPsec über ein NAT-Gerät verwendet wird.
Sicherheitsserver, View-Verbindungsse r oder Unified Access Gateway- Appliance	*	Horizon Agent	3389	TCP	Microsoft RDP-Datenverkehr an View-Desktops, wenn Tunnelverbindungen verwendet werden.
Sicherheitsserver, View-Verbindungsse r oder Unified Access Gateway- Appliance	*	Horizon Agent	9427	TCP	Windows Media-MMR-Umleitung und Clientlaufwerksumleitung, wenn Tunnelverbindungen verwendet werden.
Sicherheitsserver, View-Verbindungsse r oder Unified Access Gateway- Appliance	*	Horizon Agent	32111	TCP	USB-Umleitung und Zeitzonensynchronisierung, wenn Tunnelverbindungen verwendet werden.
Sicherheitsserver, View-Verbindungsse r oder Unified Access Gateway- Appliance	*	Horizon Agent	4172	TCP	PCoIP, wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver, View-Verbindungsse r oder Unified Access Gateway- Appliance	*	Horizon Agent	22443	TCP	VMware Blast Extreme, wenn das Blast-Sicherheitsgateway verwendet wird.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Sicherheitsserver, View-Verbindungsserver oder Unified Access Gateway-Appliance	*	Horizon Agent	22443	TCP	HTML Access, wenn Blast Secure Gateway verwendet wird.
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird. Hinweis Da es verschiedene Zielpor
Horizon Agent	4172	View-Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance	55000	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Horizon Agent	4172	Unified Access Gateway-Appliance	*	UDP	PCoIP. View-Desktops und -Anwendungen senden PCoIP-Daten von UDP-Port 4172 an eine Unified Access Gateway-Appliance zurück. Der Ziel-UDP-Port ist der Quell-Port der empfangenen UDP-Datenpakete; da es sich dabei um Antwort-Daten handelt, ist es gewöhnlich nicht nötig, dafür eine explizite Firewallregel hinzuzufügen.
Horizon Client	*	View-Verbindungsserver oder Sicherheitsserver oder Unified Access Gateway-Appliance	80	TCP	SSL (HTTPS-Zugriff) ist standardmäßig für Clientverbindungen aktiviert, in bestimmten Fällen kann jedoch Port 80 (HTTP-Zugriff) verwendet werden. Siehe HTTP-Umleitung in View .
Horizon Client	*	View-Verbindungsserver, Sicherheitsserver oder Unified Access Gateway-Appliance	443	TCP	HTTPS für die Anmeldung bei View. (Dieser Port wird auch zur Tunnelung verwendet, wenn Tunnelverbindungen verwendet werden.)
Horizon Client	*	View-Verbindungsserver oder Sicherheitsserver oder Unified Access Gateway-Appliance	4172	TCP und UDP	PCoIP, wenn PCoIP Secure Gateway verwendet wird.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Horizon Client	*	Horizon Agent	3389	TCP	Microsoft RDP-Datenverkehr an View-Desktops, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.
Horizon Client	*	Horizon Agent	9427	TCP	Windows Media MMR-Umleitung und Clientlaufwerksumleitung, wenn anstelle von Tunnelverbindungen direkte Verbindungen verwendet werden.
Horizon Client	*	Horizon Agent	32111	TCP	USB-Umleitung und Zeitzonensynchronisierung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.
Horizon Client	*	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
Horizon Client	*	View-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.
Webbrowser	*	Sicherheitsserver oder Unified Access Gateway-Appliance	8443	TCP	HTML Access.
View-Verbindungsse r	*	View-Verbindungsserv er	48080	TCP	Zur internen Kommunikation zwischen Komponenten von View-Verbindungsse r.
View-Verbindungsse r	*	vCenter Server oder View Composer	80	TCP	SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server oder View Composer deaktiviert ist.
View-Verbindungsse r	*	vCenter Server	443	TCP	SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server aktiviert ist.
View-Verbindungsse r	*	View Composer	18443	TCP	SOAP-Nachrichten, wenn SSL für den Zugriff auf View Composer aktiviert ist.
View-Verbindungsse r	*	View-Verbindungsserv er	4100	TCP	JMS-Datenverkehr zwischen Routern.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
View-Verbindungsse r	*	View-Verbindungsse r	4101	TCP	JMS-SSL-Datenverkehr zwischen Routern.
View-Verbindungsse r	*	View-Verbindungsse r	8472	TCP	Für podübergreifende Kommunikation in der Cloud-Pod-Architektur
View-Verbindungsse r	*	View-Verbindungsse r	22389	TCP	Für globale LDAP-Replizierung in der Cloud-Pod-Architektur
View-Verbindungsse r	*	View-Verbindungsse r	22636	TCP	Für sichere globale LDAP-Replizierung in der Cloud-Pod-Architektur
Unified Access Gateway-Appliance	*	View-Verbindungsse r oder Lastausgleichsdienst	443	TCP	HTTPS-Zugriff. Unified Access Gateway-Appliances stellen eine Verbindung an TCP-Port 443 her, um mit einer View-Verbindungsse-Instanz oder mit einem Lastausgleichsdienst zu kommunizieren, die/der mehreren View-Verbindungsse-Instanzen vorgelagert ist.
View Composer-Dienst	*	ESXi-Host	902	TCP	Wird verwendet, wenn View Composer Linked-Clone-Festplatten anpasst. Dazu gehören interne Festplatten von View Composer und, falls diese angegeben werden, persistente Festplatten und SDD (System-Disposable Disks).

Hinweis Die UDP-Portnummer, die von Clients für PCoIP verwendet wird, 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.

Hinweis Microsoft Windows Server erfordert einen dynamischen Bereich von Ports, die zwischen allen Verbindungsse-Servern in der Horizon 7-Umgebung geöffnet sind. Microsoft Windows benötigt diese Ports für die herkömmliche Ausführung des Remoteprozeduraufrufs (Remote Procedure Call, RPC) und der Active Directory-Replizierung. Weitere Informationen zum dynamischen Portbereich finden Sie in der Microsoft Windows Server-Dokumentation.

HTTP-Umleitung in View

Beim Versuch, eine Verbindung über HTTP herzustellen, wird im Hintergrund eine Umleitung an HTTPS durchgeführt. Die einzige Ausnahme stellen Verbindungsversuche mit View Administrator dar. Bei neueren Horizon-Clients ist keine HTTP-Umleitung erforderlich, da diese Clients standardmäßig HTTPS verwenden. Wenn Benutzer eine Verbindung mit einem Webbrowser herstellen (z. B. zum Herunterladen von Horizon Client), ist diese Option jedoch nützlich.

Das Problem der HTTP-Umleitung ist, dass es sich nicht um ein sicheres Protokoll handelt. Wenn sich ein Benutzer nicht angewöhnt, **https://** in der Adresszeile einzugeben, kann ein Angreifer über den Webbrowser schädliche Software installieren oder Anmeldeinformationen ausspähen. Dies ist selbst dann möglich, wenn die erwartete Seite ordnungsgemäß angezeigt wird.

Hinweis Eine HTTP-Umleitung ist für externe Verbindungen nur dann möglich, wenn Sie Ihre externe Firewall für das Zulassen von eingehendem Datenverkehr an TCP-Port 80 konfigurieren.

Beim Versuch, über HTTP eine Verbindung mit View Administrator herzustellen, findet keine Umleitung statt. Stattdessen wird in einer Fehlermeldung angezeigt, dass Sie HTTPS verwenden müssen.

Informationen zum Verhindern der Umleitung für alle HTTP-Verbindungsversuche finden Sie unter „Verhindern der HTTP-Umleitung für Clientverbindungen zum Verbindungsserver“ im Dokument *Installation von View*.

Verbindungen mit Port 80 einer View-Verbindungsserver-Instanz oder eines Sicherheitsservers sind auch dann möglich, wenn Sie SSL-Clientverbindungen auf ein Zwischengerät verschieben. Weitere Informationen finden Sie unter „Verschieben von SSL-Verbindungen auf Zwischenserver“ im Dokument *Administration von View*.

Informationen zum Zulassen der HTTP-Umleitung, wenn die SSL-Portnummer geändert wurde, finden Sie unter „Ändern der Portnummer für die HTTP-Umleitung zum Verbindungsserver“ im Dokument *Installation von View*.

Dienste auf einem View-Verbindungsserver-Host

Der Betrieb von View hängt von verschiedenen Diensten ab, die auf einem View-Verbindungsserver-Host ausgeführt werden.

Tabelle 3-2. View-Verbindungsserver-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access- und Blast Extreme-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu View-Verbindungsserver über ein Blast Secure Gateway herstellen.
VMware Horizon View-Verbindungsserver	Automatisch	Stellt Verbindungs-Broker-Dienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework-, Nachrichtenbus-, Sicherheits-Gateway- und Webdienste gestartet oder beendet. Dieser Dienst führt keinen Start des VMware VDMDS-Dienstes oder des VMware Horizon View-Skripthostdienstes durch bzw. beendet diese Dienste nicht.
VMware Horizon View Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Message Bus-Komponente	Manuell	Stellt Dienste für die Nachrichtenübermittlung zwischen den View-Komponenten bereit. Dieser Dienst muss immer ausgeführt werden.

Dienstname	Starttyp	Beschreibung
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu View-Verbindungsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View-Skripthost	Deaktiviert	Bietet Unterstützung für Drittanbieterskripts, die beim Löschen von virtuellen Maschinen ausgeführt werden. Dieser Dienst ist standardmäßig deaktiviert. Sie sollten diesen Dienst aktivieren, wenn Sie Skripts ausführen möchten.
VMware Horizon View Security Gateway-Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Web-Komponente	Manuell	Stellt Webdienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMwareVDMDS	Automatisch	Stellt LDAP-Verzeichnisdienste bereit. Dieser Dienst muss immer ausgeführt werden. Während Upgrade-Vorgängen von View stellt dieser Dienst sicher, dass vorhandene Daten korrekt migriert werden.

Dienste auf einem Sicherheitsserver

Der Betrieb von View hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden.

Tabelle 3-3. Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access- und Blast Extreme-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein Blast Secure Gateway herstellen.
VMware Horizon View-Sicherheitsserver	Automatisch	Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet.
VMware Horizon View Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View Security Gateway-Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.

Konfigurieren von Sicherheitsprotokollen und Cipher Suites auf einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver

4

Sie können die Sicherheitsprotokolle und Cipher Suites konfigurieren, die vom View-Verbindungsserver akzeptiert werden. Sie können eine globale Akzeptanzrichtlinie festlegen, die für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe gilt, oder Sie können eine Akzeptanzrichtlinie für einzelne View-Verbindungsserver-Instanzen und Sicherheitsserver festlegen.

Sie können auch die Sicherheitsprotokolle und Cipher Suites konfigurieren, die View-Verbindungsserver-Instanzen vorschlagen, wenn eine Verbindung zu vCenter Server und View Composer hergestellt wird. Sie können eine globale Vorschlagsrichtlinie festlegen, die für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe gilt. Sie können keine einzelnen Instanzen definieren, um eine globale Vorschlagsrichtlinie nicht anzuwenden.

Hinweis Die Sicherheitseinstellungen für den View-Verbindungsserver gelten nicht für Blast Secure Gateway (BSG). Sie müssen die Sicherheit für BSG getrennt konfigurieren. Siehe [Kapitel 5 Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway](#).

Die uneingeschränkten Richtliniendateien („Unlimited Strength Jurisdiction Policy Files“) von Oracle sind als Standard enthalten und erlauben standardmäßig 256-Bit-Schlüssel.

Dieses Kapitel enthält die folgenden Themen:

- [Standardmäßige globale Richtlinien für Sicherheitsprotokolle und Cipher Suites](#)
- [Konfigurieren globaler Akzeptanz- und Vorschlagsrichtlinien](#)
- [Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern](#)
- [Konfigurieren von Vorschlagsrichtlinien auf View-Desktops](#)
- [Ältere Protokolle und in View deaktivierte Verschlüsselungen](#)

Standardmäßige globale Richtlinien für Sicherheitsprotokolle und Cipher Suites

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

Tabelle 4-1. Standardmäßige globale Richtlinien

Standardmäßige Sicherheitsprotokolle	Standardmäßige Verschlüsselungssammlungen
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
■ TLS 1.0	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	■ TLS_RSA_WITH_AES_128_CBC_SHA
	■ TLS_RSA_WITH_AES_256_CBC_SHA

Wenn alle verbundenen Clients TLS 1.1 und/oder TLS 1.2 unterstützen, können Sie TLS 1.0 aus der Akzeptanzrichtlinie entfernen.

Konfigurieren globaler Akzeptanz- und Vorschlagsrichtlinien

Globale Akzeptanz- und Vorschlagsrichtlinien werden in den View LDAP-Attributen festgelegt. Diese Richtlinien gelten für alle View-Verbindungsserver-Instanzen und Sicherheitsserver in einer replizierten Gruppe. Sie können View LDAP auf einer beliebigen View-Verbindungsserver-Instanz bearbeiten, um eine globale Richtlinie zu ändern.

Jede Richtlinie ist ein einwertiges Attribut an folgendem View LDAP-Ort:
cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int

In View LDAP definierte globale Akzeptanz- und Vorschlagsrichtlinien

Sie können die View LDAP-Attribute bearbeiten, die die globalen Akzeptanz- und Vorschlagsrichtlinien definieren.

Globale Akzeptanzrichtlinien

Das folgende Attribut führt Sicherheitsprotokolle auf. Sie müssen die Liste sortieren, indem Sie das neueste Protokoll an den Anfang stellen:

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

Das folgende Attribut führt die Cipher Suites auf. Dieses Beispiel zeigt eine verkürzte Liste:

```
pae-ServerSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Das folgende Attribut steuert die Rangfolge der Verschlüsselungs-Suiten. In der Regel wird die Rangfolge des Servers für Verschlüsselungs-Suiten ignoriert und diejenige des Clients verwendet. Durch Festlegung des folgenden Attributs können Sie stattdessen die Rangfolge des Servers für Verschlüsselungs-Suiten verwenden:

```
pae-ServerSSLHonorClientOrder = 0
```

Globale Vorschlagsrichtlinien

Das folgende Attribut führt Sicherheitsprotokolle auf. Sie müssen die Liste sortieren, indem Sie das neueste Protokoll an den Anfang stellen:

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

Das folgende Attribut führt die Cipher Suites auf. Diese Liste sollte in der gewünschten Reihenfolge sortiert sein. Stellen Sie die bevorzugte Cipher Suite an den Anfang der Liste und sortieren Sie die restlichen Cipher Suites nach Ihrer Präferenz. Dieses Beispiel zeigt eine verkürzte Liste:

```
pae-ClientSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Ändern der globalen Akzeptanz- und Vorschlagsrichtlinien

Mit dem Dienstprogramm ADSI-Editor können Sie die View LDAP-Attribute bearbeiten, um die globalen Akzeptanz- und Vorschlagsrichtlinien für Sicherheitsprotokolle und Verschlüsselungssammlungen zu ändern.

Voraussetzungen

- Machen Sie sich mit den View LDAP-Attributen vertraut, die die Akzeptanz- und Vorschlagsrichtlinien definieren. Siehe [In View LDAP definierte globale Akzeptanz- und Vorschlagsrichtlinien](#).
- Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogrammes ADSI-Editor mit Ihrer Windows Server-Betriebssystemversion.

Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Computer.
- 2 Wählen Sie im Konsolenbaum **Verbinden mit**.
- 3 Geben Sie im Textfeld **Definierten Namen oder Namenskontext auswählen bzw. eintippen** den definierten Namen **DC=vdi**, **DC=vmware**, **DC=int** ein.

- 4 Wählen Sie im Textfeld **Domäne oder Server auswählen bzw. eintippen** `localhost:389` oder den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des View-Verbindungsserver-Computers gefolgt von Port 389 aus bzw. geben Sie dies ein.

Zum Beispiel: `localhost:389` oder `meincomputer.meinedomäne.com:389`

- 5 Erweitern Sie den Baum vom ADSI-Editor, erweitern Sie **OU=Properties**, wählen Sie **OU=Global** und wählen Sie **OU=Common** im rechten Fensterbereich aus.
- 6 Wählen Sie beim Objekt **CN=Common, OU=Global, OU=Properties** jedes Attribut aus, das Sie ändern möchten, und geben Sie die neue Liste von Sicherheitsprotokollen oder Verschlüsselungssammlungen ein.
- 7 Führen Sie einen Neustart des Windows-Diensts „VMware Horizon View Security Gateway-Komponente“ auf jeder Verbindungsserver-Instanz und jedem Sicherheitsserver durch, wenn Sie `pae-ServerSSLSecureProtocols` geändert haben.

Sie müssen für keinen Dienst einen Neustart durchführen, nachdem Sie `pae-ClientSSLSecureProtocols` geändert haben.

Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern

Zur Angabe einer lokalen Akzeptanzrichtlinie auf einer einzelnen View-Verbindungsserver-Instanz oder einem einzelnen Sicherheitsserver müssen Sie Eigenschaften zur Datei `locked.properties` hinzufügen. Wenn die Datei `locked.properties` noch nicht auf dem View Server vorhanden ist, müssen Sie diese erstellen.

Sie müssen einen Eintrag `secureProtocols.n` für jedes Sicherheitsprotokoll hinzufügen, das Sie konfigurieren möchten. Verwenden Sie die folgende Syntax: `secureProtocols.n=security protocol`.

Sie fügen den Eintrag `enabledCipherSuite.n` für jede Verschlüsselungssammlung hinzu, die Sie konfigurieren möchten. Verwenden Sie die folgende Syntax: `enabledCipherSuite.n=cipher suite`.

Die Variable `n` ist eine Ganzzahl, die Sie in aufsteigender Folge (1, 2, 3) an jeden Eintragstyp anhängen.

Sie fügen Sie einen `honorClientOrder`-Eintrag zur Festlegung der Rangfolge der Verschlüsselungs-Suiten hinzu. In der Regel wird die Rangfolge des Servers für Verschlüsselungs-Suiten ignoriert und diejenige des Clients verwendet. Mit der folgenden Syntax können Sie stattdessen die Rangfolge des Servers für Verschlüsselungs-Suiten verwenden:

```
honorClientOrder=false
```

Vergewissern Sie sich, dass die Einträge in der Datei `locked.properties` die korrekte Syntax aufweisen und dass die Namen der Verschlüsselungssammlung und Sicherheitsprotokolle korrekt geschrieben sind. Jegliche Fehler in der Datei können dazu führen, dass der Austausch zwischen Client und Server fehlschlägt.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserver-Computer.
Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\`
- 2 Sie fügen hinzu: `secureProtocols.n` und `enabledCipherSuite.n` Einträge, einschließlich der zugehörigen Sicherheitsprotokolle und Verschlüsselungssammlungen.
- 3 Speichern Sie die Datei `locked.properties`.
- 4 Starten Sie den VMware Horizon View-Verbindungsserver- oder VMware Horizon View-Sicherheitsserver-Dienst neu, damit die Änderungen wirksam werden.

Beispiel: Standard-Akzeptanzrichtlinien auf einem einzelnen Server

Das folgende Beispiel zeigt die Einträge in der Datei `locked.properties`, die zur Angabe der Standardrichtlinien benötigt werden:

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2
secureProtocols.2=TLSv1.1
secureProtocols.3=TLSv1

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA

# Use the ordering of cipher suites given above:

honorClientOrder=false
```

Konfigurieren von Vorschlagsrichtlinien auf View-Desktops

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

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

Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem View-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
```

Ältere Protokolle und in View deaktivierte Verschlüsselungen

Einige ältere Protokolle und Verschlüsselungen, die nicht mehr als sicher gelten, sind standardmäßig in View deaktiviert. Bei Bedarf können Sie diese manuell aktivieren.

DHE-Verschlüsselungssammlungen

Weitere Informationen finden Sie unter <http://kb.vmware.com/kb/2121183>. Verschlüsselungssammlungen, die mit DSA-Zertifikaten kompatibel sind, verwenden kurzlebige Diffie-Hellman-Schlüssel, und diese Verschlüsselungen sind ab Horizon 6 Version 6.2 nicht mehr standardmäßig aktiviert.

Für Verbindungsserver-Instanzen, Sicherheitsserver und View-Desktops können Sie diese Verschlüsselungssammlungen aktivieren, indem Sie die View LDAP-Datenbank, die Datei Locked.properties oder die Registrierung wie in diesem Handbuch beschrieben entsprechend bearbeiten. Weitere Informationen finden Sie unter [Ändern der globalen Akzeptanz- und Vorschlagsrichtlinien](#), [Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern](#) und [Konfigurieren von Vorschlagsrichtlinien auf View-Desktops](#). Sie können eine Liste von Verschlüsselungssammlungen definieren, die eine oder mehrere der folgenden Sammlungen in dieser Reihenfolge enthält:

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (nur TLS 1.2, nicht FIPS)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (nur TLS 1.2, nicht FIPS)

- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (nur TLS 1.2)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (nur TLS 1.2)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

Für View Composer- und VADC-Maschinen (View Agent Direct-Connection) können Sie die DHE-Verschlüsselungssammlungen aktivieren, indem Sie die folgende Liste von Verschlüsselungen mit der Vorgehensweise einfügen, die unter „Deaktivieren von schwachen Verschlüsselungen in SSL/TLS für View Composer- und Horizon Agent-Maschinen“ in der Dokumentation *Installation von View* beschrieben ist.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

Hinweis Die Unterstützung von ECDSA-Zertifikaten lässt sich nicht aktivieren. Diese Zertifikate wurden noch nie unterstützt.

SSLv3

In Horizon 7 wurde SSL Version 3.0 entfernt.

Weitere Informationen finden Sie unter <http://tools.ietf.org/html/rfc7568>.

RC4

Weitere Informationen finden Sie unter <http://tools.ietf.org/html/rfc7465>.

Für Verbindungsserver-Instanzen, Sicherheitsserver und View-Desktops können Sie RC4 auf einem Verbindungsserver, Sicherheitsserver oder einer Horizon Agent-Maschine aktivieren, indem Sie die Konfigurationsdatei C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security bearbeiten. Am Ende der Datei befindet sich ein mehrzeiliger Eintrag namens jdk.tls.legacyAlgorithms. Entfernen Sie RC4_128 und das nachfolgende Komma aus diesem Eintrag und starten Sie den Verbindungsserver, den Sicherheitsserver oder die Horizon Agent-Maschine neu.

Für View Composer- und VADC-Maschinen (View Agent Direct-Connection) können Sie RC4 aktivieren, indem Sie die folgende Liste von Verschlüsselungen mit der Vorgehensweise einfügen, die unter „Deaktivieren von schwachen Verschlüsselungen in SSL/TLS für View Composer- und Horizon Agent-Maschinen“ in der Dokumentation *Installation von View* beschrieben ist.

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

In Horizon 7 ist TLS 1.0 standardmäßig deaktiviert.

Weitere Informationen dazu finden Sie unter https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf und <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>. Anweisungen zur Aktivierung von TLS 1.0 finden Sie in den Abschnitten „Aktivieren von TLS v1 für vCenter-Verbindungen vom Verbindungsserver“ und „Aktivieren von TLSv1 für vCenter- und ESXi-Verbindungen von View Composer“ im Dokument *View-Upgrades*.

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway

5

Die Sicherheitseinstellungen für den View-Verbindungsserver gelten nicht für Blast Secure Gateway (BSG). Sie müssen die Sicherheit für BSG getrennt konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway \(BSG\)](#)

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für Blast Secure Gateway (BSG)

Sie können die Sicherheitsprotokolle und Verschlüsselungssammlungen konfigurieren, die der Listener auf der BSG-Client-Seite akzeptiert, indem Sie die Datei `absg.properties` bearbeiten.

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 Eigenschaften, `localHttpsProtocolLow` und `localHttpsProtocolHigh`, legen den Protokollbereich fest, den der BSG-Listener akzeptiert. Zum Beispiel bewirken die Einstellungen `localHttpsProtocolLow=tls1.0` und `localHttpsProtocolHigh=tls1.2`, dass der Listener TLS 1.0, TLS 1.1 und TLS 1.2 akzeptiert. Die Standardeinstellungen sind `localHttpsProtocolLow=tls1.1` und `localHttpsProtocolHigh=tls1.2`. Sie können die BSG-Datei `absg.log` überprüfen, um festzustellen, welche Werte für eine bestimmte BSG-Instanz in Kraft sind.

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 VERSCHLÜSSELUNGSLISTE` 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 Bearbeiten Sie auf der Verbindungsserver-Instanz die Datei *Installationsverzeichnis\VMware\VMware View\Server\appblastgateway\absg.properties*.

Standardmäßig ist *%ProgramFiles%* das Installationsverzeichnis.

- 2 Bearbeiten Sie die Eigenschaften `localHttpsProtocolLow` und `localHttpsProtocolHigh`, um einen Protokollbereich anzugeben.

Beispiel:

```
localHttpsProtocolLow=tls1.0  
localHttpsProtocolHigh=tls1.2
```

Um nur ein Protokoll zu aktivieren, geben Sie dasselbe Protokoll für `localHttpsProtocolLow` und `localHttpsProtocolHigh` an.

- 3 Bearbeiten Sie die Eigenschaft `localHttpsCipherSpec`, um eine Liste von Verschlüsselungssammlungen anzugeben.

Beispiel:

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

- 4 Führen Sie einen Neustart des Windows-Diensts VMware HorizonView Blast Secure Gateway durch.

Bereitstellen von USB-Geräten in einer sicheren Horizon 7-Umgebung

6

USB-Geräte können für die Sicherheitsbedrohung mit der Bezeichnung BadUSB anfällig sein, bei der die Firmware auf USB-Geräten gehackt und durch Malware ersetzt wird. Beispielsweise kann ein Gerät veranlasst werden, Netzwerkdatenverkehr umzuleiten oder eine Tastatur zu emulieren und die Tastatureingabe aufzuzeichnen. Sie können die USB-Umleitungsfunktion konfigurieren, um Ihre Horizon 7-Bereitstellung vor dieser Sicherheitslücke zu schützen.

Durch Deaktivieren der USB-Umleitung können Sie verhindern, dass USB-Geräte an die Horizon 7-Desktops und -Anwendungen Ihrer Benutzer umgeleitet werden. Alternativ können Sie die Umleitung bestimmter USB-Geräte deaktivieren, damit Benutzer in ihren Desktops und Anwendungen nur auf bestimmte Geräte Zugriff haben.

Die Entscheidung, ob Sie diese Schritte ausführen sollten, hängt von den Sicherheitsanforderungen in Ihrem Unternehmen ab. Diese Schritte sind nicht obligatorisch. Sie können die USB-Umleitung installieren und diese Funktion für alle USB-Geräte in Ihrer Horizon 7-Bereitstellung aktiviert lassen. Sie sollten sich zumindest genau überlegen, in welchem Umfang Ihr Unternehmen versuchen sollte, die Anfälligkeit für diese Sicherheitslücke zu reduzieren.

Dieses Kapitel enthält die folgenden Themen:

- [Deaktivieren der USB-Umleitung für alle Gerätetypen](#)
- [Deaktivieren der USB-Umleitung für bestimmte Geräte](#)

Deaktivieren der USB-Umleitung für alle Gerätetypen

Für bestimmte Umgebungen mit hohen Sicherheitsanforderungen müssen Sie für alle USB-Geräte, die Benutzer an ihre Clientgeräte angeschlossen haben, die Umleitung an die Remote-Desktops und -Anwendungen verhindern. Sie können die USB-Umleitung für alle Desktop-Pools, bestimmte Desktop-Pools oder bestimmte Benutzer in einem Desktop-Pool deaktivieren.

Sie können jede der folgenden Strategien Ihrer Situation entsprechend anwenden:

- Wenn Sie Horizon Agent auf einem Desktop-Image oder RDS-Host installieren, deaktivieren Sie die Setup-Option **USB-Umleitung**. (Diese Option ist standardmäßig deaktiviert.) Dadurch wird der Zugriff auf USB-Geräte auf allen Remote-Desktops und -Anwendungen verhindert, die über das Desktop-Image oder den RDS-Host bereitgestellt werden.

- Bearbeiten Sie in Horizon Administrator die Richtlinie **USB-Zugriff** für einen bestimmten Pool, um den Zugriff entweder zu verweigern oder zuzulassen. Bei dieser Vorgehensweise müssen Sie das Desktop-Image nicht ändern und können den Zugriff auf USB-Geräte in bestimmten Desktop-Pools und Anwendungspools steuern.

Nur die globale Richtlinie **USB-Zugriff** ist für RDS-Desktop-Pools und -Anwendungspools verfügbar. Diese Richtlinie kann nicht für einzelne RDS-Desktop-Pools oder Anwendungspools festgelegt werden.

- Nachdem Sie die Richtlinie in View Administrator auf Desktop- oder Anwendungspool-Ebene festgelegt haben, können Sie die Richtlinie für einen bestimmten Benutzer im Pool außer Kraft setzen, indem Sie die Einstellung **Benutzer-Außerkraftsetzung** und anschließend einen Benutzer auswählen.
- Legen Sie die Richtlinie **Exclude All Devices** auf der Horizon Agent-Seite oder auf der Client-Seite auf **true** wie erforderlich fest.
- Erstellen Sie mit Intelligente Richtlinien eine Richtlinie, die die Horizon-Richtlinieneinstellung **USB-Umleitung** deaktiviert. Mit diesem Vorgehen können Sie die USB-Umleitung auf einem bestimmten Remote-Desktop deaktivieren, wenn bestimmte Bedingungen erfüllt sind. Sie haben beispielsweise die Möglichkeit, eine Richtlinie zu konfigurieren, mit der die USB-Umleitung deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt.

Wenn Sie für die Richtlinie **Exclude All Devices** die Option **true** festlegen, verhindert Horizon Client, dass alle USB-Geräte umgeleitet werden. Sie können andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie für diese Richtlinie **false** festlegen, lässt Horizon Client zu, dass alle USB-Geräte umgeleitet werden, mit Ausnahme derer, die durch andere Richtlinieneinstellungen blockiert werden. Sie können die Richtlinie sowohl für Horizon Agent als auch für Horizon Client festlegen. Die folgende Tabelle zeigt, wie sich die Richtlinie **Exclude All Devices**, die Sie für Horizon Agent und Horizon Client festlegen können, zu einer effektiven Richtlinie für den Clientcomputer kombinieren lässt. Standardmäßig können alle USB-Geräte umgeleitet werden, es sei denn, sie wären anderweitig blockiert.

Tabelle 6-1. Auswirkungen der Kombination von „Exclude All Devices (Alle Geräte ausschließen)“

Richtlinie „Alle Geräte ausschließen“ auf Horizon Agent	Richtlinie „Alle Geräte ausschließen“ auf Horizon Client	Kombinierte effektive Richtlinie zum Ausschließen aller Geräte
false oder nicht definiert (alle USB-Geräte einschließen)	false oder nicht definiert (alle USB-Geräte einschließen)	Include all USB devices (Alle USB-Geräte einschließen)
false (alle USB-Geräte einschließen)	true (alle USB-Geräte ausschließen)	Exclude all USB devices (Alle USB-Geräte ausschließen)
true (alle USB-Geräte ausschließen)	Beliebig oder nicht definiert	Exclude all USB devices (Alle USB-Geräte ausschließen)

Wenn Sie die Richtlinie `Disable Remote Configuration Download` auf **true** setzen, wird der Wert von `Exclude All Devices` auf dem Horizon Agent nicht an Horizon Client weitergegeben. Horizon Agent und Horizon Client erzwingen dann den lokalen Wert von `Exclude All Devices`.

Diese Richtlinien sind in der ADMX-Vorlagendatei zur Konfiguration von Horizon Agent (`vdm_agent.admx`) enthalten. Weitere Informationen finden Sie unter „USB-Einstellungen in der ADMX-Vorlage für die Horizon Agent-Konfiguration“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Deaktivieren der USB-Umleitung für bestimmte Geräte

Manche Benutzer müssen möglicherweise bestimmte lokal angeschlossene USB-Geräte umleiten, damit sie Aufgaben auf ihren Remote-Desktops oder -Anwendungen ausführen können. Beispielsweise muss ein Arzt möglicherweise mithilfe eines USB-Diktiergeräts die medizinischen Daten von Patienten aufzeichnen. In diesen Fällen können Sie nicht den Zugriff auf alle USB-Geräte deaktivieren. Mithilfe von Gruppenrichtlinieneinstellungen können Sie die USB-Umleitung für bestimmte Geräte aktivieren bzw. deaktivieren.

Bevor Sie die USB-Umleitung für bestimmte Geräte aktivieren, sollten Sie sicherstellen, dass Sie den physischen Geräten vertrauen, die an Client-Computer in Ihrem Unternehmen angeschlossen sind. Stellen Sie sicher, dass Ihre Lieferkette vertrauenswürdig ist. Verfolgen Sie möglichst eine Kontrollkette für die USB-Geräte nach.

Darüber hinaus sollten Sie Ihre Mitarbeiter schulen, um sicherzustellen, dass sie keine Geräte unbekannter Herkunft anschließen. Beschränken Sie die Geräte in Ihrer Umgebung nach Möglichkeit auf jene Geräte, die nur signierte Firmware-Updates akzeptieren, FIPS 140-2 Level 3-zertifiziert sind und keinerlei vor Ort aktualisierbare Firmware unterstützen. Die Nachverfolgung dieser USB-Gerätetypen ist schwierig und je nach Ihren Geräteanforderungen sind sie möglicherweise nicht auffindbar. Diese Optionen mögen nicht wirklich praktisch sein, sollten aber in Erwägung gezogen werden.

Jedes USB-Gerät verfügt über eine eigene Hersteller- und Produkt-ID, mit der es gegenüber dem Computer identifiziert wird. Durch Konfigurieren der Gruppenrichtlinieneinstellungen für die Horizon Agent-Konfiguration können Sie eine Richtlinie für den Einschluss bekannter Gerätetypen festlegen. Durch diese Vorgehensweise entfällt das Risiko durch unbekannte Geräte in Ihrer Umgebung.

Beispielsweise können Sie verhindern, dass alle Geräte mit Ausnahme der Geräte von einem bekannten Gerätehersteller und mit einer bestimmten Produkt-ID (`vid/pid=0123/abcd`) an den Remote-Desktop oder die Remoteanwendung umgeleitet werden:

<code>ExcludeAllDevices</code>	<code>Enabled</code>
<code>IncludeVidPid</code>	<code>o:vid-0123_pid-abcd</code>

Hinweis Diese Beispielkonfiguration bietet Schutz, aber ein manipuliertes Gerät kann jede VID/PID melden, weshalb auch weiterhin Angriffe möglich sind.

Horizon 7 blockiert standardmäßig die Umleitung bestimmter Gerätefamilien an den Remote-Desktop oder die Remoteanwendung. Beispielsweise wird die Anzeige von Eingabegeräten (Human Interface Devices, HIDs) und Tastaturen für den Gast blockiert. Das Ziel von veröffentlichtem BadUSB-Code sind auch USB-Tastaturgeräte.

Sie können die Umleitung bestimmter Gerätefamilien an den Remote-Desktop oder die Remoteanwendung verhindern. Beispielsweise können Sie alle Video-, Audio- und Massenspeichergeräte blockieren:

```
ExcludeDeviceFamily o:video;audio;storage
```

Umgekehrt können Sie eine Whitelist erstellen, indem Sie die Umleitung aller Geräte verhindern, aber die Verwendung einer bestimmten Gerätefamilie zulassen. Beispielsweise können Sie alle Geräte mit Ausnahme von Speichergeräten blockieren:

```
ExcludeAllDevices Enabled
IncludeDeviceFamily o:storage
```

Ein weiteres mögliches Risiko ergibt sich aus der Tatsache, dass sich ein Remotebenutzer bei einem Desktop oder einer Anwendung anmeldet und diesen bzw. diese infiziert. Sie können den USB-Zugriff auf alle Horizon 7-Verbindungen verhindern, die von außerhalb der Unternehmensfirewall hergestellt werden. Das USB-Gerät kann intern, aber nicht extern verwendet werden.

Beachten Sie: Wenn Sie TCP-Port 32111 blockieren, um den externen Zugriff auf USB-Geräte zu deaktivieren, funktioniert die Zeitzonensynchronisierung nicht, weil der Port 32111 auch für die Zeitzonensynchronisierung verwendet wird. Für Zero-Clients ist der USB-Datenverkehr in einen virtuellen Kanal auf UDP-Port 4172 eingebettet. Da Port 4172 für das Anzeigeprotokoll sowie für die USB-Umleitung verwendet wird, können Sie Port 4172 nicht blockieren. Bei Bedarf können Sie die USB-Umleitung auf Zero-Clients deaktivieren. Weitere Informationen hierzu erhalten Sie in der Begleitdokumentation zum Zero-Client oder vom Hersteller des Zero-Clients.

Die Festlegung von Richtlinien zum Blockieren bestimmter Gerätefamilien oder bestimmter Geräte kann das Risiko einer Infizierung mit BadUSB-Malware reduzieren. Durch diese Richtlinien kann das Risiko nicht vollständig eliminiert werden, aber sie stellen eine wirkungsvolle Komponente einer Gesamtstrategie für die Sicherheit dar.

Diese Richtlinien sind in der ADMX-Vorlagendatei zur Konfiguration von Horizon Agent (`vdm_agent.admx`) enthalten. Weitere Informationen finden Sie unter *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

HTTP-Schutzmaßnahmen auf Verbindungsservern und Sicherheitsservern

7

In Horizon 7 werden bestimmte Maßnahmen zum Schutz der Kommunikation über das HTTP-Protokoll eingesetzt.

Dieses Kapitel enthält die folgenden Themen:

- [IETF-Standards](#)
- [Standards des World Wide Web Consortium](#)
- [Weitere Schutzmaßnahmen](#)
- [Konfigurieren von HTTP-Schutzmaßnahmen](#)

IETF-Standards

Verbindungsserver und Sicherheitsserver entsprechen bestimmten Internet Engineering Task Force (IETF)-Standards.

- Transport Layer Security (TLS) von RFC 5746 – Die Anzeige-Erweiterung der Neuverhandlung, auch als sichere Neuverhandlung bezeichnet, ist standardmäßig aktiviert.

Hinweis Von Clients initiierte Neuverhandlungen sind standardmäßig auf Verbindungsservern und Sicherheitsservern deaktiviert. Für die Aktivierung bearbeiten Sie den Registrierungswert [HKLM \SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions und entfernen **-Djdk.tls.rejectClientInitiatedRenegotiation=true** aus der Zeichenfolge.

- HTTP Strict Transport Security (HSTS) von RFC 6797, auch als „Transportsicherheit“ bezeichnet, ist standardmäßig aktiviert. Diese Einstellung kann nicht deaktiviert werden.
- HTTP Header Field X-Frame-Optionen von RFC 7034, auch als „Zähler-Clickjacking“ bezeichnet, sind standardmäßig aktiviert. Sie können diese deaktivieren, indem Sie den Eintrag `x-frame-options=OFF` der Datei `locked.properties` hinzufügen. Weitere Informationen zum Hinzufügen von Eigenschaften zur Datei `locked.properties` finden Sie unter [Konfigurieren von HTTP-Schutzmaßnahmen](#).

Hinweis In Versionen vor Horizon 7 Version 7.2 hat die Änderung dieser Option keine Auswirkungen auf Verbindungen mit HTML Access.

- Die Überprüfung der Herkunft nach RFC 6454, mit der die Fälschung standortübergreifender Anforderungen unterbunden wird, ist standardmäßig aktiviert. Sie können diese deaktivieren, indem Sie der Datei `locked.properties` den Eintrag `checkOrigin=false` hinzufügen. Weitere Informationen finden Sie unter [Ressourcenfreigabe zwischen verschiedenen Ursprüngen](#).

Hinweis In früheren Versionen war dieser Schutzmechanismus standardmäßig deaktiviert.

Standards des World Wide Web Consortium

Verbindungsserver und Sicherheitsserver entsprechen bestimmten W3C-Standards (World Wide Web Consortium).

- Die CORS-Funktion (Cross-Origin Resource Sharing, Ressourcenfreigabe zwischen verschiedenen Ursprüngen), die die clientseitigen Anforderungen verschiedener Ursprünge beschränkt, ist standardmäßig aktiviert. Sie können diese Funktion durch Hinzufügen des Eintrags `EnableCORS=false` zur Datei `locked.properties` deaktivieren.
- Die CSP-Funktion (Content Security Policy, Richtlinie zur Inhaltssicherheit), die die Gefährdungen durch eine umfangreiche Klasse von Sicherheitslücken beim Einfügen von Inhalten reduziert, ist standardmäßig aktiviert. Sie können diese Funktion durch Hinzufügen des Eintrags `EnableCSP=false` zur Datei `locked.properties` deaktivieren.

Ressourcenfreigabe zwischen verschiedenen Ursprüngen

Die CORS-Funktion (Cross-Origin Resource Sharing, Ressourcenfreigabe zwischen verschiedenen Ursprüngen) steuert die clientseitigen Anforderungen verschiedener Herkunft durch Bereitstellen von Richtlinienanweisungen für den Client nach Bedarf und Überprüfen der Anforderungen auf Einhaltung der Richtlinie. Diese Funktion ist standardmäßig aktiviert.

Zu den Richtlinien gehört der Satz zulässiger HTTP-Methoden sowie die Festlegung, woher Anforderungen stammen können und welche Arten von Inhalten gültig sind. Diese Richtlinien variieren je nach Anforderungs-URL und können durch Hinzufügen von Einträgen zur Datei `locked.properties` nach Bedarf neu konfiguriert werden.

Ein Auslassungszeichen nach einem Eigenschaftsnamen weist darauf hin, dass für die Eigenschaft eine Liste verwendet werden kann.

Tabelle 7-1. CORS-Eigenschaften

Eigenschaft	Werttyp	Master-Standardeinstellung	Sonstige Standardeinstellungen
enableCORS	true false	true	n/a
acceptContentType...	http-content-type	application/x-www-form-urlencoded,application/xml,text/xml	<ul style="list-style-type: none"> ■ admin=application/x-amf ■ helpdesk=application/json,application/text,application/x-www-form-urlencoded ■ view-vlsi-rest=application/json
acceptHeader...	http-header-name	*	n/a
exposeHeader...	http-header-name	*	n/a
filterHeaders	true false	true	n/a
checkOrigin	true false	true	n/a
allowCredentials	true false	false	admin=true broker=true helpdesk=true misc=true portal=true saml=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	misc=GET,HEAD saml=GET,HEAD
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	OFF	n/a

Beispiele für CORS-Eigenschaften in der Datei `Locked.properties`:

```
enableCORS = true
allowPreflight = true
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
```

```
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

Überprüfen der Herkunft

Das Überprüfen des Ursprungs, also der Herkunft, ist standardmäßig aktiviert. Wenn diese Funktion aktiviert ist, wird eine Anforderung nur ohne Ursprung akzeptiert oder wenn sie von der Adresse in der externen URL, der Adresse `balancedHost`, einer beliebigen `portalHost`-Adresse, einem beliebigen `chromeExtension`-Hash, von `null` oder `localhost` stammt. Bei einem anderen Ursprung wird der Fehler „Unerwartete Herkunft“ protokolliert und der Status „404“ zurückgegeben.

Wenn die Lasten mehrerer Verbindungsserver oder Sicherheitsserver ausgeglichen sind, müssen Sie die Adresse des Lastausgleichsdienstes angeben, indem Sie der Datei `locked.properties` einen `balancedHost`-Eintrag hinzufügen. Port 443 wird für diese Adresse vorausgesetzt.

Wenn die Clients die Verbindung über Unified Access Gateway oder ein anderes Gateway herstellen müssen, müssen Sie alle Gateway-Adressen durch Hinzufügen von `portalHost`-Einträgen zur Datei `locked.properties` angeben. Port 443 wird auch für diese Adressen vorausgesetzt. Wenn über einen anderen als den in der externen URL angegebenen Namen ein Zugriff auf einen Verbindungsserver oder Sicherheitsserver möglich sein soll, müssen Sie diesen ebenfalls in der oben genannten Datei angeben.

Chrome-Erweiterung-Clients legen ihren ersten Ursprung mit ihrer eigenen Identität fest. Damit Verbindungen erfolgreich hergestellt werden können, muss die Chrome-Erweiterung durch Hinzufügen eines `chromeExtension`-Eintrags zur Datei `locked.properties` registriert werden.

Richtlinie zur Inhaltssicherheit

Die CSP-Funktion (Content Security Policy, Richtlinie zur Inhaltssicherheit) reduziert die Gefährdungen durch eine umfangreiche Klasse von Sicherheitslücken beim Einfügen von Inhalten, wie z. B. beim Cross-Site Scripting (XSS), durch die Bereitstellung von Richtlinienanweisungen für kompatible Browser. Diese Funktion ist standardmäßig aktiviert. Sie können die Konfiguration der Richtlinienanweisungen durch Hinzufügen von Einträgen zur Datei `locked.properties` ändern.

Tabelle 7-2. CSP-Eigenschaften

Eigenschaft	Werttyp	Master-Standardeinstellung	Sonstige Standardeinstellungen
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe- eval' data::style-src 'self' 'unsafe- inline';font-src 'self' data:	portal=child-src 'self' blob;;default-src 'self';connect-src 'self' wss;;font-src 'self' data::img-src 'self' data: blob;;media-src 'self' blob;;object-src 'self' blob;;script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';frame- ancestors 'self'
x-frame-options	OFF specification	deny	portal=sameorigin
x-content-type-options	OFF specification	nosniff	n/a
x-xss-protection	OFF specification	1; mode=block	n/a

Sie können CSP-Eigenschaften zur Datei `locked.properties` hinzufügen. Beispiele für CSP-Eigenschaften:

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' data:
content-security-policy-portal = default-src 'self';frame-ancestors 'self'
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

Weitere Schutzmaßnahmen

In Horizon 7 wird die Kommunikation über das HTTP-Protokoll zusätzlich zur Verwendung der IETF (Internet Engineering Task Force)- und W3-Standards durch weitere Maßnahmen geschützt.

Reduzieren von Sicherheitsrisiken von MIME-Typen

Horizon 7 sendet standardmäßig den Header `x-content-type-options: nosniff` in seinen HTTP-Antworten und schützt so vor Angriffen, die auf MIME-Typ-Störungen basieren.

Sie können diese Funktion deaktivieren, indem Sie der Datei `locked.properties` folgenden Eintrag hinzufügen:

```
x-content-type-options=OFF
```

Abwenden von Site-übergreifenden Skriptangriffen

Horizon 7 setzt standardmäßig die XSS-Filterfunktion ein, um Site-übergreifende Angriffe auf Skripts durch Versenden des Headers `x-xss-protection=1; mode=block` in seinen HTTP-Antworten abzuwenden.

Sie können diese Funktion deaktivieren, indem Sie der Datei `locked.properties` folgenden Eintrag hinzufügen:

```
x-xss-protection=OFF
```

Überprüfen der Inhaltstypen

Standardmäßig akzeptiert Horizon 7 Anforderungen nur mit den folgenden deklarierten Inhaltstypen:

- `application/x-www-form-urlencoded`
- `application/xml`
- `text/xml`

Hinweis In früheren Versionen war dieser Schutzmechanismus standardmäßig deaktiviert.

Sie können die Inhaltstypen, die von View akzeptiert werden, beschränken, indem Sie in der Datei `locked.properties` folgenden Eintrag hinzufügen:

```
acceptContentType.1=content-type
```

Beispiel:

```
acceptContentType.1=x-www-form-urlencoded
```

Um einen anderen Inhaltstyp zu akzeptieren, fügen Sie den Eintrag `acceptContentType.2=content-type` usw. hinzu.

Um Anforderungen mit einem deklarierten Inhaltstyp zu akzeptieren, geben Sie `acceptContentType=*` an.

Hinweis In Versionen vor Horizon 7 Version 7.2 hat die Änderung dieser Liste keine Auswirkungen auf Verbindungen mit Horizon Administrator.

Positivliste für Benutzeragenten

Mit einer Positivliste lassen sich die Benutzeragenten beschränken, die mit Horizon 7 interagieren. Standardmäßig werden alle Benutzeragenten akzeptiert.

Hinweis Dies ist keine Sicherheitsfunktion im engeren Sinn. Die Ermittlung von Benutzeragenten basiert auf der Kopfzeile der Anforderung des Benutzeragenten, die vom für die Verbindung verwendeten Client oder Browser bereitgestellt wird und die manipuliert werden kann. Einige Browser erlauben die Veränderung der Anforderungskopfzeile durch den Benutzer.

Ein Benutzeragent wird durch seinen Namen und eine Mindestversion angegeben. Beispiel:

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

Dies bedeutet, dass nur Google Chrome Version 14 und höher sowie Safari Version 5.1 und höher für Herstellung einer Verbindung mithilfe von HTML Access zulässig sind. Alle Browser können eine Verbindung mit anderen Diensten herstellen.

Sie können die folgenden Namen anerkannter Benutzeragenten eingeben:

- Android
- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

Hinweis Nicht alle dieser Benutzeragenten werden von Horizon 7 unterstützt. Es handelt sich hier um Beispiele.

Konfigurieren von HTTP-Schutzmaßnahmen

Für die Konfiguration von HTTP-Schutzmaßnahmen müssen Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf der Verbindungsserver- oder Sicherheitsserver-Instanz erstellen oder bearbeiten.

Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- Verwenden Sie zur Konfiguration einer Eigenschaft in `locked.properties` die folgende Syntax:

```
myProperty = newValue
```

- Für den Eigenschaftsnamen muss immer die Groß-/Kleinschreibung beachtet werden, für den Wert kann die Groß-/Kleinschreibung berücksichtigt werden. Leerzeichen um das `=`-Zeichen sind optional.

- Für CORS- und CSP-Eigenschaften besteht die Möglichkeit, sowohl dienstspezifische Werte als auch einen Master-Wert festzulegen. So kann z. B. der Administratordienst für die Handhabung von Horizon Administrator-Anforderungen verantwortlich sein, und eine Eigenschaft für diesen Dienst durch Anhängen von `-admin` an den Eigenschaftsnamen ohne Auswirkungen auf andere Dienste festgelegt werden.

```
myProperty-admin = newValueForAdmin
```

- Wenn sowohl ein Master-Wert wie ein dienstspezifischer Wert festgelegt sind, gilt der dienstspezifische Wert für den benannten Dienst und der Master-Wert für alle anderen Dienste. Die einzige Ausnahme ist der Sonderwert „AUS“. Wenn für den Master-Wert einer Eigenschaft „AUS“ festgelegt ist, werden alle dienstspezifischen Werte für diese Eigenschaft ignoriert.

Beispiel:

```
myProperty = OFF
myProperty-admin = newValueForAdmin    ; ignored
```

- Für einige Eigenschaften können Wertelisten angegeben werden.

Um einen einzelnen Wert festzulegen, geben Sie die folgende Eigenschaft ein:

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

Um mehrere Werte für eine Eigenschaft festzulegen, die Wertelisten akzeptiert, können Sie jeden Wert in einer eigenen Zeile angeben:

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- Um den korrekten Dienstnamen für eine dienstspezifische Konfiguration zu ermitteln, suchen Sie in den Debug-Protokollen nach Zeilen mit folgender Sequenz:

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

In diesem Beispiel lautet der Dienstname `admin`. Sie können die folgenden typischen Dienstnamen verwenden:

- `admin` für Horizon Administrator
- `broker` für den Verbindungsserver
- `docroot` für den lokalen Dateidienst
- `helpdesk` für den Helpdesk
- `portal` für HTML Access
- `saml` für die SAML-Kommunikation (vIDM)

- tunnel für den sicheren Tunnel
- view-`vlsi` für die View-API
- misc für Sonstige