

View-Installation

VMware Horizon 7 7.2

vmware[®]

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

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2011–2017 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Installation von View	7
1 Systemanforderungen für Serverkomponenten	9
Horizon-Verbindungsserver – Serveranforderungen	9
View Administrator-Anforderungen	11
View Composer-Anforderungen	12
2 Systemanforderungen für Gastbetriebssysteme	15
Unterstützte Betriebssysteme für Horizon Agent	15
Unterstützte Betriebssysteme für die eigenständige Horizon Persona Management-Software	16
Unterstützung für Remote-Anzeigeprotokoll und -Software	16
3 Installieren von View in einer IPv6-Umgebung	23
Einrichten von View in einer IPv6-Umgebung	23
Unterstützte vSphere-Datenbank- und Active Directory-Versionen in einer IPv6-Umgebung	24
Unterstützte Betriebssysteme für View -Server in einer IPv6-Umgebung	24
Unterstützte Windows-Betriebssysteme für Desktops und RDS-Hosts in einer IPv6-Umgebung	25
Unterstützte Clients in einer IPv6-Umgebung	25
Unterstützte Remote-Protokolle in einer IPv6-Umgebung	25
Unterstützte Authentifizierungstypen in einer IPv6-Umgebung	26
Andere unterstützte Funktionen in einer IPv6-Umgebung	26
4 Installieren von View im FIPS-Modus	29
Überblick über die Einrichtung von View im FIPS-Modus	29
Systemanforderungen für den FIPS-Modus	30
5 Vorbereiten von Active Directory	31
Konfigurieren von Domänen und Vertrauensbeziehungen	32
Erstellen einer OU für Remote-Desktops	33
Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus	33
Erstellen von Gruppen für Benutzer	34
Erstellen eines Benutzerkontos für vCenter Server	34
Erstellen eines Benutzerkontos für einen eigenständigen View Composer Server	34
Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge	34
Erstellen eines Benutzerkontos für Instant Clone-Vorgänge	35
Konfigurieren der Richtlinie „Eingeschränkte Gruppen“	36
Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7	37
Vorbereiten von Active Directory für die Smartcard-Authentifizierung	37
Deaktivieren von schwachen Verschlüsselungen in SSL/TLS	41

- 6 Installieren von View Composer 43**
 - Vorbereiten einer View Composer-Datenbank 43
 - Konfigurieren eines SSL-Zertifikats für View Composer 52
 - Installieren des View Composer-Dienstes 52
 - Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer 54
 - Konfigurieren der Infrastruktur für View Composer 55

- 7 Installieren von View-Verbindungsserver 57**
 - Installieren der View-Verbindungsserver-Software 57
 - Installationsvoraussetzungen für View-Verbindungsserver 58
 - Installieren von View-Verbindungsserver mit einer neuen Konfiguration 59
 - Installieren einer replizierten Instanz von View-Verbindungsserver 66
 - Konfigurieren eines Kennworts für die Kombination mit einem Sicherheitsserver 73
 - Installieren eines Sicherheitsservers 74
 - Firewall-Regeln für View-Verbindungsserver 81
 - Erneutes Installieren eines View-Verbindungservers mit einer Sicherungskonfiguration 83
 - Befehlszeilenoptionen für Microsoft Windows Installer 84
 - Unbeaufsichtigtes Deinstallieren von View-Komponenten mithilfe von MSI-Befehlszeilenoptionen 87

- 8 Konfigurieren von SSL-Zertifikaten für View Servers 89**
 - Grundlegendes zu SSL-Zertifikaten für View -Server 90
 - Überblick über Aufgaben zur Einrichtung von SSL-Zertifikaten 91
 - Beziehen eines signierten SSL-Zertifikats von einer Zertifizierungsstelle 92
 - Konfigurieren des View-Verbindungservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen SSL-Zertifikats 94
 - Konfigurieren von Client-Endpunkten, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen 100
 - Konfigurieren der Zertifikatsperrüberprüfung für Serverzertifikate 102
 - Konfigurieren des PCoIP Secure Gateway zur Nutzung eines Neuen SSL-Zertifikats 103
 - Konfigurieren von View Administrator, um ein vCenter Server- oder View Composer-Zertifikat als vertrauenswürdig einzustufen 108
 - Vorteile der Verwendung von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden 108
 - Fehlerbehebung bei Problemen mit Zertifikaten auf View-Verbindungsserver und -Sicherheitsservern 109

- 9 Erstmaliges Konfigurieren von View 111**
 - Konfigurieren von Benutzerkonten für vCenter Server und View Composer 111
 - Anfängliches Konfigurieren von View-Verbindungsserver 115
 - Konfigurieren von Horizon Client -Verbindungen 128
 - Ersetzen von Standardports für View-Dienste 136
 - Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung 142

- 10 Konfigurieren der Ereignisberichterstellung 145**
 - Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse 145
 - Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung 146
 - Konfigurieren der Ereignisdatenbank 147
 - Konfigurieren der Ereignisprotokollierung für Syslog-Server 148

Index 151

Installation von View

View-Installation erklärt, wie der VMware Horizon[®] 7-Server und die Client-Komponenten installiert werden.

Zielgruppe

Diese Informationen richten sich an Benutzer, die VMware Horizon 7 installieren möchten. Die bereitgestellten Informationen sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb von Rechenzentren vertraut sind.

Systemanforderungen für Serverkomponenten

1

Hosts, die Horizon 7 Serverkomponenten ausführen, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Horizon-Verbindungsserver – Serveranforderungen“](#), auf Seite 9
- [„View Administrator-Anforderungen“](#), auf Seite 11
- [„View Composer-Anforderungen“](#), auf Seite 12

Horizon-Verbindungsserver – Serveranforderungen

Der Horizon-Verbindungsserver fungiert als Broker für Clientverbindungen, indem eingehende Benutzeranforderungen authentifiziert und an die entsprechenden Remote-Desktops und -anwendungen weitergeleitet werden. Für den Horizon-Verbindungsserver gelten bestimmte Anforderungen in Bezug auf Hardware, Betriebssystem, Installation und unterstützende Software.

- [Hardwareanforderungen für den Horizon-Verbindungsserver](#) auf Seite 10
Sie müssen alle Horizon-Verbindungsserver-Installationstypen, einschließlich Installationen von Standardservern, Replikatservern, Sicherheitsservern und Registrierungsservern, auf einer dedizierten physischen oder virtuellen Maschine installieren, die bestimmte Hardwareanforderungen erfüllt.
- [Unterstützte Betriebssysteme für den Horizon-Verbindungsserver](#) auf Seite 10
Sie müssen den Horizon-Verbindungsserver auf einem unterstützten Windows Server-Betriebssystem installieren.
- [Anforderungen im Hinblick auf die Virtualisierungssoftware für den Horizon-Verbindungsserver](#) auf Seite 10
Für den Horizon-Verbindungsserver werden bestimmte Versionen der VMware-Virtualisierungssoftware benötigt.
- [Netzwerkanforderungen für replizierte Horizon-Verbindungsserver-Instanzen](#) auf Seite 11
Wenn Sie replizierte Horizon-Verbindungsserver-Instanzen installieren, müssen Sie die Instanzen normalerweise am selben physischen Standort konfigurieren und über ein Hochleistungs-LAN verbinden. Andernfalls treten möglicherweise lange Wartezeiten auf, die dazu führen können, dass die View LDAP-Konfigurationen auf Horizon-Verbindungsserver-Instanzen inkonsistent werden. Den Benutzern wird möglicherweise der Zugriff verweigert, wenn sie eine Verbindung mit einer Horizon-Verbindungsserver-Instanz herstellen, die eine veraltete Konfiguration verwendet.

Hardwareanforderungen für den Horizon-Verbindungsserver

Sie müssen alle Horizon-Verbindungsserver-Installationstypen, einschließlich Installationen von Standardservern, Replikatservern, Sicherheitsservern und Registrierungsservern, auf einer dedizierten physischen oder virtuellen Maschine installieren, die bestimmte Hardwareanforderungen erfüllt.

Tabelle 1-1. Horizon-Verbindungsserver – Hardwareanforderungen

Hardwarekomponente	Erforderlich	Empfohlen
Prozessor	Pentium IV 2,0-GHz-Prozessor oder höher	4 CPUs
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s	Netzwerkkarten mit 1 Gbit/s
Arbeitsspeicher Windows Server 2008 R2, 64-Bit	4GB RAM oder mehr	Mindestens 10 GB RAM für Bereitstellungen ab 50 Remote-Desktops
Arbeitsspeicher Windows Server 2012 R2 (64 Bit)	4GB RAM oder mehr	Mindestens 10 GB RAM für Bereitstellungen ab 50 Remote-Desktops

Diese Anforderungen gelten auch für Replikat- und Sicherheitsserver-Instanzen des Horizon-Verbindungs-servers, die Sie für einen Hochverfügbarkeit oder für den externen Zugriff installieren.

WICHTIG Der physische Computer oder die virtuelle Maschine, der bzw. die Horizon-Verbindungsserver hostet, muss eine statische IP-Adresse verwenden. In einer IPv4-Umgebung konfigurieren Sie eine statische IP-Adresse. In einer IPv6-Umgebung erhalten Computer automatisch IP-Adressen, die nicht geändert werden.

Unterstützte Betriebssysteme für den Horizon-Verbindungsserver

Sie müssen den Horizon-Verbindungsserver auf einem unterstützten Windows Server-Betriebssystem installieren.

Die folgenden Betriebssysteme unterstützen alle Installationstypen für den Horizon-Verbindungsserver, einschließlich Installationen von Standardservern, Replikatservern und Sicherheitsservern.

Tabelle 1-2. Betriebssystemunterstützung für den Horizon-Verbindungsserver

Betriebssystem	Version	Edition
Windows Server 2008 R2 SP1	64 Bit	Standard Enterprise Datacenter
Windows Server 2012 R2	64 Bit	Standard Datacenter
Windows Server 2016	64 Bit	Standard Datacenter

HINWEIS Windows Server 2008 R2 ohne Service Pack wird nicht mehr unterstützt.

Anforderungen im Hinblick auf die Virtualisierungssoftware für den Horizon-Verbindungsserver

Für den Horizon-Verbindungsserver werden bestimmte Versionen der VMware-Virtualisierungssoftware benötigt.

Bei Verwendung von vSphere müssen Sie eine unterstützte Version von vSphere ESX/ESXi-Hosts und vCenter Server verwenden.

Einzelheiten dazu, welche Versionen von Horizon mit welchen Versionen von vCenter Server und ESXi kompatibel sind, finden Sie in der Interoperabilitätsmatrix für VMware-Produkte unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Netzwerkanforderungen für replizierte Horizon-Verbindungsserver-Instanzen

Wenn Sie replizierte Horizon-Verbindungsserver-Instanzen installieren, müssen Sie die Instanzen normalerweise am selben physischen Standort konfigurieren und über ein Hochleistungs-LAN verbinden. Andernfalls treten möglicherweise lange Wartezeiten auf, die dazu führen können, dass die View LDAP-Konfigurationen auf Horizon-Verbindungsserver-Instanzen inkonsistent werden. Den Benutzern wird möglicherweise der Zugriff verweigert, wenn sie eine Verbindung mit einer Horizon-Verbindungsserver-Instanz herstellen, die eine veraltete Konfiguration verwendet.

WICHTIG Zur Verwendung einer Gruppe replizierter Verbindungsserver-Instanzen in einem WAN, MAN (Metropolitan Area Network) oder einem anderen Netzwerk, das kein LAN ist, in einer Situation, in der die Horizon-Bereitstellung sich über mehrere Datacenter erstrecken muss, müssen Sie die Cloud-Pod-Architektur-Funktion verwenden. Sie können 25 Pods verbinden, um eine große Umgebung für das Brokering und die Verwaltung von Desktops in fünf Sites bereitzustellen, die sich an unterschiedlichen geografischen Standorten befinden. Auf diese Weise lassen sich Desktops und Anwendungen für bis zu 50.000 Sitzungen zur Verfügung stellen. Weitere Informationen finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

View Administrator-Anforderungen

Administratoren verwenden View Administrator zum Konfigurieren von View-Verbindungsservern, zum Bereitstellen und Verwalten von Remote-Desktops und -anwendungen, zum Steuern der Benutzerauthentifizierung, zum Initiieren und Untersuchen von Systemereignissen sowie zum Durchführen von Analysen. Clientsysteme müssen bestimmte Anforderungen erfüllen, um View Administrator auszuführen.

View Administrator ist eine webbasierte Anwendung, die zusammen mit View-Verbindungsserver installiert wird. Sie können für den Zugriff auf und die Verwendung von View Administrator die folgenden Webbrowser verwenden:

- Internet Explorer 9 (nicht empfohlen)
- Internet Explorer 10
- Internet Explorer 11
- Firefox (letzte unterstützte Versionen)
- Chrome (letzte unterstützte Versionen)
- Safari 6 und höher
- Microsoft Edge (Windows 10)

Zur Verwendung von View Administrator mit Ihrem Webbrowser müssen Sie Adobe Flash Player 10.1 oder höher installieren. Ihr Clientsystem muss Zugriff auf das Internet haben, damit Adobe Flash Player installiert werden kann.

Der Computer, auf dem Sie View Administrator starten, muss die Stamm- und Zwischenzertifikate des Servers, auf dem der View-Verbindungsserver gehostet wird, als vertrauenswürdig einstufen. Die unterstützten Browser enthalten bereits Zertifikate für alle bekannten Zertifizierungsstellen. Wenn Ihre Zertifikate von einer Zertifizierungsstelle stammen, die nicht gut bekannt ist, folgen Sie den Anleitungen in „[Konfigurieren von Client-Endpunkten, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen](#)“, auf Seite 100.

Für eine ordnungsgemäße Textanzeige in View Administrator sind Microsoft-spezifische Schriftarten erforderlich. Wenn Ihr Webbrowser auf einem anderen Betriebssystem als Windows, wie beispielsweise Linux, UNIX oder Mac ausgeführt wird, müssen Sie sicherstellen, dass Microsoft-spezifische Schriftarten auf Ihrem Computer installiert sind.

Derzeit werden auf der Microsoft-Website keine Microsoft-Schriftarten bereitgestellt, Sie können die Schriftarten jedoch von unabhängigen Websites herunterladen.

View Composer-Anforderungen

Mithilfe von View Composer können Sie mehrere Linked-Clone-Desktops aus einem einzelnen zentralen Basis-Image bereitstellen. Für View Composer gelten bestimmte Installations- und Speicheranforderungen.

- [Unterstützte Betriebssysteme für View Composer](#) auf Seite 12
View Composer unterstützt 64 Bit-Betriebssysteme mit spezifischen Anforderungen und Einschränkungen. Sie können View Composer auf demselben physischen Computer oder derselben virtuellen Maschine wie vCenter Server oder auf einem separaten Server installieren.
- [Hardwareanforderungen für eigenständigen View Composer](#) auf Seite 13
Wenn Sie View Composer nicht auf dem physischen Computer oder der virtuellen Maschine installieren, der/die für vCenter Server verwendet wird, müssen Sie eine dedizierte Maschine verwenden, die spezifische Hardwareanforderungen erfüllt.
- [Datenbankanforderungen für View Composer und die Ereignisdatenbank](#) auf Seite 13
Für View Composer ist eine SQL-Datenbank zum Speichern von Daten erforderlich. Die View Composer-Datenbank muss sich auf dem View Composer Server-Host befinden oder für ihn verfügbar sein. Sie können optional eine Ereignisdatenbank einrichten, mit der sich Informationen vom View-Verbindungsserver zu View-Ereignissen erfassen lassen.

Unterstützte Betriebssysteme für View Composer

View Composer unterstützt 64 Bit-Betriebssysteme mit spezifischen Anforderungen und Einschränkungen. Sie können View Composer auf demselben physischen Computer oder derselben virtuellen Maschine wie vCenter Server oder auf einem separaten Server installieren.

Tabelle 1-3. Betriebssystemunterstützung für View Composer

Betriebssystem	Version	Edition
Windows Server 2008 R2 SP1	64 Bit	Standard Enterprise Datacenter
Windows Server 2012 R2	64 Bit	Standard Datacenter
Windows Server 2016	64 Bit	Standard Datacenter

HINWEIS Windows Server 2008 R2 ohne Service Pack wird nicht mehr unterstützt.

Wenn Sie View Composer und vCenter Server nicht auf demselben physischen Computer oder derselben virtuellen Maschine installieren möchten, lesen Sie „[Hardwareanforderungen für eigenständigen View Composer](#)“, auf Seite 13.

Hardwareanforderungen für eigenständigen View Composer

Wenn Sie View Composer nicht auf dem physischen Computer oder der virtuellen Maschine installieren, der/die für vCenter Server verwendet wird, müssen Sie eine dedizierte Maschine verwenden, die spezifische Hardwareanforderungen erfüllt.

Eine eigenständige View Composer-Installation funktioniert mit vCenter Server auf einem separaten Windows Server-Computer oder mit der Linux-basierten vCenter Server-Appliance. VMware empfiehlt eine 1:1-Zuordnung zwischen jedem View Composer-Dienst und jeder vCenter Server-Instanz.

Tabelle 1-4. Hardwareanforderungen für View Composer

Hardwarekomponente	Erforderlich	Empfohlen
Prozessor	Intel 64- oder AMD 64-Prozessor, 1,4 GHz oder schneller, mit 2 CPUs	2 GHz oder schneller und 4 CPUs
Netzwerk	Mindestens eine Netzwerkkarte mit 10/100 Mbit/s	Netzwerkkarten mit 1 Gbit/s
Arbeitsspeicher	4GB RAM oder mehr	8 GB RAM oder mehr für Bereitstellungen von mindestens 50 Remote-Desktops
Speicherplatz	40 GB	60 GB

WICHTIG Der physische Computer oder die virtuelle Maschine, der bzw. die View Composer hostet, muss eine statische IP-Adresse verwenden. In einer IPv4-Umgebung konfigurieren Sie eine statische IP-Adresse. In einer IPv6-Umgebung erhalten Computer automatisch IP-Adressen, die nicht geändert werden.

Datenbankanforderungen für View Composer und die Ereignisdatenbank

Für View Composer ist eine SQL-Datenbank zum Speichern von Daten erforderlich. Die View Composer-Datenbank muss sich auf dem View Composer Server-Host befinden oder für ihn verfügbar sein. Sie können optional eine Ereignisdatenbank einrichten, mit der sich Informationen vom View-Verbindungsserver zu View-Ereignissen erfassen lassen.

Wenn bereits eine Datenbankserver-Instanz für vCenter Server vorhanden ist, kann View Composer diese vorhandene Instanz nutzen, wenn es sich um eine der in [Tabelle 1-5](#) genannten Versionen handelt. Beispielsweise kann View Composer die im Lieferumfang von vCenter Server enthaltene Microsoft SQL Server-Instanz verwenden. Wenn noch keine Datenbankserver-Instanz vorhanden ist, müssen Sie eine solche installieren.

View Composer unterstützt eine Teilmenge der von vCenter Server unterstützten Datenbankserver. Wenn Sie vCenter Server bereits mit einem Datenbankserver verwenden, der nicht von View Composer unterstützt wird, verwenden Sie diesen Datenbankserver weiterhin für vCenter Server und installieren Sie einen separaten Datenbankserver für View Composer.

WICHTIG Wenn Sie die View Composer-Datenbank auf derselben SQL Server-Instanz erstellen wie für vCenter Server, achten Sie darauf, die vCenter Server-Datenbank nicht zu überschreiben.

Die folgende Tabelle listet die unterstützten Datenbankserver und -versionen auf (Stand Veröffentlichungsdatum dieses Dokuments). Aktuelle Informationen zu unterstützten Datenbanken finden Sie in den VMware Produkt-Interoperabilität-Matrizen unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Nachdem Sie für **Lösung-/Datenbank-Interoperabilität** das Produkt und die Version ausgewählt haben, um für den Schritt „Datenbank hinzufügen“ eine Liste mit allen unterstützten Datenbanken anzuzeigen, wählen Sie **Beliebig** aus und klicken Sie auf **Hinzufügen**.

Tabelle 1-5. Unterstützte Datenbankserver für View Composer und für die Ereignisdatenbank

Datenbank	Service Packs/Versionen	Editionen
Microsoft SQL Server 2014 (32 und 64 Bit)	Kein SP, SP1	Standard Enterprise
Microsoft SQL Server 2012 (32 und 64 Bit)	SP2	Express Standard Enterprise
Microsoft SQL Server 2008 R2 (32 und 64 Bit)	SP2, SP3	Express Standard Enterprise Datacenter
Oracle 12c	Version 1 (jede Version bis 12.1.0.2)	Standard One Standard Enterprise

HINWEIS Die folgenden Versionen werden nicht mehr unterstützt: Microsoft SQL Server 2008 SP4 und Oracle 11g Release 2 (11.2.0.04).

Systemanforderungen für Gastbetriebssysteme

2

Systeme, auf denen Horizon Agent oder die eigenständige View Persona Management-Software ausgeführt wird, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Dieses Kapitel behandelt die folgenden Themen:

- „[Unterstützte Betriebssysteme für Horizon Agent](#)“, auf Seite 15
- „[Unterstützte Betriebssysteme für die eigenständige Horizon Persona Management-Software](#)“, auf Seite 16
- „[Unterstützung für Remote-Anzeigeprotokoll und -Software](#)“, auf Seite 16

Unterstützte Betriebssysteme für Horizon Agent

Die Horizon Agent-Komponente (in früheren Versionen als View Agent bezeichnet) bietet eine Sitzungsverwaltung, eine einmalige Anmeldung (Single Sign-On), eine Geräteumleitung und andere Funktionen. Sie müssen Horizon Agent auf allen virtuellen Maschinen, physischen Systemen und RDS-Hosts installieren.

Diese Betriebssysteme werden zum Zeitpunkt der Veröffentlichung dieser Dokumentation vollständig unterstützt.

Die Arten und Editionen der unterstützten Gastbetriebssysteme richten sich nach der Windows-Version. Eine aktualisierte Liste unterstützter Windows 10-Betriebssysteme finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2149393>. Zu anderen Windows-Betriebssystemen als Windows 10 finden Sie Informationen im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150295>.

Eine Liste der speziellen Funktionen für die Remoteerfahrung, die auf Windows-Betriebssystemen unterstützt werden, auf denen Horizon Agent installiert ist, erhalten Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150305>.

Für eine erweiterte Sicherheit empfiehlt VMware die Konfiguration von Verschlüsselungssammlungen, um bekannte Sicherheitslücken zu schließen. Anweisungen zur Einrichtung einer Domänenrichtlinie für Verschlüsselungssammlungen für Windows-Maschinen, auf denen View Composer oder Horizon Agent ausgeführt wird, finden Sie im Thema zur Deaktivierung schwacher Verschlüsselungen für View Composer oder Horizon Agent im Dokument „Installation von View“.

Um die Setup-Option „View Persona Management“ mit Horizon Agent verwenden zu können, muss Horizon Agent auf virtuellen Maschinen mit Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2 oder Windows Server 2016 installiert werden. Diese Option funktioniert nicht auf physischen Computern oder RDS-Hosts.

Sie können die eigenständige Version der View Persona Management-Software auf physischen Computern installieren. Siehe „[Unterstützte Betriebssysteme für die eigenständige Horizon Persona Management-Software](#)“, auf Seite 16.

HINWEIS Für die Anwendung des VMware Blast-Anzeigeprotokolls müssen Sie Horizon Agent auf einer virtuellen Einzelsitzungsmaschine oder auf einem RDS-Host installieren. Der RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein. Das VMware Blast-Anzeigeprotokoll kann nicht auf einem physischen Einzelbenutzercomputer verwendet werden.

Für eine erweiterte Sicherheit empfiehlt VMware die Konfiguration von Verschlüsselungssammlungen, um bekannte Sicherheitslücken zu schließen. Erläuterungen zur Einrichtung einer Domänenrichtlinie für Verschlüsselungssammlungen für Windows-Maschinen, auf denen View Composer oder Horizon Agent ausgeführt wird, finden Sie unter „[Deaktivieren von schwachen Verschlüsselungen in SSL/TLS](#)“, auf Seite 41.

Unterstützte Betriebssysteme für die eigenständige Horizon Persona Management-Software

Die eigenständige Horizon Persona Management-Software ermöglicht eine Persona-Verwaltung für eigenständige physische Computer und virtuelle Maschinen, auf denen Horizon Agent nicht installiert ist. Bei der Anmeldung werden die Profile der Benutzer dynamisch aus einem Remote-Profil-Repository auf ihre eigenständigen Systeme heruntergeladen.

HINWEIS Zur Konfiguration der Persona-Verwaltung für Horizon-Desktops installieren Sie Horizon Agent mit der Setup-Option **Persona-Verwaltung**. Die eigenständige Persona-Verwaltungssoftware ist ausschließlich für Nicht-Horizon-Systeme konzipiert.

Eine Liste der für die eigenständige Horizon Persona Management-Software unterstützten Betriebssysteme finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2150295>.

Für die Microsoft-Remotedesktopdienste wird die eigenständige Persona-Verwaltungssoftware nicht unterstützt.

Unterstützung für Remote-Anzeigeprotokoll und -Software

Remote-Anzeigeprotokolle und -Software bieten Zugriff auf Remote-Desktops und -anwendungen. Das verwendete Remote-Anzeigeprotokoll richtet sich nach verschiedenen Faktoren: dem Typ des Clientgeräts, ob Sie eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung herstellen und wie der Administrator den Desktop- oder Anwendungspool konfiguriert.

- **PCoIP** auf Seite 17

PCoIP (PC over IP) ermöglicht ein optimiertes Desktoperlebnis bei der Bereitstellung einer Remoteanwendung oder einer gesamten Desktopumgebung, einschließlich der Anwendungen, Bilder und Audio- und Videoinhalte, für eine Vielzahl von Benutzern im LAN oder über das WAN. PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

- **Microsoft RDP** auf Seite 19

Remote Desktop Protocol (RDP) entspricht dem Mehrkanalprotokoll, das viele Benutzer bereits nutzen, um vom ihrem Heimcomputer aus auf ihren Firmencomputer zuzugreifen. Microsoft Remote-Desktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP.

- [VMware Blast Extreme](#) auf Seite 19

VMware Blast Extreme ist für die mobile Cloud optimiert und unterstützt das breiteste Spektrum an H.264-fähigen Clientgeräten. Unter den Anzeigeprotokollen bietet VMware Blast den niedrigsten CPU-Verbrauch und die längste Akkunutzungsdauer für mobile Geräte. VMware Blast Extreme kann eine Zunahme der Latenz oder eine Verringerung der Bandbreite kompensieren und sowohl TCP als auch UDP als Netzwerktransportprotokoll verwenden.

PCoIP

PCoIP (PC over IP) ermöglicht ein optimiertes Desktoperlebnis bei der Bereitstellung einer Remoteanwendung oder einer gesamten Desktopumgebung, einschließlich der Anwendungen, Bilder und Audio- und Videoinhalte, für eine Vielzahl von Benutzern im LAN oder über das WAN. PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

Das PCoIP-Anzeigeprotokoll kann für Remoteanwendungen und für Remote-Desktops, die virtuelle Maschinen verwenden, physische Computer, die Teradici-Hostkarten verwenden, oder Desktops mit freigegebenen Sitzungen auf einem RDS-Host verwendet werden.

PCoIP-Funktionen

Zu den wichtigsten Funktionen von PCoIP zählen:

- Benutzer außerhalb der Unternehmensfirewall können dieses Protokoll mit dem Virtual Private Network (VPN) Ihrer Firma verwenden, oder Benutzer können sichere, verschlüsselte Verbindungen mit einem Sicherheitsserver oder mit einer Access Point-Appliance in der Unternehmens-DMZ herstellen.
- AES (Advanced Encryption Standard) 128 Bit-Verschlüsselung wird unterstützt und ist standardmäßig aktiviert. Sie können die Verschlüsselungsmethode jedoch auf AES-256 ändern.
- Verbindungen mit Windows-Desktops mit den in „[Unterstützte Betriebssysteme für Horizon Agent](#)“, auf Seite 15 aufgeführten Horizon Agent-Betriebssystemversionen werden unterstützt.
- Verbindungen von allen Arten von Clientgeräten.
- Optimierungssteuerungen zur Reduzierung der Bandbreitennutzung im LAN und WAN.
- Unterstützung von 32 Bit-Farben für virtuelle Anzeigeegeräte.
- ClearType-Schriftarten werden unterstützt.
- Audioumleitung mit dynamischer Anpassung der Audioqualität für LAN und WAN.
- Echtzeit-Audio-Video für die Verwendung von Webcams und Mikrofonen auf einigen Clienttypen.
- Kopieren und Einfügen von Text und auf einigen Clients von Bildern zwischen dem Client-Betriebssystem und einer Remoteanwendung oder einem Remote-Desktop. Bei anderen Clienttypen wird nur das Kopieren und Einfügen von Klartext unterstützt. Sie können jedoch keine Systemobjekte wie Ordner und Dateien zwischen den Systemen kopieren und einfügen.
- Mehrere Monitore werden für einige Client-Typen unterstützt. Auf einigen Clients können Sie bis zu vier Monitore mit einer Auflösung bis zu 2560 x 1600 pro Anzeige oder bis zu drei Monitore mit einer Auflösung von 4K (3840 x 2160) für Windows 7-Remote-Desktops mit deaktiviertem Aero verwenden. Drehung des Monitors (Pivot-Funktion) und automatische Anpassung werden ebenfalls unterstützt.
Wenn die 3D-Funktion aktiviert ist, werden bis zu zwei Monitore mit einer Auflösung bis zu 1920 x 1200 oder ein Monitor mit einer Auflösung von 4K (3840 x 2160) unterstützt.
- USB-Umleitung wird für einige Client-Typen unterstützt.
- MMR-Umleitung wird für einige Windows-Clientbetriebssysteme und einige Remote-Desktop-Betriebssysteme (mit installiertem Horizon Agent) unterstützt.

Informationen darüber, welche Desktop-Betriebssysteme bestimmte PCoIP-Funktionen unterstützen, finden Sie in der „Funktionsunterstützungs-Matrix für Horizon Agent“ im Dokument *Planung der View-Architektur*.

Informationen darüber, welche Client-Geräte spezifische PCoIP-Funktionen unterstützen, finden Sie unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Empfohlene Einstellungen für das Gastbetriebssystem

1 GB RAM oder mehr und eine Dual-CPU wird für die Wiedergabe in High-Definition, Vollbildmodus oder 720p oder höher Video empfohlen. Für die Verwendung von vDGA (Virtual Dedicated Graphics Acceleration, virtuelle zugeordnete Grafikkbeschleunigung) für grafikintensive Anwendungen wie CAD-Anwendungen sind 4 GB RAM erforderlich.

Videoqualitätsanforderungen

480p-formatiertes Video Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über eine virtuelle CPU verfügt. Wenn Sie eine Videowiedergabe in hochauflösendem Flash- oder im Vollbildmodus wünschen, erfordert der Desktop eine duale virtuelle CPU. Selbst mit einem dualen virtuellen CPU-Desktop kann ein 360p-Video, das im Vollbildmodus abgespielt wird, hinter der Audioausgabe zurückbleiben, insbesondere auf Windows-Clients.

720p-formatiertes Video Die Videowiedergabe mit 720p bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über zwei virtuelle CPUs verfügt. Bei der 720p-Videowiedergabe in hoch auflösendem oder Vollbildmodus könnte die Leistung beeinträchtigt sein.

1080p-formatiertes Video Wenn der Remote-Desktop über zwei virtuelle CPUs verfügt, können Sie 1080p-formatiertes Video wiedergeben, wobei der Media Player allerdings möglicherweise auf eine kleinere Fenstergröße angepasst werden muss.

3D-Rendering Sie können Remote-Desktops für die Verwendung von software- oder hardwarebeschleunigter Grafik konfigurieren. Die softwarebeschleunigte Grafikfunktion ermöglicht es Ihnen, ohne eine physische GPU (Grafikverarbeitungseinheit) DirectX 9- und OpenGL 2.1-Anwendungen auszuführen. Die hardwarebeschleunigten Grafikfunktionen ermöglicht es virtuellen Maschinen, die physischen GPU (Grafikverarbeitungseinheit) auf einem vSphere-Host freizugeben oder eine physische GPU für einen VM-Desktop zu reservieren.

Für 3D-Anwendungen werden bis zu zwei Monitore unterstützt, und die maximale Bildschirmauflösung beträgt 1920 x 1200. Das Gastbetriebssystem auf den Remote-Desktops muss Windows 7 oder höher sein.

Hardwareanforderungen für Clientsysteme

Informationen über Prozessor- und Speicheranforderungen für die spezifische Art von Desktop oder mobilen Clientgeräten finden Sie im Dokument „Verwenden von VMware Horizon Client“. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Microsoft RDP

Remote Desktop Protocol (RDP) entspricht dem Mehrkanalprotokoll, das viele Benutzer bereits nutzen, um vom ihrem Heimcomputer aus auf ihren Firmencomputer zuzugreifen. Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP.

Microsoft RDP ist ein unterstütztes Anzeigeprotokoll für Remote-Desktops, die virtuelle Maschinen, physische Maschinen oder Desktops mit gemeinsamen Sitzungen auf einem RDS-Host verwenden. (Für Remoteanwendungen werden nur das PCoIP-Anzeigeprotokoll und das VMware Blast-Anzeigeprotokoll unterstützt.) Microsoft RDP ermöglicht Folgendes:

- RDP 7 lässt eine echte Mehrfachmonitorunterstützung für bis zu 16 Monitore zu.
- Texte und Systemobjekte wie Ordner und Dateien können zwischen dem lokalen System und dem Remote-Desktop kopiert und eingefügt werden.
- Unterstützung von 32 Bit-Farben für virtuelle Anzeigeräte.
- RDP unterstützt die 128 Bit-Verschlüsselung.
- Benutzer außerhalb der Unternehmens-Firewall können dieses Protokoll mit dem Virtual Private Network (VPN) Ihrer Firma benutzen, oder Benutzer können sichere, verschlüsselte Verbindungen zu einem View-Sicherheitsserver in der Unternehmens-DMZ herstellen.

Sie müssen den Hotfix KB3080079 von Microsoft anwenden, damit TLSv1.1- und TLSv1.2-Verbindungen mit Windows 7 und Windows Server 2008 R2 unterstützt werden.

Hardwareanforderungen für Clientsysteme

Informationen zu Prozessor- und Arbeitsspeichieranforderungen finden Sie im Dokument „Verwendung von VMware Horizon Client“ für den jeweiligen Typ des Clientsystems. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

HINWEIS Mobile 3.x-Clientgeräte verwenden ausschließlich das PCoIP-Anzeigeprotokoll. Mobile 4.x-Clients verwenden nur das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll.

VMware Blast Extreme

VMware Blast Extreme ist für die mobile Cloud optimiert und unterstützt das breiteste Spektrum an H.264-fähigen Clientgeräten. Unter den Anzeigeprotokollen bietet VMware Blast den niedrigsten CPU-Verbrauch und die längste Akkumutzungsdauer für mobile Geräte. VMware Blast Extreme kann eine Zunahme der Latenz oder eine Verringerung der Bandbreite kompensieren und sowohl TCP als auch UDP als Netzwerktransportprotokoll verwenden.

Das VMware Blast-Anzeigeprotokoll kann für Remoteanwendungen und Remote-Desktops, die virtuelle Maschinen oder gemeinsame Sitzungen über RDS-Hosts verwenden, genutzt werden. Der RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein. Das VMware Blast-Anzeigeprotokoll kann nicht auf einem physischen Einzelbenutzercomputer verwendet werden.

Funktionen von VMware Blast Extreme

Zu den wichtigsten Funktionen von VMware Blast Extreme zählen:

- Benutzer außerhalb der Unternehmensfirewall können dieses Protokoll mit dem Virtual Private Network (VPN) des Unternehmens verwenden, oder Benutzer können sichere, verschlüsselte Verbindungen mit einem Sicherheitsserver oder mit einer Access Point-Appliance in der Unternehmens-DMZ herstellen.
- AES (Advanced Encryption Standard) 128 Bit-Verschlüsselung wird unterstützt und ist standardmäßig aktiviert. Sie können die Verschlüsselungsmethode jedoch auf AES-256 ändern.

- Verbindungen mit Windows-Desktops mit den in „[Unterstützte Betriebssysteme für Horizon Agent](#)“, auf Seite 15 aufgeführten Horizon Agent-Betriebssystemversionen werden unterstützt.
- Verbindungen von allen Arten von Clientgeräten.
- Optimierungssteuerungen zur Reduzierung der Bandbreitennutzung im LAN und WAN.
- Unterstützung von 32 Bit-Farben für virtuelle Anzeigegeräte.
- ClearType-Schriftarten werden unterstützt.
- Audioumleitung mit dynamischer Anpassung der Audioqualität für LAN und WAN.
- Echtzeit-Audio-Video für die Verwendung von Webcams und Mikrofonen auf einigen Clienttypen.
- Kopieren und Einfügen von Text und auf einigen Clients von Bildern zwischen dem Client-Betriebssystem und einer Remoteanwendung oder einem Remote-Desktop. Bei anderen Clienttypen wird nur das Kopieren und Einfügen von Klartext unterstützt. Sie können jedoch keine Systemobjekte wie Ordner und Dateien zwischen den Systemen kopieren und einfügen.
- Mehrere Monitore werden für einige Client-Typen unterstützt. Auf einigen Clients können Sie bis zu vier Monitore mit einer Auflösung bis zu 2560 x 1600 pro Anzeige oder bis zu drei Monitore mit einer Auflösung von 4K (3840 x 2160) für Windows 7-Remote-Desktops mit deaktiviertem Aero verwenden. Drehung des Monitors (Pivot-Funktion) und automatische Anpassung werden ebenfalls unterstützt.
Wenn die 3D-Funktion aktiviert ist, werden bis zu zwei Monitore mit einer Auflösung bis zu 1920 x 1200 oder ein Monitor mit einer Auflösung von 4K (3840 x 2160) unterstützt.
- USB-Umleitung wird für einige Client-Typen unterstützt.
- MMR-Umleitung wird für einige Windows-Clientbetriebssysteme und einige Remote-Desktop-Betriebssysteme (mit installiertem Horizon Agent) unterstützt.
- Es werden Verbindungen mit physischen Maschinen, an die kein Monitor angeschlossen ist, mit NVIDIA-Grafikkarten unterstützt. Für eine optimale Leistung verwenden Sie eine Grafikkarte, die die H. 264-Codierung unterstützt. Dies ist eine Tech-Preview-Funktion für Horizon 7 Version 7.1.

Wenn Sie über eine diskrete Add-In-GPU und eine eingebettete GPU verfügen, verwendet das Betriebssystem eventuell standardmäßig die eingebettete GPU. Zur Behebung dieses Problems können Sie das Gerät im Gerätemanager deaktivieren oder entfernen. Wenn das Problem weiterhin auftritt, haben Sie die Möglichkeit, den WDDM-Grafiktreiber für die eingebettete GPU zu installieren oder die eingebettete GPU im System-BIOS zu deaktivieren. Informationen zur Deaktivierung der eingebetteten GPU finden Sie in Ihrer Systemdokumentation.



VORSICHT Durch die Deaktivierung der eingebetteten GPU kann auch eine bestimmte Funktionalität wie der Konsolenzugriff auf das BIOS-Setup oder der NT Boot Loader beeinträchtigt sein.

Informationen darüber, welche Clientgeräte spezifische VMware Blast Extreme-Funktionen unterstützen, finden Sie unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Empfohlene Einstellungen für das Gastbetriebssystem

1 GB RAM oder mehr und eine Dual-CPU wird für die Wiedergabe in High-Definition, Vollbildmodus oder 720p oder höher Video empfohlen. Für die Verwendung von vDGA (Virtual Dedicated Graphics Acceleration, virtuelle zugeordnete Grafikbeschleunigung) für grafikintensive Anwendungen wie CAD-Anwendungen sind 4 GB RAM erforderlich.

Videoqualitätsanforderungen

- 480p-formatiertes Video** Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über eine virtuelle CPU verfügt. Wenn Sie eine Videowiedergabe in hochauflösendem Flash- oder im Vollbildmodus wünschen, erfordert der Desktop eine duale virtuelle CPU. Selbst mit einem dualen virtuellen CPU-Desktop kann ein 360p-Video, das im Vollbildmodus abgespielt wird, hinter der Audioausgabe zurückbleiben, insbesondere auf Windows-Clients.
- 720p-formatiertes Video** Die Videowiedergabe mit 720p bei nativen Auflösungen ist möglich, wenn der Remote-Desktop über zwei virtuelle CPUs verfügt. Bei der 720p-Videowiedergabe in hoch auflösendem oder Vollbildmodus könnte die Leistung beeinträchtigt sein.
- 1080p-formatiertes Video** Wenn der Remote-Desktop über zwei virtuelle CPUs verfügt, können Sie 1080p-formatiertes Video wiedergeben, wobei der Media Player allerdings möglicherweise auf eine kleinere Fenstergröße angepasst werden muss.
- 3D-Rendering** Sie können Remote-Desktops für die Verwendung von software- oder hardwarebeschleunigter Grafik konfigurieren. Die softwarebeschleunigte Grafikfunktion ermöglicht es Ihnen, ohne eine physische GPU (Grafikverarbeitungseinheit) DirectX 9- und OpenGL 2.1-Anwendungen auszuführen. Die hardwarebeschleunigten Grafikfunktionen ermöglichen es virtuellen Maschinen, die physischen GPUs (Grafikverarbeitungseinheiten) auf einem vSphere-Host freizugeben oder eine physische GPU für einen einzelnen virtuellen Desktop zu reservieren.
- Bei 3D-Anwendungen werden bis zu zwei Monitore unterstützt, die maximale Bildschirmauflösung beträgt 1920 x 1200. Das Gastbetriebssystem auf den Remote-Desktops muss Windows 7 oder höher sein.

Hardwareanforderungen für Clientsysteme

Informationen über Prozessor- und Speicheranforderungen für die spezifische Art von Desktop oder mobilen Clientgeräten finden Sie im Dokument „Verwenden von VMware Horizon Client“. Besuchen Sie https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Installieren von View in einer IPv6-Umgebung

3

View unterstützt IPv6 als Alternative zu IPv4. Die Umgebung muss entweder eine reine IPv6- oder eine reine IPv4-Umgebung sein. View unterstützt keine gemischten IPv6- und IPv4-Umgebungen.

Eine IPv6-Umgebung unterstützt nicht alle View-Funktionen, die in einer IPv4-Umgebung unterstützt werden. View unterstützt kein Upgrade von einer IPv4- auf eine IPv6-Umgebung. Außerdem unterstützt View keine Migration zwischen IPv4- und IPv6-Umgebungen.

WICHTIG Um View in einer IPv6-Umgebung auszuführen, müssen Sie beim Installieren aller View-Komponenten IPv6 angeben.

Dieses Kapitel behandelt die folgenden Themen:

- [„Einrichten von View in einer IPv6-Umgebung“](#), auf Seite 23
- [„Unterstützte vSphere-Datenbank- und Active Directory-Versionen in einer IPv6-Umgebung“](#), auf Seite 24
- [„Unterstützte Betriebssysteme für View-Server in einer IPv6-Umgebung“](#), auf Seite 24
- [„Unterstützte Windows-Betriebssysteme für Desktops und RDS-Hosts in einer IPv6-Umgebung“](#), auf Seite 25
- [„Unterstützte Clients in einer IPv6-Umgebung“](#), auf Seite 25
- [„Unterstützte Remote-Protokolle in einer IPv6-Umgebung“](#), auf Seite 25
- [„Unterstützte Authentifizierungstypen in einer IPv6-Umgebung“](#), auf Seite 26
- [„Andere unterstützte Funktionen in einer IPv6-Umgebung“](#), auf Seite 26

Einrichten von View in einer IPv6-Umgebung

Um View in einer IPv6-Umgebung auszuführen, müssen Sie die IPv6-spezifischen Anforderungen und Wahlmöglichkeiten beim Ausführen bestimmter Verwaltungsaufgaben kennen.

Bevor Sie View installieren, müssen Sie über eine funktionierende IPv6-Umgebung verfügen. Die folgenden View-Verwaltungsaufgaben verfügen über IPv6-spezifische Optionen.

- Installieren des View-Verbindungsservers. Siehe [„Installieren von View-Verbindungsserver mit einer neuen Konfiguration“](#), auf Seite 59.
- Installieren des View-Replikatservers. Siehe [„Installieren einer replizierten Instanz von View-Verbindungsserver“](#), auf Seite 66.
- Installieren des View-Sicherheitsservers. Siehe [„Installieren eines Sicherheitsservers“](#), auf Seite 74.
- Konfigurieren der externen PCoIP-URL. Siehe [„Konfigurieren externer URLs für sichere Gateways und Tunnelverbindungen“](#), auf Seite 131.

- Einrichten der externen PCoIP-URL. Siehe „Festlegen der externen URLs für eine View-Verbindungs-server-Instanz“, auf Seite 132.
- Ändern der externen PCoIP-URL. Siehe „Festlegen der externen URLs für eine View-Verbindungs-server-Instanz“, auf Seite 132.
- Installieren von Horizon Agent. Lesen Sie die Themen zur Horizon Agent-Installation im Dokument *Einrichten von Desktop- und Anwendungspools*.
- Installation von Horizon Client für Windows. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows* unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html. Es werden nur Windows-Clients unterstützt.

HINWEIS In View brauchen Sie für die Verwaltungsaufgaben keine IPv6-Adresse einzugeben. In den Fällen, bei denen Sie entweder einen vollqualifizierten Domännennamen (FQDN) oder eine IPv6-Adresse angeben können, wird dringend empfohlen, einen FQDN anzugeben, um potenzielle Fehler zu vermeiden.

Unterstützte vSphere-Datenbank- und Active Directory-Versionen in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View bestimmte vSphere-, Datenbankserver- und Active Directory-Versionen.

Die folgenden vSphere-Versionen werden in einer IPv6-Umgebung unterstützt:

- 6.0
- 5.5 U2

Die folgenden Datenbankserver werden in einer IPv6-Umgebung unterstützt:

Datenbankserver	Version	Edition
SQL Server 2012 SP1	32/64 Bit	Standard, Enterprise
SQL Server 2012 Express	32/64 Bit	Frei
Oracle 11g R2	32/64 Bit	Standard, Standard Edition One, Enterprise

Die folgenden Active Directory-Versionen werden in einer IPv6-Umgebung unterstützt:

- Microsoft Active Directory 2008 R2
- Microsoft Active Directory 2012 R2

Unterstützte Betriebssysteme für View -Server in einer IPv6-Umgebung

In einer IPv6-Umgebung müssen Sie View-Server unter bestimmten Windows Server-Betriebssystemen installieren.

View-Server sind beispielsweise View-Verbindungsserver-Instanzen, Replikatserver, Sicherheitsserver und View Composer-Instanzen.

Betriebssystem	Edition
Windows Server 2008 R2 SP1	Standard, Enterprise
Windows Server 2012 R2	Standard

Unterstützte Windows-Betriebssysteme für Desktops und RDS-Hosts in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View bestimmte Windows-Betriebssysteme für Desktop-Maschinen und RDS-Hosts. RDS-Hosts stellen Benutzern sitzungsbasierte Desktops und Anwendungen bereit.

Die folgenden Windows-Betriebssysteme werden für Desktop-Maschinen unterstützt:

Betriebssystem	Version	Edition
Windows 7 SP1	32/64 Bit	Enterprise, Professional
Windows 8	32/64 Bit	Enterprise, Professional
Windows 8.1	32/64 Bit	Enterprise, Professional
Windows 10	32/64 Bit	Enterprise, Professional
Windows Server 2008 R2 SP1		Datacenter

Die folgenden Windows-Betriebssysteme werden für RDS-Hosts unterstützt:

Betriebssystem	Edition
Windows Server 2008 R2 SP1	Standard, Enterprise, Datacenter
Windows Server 2012 R2	Standard, Datacenter

Unterstützte Clients in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View Clients, die unter bestimmten Desktop-Betriebssystemen ausgeführt werden.

Tabelle 3-1. Unterstützte Windows-Betriebssysteme

Betriebssystem	Version	Edition
Windows 7	32/64 Bit	Home, Professional, Enterprise, Ultimate
Windows 7 SP1	32/64 Bit	Home, Professional, Enterprise, Ultimate
Windows 8	32/64 Bit	Enterprise, Professional
Windows 8.1	32/64 Bit	Enterprise, Professional
Windows 10	32/64 Bit	Enterprise, Professional

Auf iOS-Geräten wird iOS 9.2 oder höher mit Horizon Client 4.1 oder höher unterstützt.

Die folgenden Clienttypen werden nicht unterstützt:

- Clients, die unter Mac, Android, Linux oder Windows Store ausgeführt werden
- iOS 9.1 oder früher
- PCoIP-Zero-Client

Unterstützte Remote-Protokolle in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View bestimmte Remote-Protokolle.

Die folgenden Remote-Protokolle werden unterstützt:

- RDP-
- RDP mit sicheren Tunnels

- PCoIP
- PCoIP über PCoIP Secure Gateway
- VMware Blast
- VMware Blast über Blast Secure Gateway

Unterstützte Authentifizierungstypen in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View bestimmte Authentifizierungstypen.

Die folgenden Authentifizierungstypen werden unterstützt:

- Kennwortauthentifizierung über Active Directory
- Smartcard
- Single Sign On

Die folgenden Authentifizierungstypen werden nicht unterstützt:

- SecurID
- RADIUS
- SAML

Andere unterstützte Funktionen in einer IPv6-Umgebung

In einer IPv6-Umgebung unterstützt View bestimmte Funktionen, die in den vorherigen Themen nicht behandelt werden.

Die folgenden Funktionen werden unterstützt:

- Anwendungspools
- Audio-Ausgabe
- Automatisierte Desktop-Pools mit vollständigen virtuellen Maschinen oder mit View Composer-Linked-Clones

HINWEIS Automatisierte Desktop-Pools mit Instant Clones werden nicht unterstützt.

- Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP)
- Rückgewinnung von Festplattenspeicherplatz
- Ereignisse
- LDAP-Sicherung
- Manuelle Desktop-Pools, einschließlich vCenter Server-VMs, physischer Computer und virtueller Maschinen, die nicht von vCenter Server verwaltet werden
- Systemeigene NFS-Snapshots (VAAI)
- PCoIP
- PCoIP-Smartcard
- Persona-Verwaltung
- PSG
- RDS-Desktop-Pools

- RDS-Host-3D
- Rollenbasierte Verwaltung
- Single Sign-On, einschließlich der Funktion Als aktueller Benutzer anmelden
- Systemzustand-Dashboard
- ThinApp
- Unity Touch
- USB
- USB-Umleitung
- View Composer Agent
- View-Speicherbeschleunigung
- View Composer-Datenbanksicherung
- Virtuelles Drucken
- VMware Audio
- VMware Video

Die folgenden Funktionen werden nicht unterstützt:

- Blast UDP
- Clientlaufwerksumleitung
- Client IP-Transparenz (nur 64 Bit)
- Cloud-Pod-Architektur
- Flash URL-Umleitung
- HTML-Zugriff
- Log Insight
- Lync
- Multimedia-Umleitung (MMR)
- Echtzeit-Audio/Video (RTAV)
- Scannerumleitung
- Umleitung serieller Ports
- Syslog
- Teradici TERA-Hostkarte
- TSMMR
- Virtual SAN
- Virtuelle Volumes
- vRealize Operations Desktop Agent

Installieren von View im FIPS-Modus

Mit View können Sie Verschlüsselungsvorgänge mithilfe von FIPS-Algorithmen (Federal Information Processing Standard, Bundesstandard für Informationsverarbeitung) durchführen, die mit 140-2 übereinstimmen. Zur Aktivierung dieser Algorithmen installieren Sie View im FIPS-Modus.

Allerdings werden im FIPS-Modus nicht alle View-Funktionen unterstützt. Darüber hinaus unterstützt View kein Upgrade einer Nicht-FIPS-Installation auf eine FIPS-Installation.

HINWEIS Um sicherzustellen, dass View im FIPS-Modus ausgeführt wird, müssen Sie FIPS bei der Installation aller View-Komponenten aktivieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Überblick über die Einrichtung von View im FIPS-Modus“, auf Seite 29
- „Systemanforderungen für den FIPS-Modus“, auf Seite 30

Überblick über die Einrichtung von View im FIPS-Modus

Um View im FIPS-Modus einzurichten, müssen Sie zuerst den FIPS-Modus in der Windows-Umgebung aktivieren. Anschließend installieren Sie alle View-Komponenten im FIPS-Modus.

Die Option zur Installation von View im FIPS-Modus ist nur verfügbar, wenn der FIPS-Modus in der Windows-Umgebung aktiviert wurde. Weitere Informationen zur Aktivierung des FIPS-Modus in Windows finden Sie unter <https://support.microsoft.com/en-us/kb/811833>.

HINWEIS In View Administrator wird nicht angezeigt, ob View im FIPS-Modus ausgeführt wird.

Um View im FIPS-Modus zu installieren, führen Sie die folgenden Administratortasks von View durch.

- Bei der Installation des View-Verbindungsservers wählen Sie die Option für den FIPS-Modus aus. Siehe „[Installieren von View-Verbindungsserver mit einer neuen Konfiguration](#)“, auf Seite 59.
- Bei der Installation des View-Replikatservers wählen Sie die Option für den FIPS-Modus aus. Siehe „[Installieren einer replizierten Instanz von View-Verbindungsserver](#)“, auf Seite 66.
- Vor der Installation eines Sicherheitsservers heben Sie die globale Einstellung **IPSec für Sicherheitsserververbindungen verwenden** in View Administrator auf und konfigurieren IPSec manuell. Siehe <http://kb.vmware.com/kb/2000175>.
- Bei der Installation des View-Sicherheitsservers wählen Sie die Option für den FIPS-Modus aus. Siehe „[Installieren eines Sicherheitsservers](#)“, auf Seite 74.
- Deaktivieren Sie die schwachen Verschlüsselungen für View Composer and View Agent-Maschinen. Siehe „[Deaktivieren von schwachen Verschlüsselungen in SSL/TLS](#)“, auf Seite 41.

- Bei der Installation von View Composer wählen Sie die Option für den FIPS-Modus aus. Siehe [Kapitel 6, „Installieren von View Composer“](#), auf Seite 43.
- Bei der Installation von View Agent wählen Sie die Option für den FIPS-Modus aus. Lesen Sie die Themen zur View Agent-Installation im Dokument *Einrichten von Desktop- und Anwendungspools*.
- Bei der Installation von Horizon Client für Windows wählen Sie die Option für den FIPS-Modus aus. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows* unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html. Es werden nur Windows-Clients unterstützt.

Systemanforderungen für den FIPS-Modus

Zur Unterstützung des FIPS-Modus muss Ihre View-Bereitstellung die nachfolgend aufgeführten Anforderungen erfüllen.

vSphere

- vCenter Server 6.0 oder höher
- ESXi 6.0 oder höher

View-Desktop

- Windows 7 SP1 (32 oder 64 Bit)
- View Agent 6.2 oder höher

Horizon Client

- Windows 7 SP1 (32 oder 64 Bit)
- Horizon Client für Windows 3.5 oder höher
- Horizon Client für Linux 4.0 oder höher

Kryptografisches Protokoll

- TLSv1.2

Vorbereiten von Active Directory

View nutzt die vorhandene Microsoft Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Zur Vorbereitung von Active Directory auf die Verwendung mit View müssen verschiedene Aufgaben ausgeführt werden.

View unterstützt folgende Domänenfunktionsebenen von Active Directory-Domänendiensten (AD DS):

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Dieses Kapitel behandelt die folgenden Themen:

- [„Konfigurieren von Domänen und Vertrauensbeziehungen“](#), auf Seite 32
- [„Erstellen einer OU für Remote-Desktops“](#), auf Seite 33
- [„Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus“](#), auf Seite 33
- [„Erstellen von Gruppen für Benutzer“](#), auf Seite 34
- [„Erstellen eines Benutzerkontos für vCenter Server“](#), auf Seite 34
- [„Erstellen eines Benutzerkontos für einen eigenständigen View Composer Server“](#), auf Seite 34
- [„Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge“](#), auf Seite 34
- [„Erstellen eines Benutzerkontos für Instant Clone-Vorgänge“](#), auf Seite 35
- [„Konfigurieren der Richtlinie „Eingeschränkte Gruppen““](#), auf Seite 36
- [„Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für Horizon 7“](#), auf Seite 37
- [„Vorbereiten von Active Directory für die Smartcard-Authentifizierung“](#), auf Seite 37
- [„Deaktivieren von schwachen Verschlüsselungen in SSL/TLS“](#), auf Seite 41

Konfigurieren von Domänen und Vertrauensbeziehungen

Sie müssen jeden View-Verbindungsserver-Host zu einer Active Directory-Domäne hinzufügen. Bei dem Host darf es sich nicht um einen Domänencontroller handeln.

Active Directory verwaltet auch die Horizon Agent-Computer, inklusive Einzelbenutzercomputer und RDS-Hosts, sowie die Benutzer und Gruppen in Ihrer Horizon 7-Bereitstellung. Sie können Benutzern und Gruppen Berechtigungen für Remote-Desktops und -anwendungen erteilen und Sie haben die Möglichkeit, Benutzer und Gruppen in View Administrator als Administratoren auszuwählen.

Horizon Agent-Computer, View Composer-Server und Benutzer sowie Gruppen lassen sich in den folgenden Active Directory-Domänen platzieren:

- Domäne des View-Verbindungsservers
- Eine unterschiedliche Domäne mit einer Zwei-Wege-Vertrauensbeziehung mit der Domäne des View-Verbindungsservers
- Eine Domäne in einer anderen Gesamtstruktur als die Domäne des View-Verbindungsservers, die von der Domäne des View-Verbindungsservers in einer externen oder Bereichs-Ein-Weg-Vertrauensbeziehung als vertrauenswürdig eingestuft wird.
- Eine Domäne in einer anderen Gesamtstruktur als die Domäne des View-Verbindungsservers, die von der Domäne des View-Verbindungsservers in einer transitiven Ein-Weg- oder Zwei-Wege-Gesamtstruktur-Vertrauensbeziehung als vertrauenswürdig eingestuft wird.

Benutzer werden mithilfe von Active Directory für die Domäne des View-Verbindungsservers und eine beliebige Anzahl zusätzlicher Benutzerdomänen authentifiziert, mit denen eine Vertrauensstellung besteht.

Wenn Ihre Benutzer und Gruppen sich in Domänen mit einer Ein-Weg-Vertrauensstellung befinden, müssen Sie in View Administrator für die Administrationsbenutzer sekundäre Anmeldeinformationen zur Verfügung stellen. Administratoren müssen für den Zugriff auf Domänen mit einer Ein-Weg-Vertrauensstellung über sekundäre Anmeldeinformationen verfügen. Bei Domänen mit einer Ein-Weg-Vertrauensstellung kann es sich um eine externe Domäne oder um eine Domäne in einer transitiven Gesamtstruktur-Vertrauensstellung handeln.

Sekundäre Anmeldeinformationen sind nur für View-Administrator-Sitzungen erforderlich und nicht für Desktop- und Anwendungssitzungen von Endbenutzern. Nur Administrationsbenutzer benötigen sekundäre Anmeldeinformationen.

Sie können die sekundären Anmeldeinformationen mithilfe des Befehls `vdmadmin -T` zur Verfügung stellen.

- Sekundäre Anmeldeinformationen werden für einzelne Administrationsbenutzer konfiguriert.
- Für eine Gesamtstruktur-Vertrauensstellung können Sie sekundäre Anmeldeinformationen für die Gesamtstruktur-Stammdomäne konfigurieren. Der View-Verbindungsserver hat dann die Möglichkeit, die untergeordneten Domänen in der Gesamtstruktur-Vertrauensstellung einzeln zu benennen.

Erläuterungen dazu finden Sie unter „Bereitstellen sekundärer Anmeldeinformationen mithilfe der -T-Option“ im *Administration von View*-Dokument.

HINWEIS Da Sicherheitsserver nicht auf Authentifizierungs-Repositorys (einschließlich Active Directory) zugreifen, müssen sie sich nicht in einer Active Directory-Domäne befinden.

Vertrauensbeziehungen und Domänenfilterung

Um zu ermitteln, auf welche Domänen zugegriffen werden kann, durchläuft eine View-Verbindungsserver-Instanz – beginnend bei der eigenen Domäne – die vorhandenen Vertrauensbeziehungen.

Bei einer kleinen, gut verbundenen Gruppe von Domänen kann View-Verbindungsserver umgehend eine vollständige Liste der Domänen abrufen. Die zum Erstellen der Liste benötigte Zeit steigt jedoch mit zunehmender Anzahl an Domänen oder bei einer weniger guten Verbindung zwischen den Domänen an. Die Liste kann auch Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sie sich mit ihren Remote-Desktops und -Anwendungen verbinden.

Über den Befehl `vdadmin` können Sie eine Domänenfilterung konfigurieren, um die von einer View-Verbindungsserver-Instanz durchsuchten und dem Benutzer angezeigten Domänen einzuschränken. Weitere Informationen finden Sie im Dokument *ViewVerwaltung*.

Wenn eine Gesamtstruktur-Vertrauensstellung mit Ausschlüssen für Namensuffixe konfiguriert ist, werden die konfigurierten Ausschlüsse zum Filtern der Liste der untergeordneten Gesamtstrukturdomänen verwendet. Das Filtern durch Ausschlüsse für Namensuffixe erfolgt zusätzlich zum Filtern mit dem Befehl `vdadmin`.

Erstellen einer OU für Remote-Desktops

Sie sollten eine Organisationseinheit (Organizational Unit, OU) speziell für Ihre Remote-Desktops erstellen. Eine OU ist ein Containerelement zur Unterteilung in Active Directory, das Benutzer, Gruppen, Computer oder andere OUs enthalten kann.

Um zu verhindern, dass Gruppenrichtlinieneinstellungen auf andere Windows-Server oder -Arbeitsstationen in derselben Domäne wie Ihre Desktops angewendet werden, können Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für Ihre View-Gruppenrichtlinien erstellen und es mit der OU verknüpfen, die Ihre Remote-Desktops enthält. Sie können die Steuerung der OU auch an untergeordnete Gruppen delegieren, beispielsweise an Serveroperatoren oder einzelne Benutzer.

Wenn Sie View Composer verwenden, erstellen Sie einen separaten Active Directory-Container für Linked-Clone-Desktops, der auf der OU für Ihre Remote-Desktops basiert. Administratoren, die in Active Directory OU-Administratorberechtigungen besitzen, können ohne Domänenadministratorberechtigungen Linked-Clone-Desktops bereitstellen. Wenn Sie in Active Directory die Anmeldeinformationen für Administratoren ändern, müssen Sie auch die Anmeldeinformationen in View Composer aktualisieren.

Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus

Ein Client im Kiosk-Modus ist ein Thin Client oder ein PC mit eingeschränkten Funktionen, auf dem Clientsoftware ausgeführt wird, um die Verbindung mit einer View-Verbindungsserver-Instanz herzustellen und eine Remote-Desktop-Sitzung zu starten. Wenn Sie Clients im Kiosk-Modus konfigurieren, sollten Sie in Active Directory dedizierte Organisationseinheiten (Organizational Units, OUs) und Gruppen für diese Clients konfigurieren.

Durch das Erstellen von dedizierten OUs und Gruppen für Clientkonten im Kiosk-Modus werden Client-systeme unterteilt, um sie vor einem unberechtigten Zugriff zu schützen. Gleichzeitig wird so die Konfiguration und Verwaltung der Clients vereinfacht.

Weitere Informationen finden Sie im Dokument *ViewVerwaltung*.

Erstellen von Gruppen für Benutzer

Sie sollten Gruppen für unterschiedliche Arten von Benutzern in Active Directory erstellen. Beispielsweise können Sie eine Gruppe namens „View-Benutzer“ für Ihre Endbenutzer und eine weitere Gruppe namens „View-Administratoren“ für Benutzer erstellen, die Remote-Desktops und -Anwendungen verwalten.

Erstellen eines Benutzerkontos für vCenter Server

Sie müssen ein Benutzerkonto in Active Directory erstellen, um es mit vCenter Server einzusetzen. Geben Sie dieses Benutzerkonto an, wenn Sie eine vCenter Server-Instanz in View Administrator hinzufügen.

Sie müssen dem Benutzerkonto Berechtigungen zum Ausführen bestimmter Vorgänge in vCenter Server erteilen. Sie können eine vCenter Server-Rolle mit den entsprechenden Rechten erstellen und die Rolle dem vCenter Server-Benutzer zuweisen. Die Liste der Rechte, die Sie zur vCenter Server-Rolle hinzufügen, hängt davon ab, ob Sie View mit oder ohne View Composer verwenden. Weitere Informationen zum Konfigurieren dieser Berechtigungen finden Sie unter [„Konfigurieren von Benutzerkonten für vCenter Server und View Composer“](#), auf Seite 111.

Wenn Sie View Composer auf demselben Computer wie vCenter Server installieren, müssen Sie den vCenter Server-Benutzer zur lokalen Administratorgruppe auf dem vCenter Server-Computer hinzufügen. Dies ermöglicht View die Authentifizierung beim View Composer-Dienst.

Wenn Sie View Composer auf einem anderen Computer als vCenter Server installieren, müssen Sie den vCenter Server-Benutzer nicht als lokalen Administrator auf dem vCenter Server-Computer konfigurieren. Sie müssen jedoch ein eigenständiges View Composer Server-Benutzerkonto erstellen, das ein lokaler Administrator auf dem View Composer-Computer sein muss.

Erstellen eines Benutzerkontos für einen eigenständigen View Composer Server

Wenn Sie View Composer auf einem anderen Computer als vCenter Server installieren, müssen Sie ein Domänenbenutzerkonto in Active Directory erstellen, das View für die Authentifizierung beim View Composer-Dienst auf dem eigenständigen Computer verwenden kann.

Das Benutzerkonto muss sich in derselben Domäne wie Ihr View-Verbindungsserver-Host oder in einer vertrauenswürdigen Domäne befinden. Sie müssen das Benutzerkonto zur lokalen Administratorgruppe auf dem eigenständigen View Composer-Computer hinzufügen.

Dieses Benutzerkonto geben Sie an, wenn Sie View Composer-Einstellungen in View Administrator konfigurieren und **Eigenständiger View Composer Server** auswählen. Siehe [„Konfigurieren von View Composer-Einstellungen“](#), auf Seite 119.

Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge

Wenn Sie View Composer verwenden, müssen Sie ein Benutzerkonto in Active Directory erstellen, mit dem View Composer bestimmte Vorgänge in Active Directory ausführen kann. View Composer benötigt dieses Konto, um virtuelle Linked-Clone-Maschinen zur Active Directory-Domäne hinzuzufügen.

Zur Gewährleistung der Sicherheit sollten Sie ein separates Benutzerkonto für View Composer erstellen. Durch das Erstellen eines separaten Kontos können Sie sicherstellen, dass keine zusätzlichen Berechtigungen für andere Zwecke gewährt werden. Sie können diesem Konto die Mindestberechtigungen erteilen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind für das View Composer-Konto nicht die Berechtigungen eines Domänenadministrators erforderlich.

Vorgehensweise

- 1 Erstellen Sie in Active Directory ein Benutzerkonto, das sich in derselben Domäne wie Ihr View-Verbindungs-Server-Host oder in einer vertrauenswürdigen Domäne befindet.
- 2 Fügen Sie die Berechtigungen **Computerobjekte erstellen**, **Computerobjekte löschen** und **Alle Eigenschaften schreiben** für das Konto in dem Active Directory-Container hinzu, in dem die Linked-Clone-Computerkonten erstellt werden bzw. in den die Linked-Clone-Computerkonten verschoben werden sollen.

Die folgende Liste zeigt alle für das Benutzerkonto erforderlichen Berechtigungen, einschließlich der standardmäßig zugewiesenen Berechtigungen:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Alle Eigenschaften schreiben
- Berechtigungen lesen
- Kennwort zurücksetzen
- Computerobjekte erstellen
- Computerobjekte löschen

HINWEIS Weniger Berechtigungen sind erforderlich, wenn Sie die Einstellung **Wiederverwendung bereits bestehender Computerkonten zulassen** für einen Desktop-Pool auswählen. Stellen Sie sicher, dass dem Benutzerkonto die folgenden Berechtigungen zugewiesen sind:

- Inhalt auflisten
 - Alle Eigenschaften lesen
 - Berechtigungen lesen
 - Kennwort zurücksetzen
-

- 3 Stellen Sie sicher, dass die Berechtigungen für das Benutzerkonto für den Active Directory-Container und alle untergeordneten Objekte des Containers gelten.

Weiter

Geben Sie das Konto in View Administrator an, wenn Sie View Composer-Domänen im Assistenten zum Hinzufügen von vCenter Server konfigurieren und Linked-Clone-Desktop-Pools konfigurieren und bereitstellen.

Erstellen eines Benutzerkontos für Instant Clone-Vorgänge

Vor dem Bereitstellen von Instant Clones müssen Sie ein Benutzerkonto erstellen, das über die Berechtigung verfügt, bestimmte Vorgänge in Active Directory durchzuführen.

Wählen Sie beim Hinzufügen eines Instant-Clone-Domänenadministrators dieses Konto aus, bevor Sie Instant Clone-Desktop-Pools bereitstellen. Weitere Informationen finden Sie unter „Hinzufügen eines Instant-Clone-Domänenadministrators“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Vorgehensweise

- 1 Erstellen Sie in Active Directory ein Benutzerkonto, das sich in derselben Domäne wie Ihr Verbindungs-Server oder in einer vertrauenswürdigen Domäne befindet.

- 2 Fügen Sie dem Konto auf dem Container für die Instant Clone-Computerkonten die Berechtigungen **Computerobjekte erstellen**, **Computerobjekte löschen** und **Alle Eigenschaften schreiben** hinzu.

Die folgende Liste zeigt die für das Benutzerkonto erforderlichen Berechtigungen, einschließlich der standardmäßig zugewiesenen Berechtigungen:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Alle Eigenschaften schreiben
- Berechtigungen lesen
- Kennwort zurücksetzen
- Computerobjekte erstellen
- Computerobjekte löschen

Stellen Sie sicher, dass die Berechtigungen für den richtigen Container und alle untergeordneten Objekte des Containers gelten.

Konfigurieren der Richtlinie „Eingeschränkte Gruppen“

Benutzer, die sich bei einem Remote-Desktop anmelden möchten, müssen der lokalen Gruppe „Remote-Desktop-Benutzer“ des Remote-Desktops angehören. Sie können mithilfe der Richtlinie „Eingeschränkte Gruppen“ in Active Directory Benutzer oder Gruppen zur lokalen Gruppe der Remote-Desktop-Benutzer für jeden Remote-Desktop hinzuzufügen, der Ihrer Domäne angehört.

Die Richtlinie „Eingeschränkte Gruppen“ legt die lokale Gruppenmitgliedschaft für Computer in der Domäne so fest, dass sie mit den Mitgliedschaftseinstellungen in der Richtlinie „Eingeschränkte Gruppen“ übereinstimmt. Die Mitglieder Ihrer Remote-Desktop-Benutzergruppe werden stets der lokalen Gruppe „Remote-Desktop-Benutzer“ für jeden Remote-Desktop hinzugefügt, den Sie Ihrer Domäne hinzufügen. Wenn Sie neue Benutzer hinzufügen, müssen Sie diese lediglich der Gruppe der Remote-Desktop-Benutzer hinzufügen.

Voraussetzungen

Erstellen Sie in Active Directory eine Gruppe für die Remote-Desktop-Benutzer in Ihrer Domäne.

Vorgehensweise

- 1 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 2 Erweitern Sie den Abschnitt **Computerkonfiguration** und öffnen Sie **Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel**.

- 3 Klicken Sie mit der rechten Maustaste auf **Eingeschränkte Gruppen**, wählen Sie **Gruppe hinzufügen**, und fügen Sie die Gruppe „Remote-Desktop-Benutzer“ hinzu.
- 4 Klicken Sie mit der rechten Maustaste auf die neue eingeschränkte Gruppe „Remote-Desktop-Benutzer“ und fügen Sie der Liste der Gruppenmitglieder Ihre Remote-Desktop-Benutzergruppe hinzu.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7

Horizon 7 umfasst verschiedene komponentenspezifische administrative ADMX-Vorlagendateien für Gruppenrichtlinien.

Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, stehen in einer mitgelieferten .zip-Datei namens `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` zur Verfügung, wobei `x.x.x` die Version und `yyyyyy` die Build-Nummer darstellt. Sie können die Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die mitgelieferte .zip-Datei enthält.

Sie können Remote-Desktops optimieren und schützen, indem Sie die Richtlinieneinstellungen in diesen Dateien auf ein neues oder vorhandenes Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory anwenden und das GPO mit der Organisationseinheit (Organizational Unit, OU) verknüpfen, die Ihre Desktops enthält.

Informationen zur Verwendung von Horizon 7-Gruppenrichtlinieneinstellungen erhalten Sie in den Dokumenten *Administration von View* und *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Vorbereiten von Active Directory für die Smartcard-Authentifizierung

Sie müssen in Active Directory möglicherweise bestimmte Aufgaben ausführen, wenn Sie die Smartcard-Authentifizierung implementieren.

- [Hinzufügen von UPNs für Smartcard-Benutzer](#) auf Seite 38
Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern und Administratoren, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.
- [Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen](#) auf Seite 39
Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie „Vertrauenswürdige Stammzertifizierungsstellen“ in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.
- [Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen](#) auf Seite 40
Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen.
- [Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher](#) auf Seite 40
Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Hinzufügen von UPNs für Smartcard-Benutzer

Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern und Administratoren, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, müssen Sie den Benutzer-UPN auf den alternativen Antragstellernamen (Subject Alternative Name, SAN) festlegen, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist. Wenn Ihr Stammzertifikat von einem anderen Server in der aktuellen Domäne des Smartcard-Benutzers ausgegeben wurde, ist eine Änderung des Benutzer-UPNs nicht erforderlich.

HINWEIS Sie müssen möglicherweise den UPN für integrierte Active Directory-Konten angeben, selbst wenn das Zertifikat von derselben Domäne ausgegeben wurde. Für integrierte Konten, einschließlich des Administratorkontos, ist standardmäßig kein UPN festgelegt.

Voraussetzungen

- Sie können den alternativen Antragstellernamen (SAN) abrufen, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.
- Wenn das Dienstprogramm „ADSI Edit“ nicht auf Ihrem Active Directory-Server zur Verfügung steht, laden Sie die entsprechenden Windows-Supporttools von der Microsoft-Website herunter und installieren Sie sie.

Vorgehensweise

- 1 Starten Sie auf Ihrem Active Directory-Server das Dienstprogramm ADSI-Editor.
- 2 Erweitern Sie im linken Fensterbereich die Domäne, in der sich der Benutzer befindet, und doppelklicken Sie auf CN=Users.
- 3 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Benutzer und anschließend auf **Eigenschaften**.
- 4 Doppelklicken Sie auf das Attribut `userPrincipalName` und geben Sie den SAN-Wert für das Zertifikat der vertrauenswürdigen Zertifizierungsstelle ein.
- 5 Klicken Sie auf **OK**, um die Attributeinstellung zu speichern.

Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie „Vertrauenswürdige Stammzertifizierungsstellen“ in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

- 1 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 2 Erweitern Sie den Abschnitt **Computerkonfiguration** und öffnen Sie **Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel**.
- 3 Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Importieren**.
- 4 Folgen Sie den Anweisungen des Assistenten, um das Stammzertifikat (z.B. rootCA.cer) zu importieren. Klicken Sie anschließend auf **OK**.
- 5 Schließen Sie das Fenster „Gruppenrichtlinie“.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Stammzertifikats in ihrem vertrauenswürdigen Stammspeicher.

Weiter

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen. Siehe [„Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen“](#), auf Seite 40.

Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen.

Vorgehensweise

- 1 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 2 Erweitern Sie den Abschnitt **Computerkonfiguration** und öffnen Sie die Richtlinie für **Windows-Einstellungen\Sicherheitseinstellungen\Öffentlicher Schlüssel**.
- 3 Klicken Sie mit der rechten Maustaste auf **Zwischenzertifizierungsstellen** und wählen Sie **Importieren**.
- 4 Folgen Sie den Anweisungen des Assistenten, um das Zwischenzertifikat (z.B. intermediateCA.cer) zu importieren. Klicken Sie anschließend auf **OK**.
- 5 Schließen Sie das Fenster „Gruppenrichtlinie“.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Zwischenzertifikats in ihrem Zwischenzertifizierungsstellen-Speicher.

Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

- ◆ Verwenden Sie auf dem Active Directory-Server den Befehl `certutil`, um das Zertifikat im Enterprise NTAAuth-Speicher zu veröffentlichen.

Beispiel: `certutil -dspublish -f Pfad_zum_Zertifikat_der_Stammzertifizierungsstelle NTAAuthCA`

Die Zertifizierungsstelle wird jetzt als vertrauenswürdig eingestuft und kann Zertifikate dieses Typs ausstellen.

Deaktivieren von schwachen Verschlüsselungen in SSL/TLS

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

Vorgehensweise

- 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 View Composer und die View Agent- oder Horizon Agent-Maschinen neu, damit die neue Gruppenrichtlinie wirksam wird.

Installieren von View Composer

Zur Verwendung von View Composer erstellen Sie eine View Composer-Datenbank, installieren den View Composer-Dienst und optimieren Ihre View-Infrastruktur zur Unterstützung von View Composer. Sie können den View Composer-Dienst auf demselben Host wie vCenter Server oder auf einem separaten Host installieren.

View Composer ist eine optionale Funktion. Installieren Sie View Composer, wenn Sie Linked-Clone-Desktop-Pools bereitstellen möchten.

Zu Installation und Verwendung der View Composer-Funktion benötigen Sie eine Lizenz.

Dieses Kapitel behandelt die folgenden Themen:

- „Vorbereiten einer View Composer-Datenbank“, auf Seite 43
- „Konfigurieren eines SSL-Zertifikats für View Composer“, auf Seite 52
- „Installieren des View Composer-Dienstes“, auf Seite 52
- „Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer“, auf Seite 54
- „Konfigurieren der Infrastruktur für View Composer“, auf Seite 55

Vorbereiten einer View Composer-Datenbank

Sie müssen eine Datenbank und einen Datenquellennamen (Data Source Name, DSN) zum Speichern von View Composer-Daten erstellen.

Der View Composer-Dienst umfasst keine Datenbank. Falls in Ihrer Netzwerkumgebung keine Datenbankinstanz vorhanden ist, müssen Sie eine installieren. Nach dem Installieren der Datenbankinstanz fügen Sie die View Composer-Datenbank zur Instanz hinzu.

Sie können die View Composer-Datenbank zu der Instanz hinzufügen, auf der sich die vCenter Server-Datenbank befindet. Sie können eine lokale oder Remote-Konfiguration der Datenbank auf einem mit dem Netzwerk verbundenen Linux-, UNIX- oder Windows Server-Computer durchführen.

Die View Composer-Datenbank speichert Informationen zu Verbindungen und Komponenten, die von View Composer verwendet werden:

- vCenter Server-Verbindungen
- Active Directory-Verbindungen
- Linked-Clone-Desktops, die von View Composer bereitgestellt werden
- Replikate, die von View Composer erstellt werden

Jede Instanz des View Composer-Dienstes muss über eine eigene View Composer-Datenbank verfügen. Mehrere View Composer-Dienste können eine View Composer-Datenbank nicht gemeinsam nutzen.

Eine Liste der unterstützten Datenbankversionen finden Sie unter „[Datenbankanforderungen für View Composer und die Ereignisdatenbank](#)“, auf Seite 13.

Befolgen Sie zum Hinzufügen einer View Composer-Datenbank zu einer installierten Datenbankinstanz eine dieser Vorgehensweisen.

- [Erstellen einer SQL Server-Datenbank für View Composer](#) auf Seite 44

View Composer kann Informationen zu Linked-Clone-Desktops in einer SQL Server-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu SQL Server hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

- [Erstellen einer Oracle-Datenbank für View Composer](#) auf Seite 48

View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 12c- oder Oracle 11g-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren. Sie können eine neue View Composer-Datenbank hinzufügen, indem Sie den Assistenten für die Oracle-Datenbankkonfiguration verwenden oder eine SQL-Anweisung ausführen.

Erstellen einer SQL Server-Datenbank für View Composer

View Composer kann Informationen zu Linked-Clone-Desktops in einer SQL Server-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu SQL Server hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

Vorgehensweise

- 1 [Hinzufügen einer View Composer-Datenbank zu SQL Server](#) auf Seite 44

Sie können einer vorhandenen Microsoft SQL Server-Instanz eine neue View Composer-Datenbank hinzufügen, um Linked-Clone-Daten für View Composer zu speichern.

- 2 (Optional) [Festlegen von SQL Server-Datenbankberechtigungen durch die manuelle Erstellung von Datenbankrollen](#) auf Seite 45

Mithilfe dieser empfohlenen Methode kann der View Composer-Datenbankadministrator Berechtigungen festlegen, die View Composer-Administratoren über Microsoft SQL Server-Datenbankrollen erteilt werden.

- 3 [Hinzufügen einer ODBC-Datenquelle zu SQL Server](#) auf Seite 47

Nachdem Sie eine View Composer-Datenbank zu SQL Server hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Hinzufügen einer View Composer-Datenbank zu SQL Server

Sie können einer vorhandenen Microsoft SQL Server-Instanz eine neue View Composer-Datenbank hinzufügen, um Linked-Clone-Daten für View Composer zu speichern.

Wenn die Datenbank lokal auf dem System vorhanden ist, auf dem View Composer installiert wird, können Sie das Sicherheitsmodell der integrierten Windows-Authentifizierung verwenden. Diese Authentifizierungsmethode kann nicht verwendet werden, wenn die Datenbank auf einem Remote-System vorliegt.

Voraussetzungen

- Stellen Sie sicher, dass eine unterstützte Version von SQL Server auf dem Computer, auf dem Sie View Composer installieren, oder in Ihrer Netzwerkumgebung installiert ist. Weitere Informationen finden Sie unter „[Datenbankanforderungen für View Composer und die Ereignisdatenbank](#)“, auf Seite 13.

- Verwenden Sie unbedingt SQL Server Management Studio zum Erstellen und Verwalten der Datenbank. Alternativ können Sie SQL Server Management Studio Express verwenden. Diese Anwendung können Sie über die folgende Website herunterladen und installieren.

<http://www.microsoft.com/en-us/download/details.aspx?id=7593>

Vorgehensweise

- 1 Wählen Sie auf dem View Composer-Computer **Start > Alle Programme > Microsoft SQL Server 2014, Microsoft SQL Server 2012** oder **Microsoft SQL Server 2008** aus.
- 2 Wählen Sie **SQL Server Management Studio** aus und stellen Sie eine Verbindung mit der SQL Server-Instanz her.
- 3 Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf den Datenbankeneintrag und wählen Sie **Neue Datenbank**.

Sie können die Standardwerte für die Parameter `Initial size` und `Autogrowth` für die Datenbank und die Protokolldateien verwenden.

- 4 Geben Sie im Dialogfeld „Neue Datenbank“ im Textfeld „Datenbankname“ einen Namen ein.

Beispiel: **ViewComposer**

- 5 Klicken Sie auf **OK**.

SQL Server Management Studio fügt Ihre Datenbank zum Datenbankeneintrag im Objekt-Explorer hinzu.

- 6 Beenden Sie Microsoft SQL Server Management Studio.

Weiter

Folgen Sie optional den Anweisungen unter „(Optional) Festlegen von SQL Server-Datenbankberechtigungen durch die manuelle Erstellung von Datenbankrollen“, auf Seite 45

Folgen Sie den Anweisungen unter „Hinzufügen einer ODBC-Datenquelle zu SQL Server“, auf Seite 47.

(Optional) Festlegen von SQL Server-Datenbankberechtigungen durch die manuelle Erstellung von Datenbankrollen

Mithilfe dieser empfohlenen Methode kann der View Composer-Datenbankadministrator Berechtigungen festlegen, die View Composer-Administratoren über Microsoft SQL Server-Datenbankrollen erteilt werden.

VMware empfiehlt diese Methode, da damit das Einrichten der **db_owner**-Rolle für View Composer-Administratoren entfällt, die View Composer installieren und upgraden.

In dieser Vorgehensweise können Sie eigene Namen für den Datenbank-Anmeldenamen, den Benutzernamen und die Datenbankrollen eingeben. Der Benutzer **[vcmpuser]** und die Datenbankrollen **VCMP_ADMIN_ROLE** und **VCMP_USER_ROLE** sind Beispielnamen. Das **dbo**-Schema wird angelegt, wenn Sie die View Composer-Datenbank erstellen. Sie müssen den **dbo**-Schemanamen verwenden.

Voraussetzungen

- Stellen Sie sicher, dass eine View Composer-Datenbank erstellt wird. Siehe „Hinzufügen einer View Composer-Datenbank zu SQL Server“, auf Seite 44.

Vorgehensweise

- 1 Melden Sie sich bei einer Microsoft SQL Server Management Studio-Sitzung als Sysadmin (SA) oder bei einem Benutzerkonto mit **Sysadmin**-Rechten an.

- 2 Erstellen Sie einen Benutzer, dem die entsprechenden SQL Server-Datenbankberechtigungen erteilt werden.

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

- 3 Erstellen Sie in der View Composer-Datenbank die Datenbankrolle **VCMP_ADMIN_ROLE**.
- 4 Weisen Sie in der View Composer-Datenbank der Rolle **VCMP_ADMIN_ROLE** Rechte zu.
 - a Erteilen Sie die Schemaberechtigungen **ALTER**, **REFERENCES** und **INSERT** im **dbo**-Schema.
 - b Erteilen Sie die Berechtigungen **CREATE TABLE**, **CREATE VIEW** und **CREATE PROCEDURES**.
- 5 Erstellen Sie in der View Composer-Datenbank die Rolle **VCMP_USER_ROLE**.
- 6 Erteilen Sie in der View Composer-Datenbank der Rolle **VCMP_USER_ROLE** im **dbo**-Schema die Schemaberechtigungen **SELECT**, **INSERT**, **DELETE**, **UPDATE** und **EXECUTE**.
- 7 Erteilen Sie dem Benutzer **[vcmpuser]** die Rolle **VCMP_USER_ROLE**.
- 8 Erteilen Sie dem Benutzer **[vcmpuser]** die Rolle **VCMP_ADMIN_ROLE**.
- 9 Erstellen Sie in der MSDB-Datenbank die Datenbankrolle **VCMP_ADMIN_ROLE**.
- 10 Erteilen Sie Rechte für die Rolle **VCMP_ADMIN_ROLE** in MSDB.
 - a Erteilen Sie in den MSDB-Tabellen **syscategories**, **sysjobsteps** und **sysjobs** die Berechtigung **SELECT** für den Benutzer **[vcmpuser]**.
 - b Erteilen Sie in den gespeicherten MSDB-Prozeduren **sp_add_job**, **sp_delete_job**, **sp_add_jobstep**, **sp_update_job**, **sp_add_jobserver**, **sp_add_jobschedule** und **sp_add_category** die Berechtigung **EXECUTE** für die Rolle **VCMP_ADMIN_ROLE**.
- 11 Erteilen Sie in der MSDB-Datenbank die Rolle **VCMP_ADMIN_ROLE** für den Benutzer **[vcmpuser]**.
- 12 Erstellen Sie den ODBC-DSN mithilfe des SQL Server-Anmeldenamens **vcmpuser**.
- 13 Installieren Sie View Composer.
- 14 Entziehen Sie in der MSDB-Datenbank dem Benutzer **[vcmpuser]** die Rolle **VCMP_ADMIN_ROLE**.
Nachdem Sie die Rolle entzogen haben, können Sie sie inaktiv lassen oder sie zwecks erhöhter Sicherheit entfernen.

Anweisungen zum Erstellen eines ODBC-DSN finden Sie unter „[Hinzufügen einer ODBC-Datenquelle zu SQL Server](#)“, auf Seite 47.

Anweisungen zum Installieren von View Composer finden Sie unter „[Installieren des View Composer-Dienstes](#)“, auf Seite 52.

Hinzufügen einer ODBC-Datenquelle zu SQL Server

Nachdem Sie eine View Composer-Datenbank zu SQL Server hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Wenn Sie einen ODBC DSN für View Composer konfigurieren, sichern Sie die zugrundeliegende Datenbankverbindung in einem für Ihre Umgebung angemessenen Maß ab. Weitere Informationen zum Sichern von Datenbankverbindungen finden Sie in der SQL Server-Dokumentation.

Wenn die zugrundeliegende Datenbankverbindung SSL-Verschlüsselung verwendet, empfehlen wir Ihnen, Ihre Datenbankserver mit von einer vertrauenswürdigen Zertifizierungsstelle signierten SSL-Zertifikaten zu konfigurieren. Wenn Sie selbstsignierte Zertifikate verwenden, sind Ihre Datenbankverbindungen möglicherweise anfällig für Man-in-the-Middle-Angriffe.

Voraussetzungen

Führen Sie die unter „[Hinzufügen einer View Composer-Datenbank zu SQL Server](#)“, auf Seite 44.

Vorgehensweise

- 1 Wählen Sie auf dem Computer, auf dem View Composer installiert wird, **Start > Verwaltung > Datenquelle (ODBC)** aus.
- 2 Klicken Sie auf die Registerkarte **System-DSN**.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie in der angezeigten Liste den Eintrag **SQL Native Client**.
- 4 Klicken Sie auf **Fertig stellen**.
- 5 Geben Sie im Assistenten Neue Datenquelle für SQL Server erstellen einen Namen und eine Beschreibung der View Composer-Datenbank ein.

Beispiel: **ViewComposer**

- 6 Geben Sie im Textfeld Server den Namen der SQL Server-Datenbank ein.

Verwenden Sie das Format *host_name\server_name*, wobei *host_name* für den Namen des Computers und *server_name* für die SQL Server-Instanz steht.

Beispiel: **VHOST1\VIM_SQLEXP**

- 7 Klicken Sie auf **Weiter**.
- 8 Stellen Sie sicher, dass das Kontrollkästchen **Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten** aktiviert ist, und wählen Sie eine Authentifizierungsoption.

Option	Beschreibung
Windows-Authentifizierung integrieren	Wählen Sie diese Option, wenn Sie eine lokale Instanz von SQL Server verwenden. Diese Option wird auch als vertrauenswürdige Authentifizierung bezeichnet. „Windows-Authentifizierung integrieren“ wird nur unterstützt, wenn SQL Server auf dem lokalen Computer ausgeführt wird.
SQL Server-Authentifizierung	Wählen Sie diese Option, wenn Sie eine Remote-Instanz von SQL Server verwenden. Die Windows NT-Authentifizierung wird auf Remote-Computern mit SQL Server nicht unterstützt. Wenn Sie SQL Server-Datenbankberechtigungen manuell festgelegt und einem Benutzer zugewiesen haben, authentifizieren Sie mit diesem Benutzerkonto. Authentifizieren Sie beispielsweise mit dem Benutzerkonto vcmpuser . Authentifizieren Sie andernfalls als Sysadmin (SA) oder mit einem Benutzerkonto mit Sysadmin -Rechten.

- 9 Klicken Sie auf **Weiter**.

- 10 Aktivieren Sie das Kontrollkästchen **Die Standarddatenbank ändern auf** und wählen Sie den Namen der View Composer-Datenbank in der Liste aus.

Beispiel: **ViewComposer**

- 11 Wenn die SQL Server-Verbindung mit aktiviertem SSL konfiguriert ist, navigieren Sie zur Microsoft SQL Server DSN-Konfigurationsseite und wählen Sie **Starke Verschlüsselung für Daten verwenden**.
- 12 Beenden und schließen Sie den Microsoft ODBC-Datenquellenadministrator-Assistenten.

Weiter

Installieren des neuen View Composer-Dienstes. Siehe „[Installieren des View Composer-Dienstes](#)“, auf Seite 52.

Erstellen einer Oracle-Datenbank für View Composer

View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 12c- oder Oracle 11g-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren. Sie können eine neue View Composer-Datenbank hinzufügen, indem Sie den Assistenten für die Oracle-Datenbankkonfiguration verwenden oder eine SQL-Anweisung ausführen.

- [Hinzufügen einer View Composer-Datenbank zu Oracle 12c oder 11g](#) auf Seite 48
Sie können den Assistenten für die Oracle-Datenbankkonfiguration verwenden, um eine neue View Composer-Datenbank zu einer vorhandenen Oracle 12c- oder 11g-Instanz hinzuzufügen.
- [Verwenden einer SQL-Anweisung zum Hinzufügen einer View Composer-Datenbank zu einer Oracle-Instanz](#) auf Seite 49
- [Konfigurieren eines Oracle-Datenbankbenutzers für View Composer](#) auf Seite 50
Standardmäßig verfügt der Datenbankbenutzer, der die View Composer-Datenbank ausführt, über Administratorberechtigungen für das Oracle-System. Um die Sicherheitsberechtigungen des Benutzers, der die View Composer-Datenbank ausführt, zu beschränken, muss ein Oracle-Datenbankbenutzer mit spezifischen Berechtigungen konfiguriert werden.
- [Hinzufügen einer ODBC-Datenquelle zu Oracle 12c oder 11g](#) auf Seite 51
Nachdem Sie eine View Composer-Datenbank zu einer Oracle 12c- oder Oracle 11g-Instanz hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Hinzufügen einer View Composer-Datenbank zu Oracle 12c oder 11g

Sie können den Assistenten für die Oracle-Datenbankkonfiguration verwenden, um eine neue View Composer-Datenbank zu einer vorhandenen Oracle 12c- oder 11g-Instanz hinzuzufügen.

Voraussetzungen

Stellen Sie sicher, dass auf dem lokalen oder Remote-Computer eine unterstützte Version von Oracle 12c oder 11g installiert ist. Siehe „[Datenbankanforderungen für View Composer und die Ereignisdatenbank](#)“, auf Seite 13.

Vorgehensweise

- 1 Starten Sie den **Datenbankkonfigurations-Assistent** auf dem Computer, auf dem Sie die View Composer-Datenbank hinzufügen.

Datenbankversion	Aktion
Oracle 12c	Wählen Sie Start > Alle Programme > Oracle-OraDb12c_home > Konfigurations- und Migrations-Tools > Datenbankkonfigurations-Assistent aus.
Oracle 11g	Wählen Sie Start > Alle Programme > Oracle-OraDb11g_home > Konfigurations- und Migrations-Tools > Datenbankkonfigurations-Assistent aus.

- 2 Wählen Sie auf der Seite „Operation“ die Option **Datenbank erstellen**.
- 3 Wählen Sie auf der Seite „Datenbankvorlagen“ die Vorlage **Allgemeiner Zweck oder Transaktionsverarbeitung**.
- 4 Geben Sie auf der Seite „Datenbankidentifizierung“ einen globalen Datenbanknamen und ein Präfix für die Oracle-Systemkennung (System Identifier, SID) ein.
Geben Sie der Einfachheit halber für beide Einstellungen denselben Wert an.
- 5 Klicken Sie auf der Seite „Verwaltungsoptionen“ auf **Weiter**, um die Standardeinstellungen zu akzeptieren.
- 6 Wählen Sie auf der Seite „Datenbankmeldeinformationen“ die Option **Dasselbe Verwaltungskennwort für alle Konten verwenden** und geben Sie ein Kennwort ein.
- 7 Klicken Sie auf den verbleibenden Konfigurationsseiten auf **Weiter**, um die Standardeinstellungen zu akzeptieren.
- 8 Vergewissern Sie sich, dass auf der Seite **Erstellungsoptionen** die Option „Datenbank erstellen“ aktiviert ist, und klicken Sie auf **Fertig stellen**.
- 9 Überprüfen Sie die Optionen auf der Bestätigungsseite und klicken Sie auf **OK**.
Das Konfigurationstool erstellt die Datenbank.
- 10 Klicken Sie auf der Seite „Datenbankerstellung abgeschlossen“ auf **OK**.

Weiter

Folgen Sie den Anweisungen unter [„Hinzufügen einer ODBC-Datenquelle zu Oracle 12c oder 11g“](#), auf Seite 51.

Verwenden einer SQL-Anweisung zum Hinzufügen einer View Composer-Datenbank zu einer Oracle-Instanz

Beim Erstellen der Datenbank können Sie den Speicherort von Daten und Protokolldateien anpassen.

Voraussetzungen

Die View Composer-Datenbank muss über bestimmte Tablespaces und Berechtigungen verfügen. Sie können die View Composer-Datenbank mithilfe einer SQL-Anweisung in einer Oracle 12c- oder 11g-Datenbankinstanz erstellen.

Stellen Sie sicher, dass auf dem lokalen oder Remote-Computer eine unterstützte Version von Oracle 12c oder 11g installiert ist. Weitere Informationen finden Sie unter [„Datenbankanforderungen für View Composer und die Ereignisdatenbank“](#), auf Seite 13.

Vorgehensweise

- 1 Melden Sie sich über das Systemkonto an einer SQL*Plus-Sitzung an.

- 2 Führen Sie zum Erstellen der Datenbank die folgende SQL-Anweisung aus.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

In diesem Beispiel ist VCMP der Beispielpname der View Composer-Datenbank und vcmp01.dbf der Name der Datenbankdatei.

Verwenden Sie bei einer Windows-Installation die Windows-Konventionen im Verzeichnispfad zur Datei vcmp01.dbf.

Weiter

Wenn die View Composer-Datenbank mit spezifischen Sicherheitsberechtigungen ausgeführt werden soll, befolgen Sie die Anweisungen unter „[Konfigurieren eines Oracle-Datenbankbenutzers für View Composer](#)“, auf Seite 50.

Folgen Sie den Anweisungen unter „[Hinzufügen einer ODBC-Datenquelle zu Oracle 12c oder 11g](#)“, auf Seite 51

Konfigurieren eines Oracle-Datenbankbenutzers für View Composer

Standardmäßig verfügt der Datenbankbenutzer, der die View Composer-Datenbank ausführt, über Administratorberechtigungen für das Oracle-System. Um die Sicherheitsberechtigungen des Benutzers, der die View Composer-Datenbank ausführt, zu beschränken, muss ein Oracle-Datenbankbenutzer mit spezifischen Berechtigungen konfiguriert werden.

Voraussetzungen

Stellen Sie sicher, dass eine View Composer-Datenbank in einer Oracle 12c- oder 11g-Instanz erstellt wurde.

Vorgehensweise

- 1 Melden Sie sich über das Systemkonto an einer SQL*Plus-Sitzung an.
- 2 Führen Sie den folgenden SQL-Befehl aus, um einen View Composer-Datenbankbenutzer mit den geeigneten Berechtigungen zu erstellen.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
grant connect to VCMPADMIN;
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

In diesem Beispiel lautet der Benutzername VCMPADMIN und der View Composer-Datenbankname VCMP.

Standardmäßig verfügt die Rolle resource über die Berechtigungen create procedure, create table und create sequence. Wenn die Rolle resource nicht über diese Berechtigungen verfügt, weisen Sie sie dem View Composer-Datenbankbenutzer explizit zu.

Hinzufügen einer ODBC-Datenquelle zu Oracle 12c oder 11g

Nachdem Sie eine View Composer-Datenbank zu einer Oracle 12c- oder Oracle 11g-Instanz hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Wenn Sie einen ODBC DSN für View Composer konfigurieren, sichern Sie die zugrundeliegende Datenbankverbindung in einem für Ihre Umgebung angemessenen Maß ab. Weitere Informationen zum Sichern von Datenbankverbindungen finden Sie in der Dokumentation der Oracle-Datenbank.

Wenn die zugrundeliegende Datenbankverbindung SSL-Verschlüsselung verwendet, empfehlen wir Ihnen, Ihre Datenbankserver mit von einer vertrauenswürdigen Zertifizierungsstelle signierten SSL-Zertifikaten zu konfigurieren. Wenn Sie selbstsignierte Zertifikate verwenden, sind Ihre Datenbankverbindungen möglicherweise anfällig für Man-in-the-Middle- Angriffe.

Voraussetzungen

Stellen Sie sicher, dass Sie die in „[Hinzufügen einer View Composer-Datenbank zu Oracle 12c oder 11g](#)“, auf Seite 48 oder „[Verwenden einer SQL-Anweisung zum Hinzufügen einer View Composer-Datenbank zu einer Oracle-Instanz](#)“, auf Seite 49.

Vorgehensweise

- 1 Wählen Sie auf dem View Composer-Datenbankcomputer **Start > Verwaltung > Datenquelle (ODBC)** aus.
- 2 Wechseln Sie im Microsoft ODBC-Datenquellenadministrator-Assistenten zur Registerkarte **System-DSN**.
- 3 Klicken Sie auf **Hinzufügen** und wählen Sie in der angezeigten Liste den geeigneten Oracle-Treiber aus.
Beispiel: **OraDb11g_home**
- 4 Klicken Sie auf **Fertig stellen**.
- 5 Geben Sie im Dialogfeld „Oracle-ODBC-Treiberkonfiguration“ einen DSN zur Verwendung mit View Composer, eine Beschreibung der Datenquelle sowie eine Benutzer-ID für die Verbindungsherstellung mit der Datenbank ein.

Wenn Sie für die Oracle-Datenbank eine Benutzer-ID mit spezifischen Sicherheitsberechtigungen konfiguriert haben, geben Sie diese Benutzer-ID an.

HINWEIS Sie verwenden den DSN bei der Installation des View Composer-Dienstes.

- 6 Wählen Sie als **TNS-Dienstname** den globalen Datenbanknamen im Dropdown-Menü aus.
Der Assistent für die Oracle-Datenbankkonfiguration legt den globalen Datenbanknamen fest.
- 7 Zum Überprüfen der Datenquelle klicken Sie auf **Verbindung testen** und anschließend auf **OK**.

Weiter

Installieren des neuen View Composer-Dienstes. Siehe „[Installieren des View Composer-Dienstes](#)“, auf Seite 52.

Konfigurieren eines SSL-Zertifikats für View Composer

Standardmäßig wird ein selbst signiertes Zertifikat mit View Composer installiert. Sie können das Standardzertifikat für Testzwecke verwenden, zur Verwendung in der Produktionsumgebung sollten Sie es jedoch durch ein Zertifikat ersetzen, das von einer Zertifizierungsstelle signiert wurde.

Sie können ein Zertifikat vor oder nach der Installation von View Composer konfigurieren. In View 5.1 und höher werden Zertifikate konfiguriert, indem Sie sie in den lokalen Windows-Zertifikatspeicher des Windows Server-Computers importieren, auf dem View Composer installiert ist bzw. wird.

- Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat importieren, bevor Sie View Composer installieren, wählen Sie das signierte Zertifikat während der View Composer-Installation aus. Bei diesem Ansatz muss das Standardzertifikat nach der Installation nicht manuell ersetzt werden.
- Wenn Sie ein vorhandenes Zertifikat oder das selbst signierte Standardzertifikat nach der Installation von View Composer durch ein neues Zertifikat ersetzen möchten, müssen Sie das neue Zertifikat importieren und das Dienstprogramm `SviConfig ReplaceCertificate` ausführen, um das neue Zertifikat an den von View Composer verwendeten Port zu binden.

Einzelheiten zur Konfiguration von SSL-Zertifikaten und Verwendung des Dienstprogramms `SviConfig ReplaceCertificate` finden Sie unter [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Wenn Sie vCenter Server und View Composer auf demselben Windows Server-Computer installieren, wird dasselbe SSL-Zertifikat verwendet. Sie müssen das Zertifikat jedoch für jede Komponente einzeln konfigurieren.

Installieren des View Composer-Dienstes

Um View Composer verwenden zu können, müssen Sie den View Composer-Dienst installieren. View verwendet View Composer zum Erstellen und Bereitstellen von Linked-Clone-Desktops in vCenter Server.

Sie können den View Composer-Dienst auf dem Windows Server-Computer mit vCenter Server installieren oder auf einem separaten Windows Server-Computer. Eine eigenständige View Composer-Installation kann mit vCenter Server auf einem Windows Server-Computer sowie mit der Linux-basierten vCenter Server Appliance verwendet werden.

Die View Composer-Software darf nicht auf derselben virtuellen Maschine oder demselben physischen Computer installiert sein wie eine andere Softwarekomponente von View, einschließlich eines Replikatervers, Sicherheitsservers, View-Verbindungsservers, Horizon Agent oder Horizon Client.

Für eine erweiterte Sicherheit empfehlen wir die Konfiguration von Verschlüsselungssammlungen, um bekannte Sicherheitslücken zu schließen. Erläuterungen zur Einrichtung einer Domänenrichtlinie für Verschlüsselungssammlungen für Windows-Maschinen, auf denen View Composer oder Horizon Agent ausgeführt wird, finden Sie unter [„Deaktivieren von schwachen Verschlüsselungen in SSL/TLS“](#), auf Seite 41.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Installation die unter [„View Composer-Anforderungen“](#), auf Seite 12 beschriebenen View Composer-Anforderungen erfüllt.
- Stellen Sie sicher, dass keine andere View-Komponente, einschließlich View-Verbindungsserver, Sicherheitsserver, Horizon Agent oder Horizon Client, auf dem Computer installiert ist, auf dem Sie View Composer installieren möchten.
- Stellen Sie sicher, dass Sie über eine Lizenz zur Installation und Verwendung von View Composer verfügen.

- Stellen Sie sicher, dass Sie über den DSN, den Benutzernamen des Domänenadministrators und das Kennwort verfügen, den/das Sie im ODBC-Datenquellenadministrator angegeben haben. Sie geben diese Informationen bei der Installation des View Composer-Dienstes an.
- Wenn Sie beabsichtigen, während der Installation ein SSL-Zertifikat für View Composer zu konfigurieren, das von einer Zertifizierungsstelle signiert wurde, stellen Sie während der Installation sicher, dass Ihr Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers importiert wird. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.
- Stellen Sie sicher, dass keine auf dem Computer mit View Composer ausgeführten Anwendungen SSL-Bibliotheken von Windows verwenden, für die über das Microsoft Secure Channel (Schannel)-Sicherheitspaket bereitgestellte SSL Version 2 (SSLv2) erforderlich ist. Das Installationsprogramm für View Composer deaktiviert SSLv2 für Microsoft Schannel. Anwendungen wie Tomcat, das Java SSL verwendet, oder Apache, das OpenSSL verwendet, sind nicht von dieser Einschränkung betroffen.
- Um das Installationsprogramm für View Composer auszuführen, müssen Sie ein Benutzer mit Administratorrechten auf dem System sein.

Vorgehensweise

- 1 Laden Sie das Installationsprogramm für View Composer von der VMware-Produktseite unter <http://www.vmware.com/products/> auf den Windows Server-Computer herunter.
Der Dateiname des Installationsprogramms lautet `VMware-viewcomposer-y.y.y-xxxxxx.exe`, wobei `xxxxxx` die Build-Nummer und `y.y.y` die Versionsnummer ist. Mit dieser Installationsdatei wird der View Composer-Dienst unter 64 Bit Windows Server-Betriebssystemen installiert.
- 2 Um das Installationsprogramm für View Composer zu starten, klicken Sie mit der rechten Maustaste auf die Installationsdatei und wählen Sie **Als Administrator ausführen**.
- 3 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 4 Übernehmen oder ändern Sie den Zielordner.
- 5 Geben Sie den DSN für die View Composer-Datenbank ein, den Sie im ODBC-Datenquellenadministrator-Assistenten für Microsoft oder Oracle eingegeben haben.

Beispiel: **VMware View Composer**

HINWEIS Wenn Sie keinen DSN für die View Composer-Datenbank konfiguriert haben, klicken Sie auf **ODBC-DSN-Setup**, um jetzt einen Namen zu konfigurieren.

- 6 Geben Sie den Benutzernamen des Domänenadministrators und das Kennwort ein, den/das Sie im ODBC-Datenquellenadministrator angegeben haben.
Wenn Sie für die Oracle-Datenbank einen Benutzer mit spezifischen Sicherheitsberechtigungen konfiguriert haben, geben Sie diesen Benutzernamen an.
- 7 Geben Sie eine Portnummer ein oder übernehmen Sie den Standardwert.
View-Verbindungsserver verwendet diesen Port zur Kommunikation mit dem View Composer-Dienst.
- 8 Stellen Sie ein SSL-Zertifikat bereit.

Option	Aktion
SSL-Standardzertifikat erstellen	Wählen Sie dieses Optionsfeld aus, um ein SSL-Standardzertifikat für den View Composer-Dienst zu erstellen. Nach der Installation können Sie das Standardzertifikat durch ein SSL-Zertifikat ersetzen, das von einer Zertifizierungsstelle signiert wurde.
Vorhandenes SSL-Zertifikat verwenden	Wählen Sie dieses Optionsfeld aus, wenn Sie ein signiertes SSL-Zertifikat installiert haben, das Sie für den View Composer-Dienst verwenden möchten. Wählen Sie ein SSL-Zertifikat in der Liste aus.

- 9 Klicken Sie auf **Installieren** und **Fertig stellen**, um die Installation des View Composer-Dienstes abzuschließen.

Der VMware Horizon View Composer-Dienst wird gestartet.

View Composer verwendet die kryptografischen Verschlüsselungssammlungen, die vom Windows Server-Betriebssystem bereitgestellt werden. Befolgen Sie die Richtlinien Ihrer Organisation für die Verwaltung von Verschlüsselungssammlungen auf Windows Server-Systemen. Wenn Ihre Organisation keine Richtlinien bereitstellt, empfiehlt VMware, schwache kryptografische Verschlüsselungssammlungen auf dem View Composer Server zu deaktivieren, um die Sicherheit Ihrer View-Umgebung zu verstärken. Informationen zum Verwalten kryptografischer Verschlüsselungssammlungen finden Sie in der Dokumentation von Microsoft.

Weiter

Wenn Sie über eine ältere Version von vCenter Server verfügen, finden Sie Erläuterungen unter [„Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer“](#), auf Seite 54.

Wenn Sie SQL Server-Datenbankberechtigungen manuell festgelegt und einem Benutzer zugewiesen haben, können Sie die Datenbankadministratorrolle für diesen Benutzer zurückziehen. Weitere Informationen finden Sie im letzten Verfahrensschritt unter [„\(Optional\) Festlegen von SQL Server-Datenbankberechtigungen durch die manuelle Erstellung von Datenbankrollen“](#), auf Seite 45.

Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer

In Horizon 7 und neueren Komponenten ist das TLSv1.0-Sicherheitsprotokoll standardmäßig deaktiviert. Wenn Ihre Bereitstellung eine ältere Version von vCenter Server enthält, die nur TLSv1.0 unterstützt, müssen Sie eventuell TLSv1.0 für View Composer-Verbindungen aktivieren, wenn Sie View Composer 7.0 oder eine neuere Version installiert oder ein Upgrade dafür durchgeführt haben.

Einige frühere Wartungsversionen von vCenter Server 5.0, 5.1 und 5.5 unterstützen nur die Version TLSv1.0, die in Horizon 7 und neueren Versionen standardmäßig nicht mehr aktiviert ist. Wenn ein Upgrade auf eine Version von vCenter Server, die TLSv1.1 oder TLSv1.2 unterstützt, nicht möglich ist, können Sie TLSv1.0 für View Composer-Verbindungen aktivieren.

Wenn Ihre ESXi-Hosts nicht ESXi 6.0 U1b oder höher ausführen, ist ein Upgrade nicht möglich. In diesem Fall müssen Sie auch die TLSv1.0-Verbindungen von View Composer zu den ESXi-Hosts aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass View Composer 7.0 oder eine neuere Version installiert ist.
- Stellen Sie sicher, dass Sie sich am View Composer-Computer als Administrator anmelden können, um auf den Windows Registrierungs-Editor zuzugreifen.

Vorgehensweise

- 1 Öffnen Sie auf dem Computer, der View Composer hostet, den Windows Registrierungs-Editor (regedit.exe).
- 2 Navigieren Sie zu HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client.
Erstellen Sie diesen Schlüssel, wenn er noch nicht vorhanden ist.
- 3 Löschen Sie den Wert **Enabled**, sofern vorhanden.
- 4 Erstellen oder bearbeiten Sie den **DWORD**-Wert **DisabledByDefault**, und setzen Sie ihn auf **0**.
- 5 Starten Sie den VMware Horizon View Composer-Dienst neu.

Die TLSv1.0-Verbindungen von View Composer zu vCenter sind nun aktiviert.

- 6 Navigieren Sie in der Windows Registrierung auf dem View Composer-Computer zu HKLM\SOFTWARE\VMware, Inc.\VMware View Composer.
- 7 Erstellen oder bearbeiten Sie den Zeichenfolgenwert **EnableTLS1.0** und setzen Sie ihn auf **1**.
- 8 Handelt es sich bei dem View Composer-Host um einen 64-Bit-Computer, dann navigieren Sie zu HKLM\SOFTWARE\WOW6432Node\VMware, Inc\VMware View Composer.
- 9 Erstellen oder bearbeiten Sie den Zeichenfolgenwert **EnableTLS1.0** und setzen Sie ihn auf **1**.
- 10 Starten Sie den VMware Horizon View Composer-Dienst neu.

Die TLSv1.0-Verbindungen von View Composer zu den ESXi-Hosts sind nun aktiviert.

Konfigurieren der Infrastruktur für View Composer

Sie können die Vorteile von Funktionen in vSphere, vCenter Server, Active Directory und anderen Komponenten Ihrer Infrastruktur nutzen, um die Leistung, Verfügbarkeit und Zuverlässigkeit von View Composer zu optimieren.

Konfigurieren der vSphere-Umgebung für View Composer

Zur Unterstützung von View Composer sollten Sie beim Installieren und Konfigurieren von vCenter Server, ESXi und anderer vSphere-Komponenten verschiedene empfohlene Vorgehensweisen beachten.

Die nachfolgend vorgestellten empfohlenen Vorgehensweisen sorgen dafür, dass View Composer in der vSphere-Umgebung optimal ausgeführt wird.

- Nachdem Sie die Pfad- und Ordnerinformationen für virtuelle Linked-Clone-Maschinen angegeben haben, sollten Sie die Informationen nicht in vCenter Server ändern. Verwenden Sie stattdessen View Administrator zum Ändern der Ordnerinformationen.

Wenn Sie die Informationen in vCenter Server ändern, kann View die virtuellen Maschinen in vCenter Server nicht erfolgreich ermitteln.
- Stellen Sie sicher, dass die vSwitch-Einstellungen auf dem ESXi-Host mit einer ausreichenden Anzahl von Ports konfiguriert sind, sodass die Gesamtzahl der virtuellen Netzwerkkarten unterstützt wird, die auf den auf dem ESXi-Host ausgeführten virtuellen Linked-Clone-Maschinen konfiguriert sind.
- Wenn Sie Linked-Clone-Desktop in einem Ressourcenpool bereitstellen, stellen Sie sicher, dass Ihre vSphere-Umgebung über ausreichende CPU- und Arbeitsspeicherressourcen verfügt, um die benötigte Anzahl an Desktops zu hosten. Verwenden Sie vSphere Client zur Überwachung der CPU- und Arbeitsspeichernutzung in Ressourcenpools.
- In vSphere 5.1 und höher kann ein Cluster, der für View Composer-Linked-Clones verwendet wird, mehr als acht ESXi-Hosts enthalten, wenn die Replikatfestplatten auf VMFS5-Datenspeichern oder höher oder NFS-Datenspeichern gespeichert sind. Wenn Sie Replikate in einem Datenspeicher einer früheren VMFS-Version als VMFS5 speichern, kann ein Cluster über maximal acht Hosts verfügen.

In vSphere 5.0 können Sie einen Cluster mit mehr als acht ESXi-Hosts auswählen, wenn die Replikate auf NFS-Datenspeichern gespeichert werden. Wenn Sie Repliken auf VMFS-Datenspeichern speichern, kann ein Cluster höchstens acht Hosts besitzen.
- Verwenden Sie vSphere DRS. DRS sorgt für eine effiziente Verteilung der virtuellen Linked-Clone-Maschinen auf Ihre Hosts.

HINWEIS Storage vMotion wird für Linked-Clone-Desktops nicht unterstützt.

Zusätzliche empfohlene Vorgehensweisen für View Composer

Um eine optimale Funktion von View Composer sicherzustellen, sollten Sie sich vergewissern, dass DNS (Dynamic Name Service) ordnungsgemäß arbeitet. Zusätzlich sollten Sie zeitversetzte Prüfungen mithilfe einer Antivirensoftware durchführen.

Indem Sie sicherstellen, dass die DNS-Auflösung ordnungsgemäß funktioniert, können Sie durch DNS-Fehler ausgelöste Probleme beseitigen. Der View Composer-Dienst stützt sich bei der Kommunikation mit anderen Computern auf eine dynamische Namensauflösung. Zum Testen der DNS-Funktion senden Sie ein Ping-Signal an die Active Directory- und View-Verbindungsserver-Computer. Verwenden Sie hierbei die Computernamen.

Wenn Sie die Ausführung Ihrer Antivirensoftware zeitversetzt planen, wird die Leistung der Linked-Clone-Desktops nicht beeinträchtigt. Wenn die Antivirensoftware auf allen Linked-Clone-Desktops gleichzeitig ausgeführt wird, treten übermäßige E/A-Vorgänge pro Sekunde in Ihrem Speichersubsystem auf. Diese hohe Aktivität kann sich negativ auf die Leistung der Linked-Clone-Desktops auswirken.

Installieren von View-Verbindungsserver

7

Zur Verwendung von View-Verbindungsserver installieren Sie die Software auf unterstützten Computern, konfigurieren die erforderlichen Komponenten und nehmen ggf. eine Optimierung der Komponenten vor.

Dieses Kapitel behandelt die folgenden Themen:

- „[Installieren der View-Verbindungsserver-Software](#)“, auf Seite 57
- „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58
- „[Installieren von View-Verbindungsserver mit einer neuen Konfiguration](#)“, auf Seite 59
- „[Installieren einer replizierten Instanz von View-Verbindungsserver](#)“, auf Seite 66
- „[Konfigurieren eines Kennworts für die Kombination mit einem Sicherheitsserver](#)“, auf Seite 73
- „[Installieren eines Sicherheitsservers](#)“, auf Seite 74
- „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81
- „[Erneutes Installieren eines View-Verbindungservers mit einer Sicherungskonfiguration](#)“, auf Seite 83
- „[Befehlszeilenoptionen für Microsoft Windows Installer](#)“, auf Seite 84
- „[Unbeaufsichtigtes Deinstallieren von View-Komponenten mithilfe von MSI-Befehlszeilenoptionen](#)“, auf Seite 87

Installieren der View-Verbindungsserver-Software

Je nachdem, welche Anforderungen in Bezug auf Leistung, Verfügbarkeit und Sicherheit für Ihre View-Bereitstellung gelten, können Sie eine einzelne Instanz oder replizierte Instanzen von View-Verbindungsserver und Sicherheitsserver installieren. Sie müssen mindestens eine Instanz von View-Verbindungsserver installieren.

Bei der Installation von View-Verbindungsserver wählen Sie die Art der Installation aus.

Standardinstallation	Generiert eine View-Verbindungsserver-Instanz mit einer neuen View LDAP-Konfiguration.
Replikationinstallation	Generiert eine View-Verbindungsserver-Instanz mit einer View LDAP-Konfiguration, die von einer vorhandenen Instanz kopiert wird.

Sicherheitsserverinstallation

Generiert eine Instanz von View-Verbindungsserver, die einen zusätzlichen Sicherheits-Layer zwischen dem Internet und Ihrem internen Netzwerk hinzufügt.

Installation des Registrierungsservers

Installiert einen für die True SSO-Funktion (Single Sign-On) erforderlichen Registrierungsserver. Nach der Anmeldung bei VMware Identity Manager können Benutzer damit eine Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung herstellen, ohne Anmeldeinformationen für Active Directory eingeben zu müssen. Für den Registrierungsserver sind kurzlebige Zertifikate für die Authentifizierung erforderlich.

HINWEIS Für diese Funktion muss auch eine Zertifizierungsstelle eingerichtet und eine spezielle Konfiguration durchgeführt werden. Der Installationsvorgang für den Registrierungsserver wird deshalb nicht in diesem Installationshandbuch, sondern im Dokument *Administration von View* im Kapitel „Authentifizieren von Benutzern ohne Anforderung von Anmeldeinformationen“ erläutert.

Installationsvoraussetzungen für View-Verbindungsserver

Bevor Sie View-Verbindungsserver installieren, müssen Sie sicherstellen, dass Ihre Installationsumgebung die geltenden Voraussetzungen erfüllt.

- Sie benötigen einen gültigen Lizenzschlüssel für View.
- Sie müssen View-Verbindungsserver-Host zu einer Active Directory-Domäne hinzufügen. View-Verbindungsserver unterstützen die folgenden Domänenfunktionsebenen der Active Directory-Domänendienste (Active Directory Domain Services, AD DS):
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2

Bei dem View-Verbindungsserver-Host darf es sich nicht um einen Domänencontroller handeln.

HINWEIS Durch View-Verbindungsserver werden keine Aktualisierungen am Active Directory-Schema oder der Active Directory-Konfiguration vorgenommen, und es sind auch keine Aktualisierungen erforderlich.

- Installieren Sie View-Verbindungsserver nicht auf Systemen, auf denen die Windows Terminal Server-Rolle installiert ist. Sie müssen die Windows Terminal Server-Rolle von einem System entfernen, auf dem Sie View-Verbindungsserver installieren möchten.
- Installieren Sie View-Verbindungsserver nicht auf einem System, das andere Funktionen oder Rollen innehat. Verwenden Sie beispielsweise nicht das System, das Sie zum Hosten von vCenter Server verwenden.
- Das System, auf dem Sie den View-Verbindungsserver installieren, muss über eine IP-Adresse verfügen, die sich nicht ändert. In einer IPv4-Umgebung konfigurieren Sie eine statische IP-Adresse. In einer IPv6-Umgebung erhalten Computer automatisch IP-Adressen, die nicht geändert werden.
- Zum Ausführen des View-Verbindungsserver-Installationsprogramms müssen Sie ein Domänenbenutzerkonto mit Administratorberechtigungen für das System verwenden.

- Wenn Sie View-Verbindungsserver installieren, autorisieren Sie ein Konto der View-Administratoren. Das Konto kann auch das der lokalen Administratorengruppe, das eines Domänenbenutzers oder ein Gruppenkonto sein. View weist nur diesem Konto vollständige View-Administratorenberechtigungen zu, einschließlich der Berechtigung zum Installieren von replizierten View-Verbindungsserver-Instanzen. Wenn Sie einen Domänenbenutzer oder eine Gruppe angeben, müssen Sie das Konto in Active Directory erstellen, bevor Sie das Installationsprogramm ausführen.

Installieren von View-Verbindungsserver mit einer neuen Konfiguration

Um View-Verbindungsserver als einen einzelnen Server oder als erste Instanz in einer Gruppe replizierter View-Verbindungsserver-Instanzen zu installieren, verwenden Sie die Standardinstallationsoption.

Wenn Sie die Standardinstallationsoption wählen, wird bei der Installation eine neue, lokale View LDAP-Konfiguration erstellt. Die Installation lädt Schemadefinitionen, DIT-Definition (Directory Information Tree) und ACLs und initialisiert die Daten.

Nach der Installation verwalten Sie die meisten View LDAP-Konfigurationsdaten mithilfe von View Administrator. View-Verbindungsserver verwaltet einige View LDAP-Einträge automatisch.

Die View-Verbindungsserver-Software darf nicht auf demselben physischen Computer bzw. derselben virtuellen Maschine installiert sein wie eine andere View-Softwarekomponente, einschließlich eines Replikatervers, Sicherheitsservers, View Composer, Horizon Agent oder Horizon Client.

Wenn Sie den View-Verbindungsserver mit einer neuen Konfiguration installieren, können Sie an einem Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen. VMware sammelt anonyme Daten zu Ihrer Bereitstellung, um die Reaktionen von VMware auf Benutzeranforderungen zu verbessern. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten. Wenn Sie nicht teilnehmen möchten, deaktivieren Sie diese Option während der Installation. Wenn Sie nach Abschluss der Installation Ihre Meinung hinsichtlich der Teilnahme ändern, können Sie dem Programm beitreten bzw. es verlassen, indem Sie die Seite „Produktlizenzierung und -verwendung“ in View Administrator bearbeiten. Die Liste der Felder, aus denen Daten erfasst werden, einschließlich der Felder, die anonymisiert werden, finden Sie unter „Vom Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Daten“ im Dokument *Administration von View*.

Standardmäßig wird die HTML Access-Komponente auf dem View-Verbindungsserver-Host installiert, wenn Sie View-Verbindungsserver installieren. Diese Komponente konfiguriert das View-Benutzerportal, sodass ein Symbol für HTML Access zusätzlich zum Symbol für Horizon Client angezeigt wird. Über das zusätzliche Symbol können Benutzer HTML Access auswählen, wenn sie sich mit ihren Desktops verbinden.

Eine Übersicht über das Einrichten eines View-Verbindungservers für HTML Access finden Sie unter „Vorbereiten von View-Verbindungsserver und Sicherheitsservern für HTML Access“ im Dokument *Verwenden von HTML Access* auf der Seite mit der Horizon Client-Dokumentation.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie View-Verbindungsserver installieren.
- Stellen Sie sicher, dass Ihre Installation die unter „[Horizon-Verbindungsserver – Serveranforderungen](#)“, auf Seite 9 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58.
- Wenn Sie beabsichtigen, einen Domänenbenutzer oder eine Gruppe als View Administrators-Konto zu autorisieren, stellen Sie sicher, dass Sie das Domänenkonto in Active Directory erstellt haben.

- Wenn Sie die MIT-Kerberos-Authentifizierung zur Anmeldung bei einem Windows Server 2008 R2-Computer verwenden, auf dem Sie den View-Verbindungsserver installieren, installieren Sie das Microsoft-Hotfix, das im Knowledge Base-Artikel KB 978116 unter <http://support.microsoft.com/kb/978116> beschrieben ist.
- Bereiten Sie ein Kennwort für die Datenwiederherstellung vor. Wenn Sie View-Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Um die verschlüsselte View-Sicherungskonfiguration wiederherzustellen, müssen Sie das Kennwort für die Datenwiederherstellung angeben. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.

WICHTIG Sie benötigen das Kennwort für die Datenwiederherstellung, um den Betrieb von View aufrechtzuerhalten und Ausfallzeiten in einem Szenario mit Business Continuity und Disaster Recovery (BCDR) zu vermeiden. Sie können beim Installieren des View-Verbindungsservers eine Kennworterinnerung für das Kennwort bereitstellen.

- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für die View-Verbindungsserver-Instanzen geöffnet werden müssen. Siehe „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81.
- Wenn Sie planen, einen Sicherheitsserver mit dieser Instanz von View-Verbindungsserver zu kombinieren, stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen einem Sicherheitsserver und der View-Verbindungsserver-Instanz enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y` die Versionsnummer.

- 2 Zum Starten des Verbindungsserver-Installationsprogramms doppelklicken Sie auf die Installationsdatei.
- 3 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 4 Übernehmen oder ändern Sie den Zielordner.
- 5 Wählen Sie die Installationsoption **View-Standardserver**.
- 6 Wählen Sie die Internetprotokollversion (IP) **IPv4** oder **IPv6** aus.
Sie müssen alle View-Komponenten mit derselben IP-Version installieren.
- 7 Wählen Sie aus, ob der FIPS-Modus aktiviert werden soll.
Diese Option ist nur verfügbar, wenn der FIPS-Modus in Windows aktiviert ist.
- 8 Stellen Sie sicher, dass die Option **HTML Access installieren** ausgewählt ist, wenn Benutzer die Möglichkeit haben sollen, sich über einen Webbrowser mit ihren Desktops zu verbinden.

Wird **IPv4** ausgewählt, ist diese Einstellung standardmäßig aktiviert. Wird **IPv6** ausgewählt, wird diese Einstellung nicht angezeigt, weil HTML Access in einer IPv6-Umgebung nicht unterstützt wird.

- 9 Geben Sie ein Kennwort für die Datenwiederherstellung und optional eine Kennwörterinnerung ein.
- 10 Wählen Sie Konfigurationsoptionen für den Windows-Firewall-Dienst aus.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen Netzwerkverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell. Aktivieren Sie diese Option nur dann, wenn Ihre Organisation ihre eigenen vordefinierten Regeln zum Konfigurieren der Windows-Firewall verwendet.

- 11 Autorisieren Sie ein View Administrators-Konto.

Nur Mitglieder dieses Kontos können sich bei View Administrator anmelden, Vorgänge mit vollständigen Administratorberechtigungen ausführen und replizierte View-Verbindungsserver-Instanzen und andere View-Server installieren.

Option	Beschreibung
Authorize the local Administrators group (Lokale Administratorengruppe autorisieren)	Ermöglicht Benutzern in der lokalen Administratorengruppe die Verwaltung von View.
Authorize a specific domain user or domain group (Bestimmte(n) Domänenbenutzer oder Domänengruppe autorisieren)	Ermöglicht dem angegebenen Domänenbenutzer oder der angegebenen Gruppe die Verwaltung von View.

- 12 Wenn Sie ein View Administrator-Konto für die Domäne angegeben haben und das Installationsprogramm als lokaler Administrator oder als anderer Benutzer ausführen, der keinen Zugriff auf das Domänenkonto hat, geben Sie Anmeldeinformationen an, um sich mit einem autorisierten Benutzernamen und einem Kennwort bei der Domäne anzumelden.

Verwenden Sie das Format *Domänennamen\Benutzername* oder das UPN-Format (Benutzerprinzipalname). Ein Benutzer im UPN-Format kann *benutzer@domäne.com* sein.

- 13 Wählen Sie, ob Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen möchten. Wenn ja, können Sie optional Art, Größe und Standort Ihrer Organisation auswählen.
- 14 Schließen Sie die Installation von View-Verbindungsserver mit dem Installations-Assistenten ab.
- 15 Überprüfen Sie den Windows Server-Computer auf neue Patches und führen Sie bei Bedarf Windows Update aus.

Auch wenn Sie alle verfügbaren Patches auf dem Windows Server-Computer installiert haben, bevor Sie den View-Verbindungsserver installiert haben, wurden Betriebssystemfunktionen bei der Installation möglicherweise zum ersten Mal aktiviert. Möglicherweise sind nun zusätzliche Patches erforderlich.

Die Horizon 7-Dienste sind auf dem Windows Server-Computer installiert:

- VMware Horizon-Verbindungsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Message Bus-Komponente
- VMware Horizon View-Skripthost
- VMware Horizon View Sicherheits-Gateway-Komponente
- VMware Horizon View PCoIP Secure Gateway

- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web-Komponente
- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Wenn die Einstellung **HTML Access installieren** bei der Installation ausgewählt wurde, wird die HTML Access-Komponente auf dem Windows Server-Computer installiert. Diese Komponente konfiguriert das Symbol für HTML Access im Horizon 7-Benutzerportal und aktiviert die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** in der Windows-Firewall. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, eine Verbindung mit dem Verbindungsserver über den TCP-Port 8443 herzustellen.

Weiter

Konfigurieren Sie SSL-Serverzertifikate für View-Verbindungsserver. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Wenn Sie über eine ältere Version von vCenter Server verfügen, finden Sie Erläuterungen unter [„Aktivieren von TLSv1.0 für vCenter-Verbindungen vom Verbindungsserver“](#), auf Seite 65.

Führen Sie eine anfängliche Konfiguration von View-Verbindungsserver durch. Siehe [Kapitel 9, „Erstmaliges Konfigurieren von View“](#), auf Seite 111.

Wenn Sie replizierte View-Verbindungsserver-Instanzen und Sicherheitsserver in Ihrer Bereitstellung nutzen möchten, müssen Sie jede Serverinstanz durch Ausführung der View-Verbindungsserver-Installationsdatei installieren.

Wenn Sie den View-Verbindungsserver erneut installieren und ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

Unbeaufsichtigte Installation von View-Verbindungsserver

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, eine Standardinstallation von View-Verbindungsserver auf mehreren Windows-Computern durchzuführen. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie View-Verbindungsserver installieren.
- Stellen Sie sicher, dass Ihre Installation die unter [„Horizon-Verbindungsserver – Serveranforderungen“](#), auf Seite 9 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe [„Installationsvoraussetzungen für View-Verbindungsserver“](#), auf Seite 58.
- Wenn Sie beabsichtigen, einen Domänenbenutzer oder eine Gruppe als View Administrators-Konto zu autorisieren, stellen Sie sicher, dass Sie das Domänenkonto in Active Directory erstellt haben.
- Wenn Sie die MIT-Kerberos-Authentifizierung zur Anmeldung bei einem Windows Server 2008 R2-Computer verwenden, auf dem Sie den View-Verbindungsserver installieren, installieren Sie das Microsoft-Hotfix, das im Knowledge Base-Artikel KB 978116 unter <http://support.microsoft.com/kb/978116> beschrieben ist.
- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für die View-Verbindungsserver-Instanzen geöffnet werden müssen. Siehe [„Firewall-Regeln für View-Verbindungsserver“](#), auf Seite 81.

- Wenn Sie planen, einen Sicherheitsserver mit dieser Instanz von View-Verbindungsserver zu kombinieren, stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen einem Sicherheitsserver und der View-Verbindungsserver-Instanz enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.
- Stellen Sie sicher, dass der Windows-Computer, auf dem Sie View-Verbindungsserver installieren, über Version 2.0 oder eine höhere Version des MSI-Laufzeitmoduls verfügt. Weitere Informationen finden Sie auf der Microsoft-Website.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „[Befehlszeilenoptionen für Microsoft Windows Installer](#)“, auf Seite 84.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation einer Standardinstallation von View-Verbindungsserver vertraut. Siehe „[Eigenschaften für die unbeaufsichtigte Installation einer View-Verbindungsserver-Standardinstallation](#)“, auf Seite 64.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y.y` die Versionsnummer.

- 2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.
- 3 Geben Sie den Installationsbefehl in einer Zeile ein.

```
Beispiel: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1
VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_RE-
MINDER=""First car"""
```

WICHTIG Wenn Sie eine unbeaufsichtigte Installation durchführen, wird die gesamte Befehlszeile, einschließlich des Kennworts für die Datenwiederherstellung, in der Datei `vminst.log` des Installationsprogramms protokolliert. Nach Abschluss der Installation löschen Sie diese Protokolldatei oder ändern Sie das Kennwort für die Datenwiederherstellung in View Administrator.

- 4 Überprüfen Sie den Windows Server-Computer auf neue Patches und führen Sie bei Bedarf Windows Update aus.

Auch wenn Sie alle verfügbaren Patches auf dem Windows Server-Computer installiert haben, bevor Sie den View-Verbindungsserver installiert haben, wurden Betriebssystemfunktionen bei der Installation möglicherweise zum ersten Mal aktiviert. Möglicherweise sind nun zusätzliche Patches erforderlich.

Die Horizon 7-Dienste sind auf dem Windows Server-Computer installiert:

- VMware Horizon-Verbindungsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Message Bus-Komponente
- VMware Horizon View-Skripthost
- VMware Horizon View Sicherheits-Gateway-Komponente

- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web-Komponente
- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Wenn die Einstellung **HTML Access installieren** bei der Installation ausgewählt wurde, wird die HTML Access-Komponente auf dem Windows Server-Computer installiert. Diese Komponente konfiguriert das Symbol für HTML Access im Horizon 7-Benutzerportal und aktiviert die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** in der Windows-Firewall. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, eine Verbindung mit dem Verbindungsserver über den TCP-Port 8443 herzustellen.

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Weiter

Konfigurieren Sie SSL-Serverzertifikate für View-Verbindungsserver. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Wenn Sie über eine ältere Version von vCenter Server verfügen, finden Sie Erläuterungen unter [„Aktivieren von TLSv1.0 für vCenter-Verbindungen vom Verbindungsserver“](#), auf Seite 65.

Wenn Sie View zum ersten Mal konfigurieren, führen Sie die anfängliche Konfiguration auf dem View-Verbindungsserver durch. Siehe [Kapitel 9, „Erstmaliges Konfigurieren von View“](#), auf Seite 111.

Eigenschaften für die unbeaufsichtigte Installation einer View-Verbindungsserver-Standardinstallation

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation einer View-Verbindungsserver-Standardinstallation über die Befehlszeile ausführen. Sie müssen das Format *PROPERTY=value* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 7-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View-Verbindungsserver in einer Standardinstallation

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View-Verbindungsserver-Software installiert wird. Beispiel: <code>INSTALLDIR=""D:\abc\mein Ordner""</code> Die Paare doppelter Anführungszeichen, die den Pfad umschließen, ermöglichen es dem MSI Installer, das Leerzeichen als gültigen Teil des Pfades zu interpretieren.	%ProgramFiles%\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	Die Art der View Server-Installation: <ul style="list-style-type: none"> ■ 1. Standardinstallation ■ 2. Replikainstallation ■ 3. Sicherheitsserverinstallation ■ 5. Installation des Registrierungsservers Für eine Standardinstallation definieren Sie <code>VDM_SERVER_INSTANCE_TYPE=1</code>	1
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View-Verbindungsserver-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall konfiguriert. Mit dem Wert 2 wird keine Firewall konfiguriert. Zum Beispiel: <code>FWCHOICE=1</code>	1

Tabelle 7-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View-Verbindungsserver in einer Standardinstallation (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
VDM_INITIAL_ADMIN_SID	Die SID des initialen View Administrators-Benutzers oder der -Gruppe, der/die in View über vollständige Administrationsrechte verfügt. Der Standardwert ist die SID der lokalen Administratorengruppe auf dem View -Verbindungsserver-Computer. Sie können eine SID eines Domänenbenutzers oder eines Gruppenkontos angeben.	S-1-5-32-544
VDM_SERVER_RECOVERY_PWD	Das Kennwort für die Datenwiederherstellung. Wenn in View LDAP kein Kennwort für die Datenwiederherstellung festgelegt ist, muss diese Eigenschaft verwendet werden. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.	Keine.
VDM_SERVER_RECOVERY_PWD_REMINDER	Die Kennwörterinnerung für die Datenwiederherstellung. Diese Eigenschaft ist optional.	Keine.
VDM_IP_PROTOCOL_NUTZUNG	Gibt die IP-Version an, die von View-Komponenten für die Kommunikation verwendet wird. Mögliche Werte sind IPv4 und IPv6 .	IPv4
VDM_FIPS_ENABLED	Geben Sie an, ob der FIPS-Modus aktiviert werden soll. Der Wert 1 aktiviert den FIPS-Modus. Der Wert 0 deaktiviert den FIPS-Modus. Wenn für diese Eigenschaft 1 gewählt wurde und Windows sich nicht im FIPS-Modus befindet, wird der Installationsvorgang abgebrochen.	0
HTMLACCESS	Steuert die HTML Access-Add-On-Installation. Wenn Sie HTML Access konfigurieren möchten, legen Sie für diese Eigenschaft 1 fest. Wenn Sie HTML Access nicht benötigen, lassen Sie diese Eigenschaft leer.	1

Aktivieren von TLSv1.0 für vCenter-Verbindungen vom Verbindungsserver

In Horizon 7 und neueren Komponenten ist das TLSv1.0-Sicherheitsprotokoll standardmäßig deaktiviert. Wenn Ihre Bereitstellung eine ältere Version von vCenter Server enthält, die nur TLSv1.0 unterstützt, müssen Sie TLSv1.0 für Verbindungsserver-Verbindungen aktivieren, wenn Sie Verbindungsserver 7.0 oder eine neuere Version installiert oder aktualisiert haben.

Einige frühere Wartungsversionen von vCenter Server 5.0, 5.1 und 5.5 unterstützen nur die Version TLSv1.0, die in Horizon 7 und neueren Versionen standardmäßig nicht mehr aktiviert ist. Wenn ein Upgrade auf eine Version von vCenter Server, die TLSv1.1 oder TLSv1.2 unterstützt, nicht möglich ist, können Sie TLSv1.0 für Verbindungsserver-Verbindungen aktivieren.

Voraussetzungen

- Wenn Sie ein Upgrade auf Horizon 7 planen, führen Sie diesen Vorgang vor dem Upgrade aus, damit Sie den Dienst nicht zu oft neu starten müssen. Während eines Upgrades wird der VMware Horizon View-Verbindungsserver-Dienst neu gestartet. Ein Neustart ist auch erforderlich, um die Konfigurationsänderungen, die in dieser Vorgehensweise beschrieben werden, zu übernehmen. Wenn Sie das Upgrade vor der Durchführung dieses Vorgangs ausführen, müssen Sie den Dienst ein zweites Mal neu starten.
- Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion.

Vorgehensweise

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem Verbindungsserver-Host.
- 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 Bereich „Computer“ **localhost:389** aus oder geben Sie diesen Wert oder einen vollqualifizierten Domänennamen (FQDN) des Verbindungsserver-Hosts, gefolgt von Port 389, ein.
Beispiel: **localhost:389** oder **meincomputer.example.com:389**
- 5 Erweitern Sie den ADSI-Editor-Strukturbaum, erweitern Sie **OU=Properties**, wählen Sie **OU=Global** aus, und doppelklicken Sie auf **CN=Common** im rechten Bereich.
- 6 Im Dialogfeld „Eigenschaften“ bearbeiten Sie das Attribut **pae-ClientSSLSecureProtocols**, um die folgenden Werte hinzuzufügen:
\LIST:TLSv1.2,TLSv1.1,TLSv1
Stellen Sie sicher, dass am Anfang der Zeile ein Rückschrägstrich steht.
- 7 Klicken Sie auf **OK**.
- 8 Wenn es sich um eine Neuinstallation handelt, müssen Sie den VMware Horizon View-Verbindungsserver-Dienst auf jeder Verbindungsserver-Instanz neu starten, um die Konfigurationsänderungen zu übernehmen.
Wenn Sie ein Upgrade planen, müssen Sie den Dienst nicht neu starten, da der Dienst beim Upgrade-Vorgang automatisch neu gestartet wird.

Installieren einer replizierten Instanz von View-Verbindungsserver

Zur Bereitstellung von hoher Verfügbarkeit und Lastausgleich können Sie eine oder mehrere zusätzliche Instanzen von View-Verbindungsserver installieren, die eine vorhandene View-Verbindungsserver-Instanz replizieren. Nach einer Replikation sind die vorhandene und neu installierte Instanzen von View-Verbindungsserver identisch.

Wenn Sie eine replizierte Instanz installieren, kopiert View die View LDAP-Konfigurationsdaten von der vorhandenen View-Verbindungsserver-Instanz.

Nach der Installation werden identische View LDAP-Konfigurationsdaten auf allen View-Verbindungsserver-Instanzen in der replizierten Gruppe verwaltet. Werden an einer Instanz Änderungen vorgenommen, werden die aktualisierten Informationen auf die weiteren Instanzen kopiert.

Fällt eine replizierte Instanz aus, setzen die weiteren Instanzen in der Gruppe ihren Betrieb fort. Sobald die ausgefallene Instanz ihren Betrieb wieder aufnimmt, wird ihre Konfiguration mit den Änderungen aktualisiert, die während des Ausfalls durchgeführt wurden.

HINWEIS Diese Replikationsfunktionalität wird über View LDAP bereitgestellt, das dieselbe Replikationstechnologie verwendet wie Active Directory.

Die Replikatserver-Software darf nicht auf demselben physischen Computer bzw. derselben virtuellen Maschine installiert sein wie eine andere View-Softwarekomponente, einschließlich eines Sicherheitsservers, View-Verbindungsservers, View Composer, Horizon Agent oder Horizon Client.

Standardmäßig wird die HTML Access-Komponente auf dem View-Verbindungsserver-Host installiert, wenn Sie View-Verbindungsserver installieren. Diese Komponente konfiguriert das View-Benutzerportal, sodass ein Symbol für HTML Access zusätzlich zum Symbol für Horizon Client angezeigt wird. Über das zusätzliche Symbol können Benutzer HTML Access auswählen, wenn sie sich mit ihren Desktops verbinden.

Eine Übersicht über das Einrichten eines View-Verbindungsservers für HTML Access finden Sie unter „Vorbereiten von View-Verbindungsserver und Sicherheitsservern für HTML Access“ im Dokument *Verwenden von HTML Access* auf der Seite mit der Horizon Client-Dokumentation.

Voraussetzungen

- Stellen Sie sicher, dass mindestens eine View-Verbindungsserver-Instanz im Netzwerk installiert und konfiguriert wurde.
- Zum Installieren einer replizierten Instanz müssen Sie sich als Benutzer mit der View-Administratorrolle anmelden. Sie geben das Konto oder die Gruppe mit der View-Administratorrolle beim Installieren der ersten Instanz des View-Verbindungsservers an. Die Rolle kann der lokalen Administratorengruppe, einem Domänenbenutzer oder einer Gruppe zugewiesen werden. Siehe „[Installieren von View-Verbindungsserver mit einer neuen Konfiguration](#)“, auf Seite 59.
- Wenn sich die vorhandene View-Verbindungsserver-Instanz in einer anderen Domäne befindet als die replizierte Instanz, muss der Domänenbenutzer zusätzlich über View-Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem die vorhandene Instanz installiert ist.
- Wenn Sie die MIT-Kerberos-Authentifizierung zur Anmeldung bei einem Windows Server 2008 R2-Computer verwenden, auf dem Sie den View-Verbindungsserver installieren, installieren Sie das Microsoft-Hotfix, das im Knowledge Base-Artikel KB 978116 unter <http://support.microsoft.com/kb/978116> beschrieben ist.
- Stellen Sie sicher, dass Ihre Installation die unter „[Horizon-Verbindungsserver – Serveranforderungen](#)“, auf Seite 9 beschriebenen Anforderungen erfüllt.
- Stellen Sie sicher, dass die Computer, auf denen Sie replizierte View-Verbindungsserver-Instanzen installieren, über ein Hochleistungs-LAN miteinander verbunden sind. Siehe „[Netzwerkanforderungen für replizierte Horizon-Verbindungsserver-Instanzen](#)“, auf Seite 11.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58.
- Wenn Sie eine replizierte View-Verbindungsserver-Instanz von View 5.1 oder höher installieren und die Version der vorhandenen View-Verbindungsserver-Instanz, die Sie replizieren, View 5.0.x oder früher ist, bereiten Sie ein Kennwort für die Datenwiederherstellung vor. Siehe „[Installieren von View-Verbindungsserver mit einer neuen Konfiguration](#)“, auf Seite 59.
- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für die View-Verbindungsserver-Instanzen geöffnet werden müssen. Siehe „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81.
- Wenn Sie planen, einen Sicherheitsserver mit dieser Instanz von View-Verbindungsserver zu kombinieren, stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen einem Sicherheitsserver und der View-Verbindungsserver-Instanz enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y` die Versionsnummer.

- 2 Zum Starten des Verbindungsserver-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

- 3 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 4 Übernehmen oder ändern Sie den Zielordner.
- 5 Wählen Sie die Installationsoption **View-Replikatserver**.
- 6 Wählen Sie die Internetprotokollversion (IP) **IPv4** oder **IPv6** aus.
Sie müssen alle View-Komponenten mit derselben IP-Version installieren.
- 7 Wählen Sie aus, ob der FIPS-Modus aktiviert werden soll.
Diese Option ist nur verfügbar, wenn der FIPS-Modus in Windows aktiviert ist.
- 8 Stellen Sie sicher, dass die Option **HTML Access installieren** ausgewählt ist, wenn Benutzer die Möglichkeit haben sollen, sich über HTML Access mit ihren Desktops zu verbinden.
Wird **IPv4** ausgewählt, ist diese Einstellung standardmäßig aktiviert. Wird **IPv6** ausgewählt, wird diese Einstellung nicht angezeigt, weil HTML Access in einer IPv6-Umgebung nicht unterstützt wird.
- 9 Geben Sie den Hostnamen oder die IP-Adresse der vorhandenen View-Verbindungsserver-Instanz ein, die Sie replizieren möchten.
- 10 Geben Sie ein Kennwort für die Datenwiederherstellung und optional eine Kennwörterinnerung ein.
Sie werden nur zur Eingabe eines Kennworts für die Datenwiederherstellung aufgefordert, wenn die Version der vorhandenen View-Verbindungsserver-Instanz, die Sie replizieren möchten, View 5.0.x oder früher ist.
- 11 Wählen Sie Konfigurationsoptionen für den Windows-Firewall-Dienst aus.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen Netzwerkverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell. Aktivieren Sie diese Option nur dann, wenn Ihre Organisation ihre eigenen vordefinierten Regeln zum Konfigurieren der Windows-Firewall verwendet.

- 12 Schließen Sie die Installation der replizierten Instanz mit dem Installations-Assistenten ab.
- 13 Überprüfen Sie den Windows Server-Computer auf neue Patches und führen Sie bei Bedarf Windows Update aus.
Auch wenn Sie alle verfügbaren Patches auf dem Windows Server-Computer installiert haben, bevor Sie den View-Verbindungsserver installiert haben, wurden Betriebssystemfunktionen bei der Installation möglicherweise zum ersten Mal aktiviert. Möglicherweise sind nun zusätzliche Patches erforderlich.

Die Horizon 7-Dienste sind auf dem Windows Server-Computer installiert:

- VMware Horizon-Verbindungsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Message Bus-Komponente
- VMware Horizon View-Skriphost
- VMware Horizon View Sicherheits-Gateway-Komponente
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web-Komponente

- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Wenn die Einstellung **HTML Access installieren** bei der Installation ausgewählt wurde, wird die HTML Access-Komponente auf dem Windows Server-Computer installiert. Diese Komponente konfiguriert das Symbol für HTML Access im Horizon 7-Benutzerportal und aktiviert die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** in der Windows-Firewall. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, eine Verbindung mit dem Verbindungsserver über den TCP-Port 8443 herzustellen.

Weiter

Konfigurieren Sie ein SSL-Serverzertifikat für die View-Verbindungsserver-Instanz. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Für eine replizierte Instanz von View-Verbindungsserver müssen Sie keine anfängliche View-Konfiguration durchführen. Die replizierte Instanz erbt ihre Konfiguration von der vorhandenen View-Verbindungsserver-Instanz.

Möglicherweise müssen Sie jedoch Clientverbindungs-Einstellungen für diese View-Verbindungsserver-Instanz konfigurieren, und Sie können Windows Server-Einstellungen für die Unterstützung einer großen Bereitstellung optimieren. Siehe [„Konfigurieren von Horizon Client-Verbindungen“](#), auf Seite 128 und [„Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung“](#), auf Seite 142.

Wenn Sie den View-Verbindungsserver erneut installieren und ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

Unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, eine replizierte Instanz von View-Verbindungsserver auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Stellen Sie sicher, dass mindestens eine View-Verbindungsserver-Instanz im Netzwerk installiert und konfiguriert wurde.
- Zum Installieren einer replizierten Instanz müssen Sie sich als ein Benutzer mit Anmeldeinformationen für den Zugriff auf das View Administrators-Konto anmelden. Sie geben das View Administrators-Konto an, wenn Sie die erste Instanz von View-Verbindungsserver installieren. Das Konto kann auch das der lokalen Administratorengruppe, das eines Domänenbenutzers oder ein Gruppenkonto sein. Siehe [„Installieren von View-Verbindungsserver mit einer neuen Konfiguration“](#), auf Seite 59.
- Wenn sich die vorhandene View-Verbindungsserver-Instanz in einer anderen Domäne befindet als die replizierte Instanz, muss der Domänenbenutzer zusätzlich über View Administrator-Berechtigungen auf dem Windows Server-Computer verfügen, auf dem die vorhandene Instanz installiert ist.
- Wenn Sie die MIT-Kerberos-Authentifizierung zur Anmeldung bei einem Windows Server 2008 R2-Computer verwenden, auf dem Sie den View-Verbindungsserver installieren, installieren Sie das Microsoft-Hotfix, das im Knowledge Base-Artikel KB 978116 unter <http://support.microsoft.com/kb/978116> beschrieben ist.
- Stellen Sie sicher, dass Ihre Installation die unter [„Horizon-Verbindungsserver – Serveranforderungen“](#), auf Seite 9 beschriebenen Anforderungen erfüllt.

- Stellen Sie sicher, dass die Computer, auf denen Sie replizierte View-Verbindungsserver-Instanzen installieren, über ein Hochleistungs-LAN miteinander verbunden sind. Siehe „[Netzwerkanforderungen für replizierte Horizon-Verbindungsserver-Instanzen](#)“, auf Seite 11.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58.
- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für die View-Verbindungsserver-Instanzen geöffnet werden müssen. Siehe „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81.
- Wenn Sie planen, einen Sicherheitsserver mit dieser Instanz von View-Verbindungsserver zu kombinieren, stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen einem Sicherheitsserver und der View-Verbindungsserver-Instanz enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „[Befehlszeilenoptionen für Microsoft Windows Installer](#)“, auf Seite 84.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver vertraut. Siehe „[Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver](#)“, auf Seite 72.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y.y` die Versionsnummer.

- 2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.
- 3 Geben Sie den Installationsbefehl in einer Zeile ein.

Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`

Wenn Sie eine replizierte View-Verbindungsserver-Instanz von View 5.1 oder höher installieren und die Version der vorhandenen View-Verbindungsserver-Instanz, die Sie replizieren, View 5.0.x oder früher lautet, müssen Sie ein Kennwort für die Datenwiederherstellung angeben, und Sie können eine Kennworterinnerung hinzufügen. Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car""`

WICHTIG Wenn Sie eine unbeaufsichtigte Installation durchführen, wird die gesamte Befehlszeile, einschließlich des Kennworts für die Datenwiederherstellung, in der Datei `vminst.log` des Installationsprogramms protokolliert. Nach Abschluss der Installation löschen Sie diese Protokolldatei oder ändern Sie das Kennwort für die Datenwiederherstellung in View Administrator.

- 4 Überprüfen Sie den Windows Server-Computer auf neue Patches und führen Sie bei Bedarf Windows Update aus.

Auch wenn Sie alle verfügbaren Patches auf dem Windows Server-Computer installiert haben, bevor Sie den View-Verbindungsserver installiert haben, wurden Betriebssystemfunktionen bei der Installation möglicherweise zum ersten Mal aktiviert. Möglicherweise sind nun zusätzliche Patches erforderlich.

Die Horizon 7-Dienste sind auf dem Windows Server-Computer installiert:

- VMware Horizon-Verbindungsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Message Bus-Komponente
- VMware Horizon View-Skripthost
- VMware Horizon View Sicherheits-Gateway-Komponente
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web-Komponente
- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Wenn die Einstellung **HTML Access installieren** bei der Installation ausgewählt wurde, wird die HTML Access-Komponente auf dem Windows Server-Computer installiert. Diese Komponente konfiguriert das Symbol für HTML Access im Horizon 7-Benutzerportal und aktiviert die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** in der Windows-Firewall. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, eine Verbindung mit dem Verbindungsserver über den TCP-Port 8443 herzustellen.

Weiter

Konfigurieren Sie ein SSL-Serverzertifikat für die View-Verbindungsserver-Instanz. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Für eine replizierte Instanz von View-Verbindungsserver müssen Sie keine anfängliche View-Konfiguration durchführen. Die replizierte Instanz erbt ihre Konfiguration von der vorhandenen View-Verbindungsserver-Instanz.

Möglicherweise müssen Sie jedoch Clientverbindungs-Einstellungen für diese View-Verbindungsserver-Instanz konfigurieren, und Sie können Windows Server-Einstellungen für die Unterstützung einer großen Bereitstellung optimieren. Siehe [„Konfigurieren von Horizon Client-Verbindungen“](#), auf Seite 128 und [„Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung“](#), auf Seite 142.

Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver über die Befehlszeile ausführen. Sie müssen das Format *PROPERTY=value* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 7-2. MSI-Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View-Verbindungsserver-Software installiert wird. Beispiel: <code>INSTALLDIR=""D:\abc\mein Ordner""</code> Die Paare doppelter Anführungszeichen, die den Pfad umschließen, ermöglichen es dem MSI Installer, das Leerzeichen als gültigen Teil des Pfades zu interpretieren. Diese MSI-Eigenschaft ist optional.	%ProgramFiles %\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	Die Art der View Server-Installation: <ul style="list-style-type: none"> ■ 1. Standardinstallation ■ 2. Replikationinstallation ■ 3. Sicherheitsserverinstallation Für die Installation einer replizierten Instanz verwenden Sie <code>VDM_SERVER_INSTANCE_TYPE=2</code> Diese MSI-Eigenschaft ist bei der Installation eines Replikats erforderlich.	1
ADAM_PRIMARY_NAME	Der Hostname oder die IP-Adresse der vorhandenen View-Verbindungsserver-Instanz, die Sie replizieren möchten. Zum Beispiel: <code>ADAM_PRIMARY_NAME=cs1.companydomain.com</code> Diese MSI-Eigenschaft ist erforderlich.	Keine.
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View-Verbindungsserver-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall konfiguriert. Mit dem Wert 2 wird keine Firewall konfiguriert. Zum Beispiel: <code>FWCHOICE=1</code> Diese MSI-Eigenschaft ist optional.	1
VDM_SERVER_RECOVERY_PWD	Das Kennwort für die Datenwiederherstellung. Wenn in View LDAP kein Kennwort für die Datenwiederherstellung festgelegt ist, muss diese Eigenschaft verwendet werden. HINWEIS Das Kennwort für die Datenwiederherstellung wird in View LDAP nicht festgelegt, wenn es sich bei der standardmäßigen View-Verbindungsserver-Instanz, die repliziert wird, um eine Instanz der View-Version 5.0 oder früher handelt. Wenn es sich bei der zu replizierenden View-Verbindungsserver-Instanz um View 5.1 oder höher handelt, muss diese Eigenschaft nicht angegeben werden. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.	Keine.
VDM_SERVER_RECOVERY_PWD_REMINDER	Die Kennwörterinnerung für die Datenwiederherstellung. Diese Eigenschaft ist optional.	Keine.

Tabelle 7-2. MSI-Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View-Verbindungsserver (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
VDM_IP_PROTOCOL_NUTZUNG	Gibt die IP-Version an, die von View-Komponenten für die Kommunikation verwendet wird. Mögliche Werte sind IPv4 und IPv6 .	IPv4
VDM_FIPS_ENABLED	Geben Sie an, ob der FIPS-Modus aktiviert werden soll. Der Wert 1 aktiviert den FIPS-Modus. Der Wert 0 deaktiviert den FIPS-Modus. Wenn für diese Eigenschaft 1 gewählt wurde und Windows sich nicht im FIPS-Modus befindet, wird der Installationsvorgang abgebrochen.	0

Konfigurieren eines Kennworts für die Kombination mit einem Sicherheitsserver

Bevor Sie einen Sicherheitsserver installieren können, müssen Sie ein Kennwort für die Kombination mit dem Sicherheitsserver konfigurieren. Wenn Sie mit dem View-Verbindungsserver-Installationsprogramm einen Sicherheitsserver installieren, fordert Sie das Programm während der Installation auf, dieses Kennwort einzugeben.

Das Kennwort für die Kombination mit dem Sicherheitsserver ist ein einmaliges Kennwort, das einem Sicherheitsserver die Kombination mit einer View-Verbindungsserver-Instanz ermöglicht. Das Kennwort läuft ab, nachdem Sie es im View-Verbindungsserver-Installationsprogramm angegeben haben.

HINWEIS Sie können keine ältere Version des Sicherheitsservers mit der aktuellen Version des View-Verbindungsservers kombinieren. Wenn Sie ein Kennwort für die Kombination in der aktuellen Version des View-Verbindungsservers konfigurieren und versuchen, eine ältere Version des Sicherheitsservers zu installieren, wird das Kennwort für die Kombination ungültig.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server**.
- 2 Wählen Sie auf der Registerkarte für Verbindungsserver die View-Verbindungsserver-Instanz, die mit dem Sicherheitsserver kombiniert werden soll.
- 3 Wählen Sie im Dropdown-Menü **Weitere Befehle** die Einstellung **Kennwort für die Sicherheitsserver-Kombination angeben**.
- 4 Geben Sie das Kennwort in den Textfeldern Kennwort für Kombination und Kennwort bestätigen ein und geben Sie einen Zeitüberschreitungswert für das Kennwort ein.
Sie müssen das Kennwort innerhalb der angegebenen Zeitspanne verwenden.
- 5 Klicken Sie auf **OK**, um das Kennwort zu konfigurieren.

Weiter

Installieren Sie einen Sicherheitsserver. Siehe „[Installieren eines Sicherheitsservers](#)“, auf Seite 74.

WICHTIG Wenn Sie das Kennwort für die Kombination mit dem Sicherheitsserver nicht innerhalb des angegebenen Zeitraums im View-Verbindungsserver-Installationsprogramm angeben, wird das Kennwort ungültig und Sie müssen ein neues Kennwort konfigurieren.

Installieren eines Sicherheitsservers

Ein Sicherheitsserver ist eine Instanz von View-Verbindungsserver, die einen zusätzlichen Sicherheits-Layer zwischen dem Internet und Ihrem internen Netzwerk hinzufügt. Sie können einen oder mehrere Sicherheitsserver installieren, die mit einer View-Verbindungsserver-Instanz verbunden werden.

Die Sicherheitsserver-Software darf nicht auf demselben physischen Computer bzw. derselben virtuellen Maschine installiert sein wie eine andere View-Softwarekomponente, einschließlich eines Replikatsservers, View-Verbindungsservers, View Composer, Horizon Agent oder Horizon Client.

Voraussetzungen

- Legen Sie fest, welche Topologie verwendet werden soll. Sie können sich beispielsweise für eine bestimmte Lastenausgleichslösung entscheiden. Entscheiden Sie, ob die mit Sicherheitsservern gekoppelten Verbindungsserver-Instanzen für Benutzer des externen Netzwerks reserviert werden sollen. Weitere Informationen finden Sie im Dokument *Planung der View-Architektur*.

WICHTIG Wenn Sie einen Lastausgleichsdienst verwenden, benötigt er eine IP-Adresse, die nicht geändert wird. In einer IPv4-Umgebung konfigurieren Sie eine statische IP-Adresse. In einer IPv6-Umgebung erhalten Computer automatisch IP-Adressen, die nicht geändert werden.

- Stellen Sie sicher, dass Ihre Installation die unter „[Horizon-Verbindungsserver – Serveranforderungen](#)“, auf Seite 9 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58.
- Stellen Sie sicher, dass die Verbindungsserver-Instanz, die mit dem Sicherheitsserver gekoppelt werden soll, installiert und konfiguriert ist und eine Verbindungsserver-Version ausführt, die mit der Version des Sicherheitsservers kompatibel ist. Einzelheiten finden Sie in der „[Kompatibilitätstabelle für View-Komponenten](#)“ im Dokument *View-Upgrades*.
- Stellen Sie sicher, dass der Computer, auf dem Sie den Sicherheitsserver installieren möchten, auf die mit dem Sicherheitsserver zu koppelnde Verbindungsserver-Instanz zugreifen kann.
- Konfigurieren Sie ein Kennwort für die Paarbildung mit dem Sicherheitsserver. Siehe „[Konfigurieren eines Kennworts für die Kombination mit einem Sicherheitsserver](#)“, auf Seite 73.
- Machen Sie sich mit dem Format externer URLs vertraut. Siehe „[Konfigurieren externer URLs für sichere Gateways und Tunnelverbindungen](#)“, auf Seite 131.
- Stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für einen Sicherheitsserver geöffnet werden müssen. Siehe „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen dem Sicherheitsserver und dem View-Verbindungsserver enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.
- Wenn Sie den Sicherheitsserver aktualisieren oder neu installieren, überprüfen Sie, ob die vorhandenen IPsec-Regeln für den Sicherheitsserver entfernt wurden. Siehe „[Entfernen von IPsec-Regeln für Sicherheitsserver](#)“, auf Seite 80.
- Wenn Sie View im FIPS-Modus installieren, müssen Sie die Auswahl der globalen Einstellung **IPSec für Sicherheitsserververbindungen verwenden** in View Administrator aufheben, da im FIPS-Modus IPSec nach der Installation eines Sicherheitsservers manuell konfiguriert werden muss.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y.y` die Versionsnummer.

- 2 Zum Starten des Verbindungsserver-Installationsprogramms doppelklicken Sie auf die Installationsdatei.
- 3 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 4 Übernehmen oder ändern Sie den Zielordner.
- 5 Wählen Sie die Installationsoption **View-Sicherheitsserver**.
- 6 Wählen Sie die Internetprotokollversion (IP) **IPv4** oder **IPv6** aus.

Sie müssen alle View-Komponenten mit derselben IP-Version installieren.

- 7 Wählen Sie aus, ob der FIPS-Modus aktiviert werden soll.

Diese Option ist nur verfügbar, wenn der FIPS-Modus in Windows aktiviert ist.

- 8 Geben Sie den vollqualifizierten Domännennamen oder die IP-Adresse der für die Paarbildung mit dem Sicherheitsserver vorgesehenen View-Verbindungsserver-Instanz im Textfeld **Server** ein.

Der Sicherheitsserver leitet den Netzwerkdatenverkehr an diese View-Verbindungsserver-Instanz weiter.

- 9 Geben Sie das Kennwort für die Paarbildung mit dem Sicherheitsserver in das Textfeld **Kennwort** ein.

Wenn das Kennwort abgelaufen ist, können Sie mit View Administrator ein neues Kennwort konfigurieren und das neue Kennwort im Installationsprogramm angeben.

- 10 Geben Sie in das Textfeld **Externe URL** die externe URL des Sicherheitsservers für Client-Endpunkte ein, die das RDP- oder das PCoIP-Anzeigeprotokoll verwenden.

Die URL muss das Protokoll, den durch den Client auflösbaren Namen des Sicherheitsservers sowie die Portnummer enthalten. Tunnelclients, die außerhalb Ihres Netzwerks ausgeführt werden, verwenden diese URL zur Verbindungsherstellung mit dem Sicherheitsserver.

Beispiel: `https://view.example.com:443`

- 11 Geben Sie in das Textfeld **PCoIP – Externe URL** die externe URL des Sicherheitsservers für Client-Endpunkte ein, die das PCoIP-Anzeigeprotokoll verwenden.

Geben Sie in einer IPv4-Umgebung die externe PCoIP-URL in Form einer IP-Adresse mit der Portnummer 4172 an. In einer IPv6-Umgebung können Sie eine IP-Adresse oder einen vollqualifizierten Domännennamen und die Portnummer 4172 angeben. In beiden Fällen geben Sie keinen Protokollnamen an.

Beispiel für eine IPv4-Umgebung: `10.20.30.40:4172`

Clients müssen die URL verwenden können, um den Sicherheitsserver zu erreichen.

- 12 Geben Sie in das Textfeld **Externe Blast-URL** die externe URL des Sicherheitsservers für Benutzer ein, die HTML Access für die Verbindung mit Remote-Desktops verwenden.

Die URL muss das HTTPS-Protokoll, den durch den Client auflösbaren Hostnamen sowie die Portnummer enthalten.

Beispiel: `https://myserver.example.com:8443`

Standardmäßig schließt die URL den FQDN der externen URL für den sicheren Tunnel sowie die standardmäßige Portnummer 8443 ein. Die URL muss den FQDN und die Portnummer enthalten, über die ein Clientsystem diesen Sicherheitsserver erreichen kann.

- 13 Wählen Sie Konfigurationsoptionen für den Windows-Firewall-Dienst aus.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen Netzwerkverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell. Aktivieren Sie diese Option nur dann, wenn Ihre Organisation ihre eigenen vordefinierten Regeln zum Konfigurieren der Windows-Firewall verwendet.

- 14 Schließen Sie die Installation des Sicherheitsservers mit dem Installations-Assistenten ab.

Die Dienste für den Sicherheitsserver werden auf dem Windows Server-Computer installiert:

- VMware Horizon View-Sicherheitsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Sicherheits-Gateway-Komponente
- VMware Horizon View PCoIP Secure Gateway
- VMware Blast Secure Gateway

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Der Sicherheitsserver erscheint im Fensterbereich „Sicherheitsserver“ von View Administrator.

Die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** ist in der Windows-Firewall auf dem Sicherheitsserver aktiviert. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, mithilfe von HTML Access eine Verbindung mit dem Sicherheitsserver über den TCP-Port 8443 herzustellen.

HINWEIS Wenn die Installation vom Benutzer oder anderweitig abgebrochen wurde, müssen Sie möglicherweise IPsec-Regeln für den Sicherheitsserver entfernen, bevor Sie die Installation neu starten können. Führen Sie diesen Schritt auch dann durch, wenn Sie IPsec-Regeln bereits vor der erneuten Installation oder dem Upgrade des Sicherheitsservers entfernt haben. Anleitungen zum Entfernen von IPsec-Regeln finden Sie unter „[Entfernen von IPsec-Regeln für Sicherheitsserver](#)“, auf Seite 80.

Weiter

Konfigurieren Sie ein SSL-Serverzertifikat für den Sicherheitsserver. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Möglicherweise müssen Sie Clientverbindungs-Einstellungen für den Sicherheitsserver konfigurieren, und Sie können Windows Server-Einstellungen für die Unterstützung einer großen Bereitstellung optimieren. Siehe „[Konfigurieren von Horizon Client-Verbindungen](#)“, auf Seite 128 und „[Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung](#)“, auf Seite 142.

Wenn Sie den Sicherheitsserver erneut installieren und ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

Unbeaufsichtigte Installation eines Sicherheitservers

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, einen Sicherheitsserver auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Legen Sie fest, welche Topologie verwendet werden soll. Sie können sich beispielsweise für eine bestimmte Lastenausgleichslösung entscheiden. Entscheiden Sie, ob die mit Sicherheitsservern gekoppelten Verbindungsserver-Instanzen für Benutzer des externen Netzwerks reserviert werden sollen. Weitere Informationen finden Sie im Dokument *Planung der View-Architektur*.

WICHTIG Wenn Sie einen Lastausgleichsdienst verwenden, benötigt er eine IP-Adresse, die nicht geändert wird. In einer IPv4-Umgebung konfigurieren Sie eine statische IP-Adresse. In einer IPv6-Umgebung erhalten Computer automatisch IP-Adressen, die nicht geändert werden.

- Stellen Sie sicher, dass Ihre Installation die unter „[Horizon-Verbindungsserver – Serveranforderungen](#)“, auf Seite 9 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „[Installationsvoraussetzungen für View-Verbindungsserver](#)“, auf Seite 58.
- Stellen Sie sicher, dass die Verbindungsserver-Instanz, die mit dem Sicherheitsserver gekoppelt werden soll, installiert und konfiguriert ist und eine Verbindungsserver-Version ausführt, die mit der Version des Sicherheitservers kompatibel ist. Einzelheiten finden Sie in der „Kompatibilitätstabelle für View-Komponenten“ im Dokument *View-Upgrades*.
- Stellen Sie sicher, dass der Computer, auf dem Sie den Sicherheitsserver installieren möchten, auf die mit dem Sicherheitsserver zu koppelnde Verbindungsserver-Instanz zugreifen kann.
- Konfigurieren Sie ein Kennwort für die Paarbildung mit dem Sicherheitsserver. Siehe „[Konfigurieren eines Kennworts für die Kombination mit einem Sicherheitsserver](#)“, auf Seite 73.
- Machen Sie sich mit dem Format externer URLs vertraut. Siehe „[Konfigurieren externer URLs für sichere Gateways und Tunnelverbindungen](#)“, auf Seite 131.
- Stellen Sie sicher, dass in den aktiven Protokollen „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist. Es wird empfohlen, diese Einstellung für alle Profile zu **aktivieren**. Standardmäßig gelten IPsec-Regeln für Verbindungen zwischen dem Sicherheitsserver und dem View-Verbindungsserver und erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Machen Sie sich mit den Netzwerkports vertraut, die in der Windows-Firewall für einen Sicherheitsserver geöffnet werden müssen. Siehe „[Firewall-Regeln für View-Verbindungsserver](#)“, auf Seite 81.
- Wenn Ihre Netzwerktopologie eine Back-End-Firewall zwischen dem Sicherheitsserver und dem View-Verbindungsserver enthält, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe „[Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec](#)“, auf Seite 82.
- Wenn Sie den Sicherheitsserver aktualisieren oder neu installieren, überprüfen Sie, ob die vorhandenen IPsec-Regeln für den Sicherheitsserver entfernt wurden. Siehe „[Entfernen von IPsec-Regeln für Sicherheitsserver](#)“, auf Seite 80.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „[Befehlszeilenoptionen für Microsoft Windows Installer](#)“, auf Seite 84.

- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers vertraut. Siehe „[Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers](#)“, auf Seite 79.
- Wenn Sie View im FIPS-Modus installieren, müssen Sie die Auswahl der globalen Einstellung **IPSec für Sicherheitsserververbindungen verwenden** in View Administrator aufheben, da im FIPS-Modus IPSec nach der Installation eines Sicherheitsservers manuell konfiguriert werden muss.

Vorgehensweise

- 1 Laden Sie die Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

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

Der Dateiname des Installationsprogramms lautet `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`. Hierbei ist `xxxxxx` die Buildnummer und `y.y.y` die Versionsnummer.

- 2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.
- 3 Geben Sie den Installationsbefehl in einer Zeile ein.

```
Beispiel: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:
443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SER-
VER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443
VDM_SERVER_SS_PWD=secret"
```

Die Dienste für den Sicherheitsserver werden auf dem Windows Server-Computer installiert:

- VMware Horizon View-Sicherheitsserver
- VMware Horizon View Framework-Komponente
- VMware Horizon View Sicherheits-Gateway-Komponente
- VMware Horizon View PCoIP Secure Gateway
- VMware Blast Secure Gateway

Informationen zu diesen Diensten finden Sie im Dokument *Administration von View*.

Der Sicherheitsserver erscheint im Fensterbereich „Sicherheitsserver“ von View Administrator.

Die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** ist in der Windows-Firewall auf dem Sicherheitsserver aktiviert. Diese Firewallregel ermöglicht es Webbrowsern auf Clientgeräten, mithilfe von HTML Access eine Verbindung mit dem Sicherheitsserver über den TCP-Port 8443 herzustellen.

HINWEIS Wenn die Installation vom Benutzer oder anderweitig abgebrochen wurde, müssen Sie möglicherweise IPsec-Regeln für den Sicherheitsserver entfernen, bevor Sie die Installation neu starten können. Führen Sie diesen Schritt auch dann durch, wenn Sie IPsec-Regeln bereits vor der erneuten Installation oder dem Upgrade des Sicherheitsservers entfernt haben. Anleitungen zum Entfernen von IPsec-Regeln finden Sie unter „[Entfernen von IPsec-Regeln für Sicherheitsserver](#)“, auf Seite 80.

Weiter

Konfigurieren Sie ein SSL-Serverzertifikat für den Sicherheitsserver. Siehe [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Möglicherweise müssen Sie Clientverbindungs-Einstellungen für den Sicherheitsserver konfigurieren, und Sie können Windows Server-Einstellungen für die Unterstützung einer großen Bereitstellung optimieren. Siehe „[Konfigurieren von Horizon Client-Verbindungen](#)“, auf Seite 128 und „[Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung](#)“, auf Seite 142.

Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation eines Sicherheitsservers über die Befehlszeile ausführen. Sie müssen das Format *PROPERTY=value* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 7-3. MSI-Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View-Verbindungsserver-Software installiert wird. Beispiel: <code>INSTALLDIR=""D:\abc\mein Ordner""</code> Die Paare doppelter Anführungszeichen, die den Pfad umschließen, ermöglichen es dem MSI Installer, das Leerzeichen als gültigen Teil des Pfades zu interpretieren. Diese MSI-Eigenschaft ist optional.	%ProgramFiles %VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	Die Art der View Server-Installation: <ul style="list-style-type: none"> ■ 1. Standardinstallation ■ 2. Replikainstallation ■ 3. Sicherheitsserverinstallation Für die Installation eines Sicherheitsservers verwenden Sie <code>VDM_SERVER_INSTANCE_TYPE=3</code> Diese MSI-Eigenschaft ist bei der Installation eines Sicherheitsservers erforderlich.	1
VDM_SERVER_NAME	Der Hostname oder die IP-Adresse der vorhandenen View-Verbindungsserver-Instanz, die ein Paar mit dem Sicherheitsserver bildet. Zum Beispiel: <code>VDM_SERVER_NAME=cs1.internaldomain.com</code> Diese MSI-Eigenschaft ist erforderlich.	Keine.
VDM_SERVER_SS_EXTURL	Die externe URL des Sicherheitsservers. Die URL muss das Protokoll, den extern auflösbaren Namen des Sicherheitsservers und die Portnummer enthalten. Zum Beispiel: <code>VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443</code> Diese MSI-Eigenschaft ist erforderlich.	Keine.
VDM_SERVER_SS_PWD	Das Kennwort für die Paarbildung mit dem Sicherheitsserver. Zum Beispiel: <code>VDM_SERVER_SS_PWD=secret</code> Diese MSI-Eigenschaft ist erforderlich.	Keine.
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View-Verbindungsserver-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall konfiguriert. Mit dem Wert 2 wird keine Firewall konfiguriert. Zum Beispiel: <code>FWCHOICE=1</code> Diese MSI-Eigenschaft ist optional.	1
VDM_SERVER_SS_PCOIP_IPADDR	Die externe IP-Adresse des PCoIP Secure Gateway. In einer IPv6-Umgebung kann diese Eigenschaft auch auf den FQDN des PCoIP Secure Gateway festgelegt werden. Diese Eigenschaft wird nur unterstützt, wenn der Sicherheitsserver auf Windows Server 2008 R2 oder höher installiert ist. Zum Beispiel: <code>VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40</code> Diese Eigenschaft ist erforderlich, wenn Sie planen, die PCoIP Secure Gateway-Komponente zu verwenden.	Keine.

Tabelle 7-3. MSI-Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
VDM_SERVER_SS_PCO- IP_TCPPORT	Die externe TCP-Portnummer des PCoIP Secure Gateway. Diese Eigenschaft wird nur unterstützt, wenn der Sicherheitsserver auf Windows Server 2008 R2 oder höher installiert ist. Zum Beispiel: VDM_SERVER_SS_PCOIP_TCPPORT=4172 Diese Eigenschaft ist erforderlich, wenn Sie planen, die PCoIP Secure Gateway-Komponente zu verwenden.	Keine.
VDM_SERVER_SS_PCO- IP_UDPPORT	Die externe UDP-Portnummer des PCoIP Secure Gateway. Diese Eigenschaft wird nur unterstützt, wenn der Sicherheitsserver auf Windows Server 2008 R2 oder höher installiert ist. Zum Beispiel: VDM_SERVER_SS_PCOIP_UDPPORT=4172 Diese Eigenschaft ist erforderlich, wenn Sie planen, die PCoIP Secure Gateway-Komponente zu verwenden.	Keine.
VDM_SERVER_SS_BSG_EX- TURL	Die externe URL für das Blast Secure Gateway. Die URL muss das HTTPS-Protokoll, einen extern auflösbaren Namen des Sicherheitsservers und die Portnummer enthalten. Zum Beispiel: VDM_SERVER_SS_BSG_EXTURL=https://view.company-domain.com:8443 Die standardmäßige Portnummer lautet 8443. Das Blast Secure Gateway muss auf dem Sicherheitsserver installiert werden, damit Benutzer Internetverbindungen mit View-Desktops herstellen können.	Keine.
VDM_SERVER_SS_FORCE_IPSEC	Erzwingt die Verwendung von IPsec zwischen dem Sicherheitsserver und der View-Verbindungsserver-Instanz, mit der der Sicherheitsserver kombiniert ist. Wenn eine unbeaufsichtigte Installation und Kombination für einen Sicherheitsserver und eine View-Verbindungsserver-Instanz durchgeführt wird, ohne IPsec zu aktivieren, schlägt die Kombination fehl. Mit dem Standardwert 1 wird die IPsec-Kombination erzwungen. Legen Sie diesen Wert auf 0 fest, um eine Kombination ohne IPsec zuzulassen.	1
VDM_IP_PROTOCOL_USA- GE	Gibt die IP-Version an, die von View-Komponenten für die Kommunikation verwendet wird. Mögliche Werte sind IPv4 und IPv6 .	IPv4
VDM_FIPS_ENABLED	Geben Sie an, ob der FIPS-Modus aktiviert werden soll. Der Wert 1 aktiviert den FIPS-Modus. Der Wert 0 deaktiviert den FIPS-Modus. Wenn für diese Eigenschaft 1 gewählt wurde und Windows sich nicht im FIPS-Modus befindet, wird der Installationsvorgang abgebrochen.	0

Entfernen von IPsec-Regeln für Sicherheitsserver

Bevor Sie eine Sicherheitsserver-Instanz aktualisieren oder neu installieren, müssen Sie die aktuellen IPsec-Regeln entfernen, welche die Kommunikation zwischen dem Sicherheitsserver und der dazugehörigen View-Verbindungsserver-Instanz regeln. Wenn Sie diesen Schritt nicht vollziehen, schlägt die Aktualisierung oder die Neuinstallation fehl.

Standardmäßig wird die Kommunikation zwischen einem Sicherheitsserver und der dazugehörigen View-Verbindungsserver-Instanz durch IPsec Regeln gesteuert. Wenn Sie den Sicherheitsserver aktualisieren oder installieren und wieder mit der View-Verbindungsserver-Instanz kombinieren, muss ein neuer Satz von IPsec-Regeln eingerichtet werden. Wenn die vorhandenen IPsec-Regeln nicht entfernt werden, bevor Sie aktualisieren oder neu installieren, schlägt die Paarung fehl.

Sie müssen diesen Schritt vollziehen, wenn Sie einen Sicherheitsserver aktualisieren oder neu installieren und IPsec verwenden, um die Kommunikation zwischen dem Sicherheitsserver und dem View-Verbindungsserver zu schützen.

Sie können eine erste Sicherheitsserverpaarung ohne IPsec-Regeln konfigurieren. Bevor Sie den Sicherheitsserver installieren, können Sie View Administrator öffnen, und die globale Einstellung **Verwenden von IPsec für Sicherheitsserververbindungen** deaktivieren, die standardmäßig aktiviert ist. Wenn keine IPsec-Regeln in Kraft sind, müssen Sie sie vor der Aktualisierung oder Neuinstallation nicht entfernen.

HINWEIS Sie müssen einen Sicherheitsserver nicht aus View Administrator entfernen, bevor Sie den Sicherheitsserver aktualisieren oder installieren. Entfernen Sie einen Sicherheitsserver aus View Administrator nur dann, wenn Sie den Sicherheitsserver dauerhaft aus der View-Umgebung entfernen wollen.

Bei View 5.0.x und früheren Versionen konnten Sie einen Sicherheitsserver entweder aus der View Administrator-Benutzeroberfläche oder über die `vdmadmin -S` Befehlszeile entfernen. Bei View 5.1 und höheren Versionen müssen Sie `vdmadmin -S` benutzen. Siehe „Entfernen des Eintrags für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option -S“ im Dokument *View Administration (Verwaltung)*.



VORSICHT Wenn Sie die IPsec-Regeln für einen aktiven Sicherheitsserver entfernen, verlieren Sie solange die gesamte Kommunikation mit dem Sicherheitsserver, bis Sie den Sicherheitsserver wieder installieren. Aus diesem Grund sollten Sie, wenn Sie eine Gruppe von Sicherheitsservern mithilfe eines Lastausgleichsdienstes verwalten, diese Schritte auf einem Server ausführen und für diesen Server dann ein Upgrade durchführen, bevor Sie die IPsec-Regeln für den nächsten Server entfernen. Sie können Server aus der Produktion entfernen und diese dann erneut einzeln in dieser Weise hinzufügen, um Ausfallzeiten für Ihre Endbenutzer zu vermeiden.

Vorgehensweise

- 1 Klicken Sie in View Administrator auf **View-Konfiguration > Server**.
- 2 In der Registerkarte **Sicherheitsserver** wählen Sie einen Sicherheitsserver aus und klicken auf **Weitere Befehle > Auf Aktualisierung oder Neuinstallation vorbereiten**.

Wenn Sie IPsec-Regeln deaktiviert haben, bevor Sie den Sicherheitsserver installierten, ist diese Einstellung inaktiv. In diesem Fall müssen Sie keine IPsec-Regeln entfernen, bevor Sie neu installieren oder aktualisieren.

- 3 Klicken Sie auf **OK**.

Die IPsec-Regeln werden entfernt und die Einstellung **Auf Aktualisierung oder Neuinstallation vorbereiten** wird inaktiv, was anzeigt, dass Sie den Sicherheitsserver installieren oder aktualisieren können.

Weiter

Aktualisierung oder Neuinstallation des Sicherheitsservers.

Firewall-Regeln für View-Verbindungsserver

Bestimmte Ports müssen an der Firewall für View-Verbindungsserver-Instanzen und Sicherheitsserver geöffnet werden.

Wenn Sie View-Verbindungsserver installieren, kann das Installationsprogramm optional die erforderlichen Regeln für die Windows-Firewall für Sie konfigurieren. Mit diesen Regeln werden die standardmäßig verwendeten Ports geöffnet. Wenn Sie nach der Installation die Standardports ändern, müssen Sie die Windows-Firewall manuell konfigurieren, damit Horizon Client-Geräte über die aktualisierten Ports eine Verbindung mit View herstellen können.

Die folgende Tabelle enthält eine Aufstellung der Standardports, die automatisch während der Installation geöffnet werden können. Wenn nicht anders angegeben, handelt es sich hierbei um eingehende Ports.

Tabelle 7-4. Ports, die während der View-Verbindungsserver-Installation geöffnet werden

Protokoll	Ports	Typ der View-Verbindungsserver-Instanz
JMS	TCP 4001	Standard- und Replikatserver
JMS	TCP 4002	Standard- und Replikatserver
JMSIR	TCP 4100	Standard- und Replikatserver
JMSIR	TCP 4101	Standard- und Replikatserver
AJP13	TCP 8009	Standard- und Replikatserver
HTTP	TCP 80	Standard-, Replikat- und Sicherheitsserver
HTTPS	TCP 443	Standard-, Replikat- und Sicherheitsserver
PCoIP	TCP 4172 eingehend; UDP 4172 beide Richtungen	Standard-, Replikat- und Sicherheitsserver
HTTPS	TCP 8443 UDP 8443	Standard-, Replikat- und Sicherheitsserver. Nachdem die erste Verbindung mit View hergestellt worden ist, stellt der Webbrowser oder das Clientgerät eine Verbindung mit dem Blast Secure Gateway an TCP-Port 8443 her. Die zweite Verbindung kann nur hergestellt werden, wenn das Blast Secure Gateway auf einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz aktiviert ist.
HTTPS	TCP 8472	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die podübergreifende Kommunikation verwendet.
HTTP	TCP 22389	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die globale LDAP-Replikation verwendet.
HTTPS	TCP 22636	Standard- und Replikatserver Für die Funktion Cloud-Pod-Architektur: für die sichere globale LDAP-Replikation verwendet.

Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec

Wenn Ihre Netzwerk-Topologie eine Back-End-Firewall zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen enthält, müssen Sie die Firewall so konfigurieren, dass bestimmte Protokolle und Ports diese IPsec unterstützen. Ohne ordnungsgemäße Konfiguration lässt die Firewall Daten, die zwischen einem Sicherheitsserver und der View-Verbindungsserver-Instanz gesendet werden, nicht passieren.

Standardmäßig steuern IPsec-Regeln die Verbindungen zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen. Zur Unterstützung von IPsec kann das View-Verbindungsserver-Installationsprogramm die Windows-Firewallregeln auf den Windows Server-Hosts konfigurieren, auf denen View servers installiert sind. Für eine Back-End-Firewall müssen Sie die Regeln selbst konfigurieren.

HINWEIS Es wird dringend empfohlen, IPsec zu verwenden. Alternativ dazu können Sie die globale Einstellung **IPSec für Sicherheitsserver-Verbindungen verwenden** von View Administrator deaktivieren.

Die folgenden Regeln müssen bidirektionalen Datenverkehr zulassen. Möglicherweise müssen Sie separate Regeln für eingehenden und ausgehenden Datenverkehr auf Ihrer Firewall angeben.

Für Firewalls mit bzw. ohne Netzwerkadressübersetzung (Network Address Translation, NAT) gelten jeweils andere Regeln.

Tabelle 7-5. Unterstützung von IPsec-Regeln bei Firewall-Anforderungen ohne NAT

Quelle	Protokoll	Port	Ziel	Hinweise
Sicherheitsserver	ISAKMP	UDP 500	View-Verbindungsserver	Sicherheitsserver verwenden die UDP-Portnummer 500 zum Aushandeln der IPsec-Sicherheit.
Sicherheitsserver	ESP	–	View-Verbindungsserver	Das ESP-Protokoll kapselt IPsec-verschlüsselten Datenverkehr ein. Sie müssen als Teil der Regel keinen Port für ESP angeben. Falls nötig können Sie Quell- und Ziel-IP-Adressen angeben, um den Geltungsbereich der Regel zu verkleinern.

Die folgenden Regeln gelten für Firewalls, die NAT verwenden.

Tabelle 7-6. Anforderungen an NAT-Firewalls für die Unterstützung von IPsec-Regel

Quelle	Protokoll	Port	Ziel	Hinweise
Sicherheitsserver	ISAKMP	UDP 500	View-Verbindungsserver	Sicherheitsserver verwenden die UDP-Portnummer 500, um die Aushandlung der IPsec-Sicherheit zu initiieren.
Sicherheitsserver	NAT-T ISAKMP	UDP 4500	View-Verbindungsserver	Sicherheitsserver verwenden die UDP-Portnummer 4500 zum Durchlaufen von NATs und zum Aushandeln der IPsec-Sicherheit.

Erneutes Installieren eines View-Verbindungsservers mit einer Sicherungskonfiguration

In bestimmten Situationen müssen Sie die aktuelle Version der View-Verbindungsserver-Instanz neu installieren und die vorhandene View-Konfiguration wiederherstellen, indem Sie eine LDIF-Sicherungsdatei mit den View LDAP-Konfigurationsdaten importieren.

Beispielsweise sollten Sie als Teil eines Business Continuity- und Disaster Recovery-Plans (BC/DR) über eine definierte Vorgehensweise für den Fall verfügen, dass ein Rechenzentrum nicht mehr ordnungsgemäß funktioniert. Dabei sollten Sie zunächst sicherstellen, dass die View LDAP-Konfiguration an einem anderen Standort gesichert wird. Der zweite Schritt ist die Installation des View-Verbindungsservers an einem neuen Standort und das Importieren der Sicherungskonfiguration, wie in dieser Vorgehensweise beschrieben.

Sie sollten diese Schritte gegebenenfalls auch beim Einrichten eines zweiten Rechenzentrums mit der vorhandenen View-Konfiguration ausführen. Oder in Situationen, in denen Ihre View-Bereitstellung nur eine einzige View-Verbindungsserver-Instanz umfasst und Probleme mit diesem Server auftreten.

Wenn Sie über mehrere View-Verbindungsserver-Instanzen in einer replizierten Gruppe verfügen und eine einzelne Instanz ausfällt, müssen Sie diese Schritte nicht ausführen. Sie können den View-Verbindungsserver ganz einfach als replizierte Instanz neu installieren. Während der Installation geben Sie Informationen zur Verbindung mit einer anderen View-Verbindungsserver-Instanz an und View stellt die View LDAP-Konfiguration anhand der anderen Instanz wieder her.

Voraussetzungen

- Überprüfen Sie, ob die View LDAP-Konfiguration in einer verschlüsselten LDIF-Datei gesichert wurde.
- Machen Sie sich mit der Wiederherstellung einer View LDAP-Konfiguration anhand einer LDIF-Sicherungsdatei mithilfe des Befehls `vdmimport` vertraut.

Lesen Sie den Abschnitt „Sichern und Wiederherstellen von View-Konfigurationsdaten“ im Dokument *Administration von View*.

- Machen Sie sich mit den Schritten zur Installation einer neuen View-Verbindungsserver-Instanz vertraut. Siehe „[Installieren von View-Verbindungsserver mit einer neuen Konfiguration](#)“, auf Seite 59.

Vorgehensweise

- 1 Installieren Sie den View-Verbindungsserver mit einer neuen Konfiguration.
- 2 Entschlüsseln Sie die verschlüsselte LDIF-Datei.

Beispiel:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

- 3 Importieren Sie die entschlüsselte LDIF-Datei, um die View LDAP-Konfiguration wiederherzustellen.

Beispiel:

```
vdmimport -f MyDecryptedexport.LDF
```

HINWEIS Zu diesem Zeitpunkt kann noch nicht auf die View-Konfiguration zugegriffen werden. Clients können nicht auf den View-Verbindungsserver zugreifen oder eine Verbindung mit ihren Desktops herstellen.

- 4 Deinstallieren Sie den View-Verbindungsserver mithilfe des Windows-Dienstprogramms **Programme hinzufügen/entfernen**.

Die View LDAP-Konfiguration, auch als AD LDS-Instanz VMwareVDMDS bezeichnet, darf nicht deinstalliert werden. Mithilfe des Dienstprogramms **Programme hinzufügen/entfernen** können Sie sicherstellen, dass die AD LDS-Instanz „VMwareVDMDS“ nicht vom Windows Server-Computer entfernt wurde.

- 5 Installieren Sie den View-Verbindungsserver neu.

Übernehmen Sie bei Aufforderung durch das Installationsprogramm das vorhandene View LDAP-Verzeichnis.

Weiter

Konfigurieren Sie den View-Verbindungsserver und Ihre View-Umgebung wie nach der Installation einer View-Verbindungsserver-Instanz mit einer neuen Konfiguration.

Befehlszeilenoptionen für Microsoft Windows Installer

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen.

Einzelheiten zu MSI finden Sie auf der Website von Microsoft. Informationen zu MSI-Befehlszeilenoptionen finden Sie auf der Website der MSDN-Bibliothek (Microsoft Developer Network), wenn Sie nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

An der Befehlszeile müssen Sie die Befehlszeilenoptionen eingeben, die das Bootstrap-Programm des Installers steuern.

Tabelle 7-7. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente

Option	Beschreibung
/s	<p>Deaktiviert den Bootstrap-Splash-Bildschirm und das Dialogfeld für die Extraktion, wodurch die Anzeige interaktiver Dialogfelder unterbunden wird.</p> <p>Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code></p> <p>Die Option /s ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p>
/v" <i>MSI-Befehlszeilenoptionen</i> "	<p>Weist den Installer an, die in doppelten Anführungszeichen eingeschlossene Zeichenfolge, die Sie an der Befehlszeile eingeben, als Befehlssatz zur Interpretation durch MSI zu übergeben. Sie müssen Ihre Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Geben Sie ein doppeltes Anführungszeichen nach /v und am Ende der Befehlszeile ein.</p> <p>Beispiel: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"<i>Befehlszeilenoptionen</i>"</code></p> <p>Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält.</p> <p>Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"<i>Befehlszeilenoptionen</i> INSTALLDIR=""d:\abc\mein Ordner""</code></p> <p>In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen.</p> <p>Die Option /v"<i>Befehlszeilenoptionen</i>" ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p>

Sie steuern die verbleibenden Schritte einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaftswerte an den MSI Installer, `msiexec.exe`, übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

Tabelle 7-8. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
/qn	<p>Weist den MSI Installer an, keine Seiten des Installationsassistenten anzuzeigen.</p> <p>Angenommen, Sie möchten den Horizon Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden:</p> <p><code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</code></p> <p>Alternativ können Sie die Option /qb zur Anzeige der Assistentenseiten in einer nicht interaktiven, automatisierten Installation verwenden. Während die Installation durchgeführt wird, werden die Assistentenseiten angezeigt, Sie können jedoch keine Eingaben vornehmen.</p> <p>Die Option /qn oder /qb ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p>
INSTALLDIR	<p>Gibt einen alternativen Installationspfad für die View-Komponente an.</p> <p>Verwenden Sie das Format <code>INSTALLDIR=Pfad</code>, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten.</p> <p>Diese MSI-Eigenschaft ist optional.</p>

Tabelle 7-8. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
ADDLOCAL	<p>Legt die komponentenspezifischen Optionen fest, die installiert werden sollen.</p> <p>Bei einer interaktiven Installation zeigt das View-Installationsprogramm benutzerdefinierte Setup-Optionen an, die Sie aus- oder abwählen können. Bei einer unbeaufsichtigten Installation können Sie mithilfe der ADDLOCAL-Eigenschaft bestimmte Setup-Optionen selektiv installieren, indem Sie die Optionen in der Befehlszeile angeben. Optionen, die Sie nicht explizit angeben, werden nicht installiert.</p> <p>Bei der interaktiven und der unbeaufsichtigten Installation werden bestimmte Funktionen automatisch vom View-Installationsprogramm installiert. Mit der ADDLOCAL-Eigenschaft können Sie nicht festlegen, ob diese nicht optionalen Funktionen installiert werden sollen.</p> <p>Geben Sie ADDLOCAL=ALL ein, um alle benutzerdefinierten Setup-Optionen zu installieren, die während einer interaktiven Installation installiert werden können, einschließlich jener, die standardmäßig installiert werden, und jener, die Sie für die Installation auswählen müssen, außer NGVC. NGVC und SVI-Agent schließen sich gegenseitig aus.</p> <p>Das folgende Beispiel installiert Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG sowie alle Funktionen, die vom Gastbetriebssystem unterstützt werden: VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>Wenn Sie die ADDLOCAL-Eigenschaft nicht verwenden, werden die standardmäßig installierten benutzerdefinierten Setup-Optionen und die automatisch installierten Funktionen installiert. Standardmäßig nicht ausgewählte benutzerdefinierte Setup-Optionen werden nicht installiert.</p> <p>Das folgende Beispiel installiert Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG sowie die standardmäßig installierten benutzerdefinierten Setup-Optionen, die vom Gastbetriebssystem unterstützt werden: VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format ADDLOCAL=Wert,Wert,Wert....</p> <p>Wenn Sie die Eigenschaft ADDLOCAL=Wert,Wert,Wert... verwenden, müssen Sie Core angeben. Im folgenden Beispiel wird Horizon Agent mit den Funktionen Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, Instant Clone Agent und Virtual Printing für das virtuelle Drucken installiert:</p> <p>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</p> <p>Das obige Beispiel installiert keine anderen Komponenten, auch nicht jene, die standardmäßig interaktiv installiert werden.</p> <p>Die MSI-Eigenschaft ADDLOCAL ist optional.</p>
REBOOT	<p>Sie können die Option REBOOT=ReallySuppress verwenden, um die Ausführung von Systemkonfigurationsaufgaben zuzulassen, bevor das System neu gestartet wird.</p> <p>Diese MSI-Eigenschaft ist optional.</p>
/l*v Protokolldatei	<p>Schreibt ausführliche Protokollinformationen in die angegebene Protokolldatei.</p> <p>Beispiel: /l*v ""%TEMP%\vmmsi.log""</p> <p>In diesem Beispiel wird eine detaillierte Protokolldatei generiert, die dem Protokoll ähnelt, das während einer interaktiven Installation erstellt wird.</p> <p>Sie können diese Option dazu verwenden, benutzerdefinierte Funktionen aufzuzeichnen, die möglicherweise nur für Ihre Installation gelten. Sie können die aufgezeichneten Informationen dazu verwenden, Installationsfunktionen für unbeaufsichtigte Installationen anzugeben.</p> <p>Die Option /l*v ist optional.</p>

Unbeaufsichtigtes Deinstallieren von View-Komponenten mithilfe von MSI-Befehlszeilenoptionen

Sie können View-Komponenten mithilfe von Microsoft Windows Installer (MSI)-Befehlszeilenoptionen deinstallieren.

Syntax

```
msiexec.exe
/qb
/x
product_code
```

Optionen

Die Option `/qb` zeigt den Deinstallationsfortschrittsbalken an. Um die Anzeige des Deinstallationsfortschrittsbalkens zu unterdrücken, ersetzen Sie die Option `/qb` durch die Option `/qn`.

Mit der Option `/x` wird die View-Komponente deinstalliert.

Die Zeichenfolge `product_code` kennzeichnet die View-Komponentenproduktdateien für das MSI-Deinstallationsprogramm. Sie finden die Zeichenfolge `produkt_code`, wenn Sie in der während der Installation erstellten Datei `%TEMP%\vmmsi.log` nach `ProductCode` suchen. Erläuterungen zur Ermittlung der Zeichenfolge `product_code` für ältere Versionen von View-Komponenten finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/2064845>.

Informationen zu MSI-Befehlszeilenoptionen finden Sie unter „[Befehlszeilenoptionen für Microsoft Windows Installer](#)“, auf Seite 84.

Deinstallieren eines Horizon Agent-Beispiels

Um die 32-Bit-Version von Horizon Agent 7.0.2 zu deinstallieren, geben Sie folgenden Befehl ein:

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

Um die 64-Bit-Version von Horizon Agent 7.0.2 zu deinstallieren, geben Sie folgenden Befehl ein:

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

Fügen Sie dem Befehl ein ausführliches Protokoll hinzu.

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

Wenn Sie die Option `/l` nicht explizit übergeben, ist `%TEMP%\MSI $nnnn$.log` die Standarddatei für das ausführliche Protokoll, wobei $nnnn$ eine GUID aus vier Zeichen darstellt.

Bei der Deinstallation von Horizon Agent werden einige Registrierungsschlüssel beibehalten, also nicht entfernt. Diese Registrierungsschlüssel sind für die Konfigurationsinformationen des Verbindungservers erforderlich, mit denen der Remote-Desktop mit dem Verbindungsserver weiterhin kombiniert werden kann, auch wenn der Agent deinstalliert und danach neu installiert wird. Durch Entfernung dieser Registrierungsschlüssel wird diese Kombination getrennt.

Die folgenden Registrierungsschlüssel werden beibehalten:

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs

- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Konfigurieren von SSL-Zertifikaten für View Servers

8

VMware empfiehlt ausdrücklich, dass Sie die SSL-Zertifikate zur Authentifizierung von View-Verbindungsserver-Instanzen, Sicherheitsservern und View Composer-Dienstinstanzen konfigurieren.

Bei der Installation von View-Verbindungsserver-Instanzen, Sicherheitsservern oder View Composer-Instanzen wird ein SSL-Standardserverzertifikat erstellt. Sie können das Standardzertifikat für Testzwecke verwenden.

WICHTIG Ersetzen Sie das Standardzertifikat so schnell wie möglich. Das Standardzertifikat ist nicht von einer Zertifizierungsstelle signiert. Die Verwendung von Zertifikaten, die nicht von einer Zertifizierungsstelle signiert wurden, kann von nicht vertrauenswürdigen Parteien dazu ausgenutzt werden, sich als Ihr Server auszugeben und Daten abzufangen.

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlegendes zu SSL-Zertifikaten für View-Server“, auf Seite 90
- „Überblick über Aufgaben zur Einrichtung von SSL-Zertifikaten“, auf Seite 91
- „Beziehen eines signierten SSL-Zertifikats von einer Zertifizierungsstelle“, auf Seite 92
- „Konfigurieren des View-Verbindungsservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen SSL-Zertifikats“, auf Seite 94
- „Konfigurieren von Client-Endpunkten, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen“, auf Seite 100
- „Konfigurieren der Zertifikatsperrüberprüfung für Serverzertifikate“, auf Seite 102
- „Konfigurieren des PCoIP Secure Gateway zur Nutzung eines Neuen SSL-Zertifikats“, auf Seite 103
- „Konfigurieren von View Administrator, um ein vCenter Server- oder View Composer-Zertifikat als vertrauenswürdig einzustufen“, auf Seite 108
- „Vorteile der Verwendung von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden“, auf Seite 108
- „Fehlerbehebung bei Problemen mit Zertifikaten auf View-Verbindungsserver und -Sicherheitsservern“, auf Seite 109

Grundlegendes zu SSL-Zertifikaten für View -Server

Bei der Konfiguration von SSL-Zertifikaten für View-Server- und verknüpfte Komponenten müssen bestimmte Richtlinien befolgt werden.

View-Verbindungsserver und Sicherheitsserver

SSL ist für Clientverbindungen mit einem Server erforderlich. Für View-Verbindungsserver-Instanzen mit Clientverbindung, Sicherheitsserver und Zwischenserver, die als Endpunkt für SSL-Verbindungen fungieren, sind SSL-Serverzertifikate erforderlich.

Bei der Installation eines View-Verbindungsservers oder Sicherheitsservers wird standardmäßig ein selbstsigniertes Zertifikat für den Server generiert. In den folgenden Fällen wird bei der Installation jedoch ein vorhandenes Zertifikat verwendet:

- Wenn im Windows-Zertifikatspeicher bereits ein gültiges Zertifikat mit dem Anzeigenamen `vdm` vorhanden ist.
- Wenn Sie ein Upgrade auf View 5.1 oder höher durchführen und auf dem Windows Server-Computer eine gültige Schlüsselspeicherdatei konfiguriert ist. Bei der Installation werden die Schlüssel und Zertifikate extrahiert und in den Windows-Zertifikatspeicher importiert.

vCenter Server und View Composer

Stellen Sie vor dem Hinzufügen von vCenter Server und View Composer zu View in einer Produktionsumgebung sicher, dass die von vCenter Server und View Composer verwendeten Zertifikate von einer Zertifizierungsstelle signiert wurden.

Informationen zum Ersetzen des Standardzertifikats für vCenter Server finden Sie unter „Replacing vCenter Server Certificates“ auf der VMware Technical Papers-Website unter <http://www.vmware.com/resources/techresources/>.

Wenn Sie vCenter Server und View Composer auf demselben Windows Server-Host installieren, wird dasselbe SSL-Zertifikat verwendet. Sie müssen das Zertifikat jedoch für jede Komponente einzeln konfigurieren.

PCoIP Secure Gateway

Um Industrie- oder Gesetzessicherheitsvorschriften zu entsprechen, können Sie das Standard-SSL-Zertifikat ersetzen, das vom PCoIP Secure Gateway (PSG) Service mit einem von einer Zertifizierungsstelle signierten Zertifikat erzeugt wird. Die Konfiguration des PSG-Service für die Nutzung eines CA-signierten Zertifikats wird dringend empfohlen, und dies besonders für Inbetriebnahmen, bei denen Sie Sicherheitsscanner verwenden müssen, um die Compliance-Tests zu bestehen. Siehe „[Konfigurieren des PCoIP Secure Gateway zur Nutzung eines Neuen SSL-Zertifikats](#)“, auf Seite 103.

Blast Secure Gateway

Standardmäßig verwendet das Blast Secure Gateway (BSG) das SSL-Zertifikat, das für die View-Verbindungsserver-Instanz oder den Sicherheitsserver konfiguriert ist, auf dem das BSG läuft. Wenn Sie das standardmäßige, selbstsignierte Zertifikat für einen Server durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzen, verwendet das BSG auch das von der Zertifizierungsstelle signierte Zertifikat.

SAML 2.0-Authentifikator

VMware Identity Manager verwendet SAML 2.0-Authentifikatoren für eine webbasierte Authentifizierung und Autorisierung innerhalb von Sicherheitsdomänen. Wenn View die Authentifizierung an VMware Identity Manager delegieren soll, können Sie View so konfigurieren, dass über SAML 2.0 authentifizierte Sitzungen von VMware Identity Manager akzeptiert werden. Wenn VMware Identity Manager für die Unterstützung von View konfiguriert ist, können VMware Identity Manager-Benutzer eine Verbindung mit Remote-Desktops herstellen, indem sie im Horizon-Benutzerportal Desktopsymbole auswählen.

In View Administrator können SAML 2.0-Authentifikatoren für die Verwendung mit View-Verbindungsserver-Instanzen konfiguriert werden.

Stellen Sie vor dem Hinzufügen eines SAML 2.0-Authentifikators in View Administrator sicher, dass der SAML 2.0-Authentifikator ein von einer Zertifizierungsstelle signiertes Zertifikat verwendet.

Weitere Richtlinien

[„Vorteile der Verwendung von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden“](#), auf Seite 108 Allgemeine Informationen zum Anfordern und Verwenden von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden, finden Sie unter .

Wenn Clientendpunkte eine Verbindung mit einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver herstellen, werden ihnen das SSL-Serverzertifikat sowie alle Zwischenzertifikate in der Vertrauenskette angezeigt. Um das Serverzertifikat als vertrauenswürdig einzustufen, muss auf den Clientsystemen das Stammzertifikat der signierenden Zertifizierungsstelle installiert sein.

Wenn der View-Verbindungsserver mit vCenter Server und View Composer kommuniziert, werden dem View-Verbindungsserver SSL-Serverzertifikate und Zwischenzertifikate dieser Server angezeigt. Um die vCenter Server- und View Composer Server als vertrauenswürdig einzustufen, muss auf dem View-Verbindungsserver das Stammzertifikat der signierenden Zertifizierungsstelle installiert sein.

Wenn ein SAML 2.0-Authentifikator für den View-Verbindungsserver konfiguriert ist, muss auf dem View-Verbindungsserver-Computer gleichermaßen das Stammzertifikat der signierenden Zertifizierungsstelle für das SAML 2.0-Serverzertifikat installiert sein.

Überblick über Aufgaben zur Einrichtung von SSL-Zertifikaten

Um SSL-Serverzertifikate für View Server einzurichten, müssen Sie mehrere allgemeine Aufgaben durchführen.

In einem Pod mit replizierten View-Verbindungsserver-Instanzen müssen Sie diese Aufgaben auf allen Instanzen im Pod ausführen.

Die Verfahren für die Durchführung dieser Aufgaben werden in den Themen nach dieser Übersicht beschrieben.

- 1 Ermitteln Sie, ob Sie ein neues signiertes SSL-Zertifikat von einer Zertifizierungsstelle beziehen müssen.

Wenn Ihre Organisation bereits über ein gültiges SSL-Serverzertifikat verfügt, können Sie damit das standardmäßige SSL-Serverzertifikat ersetzen, das auf dem View-Verbindungsserver, Sicherheitsserver oder in View Composer bereitgestellt wird. Zur Verwendung eines vorhandenen Zertifikats benötigen Sie auch den zugehörigen privaten Schlüssel.

Ausgangssituation	Aktion
Ihre Organisation hat Ihnen ein gültiges SSL-Serverzertifikat zur Verfügung gestellt.	Fahren Sie direkt mit Schritt 2 fort.
Sie verfügen über kein SSL-Serverzertifikat.	Beziehen Sie ein signiertes SSL-Serverzertifikat von einer Zertifizierungsstelle.

- 2 Importieren Sie das SSL-Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem View Server-Host.
- 3 View-Verbindungsserver-Instanzen und Sicherheitsserver: Ändern Sie den Anzeigenamen des Zertifikats in **vdm**.

Geben Sie pro View Server-Host nur einem Zertifikat den Anzeigenamen **vdm**.

- 4 Computer mit View-Verbindungsservern: Wenn der Windows Server-Host das Stammzertifikat nicht als vertrauenswürdig einstuft, importieren Sie das Stammzertifikat in den Zertifikatspeicher des lokalen Windows-Computers.

Wenn die View-Verbindungsserver-Instanzen den Stammzertifikaten der SSL-Serverzertifikate nicht vertrauen, die für die Hosts für den Sicherheitsserver, für View Composer und für vCenter Server konfiguriert sind, müssen Sie auch diese Stammzertifikate importieren. Führen Sie diese Schritte nur für View-Verbindungsserver-Instanzen aus. Sie müssen das Stammzertifikat nicht auf Hosts mit View Composer, vCenter Server oder Sicherheitsservern importieren.

- 5 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie die Zwischenzertifikate in den Zertifikatspeicher des lokalen Windows-Computers.

Um die Clientkonfiguration zu vereinfachen, importieren Sie die gesamte Zertifikatkette in den Zertifikatspeicher des lokalen Windows-Computers. Wenn auf dem View Server Zwischenzertifikate fehlen, müssen sie für Clients und Computer konfiguriert werden, auf denen View Administrator gestartet wird.

- 6 View Composer-Instanzen: Führen Sie einen der folgenden Schritte aus:

- Wenn Sie Ihr Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers importieren, bevor Sie View Composer installieren, können Sie es während der View Composer-Installation auswählen.
- Wenn Sie ein vorhandenes Zertifikat oder das selbst signierte Standardzertifikat nach der Installation von View Composer durch ein neues Zertifikat ersetzen möchten, führen Sie das Dienstprogramm `SviConfig ReplaceCertificate` aus, um das neue Zertifikat an den von View Composer verwendeten Port zu binden.

- 7 Wenn Ihre Zertifizierungsstelle nicht bekannt ist, konfigurieren Sie Clients so, dass sie dem Stammzertifikat und den Zwischenzertifikaten vertrauen.

Stellen Sie außerdem sicher, dass die Computer, auf denen Sie View Administrator starten, dem Stammzertifikat und den Zwischenzertifikaten vertrauen.

- 8 Ermitteln Sie, ob Sie die Zertifikatsperrüberprüfung neu konfigurieren müssen.

Der View-Verbindungsserver führt die Zertifikatsperrüberprüfung für View Server, View Composer und vCenter Server durch. Die meisten von einer Zertifizierungsstelle signierten Zertifikate enthalten Informationen zur Zertifikatsperrung. Wenn Ihre Zertifizierungsstelle diese Informationen nicht einschließt, können Sie den Server so konfigurieren, dass er Zertifikate nicht auf Sperrung überprüft.

Wenn ein SAML-Authentifikator zur Verwendung mit einer View-Verbindungsserver-Instanz konfiguriert ist, führt der View-Verbindungsserver auch die Zertifikatsperrüberprüfung für das SAML-Serverzertifikat durch.

Beziehen eines signierten SSL-Zertifikats von einer Zertifizierungsstelle

Wenn Ihre Organisation Ihnen kein SSL-Serverzertifikat zur Verfügung stellt, müssen Sie ein neues Zertifikat anfordern, das von einer Zertifizierungsstelle signiert ist.

Sie haben mehrere Möglichkeiten, ein neues signiertes Zertifikat zu beziehen. Beispielsweise können Sie das Microsoft-Dienstprogramm `certreq` verwenden, um eine CSR-Anfrage (Certificate Signing Request) zu generieren und eine Zertifikatanfrage an eine Zertifizierungsstelle zu senden.

Im Dokument *Scenarios for Setting Up SSL Certificates for View (Szenarien zum Einrichten von SSL-Zertifikaten für View)* finden Sie ein Beispiel für die Verwendung von `certreq` für diese Aufgabe.

Zu Testzwecken stellen CA-Anbieter ein kostenloses temporäres Zertifikat zur Verfügung, das auf einem nicht vertrauenswürdigen Stamm basiert.

WICHTIG Beim Beziehen signierter SSL-Zertifikate von einer Zertifizierungsstelle müssen Sie bestimmte Regeln und Richtlinien einhalten.

- Stellen Sie beim Generieren einer Zertifikatanfrage auf einem Computer sicher, dass auch ein privater Schlüssel generiert wird. Wenn Sie das SSL-Serverzertifikat beziehen und es in den Zertifikatspeicher des lokalen Windows-Computers importieren, muss ein zugehöriger privater Schlüssel vorhanden sein, der dem Zertifikat entspricht.
 - Verwenden Sie zur Einhaltung der VMware-Sicherheitsempfehlungen den vollqualifizierten Domänennamen (FQDN), mit dem Clientgeräte eine Verbindung mit dem Host herstellen. Verwenden Sie selbst für die Kommunikation innerhalb Ihrer internen Domäne keinen einfachen Servernamen bzw. keine einfache IP-Adresse.
 - Erstellen Sie Zertifikate für Server nicht mithilfe einer Zertifikatvorlage, die nur mit einer Unternehmenszertifizierungsstelle unter Windows Server 2008 oder höher kompatibel ist.
 - Generieren Sie Zertifikate für Server nicht mithilfe eines `keyLength`-Wertes unter 1024. Client-Endpunkte validieren auf Servern keine Zertifikate, die mit einem `keyLength`-Wert unter 1024 generiert wurden, und die Clients können keine Verbindung mit dem Server herstellen. Auch vom View-Verbindungsserver durchgeführte Zertifikatüberprüfungen schlagen fehl, sodass die betreffenden Server im View Administrator-Dashboard in Rot angezeigt werden.
-

Allgemeine Informationen zum Beziehen von Zertifikaten finden Sie in der Microsoft-Onlinehilfe für das MMC-Snap-In „Zertifikate“. Wenn das Snap-In „Zertifikate“ noch nicht auf Ihrem Computer installiert ist, lesen Sie [„Hinzufügen des Zertifikat-Snap-Ins zu MMC“](#), auf Seite 95.

Erwerben eines signierten Zertifikats von einer Windows-Domäne oder Unternehmenszertifizierungsstelle

Zum Erwerben eines signierten Zertifikats von einer Windows-Domäne oder Unternehmenszertifizierungsstelle können Sie den Assistenten für die Windows-Zertifikatregistrierung im Windows-Zertifikatspeicher verwenden.

Diese Methode zum Anfordern eines Zertifikats ist geeignet, wenn die Kommunikation zwischen Computern ausschließlich innerhalb Ihrer internen Domäne stattfindet. Der Erwerb eines signierten Zertifikats von einer Windows-Domänen-Zertifizierungsstelle ist beispielsweise möglich, wenn die Kommunikation zwischen Servern erfolgt.

Wenn Ihre Clients sich von einem externen Netzwerk aus bei View Servern anmelden, fordern Sie SSL-Serverzertifikate an, die von einer vertrauenswürdigen Drittanbieter-Zertifizierungsstelle signiert sind.

Voraussetzungen

- Bestimmen Sie den vollqualifizierten Domänennamen (FQDN), den Clientgeräte für die Verbindung mit dem Host verwenden.
Verwenden Sie selbst für die Kommunikation innerhalb Ihrer internen Domäne zur Einhaltung der VMware-Sicherheitsempfehlungen keinen einfachen Servernamen bzw. keine einfache IP-Adresse, sondern den FQDN.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe [„Hinzufügen des Zertifikat-Snap-Ins zu MMC“](#), auf Seite 95.
- Überprüfen Sie, ob Sie über die erforderlichen Berechtigungen zum Anfordern eines Zertifikats verfügen, das für einen Computer oder einen Dienst ausgegeben werden kann.

Vorgehensweise

- 1 Erweitern Sie im MMC-Fenster auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich** aus.
- 2 Wählen Sie im Menü **Aktion** die Optionen **Alle Aufgaben > Neues Zertifikat anfordern** aus, um den Assistenten für die Zertifikatregistrierung anzuzeigen.
- 3 Wählen Sie eine Richtlinie für die Zertifikatregistrierung aus.
- 4 Wählen Sie die Zertifikattypen aus, die Sie anfordern möchten, wählen Sie die Option **Privaten Schlüssel exportierbar machen** aus und klicken Sie auf **Registrieren**.
- 5 Klicken Sie auf **Fertig stellen**.

Das neue signierte Zertifikat wird dem Ordner **Persönlich > Zertifikate** im Windows-Zertifikatspeicher hinzugefügt.

Weiter

- Überprüfen Sie, ob das Serverzertifikat und die Zertifikatkette in den Windows-Zertifikatspeicher importiert wurden.
- Ändern Sie den Anzeigenamen des Zertifikats für eine View-Verbindungsserver-Instanz oder für einen Sicherheitsserver in **vdm**. Siehe [„Ändern des Anzeigenamens eines Zertifikats“](#), auf Seite 97.
- Binden Sie das neue Zertifikat für einen View Composer Server an den Port, der von View Composer verwendet wird. Siehe [„Bindung eines neuen SSL-Zertifikats an den von View Composer verwendeten Port“](#), auf Seite 99.

Konfigurieren des View-Verbindungsservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen SSL-Zertifikats

Um eine View-Verbindungsserver-Instanz, einen Sicherheitsserver oder eine View Composer-Instanz für den Gebrauch eines SSL-Zertifikats zu konfigurieren, müssen Sie das Serverzertifikat und die gesamte Zertifikatskette in den lokalen Windows-Zertifikatspeicher auf den View-Verbindungsserver, Sicherheitsserver oder View Composer Host importieren.

In einem Pod replizierter View-Verbindungsserver-Instanzen müssen Sie das Serverzertifikat und die Zertifikatskette auf allen Instanzen im Pod importieren.

Standardmäßig verwendet das Blast Secure Gateway (BSG) das SSL-Zertifikat, das für die View-Verbindungsserver-Instanz oder den Sicherheitsserver konfiguriert ist, auf dem das BSG läuft. Wenn Sie das standardmäßige, selbst signierte Zertifikat für einen View Server durch ein CA-Zertifikat ersetzen, benutzt das BSG auch das CA-Zertifikat.

WICHTIG Um den View-Verbindungsserver oder den Sicherheitsserver zu konfigurieren, ein Zertifikat zu verwenden, müssen Sie den Anzeigenamen des Zertifikats in **vdm** ändern. Außerdem muss das Zertifikat einen begleitenden privaten Schlüssel besitzen.

Wenn Sie ein vorhandenes oder das standardmäßige, selbst signierte Zertifikat durch ein neues Zertifikat ersetzen möchten, nachdem Sie View Composer installiert haben, müssen Sie das Dienstprogramm **SviConfig ReplaceCertificate** ausführen, um das neue Zertifikat an den Port zu binden, der von View verwendet wird.

Vorgehensweise

- 1 [Hinzufügen des Zertifikat-Snap-Ins zu MMC](#) auf Seite 95
Bevor Sie Zertifikate zum Windows-Zertifikatspeicher hinzufügen können, müssen Sie das Zertifikat-Snap-In zur Microsoft Management Console (MMC) auf dem Windows Server-Host hinzufügen, auf dem View server installiert ist.

- 2 [Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher](#) auf Seite 96
Sie müssen das SSL-Serverzertifikat in den lokalen Zertifikatspeicher des Windows-Computers auf dem Windows Server-Host importieren, auf dem die View-Verbindungsserver-Instanz oder der Sicherheitsserver-Dienst installiert ist.
- 3 [Ändern des Anzeigenamens eines Zertifikats](#) auf Seite 97
Um die View-Verbindungsserver-Instanz oder den Sicherheitsserver für die Erkennung und Verwendung eines SSL-Zertifikats zu konfigurieren, müssen Sie den Anzeigenamen des Zertifikats in `vdm` ändern.
- 4 [Importieren eines Stamm- und Zwischenzertifikats in einen Windows-Zertifikatspeicher](#) auf Seite 97
Wenn der Windows Server-Host, auf dem der View-Verbindungsserver installiert ist, dem Stammzertifikat für das signierte SSL-Serverzertifikat nicht vertraut, müssen Sie das Stammzertifikat in den Zertifikatspeicher des lokalen Windows-Computers importieren. Wenn der Host des View-Verbindungs-servers den Stammzertifikaten der SSL-Serverzertifikate nicht vertraut, die für die Hosts für den Sicherheitsserver, für View Composer und für vCenter Server konfiguriert sind, müssen Sie auch diese Stammzertifikate importieren.
- 5 [Bindung eines neuen SSL-Zertifikats an den von View Composer verwendeten Port](#) auf Seite 99
Wenn Sie nach der Installation von View Composer ein neues SSL-Zertifikat konfigurieren, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` ausführen, um das an den von View Composer verwendeten Port gebundene Zertifikat zu ersetzen. Dieses Dienstprogramm hebt die Bindung des bestehenden Zertifikats auf und bindet das neue Zertifikat an den Port.

Hinzufügen des Zertifikat-Snap-Ins zu MMC

Bevor Sie Zertifikate zum Windows-Zertifikatspeicher hinzufügen können, müssen Sie das Zertifikat-Snap-In zur Microsoft Management Console (MMC) auf dem Windows Server-Host hinzufügen, auf dem View server installiert ist.

Voraussetzungen

Stellen Sie sicher, dass das MMC- und das Zertifikat-Snap-In auf dem Windows Server-Computer verfügbar sind, auf dem View server installiert ist.

Vorgehensweise

- 1 Klicken Sie auf dem Windows Server-Computer auf **Start** und geben Sie `mmc.exe` ein.
- 2 Gehen Sie im Fenster MMC auf **Datei > Snap-In hinzufügen/entfernen**.
- 3 Wählen Sie im Fenster Snap-Ins hinzufügen oder entfernen **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
- 4 Wählen Sie im Fenster Zertifikat-Snap-In **Computerkonto**, klicken Sie auf **Weiter**, wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.
- 5 Klicken Sie im Fenster Snap-In hinzufügen oder entfernen auf **OK**.

Weiter

Importieren Sie das SSL-Serverzertifikat in den Windows-Zertifikatspeicher.

Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher

Sie müssen das SSL-Serverzertifikat in den lokalen Zertifikatspeicher des Windows-Computers auf dem Windows Server-Host importieren, auf dem die View-Verbindungsserver-Instanz oder der Sicherheitsserver-Dienst installiert ist.

Sie müssen diesen Vorgang auch auf dem Windows Server-Host durchführen, auf dem der View Composer-Dienst installiert ist.

Je nach Format Ihrer Zertifikatdateien wird möglicherweise die gesamte Zertifikatkette, die sich in der Schlüsselspeicherdatei befindet, in den Zertifikatspeicher des lokalen Windows-Computers importiert. Beispielsweise können das Serverzertifikat, Zwischenzertifikat und Stammzertifikat importiert werden.

Bei anderen Arten von Zertifikatdateien wird nur das Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers importiert. In diesem Fall müssen Sie separate Schritte ausführen, um das Stammzertifikat und ggf. alle Zwischenzertifikate in der Zertifikatkette zu importieren.

Weitere Informationen zu Zertifikaten finden Sie in der Microsoft-Onlinehilfe für das MMC-Snap-In „Zertifikate“.

HINWEIS Wenn Sie SSL-Verbindungen auf einen Zwischenserver auslagern, müssen Sie dasselbe SSL-Serverzertifikat auf den Zwischenserver und auf den ausgelagerten View Server importieren. Details finden Sie unter „Auslagern von SSL-Verbindungen auf Zwischenserver“ im Dokument *Administration von View*.

Voraussetzungen

Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe „[Hinzufügen des Zertifikat-Snap-Ins zu MMC](#)“, auf Seite 95.

Vorgehensweise

- 1 Erweitern Sie im MMC-Fenster auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich**.
- 2 Wechseln Sie im Bereich „Aktionen“ zu **Weitere Aktionen > Alle Aufgaben > Importieren**.
- 3 Klicken Sie im Zertifikatimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.
- 4 Wählen Sie die Zertifikatdatei und klicken Sie auf **Öffnen**.
Um den Typ Ihrer Zertifikatdatei anzuzeigen, können Sie ihr Dateiformat im Dropdown-Menü **Dateiname** auswählen.
- 5 Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatdatei ein.
- 6 Wählen Sie **Schlüssel als exportierbar markieren**.
- 7 Aktivieren Sie **Alle erweiterten Eigenschaften mit einbeziehen**.
- 8 Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

Das neue Zertifikat wird im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** angezeigt.

- 9 Überprüfen Sie, ob das neue Zertifikat einen privaten Schlüssel enthält.
 - a Doppelklicken Sie im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** auf das neue Zertifikat.
 - b Prüfen Sie, ob die folgende Meldung im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ angezeigt wird: Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Weiter

Ändern Sie den Anzeigenamen des Zertifikats auf **vdm**.

Ändern des Anzeigenamens eines Zertifikats

Um die View-Verbindungsserver-Instanz oder den Sicherheitsserver für die Erkennung und Verwendung eines SSL-Zertifikats zu konfigurieren, müssen Sie den Anzeigenamen des Zertifikats in **vdm** ändern.

Sie müssen den Anzeigenamen von SSL-Zertifikaten, die von View Composer verwendet werden, nicht ändern.

Voraussetzungen

Prüfen Sie, ob das Serverzertifikat in den Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** im Windows-Zertifikatspeicher importiert wird. Siehe „[Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher](#)“, auf Seite 96.

Vorgehensweise

- 1 Erweitern Sie im MMC-Fenster auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich > Zertifikate** aus.
- 2 Klicken Sie mit der rechten Maustaste auf das Zertifikat, das für den View Server-Host ausgestellt ist, und klicken Sie auf **Eigenschaften**.
- 3 Löschen Sie auf der Registerkarte „Allgemein“ den Text **Anzeigename** und geben Sie **vdm** ein.
- 4 Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- 5 Stellen Sie sicher, dass keine anderen Serverzertifikate im Ordner **Persönlich > Zertifikate** den Anzeigenamen **vdm** haben.
 - a Suchen Sie die anderen Serverzertifikate, klicken Sie mit der rechten Maustaste auf das Zertifikat und klicken Sie auf **Eigenschaften**.
 - b Wenn das Zertifikat den Anzeigenamen **vdm** hat, löschen Sie den Namen und klicken Sie auf **Anwenden** und danach auf **OK**.

Weiter

Importieren Sie das Stammzertifikat und die Zwischenzertifikate in den Zertifikatspeicher des lokalen Windows-Computers.

Nach dem Import aller Zertifikate aus der Kette müssen Sie den View-Verbindungsserver-Dienst oder den Sicherheitsserverdienst neu starten, damit die Änderungen wirksam werden.

Importieren eines Stamm- und Zwischenzertifikats in einen Windows-Zertifikatspeicher

Wenn der Windows Server-Host, auf dem der View-Verbindungsserver installiert ist, dem Stammzertifikat für das signierte SSL-Serverzertifikat nicht vertraut, müssen Sie das Stammzertifikat in den Zertifikatspeicher des lokalen Windows-Computers importieren. Wenn der Host des View-Verbindungservers den Stammzertifikaten der SSL-Serverzertifikate nicht vertraut, die für die Hosts für den Sicherheitsserver, für View Composer und für vCenter Server konfiguriert sind, müssen Sie auch diese Stammzertifikate importieren.

Wenn die Zertifikate für den View-Verbindungsserver, den Sicherheitsserver, View Composer und vCenter Server von einer Stammzertifizierungsstelle signiert sind, die dem Host des View-Verbindungservers bekannt und für ihn vertrauenswürdig ist, und Ihre Zertifikatketten keine Zwischenzertifikate enthalten, können Sie diese Aufgabe überspringen. Häufig verwendeten Zertifizierungsstellen vertraut der Host im Allgemeinen.

Sie müssen nicht vertrauenswürdige Stammzertifikate auf allen replizierten View-Verbindungsserver-Instanzen in einem Pod importieren.

HINWEIS Sie müssen das Stammzertifikat nicht auf Hosts für View Composer, vCenter Server oder Sicherheitsserver importieren.

Wenn ein Serverzertifikat von einer Zwischenzertifizierungsstelle unterzeichnet wurde, müssen Sie auch alle Zwischenzertifikate in der Zertifikatkette importieren. Um die Clientkonfiguration zu vereinfachen, importieren Sie die gesamte Kette der Zwischenzertifikate auf die Hosts für den Sicherheitsserver, für View Composer und für vCenter Server sowie auf die Hosts für View-Verbindungsserver. Wenn auf einem Host für View-Verbindungsserver oder Sicherheitsserver Zwischenzertifikate fehlen, müssen sie für Clients und Computer konfiguriert werden, auf denen View Administrator gestartet wird. Wenn Zwischenzertifikate auf einem Host für View Composer oder vCenter Server fehlen, müssen sie für jede Instanz des View-Verbindungsservers konfiguriert werden.

Wenn Sie sich bereits vergewissert haben, dass die gesamte Zertifikatkette in den Zertifikatspeicher des lokalen Windows-Computers importiert wird, können Sie diese Aufgabe überspringen.

HINWEIS Wenn ein SAML-Authentifikator für die Verwendung durch eine View-Verbindungsserver-Instanz konfiguriert ist, gelten für den SAML 2.0-Authentifikator die gleichen Richtlinien. Wenn der Host des View-Verbindungsservers dem Stammzertifikat nicht vertraut, das für einen SAML-Authentifikator konfiguriert ist, oder wenn das SAML-Serverzertifikat von einer Zwischenzertifizierungsstelle signiert ist, müssen Sie sicherstellen, dass die Zertifikatkette in den lokalen Windows-Zertifikatspeicher des Computers importiert wird.

Vorgehensweise

- 1 Erweitern Sie an der MMC-Konsole auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wechseln Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
 - Wenn Ihr Stammzertifikat sich in diesem Ordner befindet und Ihre Zertifikatkette keine Zwischenzertifikate enthält, fahren Sie mit Schritt 7 fort.
 - Wenn Ihr Stammzertifikat sich nicht in diesem Ordner befindet, fahren Sie mit Schritt 2 fort.
- 2 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.
- 3 Klicken Sie im Zertifikatsimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.
- 4 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.
- 5 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.
- 6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den Zertifikatspeicher des lokalen Windows-Computers.
 - a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.
 - b Wiederholen Sie die Schritte 3 bis 6 für jedes zu importierende Zwischenzertifikat.
- 7 Starten Sie den View-Verbindungsserver-Dienst, Sicherheitsserver-Dienst, View Composer-Dienst oder vCenter Server-Dienst neu, damit Ihre Änderungen wirksam werden.

Bindung eines neuen SSL-Zertifikats an den von View Composer verwendeten Port

Wenn Sie nach der Installation von View Composer ein neues SSL-Zertifikat konfigurieren, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` ausführen, um das an den von View Composer verwendeten Port gebundene Zertifikat zu ersetzen. Dieses Dienstprogramm hebt die Bindung des bestehenden Zertifikats auf und bindet das neue Zertifikat an den Port.

Wenn Sie das neue Zertifikat vor der Installation von View Composer auf dem Windows Server-Computer installieren, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` nicht ausführen. Wenn Sie das View Composer-Installationsprogramm ausführen, können Sie statt des selbstsignierten Standard-Zertifikats ein Zertifikat auswählen, das von einer Zertifizierungsstelle signiert wurde. Während der Installation ist das ausgewählte Zertifikat an den von View Composer verwendeten Port gebunden.

Wenn Sie ein bestehendes Zertifikat oder das selbstsignierte Standardzertifikat durch ein neues Zertifikat ersetzen möchten, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` verwenden.

Voraussetzungen

Überprüfen Sie, ob das neue Zertifikat in den Windows-Zertifikatspeicher des lokalen Computers auf dem Windows Server-Computer importiert wurde, auf dem View Composer installiert ist.

Vorgehensweise

- 1 Halten Sie den View Composer-Dienst an.
- 2 Öffnen Sie eine Eingabeaufforderung auf dem Windows Server Host, auf dem View Composer installiert ist.
- 3 Navigieren Sie zur ausführbaren Datei `SviConfig`.

Die Datei befindet sich im Ordner der View Composer-Anwendung. Der Standardpfad lautet `C:\Programme (x86)\VMware\VMware View Composer\sviconfig.exe`.

- 4 Geben Sie den Befehl `SviConfig ReplaceCertificate` ein.

Beispiel:

```
sviconfig -operation=ReplaceCertificate
         -delete=false
```

Hierbei gilt: `-delete` ist ein erforderlicher Parameter, der auf dem Zertifikat operiert, das ersetzt wird. Sie müssen entweder `-delete=true` eingeben, um das alte Zertifikat aus dem Windows-Zertifikatspeicher des lokalen Computers zu löschen, oder `-delete=false`, um das alte Zertifikat im Windows-Zertifikatspeicher beizubehalten.

Das Dienstprogramm zeigt eine nummerierte Liste mit SSL-Zertifikaten an, die im Windows-Zertifikatspeicher des lokalen Computers vorhanden sind.

- 5 Geben Sie zum Auswählen eines Zertifikats die Nummer des Zertifikats ein und drücken Sie auf „Eingabe“.
- 6 Starten Sie den View Composer-Dienst neu, damit die Änderungen wirksam werden.

Beispiel: `sviconfig ReplaceCertificate`

Das folgende Beispiel ersetzt das Zertifikat, das an den View Composer-Port gebunden ist:

```
sviconfig -operation=ReplaceCertificate
         -delete=false
```

Konfigurieren von Client-Endpunkten, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen

Wenn ein View-Serverzertifikat von einer Zertifizierungsstelle signiert ist, die von Clientcomputern und Clientcomputern, die auf View Administrator zugreifen, nicht als vertrauenswürdig eingestuft wird, können Sie alle Windows-Clientsysteme in einer Domäne so konfigurieren, dass Stamm- und Zwischenzertifikate als vertrauenswürdig eingestuft werden. Dazu müssen Sie den öffentlichen Schlüssel für das Stammzertifikat zur Gruppenrichtlinie „Vertrauenswürdige Stammzertifizierungsstellen“ in Active Directory und das Stammzertifikat zum Enterprise NTAAuth-Speicher hinzufügen.

Sie müssen diese Maßnahme z. B. möglicherweise ergreifen, wenn Ihre Organisation einen internen Zertifikatsdienst verwendet.

Diese Schritte müssen nicht ausgeführt werden, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert oder wenn Ihre Zertifikate von einer bekannten Zertifizierungsstelle signiert wurden. Bei bekannten Zertifizierungsstellen installiert der Betriebssystem-Hersteller das Stammzertifikat bereits vorab auf den Clientsystemen.

Wenn Ihre Serverzertifikate von einer wenig bekannten Zwischenzertifizierungsstelle signiert wurden, müssen Sie das Zwischenzertifikat der Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen.

Für Clientgeräte, die andere Betriebssysteme als Windows verwenden, gelten die folgenden Anleitungen für das Verteilen von Stamm- und Zwischenzertifikaten, die von Benutzern installiert werden können:

- Horizon Client für Mac: „[Konfigurieren von Horizon Client für Mac, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen](#)“, auf Seite 101.
- Horizon Client für iOS: „[Konfigurieren von Horizon Client für iOS, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen](#)“, auf Seite 102.
- Horizon Client für Android: Dokumentation auf der Google-Website, z. B. das *Benutzerhandbuch für Android 3.0*.
- Horizon Client für Linux: Dokumentation zu Ubuntu.

Voraussetzungen

Stellen Sie sicher, dass das Serverzertifikat mit einem KeyLength-Wert von mindestens 1024 generiert wurde. Client-Endpunkte validieren auf Servern keine Zertifikate, die mit einem KeyLength-Wert unter 1024 generiert wurden, und die Clients können keine Verbindung mit dem Server herstellen.

Vorgehensweise

- 1 Verwenden Sie auf dem Active Directory-Server den Befehl `certutil`, um das Zertifikat im Enterprise NTAAuth-Speicher zu veröffentlichen.

Beispiel: `certutil -dspublish -f Pfad_zum_Zertifikat_der_Stammzertifizierungsstelle NTAAuthCA`

- 2 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 3 Erweitern Sie den Abschnitt **Computerkonfiguration** und wechseln Sie zu **Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien öffentlicher Schlüssel**.
- 4 Importieren Sie das Zertifikat.

Option	Beschreibung
Stammzertifikat	<ol style="list-style-type: none"> Klicken Sie mit der rechten Maustaste auf Vertrauenswürdige Stammzertifizierungsstellen und wählen Sie Importieren. Folgen Sie den Anweisungen des Assistenten, um das Stammzertifikat (z.B. rootCA.cer) zu importieren. Klicken Sie anschließend auf OK.
Zwischenzertifikat	<ol style="list-style-type: none"> Klicken Sie mit der rechten Maustaste auf Zwischenzertifizierungsstellen und wählen Sie Importieren. Folgen Sie den Anweisungen des Assistenten, um das Zwischenzertifikat (z.B. intermediateCA.cer) zu importieren. Klicken Sie anschließend auf OK.

- 5 Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

Sämtliche Systeme in der Domäne verfügen nun über Zertifikatinformationen in ihren Speichern für vertrauenswürdige Stammzertifikate und Zwischenzertifikate, durch die sie diese Zertifikate als vertrauenswürdig einstufen können.

Konfigurieren von Horizon Client für Mac, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen

Wenn ein Serverzertifikat von einer für die Computer, auf denen Horizon Client für Mac ausgeführt wird, nicht vertrauenswürdigen Zertifizierungsstelle signiert wurde, können Sie diese Computer so konfigurieren, dass sie dem Stamm- und den Zwischenzertifikaten vertrauen. Sie müssen das Stammzertifikat und alle Zwischenzertifikate in der Vertrauenskette an die Clientcomputer verteilen.

Vorgehensweise

- 1 Stellen Sie das Stammzertifikat und Zwischenzertifikate für den Computer bereit, auf dem Horizon Client für Mac ausgeführt wird
- 2 Öffnen Sie das Stammzertifikat auf dem Mac-Computer.

Das Zertifikat gibt die folgende Meldung aus: Sollen von Ihrem Computer die von *Name der Zertifizierungsstelle* signierten Zertifikate ab jetzt als vertrauenswürdig eingestuft werden?

- 3 Klicken Sie auf **Immer vertrauen**

- 4 Geben Sie das Benutzerkennwort ein.
- 5 Wiederholen Sie die Schritte 2 bis 4 für alle Zwischenzertifikate in der Vertrauenskette.

Konfigurieren von Horizon Client für iOS, um Stamm- und Zwischenzertifikate als vertrauenswürdig einzustufen

Wenn ein Serverzertifikat von einer für die iPads und iPhones, auf denen Horizon Client für iOS ausgeführt wird, nicht vertrauenswürdigen Zertifizierungsstelle signiert wurde, können Sie die Geräte so konfigurieren, dass sie dem Stammzertifikat und den Zwischenzertifikaten vertrauen. Sie müssen das Stammzertifikat und alle Zwischenzertifikate in der Vertrauenskette an die Geräte verteilen.

Vorgehensweise

- 1 Senden Sie das Stammzertifikat und die Zwischenzertifikate als E-Mail-Anlagen an das iPad.
- 2 Öffnen Sie die E-Mail-Anlage mit dem Stammzertifikat und wählen Sie **Installieren** aus.

Das Zertifikat zeigt die folgende Meldung an:

Nicht nachweisbares Profil. Die Authentizität von *Zertifikatname* kann nicht überprüft werden. Durch die Installation dieses Profils werden Einstellungen auf Ihrem iPad geändert. Stammzertifikat. Durch die Installation des Zertifikats *Zertifikatname* wird es der Liste vertrauenswürdiger Zertifikate auf Ihrem iPad hinzugefügt.

- 3 Wählen Sie noch einmal **Installieren** aus.
- 4 Wiederholen Sie die Schritte 2 und 3 für alle Zwischenzertifikate in der Vertrauenskette.

Konfigurieren der Zertifikatsperrüberprüfung für Serverzertifikate

Jede View-Verbindungsserver-Instanz führt eine Zertifikatsperrüberprüfung für ihre eigenen Zertifikate und für die Zertifikate auf dem Sicherheitsserver durch, mit dem der Verbindungsserver kombiniert ist. Darüber hinaus überprüft jede Instanz die Zertifikate von vCenter- und View Composer Servern, wenn sie eine Verbindung mit diesen Servern herstellt. Standardmäßig werden mit Ausnahme des Stammzertifikats alle Zertifikate in der Kette überprüft. Sie können diese Standardeinstellung jedoch ändern.

Wenn ein SAML 2.0-Authentifikator für die Verwendung durch eine View-Verbindungsserver-Instanz konfiguriert ist, führt der View-Verbindungsserver auch für das SAML 2.0-Serverzertifikat eine Zertifikatsperrüberprüfung durch.

View unterstützt verschiedene Methoden zur Zertifikatsperrüberprüfung, z. B. Zertifikatsperrlisten und OCSP (Online Certificate Status Protocol). Eine Zertifikatsperrliste ist eine Liste mit gesperrten Zertifikaten, die von der Zertifizierungsstelle veröffentlicht wird, die das Zertifikat ausgestellt hat. OCSP ist ein Zertifikatüberprüfungsprotokoll, das zum Abrufen des Sperrstatus eines X.509-Zertifikats verwendet wird.

Mit Zertifikatsperrlisten wird die Liste der widerrufenen Zertifikate von einem Verteilungspunkt für Zertifikate heruntergeladen, der häufig im Zertifikat angegeben ist. Der Server lädt die Liste regelmäßig über die im Zertifikat angegebene URL dieses Verteilungspunkts herunter und prüft, ob das Serverzertifikat widerrufen wurde. Mit OCSP sendet der Server eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus des Zertifikats zu ermitteln.

Wenn Sie ein Serverzertifikat von einer Zertifizierungsstelle eines Drittanbieters erwerben, umfasst das Zertifikat mindestens eine Methode zum Ermitteln des Sperrstatus. Dazu zählen z. B. die URL eines Verteilungspunkts für Zertifikatsperrlisten oder die URL eines OCSP-Antwortdiensts. Wenn Sie über eine eigene Zertifizierungsstelle verfügen und ein Zertifikat generieren, ohne Sperrinformationen aufzunehmen, schlägt die Zertifikatsperrüberprüfung fehl. Ein Beispiel für Sperrinformationen ist z. B. die URL eines webbasierten Verteilungspunkts für Zertifikatsperrlisten auf einem Server, auf dem eine solche Zertifikatsperrliste gehostet wird.

Wenn Sie über eine eigene Zertifizierungsstelle verfügen, jedoch keine Sperrinformationen für ein Zertifikat aufnehmen bzw. aufnehmen können, können Sie festlegen, dass für sämtliche oder bestimmte Zertifikate in der Kette keine Zertifikatsperrüberprüfung durchgeführt wird. Sie können auf dem Server mithilfe des Registrierungs-Editors von Windows unter **HKLM\Software\VMware, Inc.\VMware VDM\Security** den Zeichenkettenwert (REG_SZ) `CertificateRevocationCheckType` erstellen und diesen Wert auf einen der folgenden Datenwerte festlegen.

Wert	Beschreibung
1	Es wird keine Zertifikatsperrüberprüfung durchgeführt.
2	Es werden lediglich Serverzertifikate überprüft. Weitere Zertifikate in der Kette werden nicht überprüft.
3	Es werden alle Zertifikate in der Kette überprüft.
4	(Standardwert) Mit Ausnahme des Stammzertifikats werden alle Zertifikate überprüft.

Wenn dieser Registrierungswert nicht oder auf einen ungültigen Wert (einen anderen Wert als 1, 2, 3 oder 4) festgelegt wird, werden mit Ausnahme des Stammzertifikats alle Zertifikate überprüft. Legen Sie diesen Registrierungswert auf jedem Server fest, auf dem die Zertifikatsperrüberprüfung geändert werden soll. Nach dem Festlegen dieses Werts muss das System nicht gestartet werden.

HINWEIS Wenn Ihre Organisation für den Internetzugriff Proxyeinstellungen verwendet, müssen Sie Ihre View-Verbindungsserver-Computer möglicherweise für die Verwendung dieser Proxyeinstellungen konfigurieren. Auf diese Weise wird sichergestellt, dass die Zertifikatsperrüberprüfung für Sicherheitsserver oder View-Verbindungsserver-Instanzen durchgeführt werden kann, die für sichere Clientverbindungen verwendet werden. Wenn eine View-Verbindungsserver-Instanz nicht auf das Internet zugreifen kann, schlägt die Zertifikatsperrüberprüfung möglicherweise fehl und die View-Verbindungsserver-Instanz oder kombinierte Sicherheitsserver werden auf dem View Administrator-Dashboard möglicherweise mit roter Markierung angezeigt. Informationen zum Beheben dieses Problems finden Sie unter „Behandeln von Problemen bei der Zertifikatsperrüberprüfung für Sicherheitsserver“ im Dokument *Administration von View*.

Konfigurieren des PCoIP Secure Gateway zur Nutzung eines Neuen SSL-Zertifikats

Um Industrie- oder Gesetzessicherheitsvorschriften zu entsprechen, können Sie das Standard-SSL-Zertifikat ersetzen, das vom PCoIP Secure Gateway (PSG) Service mit einem von einer Zertifizierungsstelle signierten Zertifikat erzeugt wird.

In View 5.2 oder in späteren Versionen erstellt der PSG-Dienst ein selbst signiertes SSL-Standardzertifikat, wenn der Dienst gestartet wird. Der PSG-Dienst präsentiert das selbst signierte Zertifikat den Clients, die Horizon Client 2.0 (oder Horizon Client 5.2 für Windows) oder spätere Versionen ausführen und sich mit dem PSG verbinden.

Das PSG bietet auch ein Standard-Legacy-SSL-Zertifikat, das Clients präsentiert wird, die ältere Clients oder ältere Versionen ausführen und sich mit dem PSG verbinden.

Die Standardzertifikate bieten sichere Verbindungen von Client-Endpunkten zum PSG und erfordern keine weitere Konfiguration in View Administrator. Allerdings wird die Konfiguration des PSG-Dienstes für die Nutzung eines CA-signierten Zertifikats dringend empfohlen, und dies besonders für Inbetriebnahmen, bei denen Sie Sicherheitsscanner verwenden müssen, um die Compliance-Tests zu bestehen.

Es ist zwar nicht erforderlich, aber sehr wahrscheinlich, dass Sie für Ihre Server neue, von einer Zertifizierungsstelle signierte SSL-Zertifikate konfigurieren, bevor Sie das Standard-PSG-Zertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzen. Die folgenden Verfahren gehen davon aus, dass Sie für den Server, auf dem das PSG läuft, bereits ein von einer Zertifizierungsstelle signiertes Zertifikat in den Windows-Zertifikatspeicher importiert haben.

HINWEIS Wenn Sie einen Sicherheitsscanner für Compliance-Tests verwenden, empfiehlt es sich möglicherweise, zunächst das PSG so einzustellen, dass es dasselbe Zertifikat wie der Server verwendet, und den View-Port vor dem PSG-Port zu scannen. Sie können Vertrauens- oder Validierungsprobleme, die während des Scans des View Ports auftreten, lösen, um sicherzustellen, dass diese Probleme Ihren Test des PSG Ports und Zertifikats nicht ungültig machen. Als nächstes können Sie ein einzigartiges Zertifikat für das PSG konfigurieren und einen weiteren Scan durchführen.

Vorgehensweise

- 1 [Sicherstellen, dass der Servername dem PSG-Zertifikatsthemenamen entspricht](#) auf Seite 104
Wenn eine View-Verbindungsserver-Instanz oder Sicherheitsserver installiert ist, erstellt das Installationsprogramm eine Registrierungseinstellung mit einem Wert, der den FQDN des Computers enthält. Sie müssen sicherstellen, dass dieser Wert dem Servernamensteil der URL entspricht, mit deren Hilfe Sicherheitsscanner den PSG-Port erreichen. Der Servername muss auch dem Themenamen oder einem alternativen Themenamen (SAN) des SSL-Zertifikats entsprechen, das Sie für das PSG verwenden wollen.
- 2 [Konfigurieren eines PSG-Zertifikats im Windows-Zertifikatspeicher](#) auf Seite 105
Um ein Standard-PSG-Zertifikat mit einem CA-signierten Zertifikat zu ersetzen, müssen Sie das Zertifikat und den privaten Schlüssel im lokalen Windows-Zertifikatspeicher auf dem View-Verbindungsserver oder dem Sicherheitsserver-Computer, auf dem PSG läuft, konfigurieren.
- 3 [Festlegen des Anzeigenamens des PSG-Zertifikats in der Windows-Registrierung](#) auf Seite 106
Das PSG identifiziert das zu verwendende SSL-Zertifikat anhand des Servernamens und den Anzeigenamens des Zertifikats. Sie müssen den Wert für den Anzeigenamen in der Windows-Registrierung auf dem View-Verbindungsserver oder Sicherheitsserver-Computer einrichten, auf dem das PSG läuft.
- 4 [\(Optional\) Erzwingen, dass ein CA-signiertes Zertifikat für die Verbindungen mit dem PSG benutzt wird](#) auf Seite 107
Sie können sicherstellen, dass alle Clientverbindungen mit dem PSG das von der Zertifizierungsstelle signierte Zertifikat für das PSG anstelle des Standard-Legacy-Zertifikats verwenden. Dieses Verfahren ist nicht erforderlich, um ein CA-Zertifikat für das PSG zu konfigurieren. Führen Sie diese Schritte nur dann aus, wenn es sinnvoll ist, die Verwendung eines von der Zertifizierungsstelle signierten Zertifikats in Ihrer View-Bereitstellung zu erzwingen.

Sicherstellen, dass der Servername dem PSG-Zertifikatsthemenamen entspricht

Wenn eine View-Verbindungsserver-Instanz oder Sicherheitsserver installiert ist, erstellt das Installationsprogramm eine Registrierungseinstellung mit einem Wert, der den FQDN des Computers enthält. Sie müssen sicherstellen, dass dieser Wert dem Servernamensteil der URL entspricht, mit deren Hilfe Sicherheitsscanner den PSG-Port erreichen. Der Servername muss auch dem Themenamen oder einem alternativen Themenamen (SAN) des SSL-Zertifikats entsprechen, das Sie für das PSG verwenden wollen.

Wenn beispielsweise ein Scanner sich mit der URL `https://view.customer.com:4172` mit dem PSG verbindet, muss die Registrierungseinstellung den Wert `view.customer.com` haben. Beachten Sie, dass der FQDN des View-Verbindungsserver oder Sicherheitsserver-Computers, der während der Installation festgelegt wurde, eventuell nicht dasselbe wie dieser externe Servername ist.

Vorgehensweise

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem View-Verbindungsserver- oder Sicherheitsserver-Host, auf dem das PCoIP Secure Gateway läuft.
- 2 Navigieren Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni.
- 3 Stellen Sie sicher, dass der Wert der Einstellung SSLCertPsgSni dem Servernamen in der URL entspricht, den Scanner verwenden, um das PSG zu erreichen und dem Themennamen oder alternativen Themennamen des SSL-Zertifikats entspricht, das Sie auf dem PSG installieren möchten.

Wenn der Wert nicht passt, ersetzen Sie ihn durch den richtigen Wert.
- 4 Starten Sie den Dienst „VMware Horizon View PCoIP Secure Gateway“ neu, damit Ihre Änderungen wirksam werden.

Weiter

Importieren Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers und konfigurieren Sie den Zertifikatanzeigenamen.

Konfigurieren eines PSG-Zertifikats im Windows-Zertifikatspeicher

Um ein Standard-PSG-Zertifikat mit einem CA-signierten Zertifikat zu ersetzen, müssen Sie das Zertifikat und den privaten Schlüssel im lokalen Windows-Zertifikatspeicher auf dem View-Verbindungsserver oder dem Sicherheitsserver-Computer, auf dem PSG läuft, konfigurieren.

Wenn PSG ein einzigartiges Zertifikat verwenden soll, müssen Sie das Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers mit einem exportierbaren privaten Schlüssel importieren und den entsprechenden Anzeigenamen festlegen.

Wenn das PSG dasselbe Zertifikat wie der Server verwenden soll, müssen Sie dieses Verfahren nicht anwenden. Allerdings müssen Sie in der Windows-Registrierung den Servernamen so festlegen, dass er mit dem Antragstellernamen des Serverzertifikats übereinstimmt, und den Anzeigenamen auf **vdm** einstellen.

Voraussetzungen

- Stellen Sie sicher, dass die Schlüssellänge mindestens 1024 Bits beträgt.
- Stellen Sie sicher, dass das SSL-Zertifikat gültig ist. Die aktuelle Zeit auf dem Server-Computer muss innerhalb des Start- und Enddatums des Zertifikats liegen.
- Stellen Sie sicher, dass der Zertifikatsthemenname oder ein alternativer Subjektnamen mit den Einstellungen SSLCertPsgSni in der Windows-Registrierung übereinstimmt. Siehe [„Sicherstellen, dass der Servername dem PSG-Zertifikatsthemenamen entspricht“](#), auf Seite 104.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe [„Hinzufügen des Zertifikat-Snap-Ins zu MMC“](#), auf Seite 95.
- Machen Sie sich mit dem Import eines Zertifikats in dem Windows-Zertifikatspeicher vertraut. Siehe [„Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“](#), auf Seite 96.
- Machen Sie sich mit der Modifizierung des Anzeigenamens des Zertifikats vertraut. Siehe [„Ändern des Anzeigenamens eines Zertifikats“](#), auf Seite 97.

Vorgehensweise

- 1 Öffnen Sie im MMC-Fenster auf dem Windows Server-Host den Ordner **Zertifikate (Lokaler Computer) > Persönlich**.

- 2 Importieren Sie das an PSG ausgegebene SSL-Zertifikat, indem Sie **Weitere Aktionen > Alle Aufgaben > Importieren** auswählen.

Wählen Sie die folgenden Einstellungen im Assistenten Zertifikat Import:

- a **Markieren Sie diesen Schlüssel als exportierbar**
- b **Schließen Sie alle erweiterbaren Eigenschaften mit ein**

Schließen Sie den Assistenten, um das Importieren des Zertifikats in den Ordner **Persönlich** zu beenden

- 3 Stellen Sie sicher, dass das neue Zertifikat einen privaten Schlüssel enthält, indem Sie einen dieser Schritte ausführen:
 - Stellen Sie sicher, dass ein gelber Schlüssel auf dem Symbol Zertifikat erscheint.
 - Doppelklicken Sie auf das Zertifikat, und überprüfen Sie, dass die folgende Anweisung im Dialogfeld Zertifikatsinformationen erscheint: *Sie besitzen einen privaten Schlüssel für dieses Zertifikat..*
- 4 Klicken Sie mit der rechten Maustaste auf das neue Zertifikat und anschließend auf **Eigenschaften**.
- 5 Auf der Registerkarte Allgemein löschen Sie den Text **Anzeigename** und geben den Anzeigenamen ein, den Sie gewählt haben.

Stellen Sie sicher, dass Sie genau denselben Namen in die Einstellung SSLCertWinCertFriendlyName in der Windows-Registrierung eingeben, wie im nächsten Verfahren beschrieben.
- 6 Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Das PSG präsentiert das von einer Zertifizierungsstelle signierte Zertifikat den Clientgeräten, die sich über PCoIP mit dem Server verbinden.

HINWEIS Dieses Verfahren hat keinen Einfluss auf Legacy-Clientgeräte. Das PSG präsentiert Legacy-Clientgeräten weiterhin das Standard-Legacy-Zertifikat, wenn diese sich über PCoIP mit dem Server verbinden.

Weiter

Konfigurieren Sie den Anzeigenamen des Zertifikats in der Windows-Registrierung.

Festlegen des Anzeigenamens des PSG-Zertifikats in der Windows-Registrierung

Das PSG identifiziert das zu verwendende SSL-Zertifikat anhand des Servernamens und den Anzeigenamen des Zertifikats. Sie müssen den Wert für den Anzeigenamen in der Windows-Registrierung auf dem View-Verbindungsserver oder Sicherheitsserver-Computer einrichten, auf dem das PSG läuft.

Der Zertifikatsanzeigename **vdm** wird von allen View-Verbindungsserver-Instanzen und Sicherheitsservern verwendet. Im Gegensatz dazu können Sie Ihren eigenen Zertifikatsanzeigenamen für das PSG-Zertifikat konfigurieren. Sie müssen eine Windows-Registrierungseinstellung konfigurieren, um das PSG in die Lage zu versetzen, den richtigen Namen mit dem Anzeigenamen abzugleichen, den Sie im Windows-Zertifikatspeicher einstellen werden.

Das PSG kann dasselbe SSL-Zertifikat wie der Server verwenden, auf dem das PSG läuft. Wenn Sie das PSG so konfigurieren, dass es dasselbe Zertifikat wie der Server verwendet, muss der Anzeigename **vdm** sein.

Der Anzeigenamenwert beachtet in der Registrierung und im Windows-Zertifikatspeicher die Groß- und Kleinschreibung.

Voraussetzungen

- Stellen Sie sicher, dass die Windows-Registrierung den richtigen Subjektnamen enthält, der dazu verwendet wird, um den PSG-Port zu erreichen und der dem PSG-Zertifikatssubjektnamen oder dem alternativen Subjektnamen entspricht. Siehe „Sicherstellen, dass der Servername dem PSG-Zertifikatsthemenamen entspricht“, auf Seite 104.
- Stellen Sie sicher, dass der Anzeigename des Zertifikats im lokalen Windows-Zertifikatsspeicher des Computers konfiguriert ist. Siehe „Konfigurieren eines PSG-Zertifikats im Windows-Zertifikatsspeicher“, auf Seite 105.

Vorgehensweise

- 1 Starten Sie den Windows Registrierungs-Editor auf dem View-Verbindungsserver oder Sicherheitsserver-Computer, auf dem das PCoIP Secure Gateway läuft.
- 2 Navigieren Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway.
- 3 Fügen Sie einen neuen Zeichenfolgenwert (G_SZ) SSLCertWinCertFriendlyName zu diesem Registrierungsschlüssel hinzu.
- 4 Ändern Sie den Wert SSLCertWinCertFriendlyName und geben Sie den Zertifikatsanzeigenamen ein, der von dem PSG verwendet werden.

Beispiel: **pcoip**

Wenn Sie dasselbe Zertifikat wie der Server verwenden, muss der Wert **vdm** sein.

- 5 Starten Sie den Dienst „VMware Horizon View PCoIP Secure Gateway“ neu, damit Ihre Änderungen wirksam werden.

Weiter

Stellen Sie sicher, dass sich Clientgeräte auch weiterhin mit dem PSG verbinden.

Wenn Sie einen Sicherheitsscanner für Compliance-Tests verwenden, scannen Sie den PSG-Port.

(Optional) Erzwingen, dass ein CA-signiertes Zertifikat für die Verbindungen mit dem PSG benutzt wird

Sie können sicherstellen, dass alle Clientverbindungen mit dem PSG das von der Zertifizierungsstelle signierte Zertifikat für das PSG anstelle des Standard-Legacy-Zertifikats verwenden. Dieses Verfahren ist nicht erforderlich, um ein CA-Zertifikat für das PSG zu konfigurieren. Führen Sie diese Schritte nur dann aus, wenn es sinnvoll ist, die Verwendung eines von der Zertifizierungsstelle signierten Zertifikats in Ihrer View-Bereitstellung zu erzwingen.

In einigen Fällen kann es sein, dass das PSG das Standard-Legacy-Zertifikat, anstelle des CA-signierten Zertifikats gegenüber einem Sicherheitsscanner präsentiert, und damit den Compliance-Test auf dem PSG-Port ungültig macht. Um dieses Problem zu beheben, können Sie das PSG so konfigurieren, dass es keinem Gerät das Standard-Legacy-Zertifikat präsentiert, das eine Verbindung herzustellen versucht.

WICHTIG Dieses Verfahren stellt sicher, dass keine Legacy-Clients über PCoIP eine Verbindung mit diesem Server herstellen.

Voraussetzungen

Stellen Sie sicher, dass alle Clientgeräte, einschließlich Thin Clients, die eine Verbindung mit diesem Server herstellen, Horizon Client 5.2 für Windows oder Horizon Client 2.0 oder höhere Versionen ausführen. Sie müssen die Legacy-Clients aktualisieren.

Vorgehensweise

- 1 Starten Sie den Windows Registrierungs-Editor auf dem View-Verbindungsserver oder Sicherheitsserver-Computer, auf dem das PCoIP Secure Gateway läuft.
- 2 Navigieren Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway.
- 3 Fügen Sie einen neuen Zeichenfolgenwert (G_SZ) SSLCertPresentLegacyCertificate zu diesem Registrierungsschlüssel hinzu.
- 4 Stellen Sie den Wert SSLCertPresentLegacyCertificate 0.
- 5 Starten Sie den Dienst „VMware Horizon View PCoIP Secure Gateway“ neu, damit Ihre Änderungen wirksam werden.

Konfigurieren von View Administrator, um ein vCenter Server- oder View Composer-Zertifikat als vertrauenswürdig einzustufen

Auf dem View Administrator-Dashboard kann View so konfiguriert werden, dass ein als nicht vertrauenswürdig eingestuftes vCenter Server- oder View Composer-Zertifikat als vertrauenswürdig eingestuft wird.

VMware empfiehlt dringend, vCenter Server und View Composer für die Verwendung von SSL-Zertifikaten zu konfigurieren, die von einer Zertifizierungsstelle signiert wurden. Alternativ können Sie den Fingerabdruck des Standardzertifikats für vCenter Server oder View Composer akzeptieren.

Gleichermaßen empfiehlt VMware, SAML 2.0-Authentifikatoren für die Verwendung von SSL-Zertifikaten zu konfigurieren, die von einer Zertifizierungsstelle signiert wurden. Alternativ können Sie auf dem View Administrator-Dashboard festlegen, dass View ein nicht als vertrauenswürdig eingestuftes SAML 2.0-Serverzertifikat als vertrauenswürdig einstuft, indem Sie den Fingerabdruck des Standardzertifikats akzeptieren.

Vorteile der Verwendung von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden

Eine Zertifizierungsstelle ist eine vertrauenswürdige Instanz, welche die Identität des Zertifikats und seines Erstellers bestätigt. Wenn ein Zertifikat durch eine vertrauenswürdige Zertifizierungsstelle signiert wurde, werden die Benutzer nicht länger über Meldungen aufgefordert, das Zertifikat zu überprüfen, und Thin Client-Geräte können ohne zusätzliche Konfiguration eine Verbindung herstellen.

Sie können ein SSL-Serverzertifikat anfordern, das für eine Webdomäne wie `www.mycorp.com` spezifisch ist, oder Sie können ein SSL-Platzhalterserverzertifikat anfordern, das innerhalb der gesamten Domäne, z. B. `*.mycorp.com`, verwendet werden kann. Um die Verwaltung zu vereinfachen, können Sie ein Platzhalterzertifikat anfordern, wenn Sie das Zertifikat auf mehreren Servern oder Subdomänen installieren müssen.

Normalerweise werden domänenspezifische Zertifikate in sicheren Installationen verwendet, und die Zertifizierungsstellen sichern für domänenspezifische Zertifikate im Allgemeinen höheren Schutz vor Verlust als für Platzhalterzertifikate zu. Wenn Sie ein Platzhalterzertifikat verwenden, das mit anderen Diensten gemeinsam genutzt wird, richtet sich die Sicherheit des VMware Horizon-Produkts auch nach der Sicherheit der anderen Dienste. Wenn Sie ein Platzhalterzertifikat verwenden, müssen Sie sicherstellen, dass der private Schlüssel zwischen den Servern übertragbar ist.

Wenn Sie das Standardzertifikat durch Ihr eigenes Zertifikat ersetzen, verwenden Clients für die Authentifizierung des Servers Ihr eigenes Zertifikat. Wenn Ihr Zertifikat durch eine Zertifizierungsstelle signiert wurde, ist das Zertifikat für die Zertifizierungsstelle selbst in der Regel in den Browser eingebettet oder befindet sich in einer vertrauenswürdigen Datenbank, auf die der Client Zugriff hat. Nachdem ein Client das Zertifikat akzeptiert hat, sendet er als Antwort einen geheimen Schlüssel, der mit dem im Zertifikat enthaltenen öffentlichen Schlüssel verschlüsselt wird. Der geheime Schlüssel wird verwendet, um den Datenverkehr zwischen dem Client und dem Server zu verschlüsseln.

Fehlerbehebung bei Problemen mit Zertifikaten auf View-Verbindungsserver und -Sicherheitsservern

Wenn Probleme mit Zertifikaten auf einem ViewServer vorliegen, können Sie sich nicht bei View Administrator anmelden, oder der Systemzustand des Servers wird rot angezeigt.

Problem

In der View-Verbindungsserver-Instanz, auf der das Problem auftritt, können Sie sich nicht bei View Administrator anmelden. Wenn Sie in einer anderen View-Verbindungsserver-Instanz im selben Pod eine Verbindung mit View Administrator herstellen, wird der Systemzustand der problematischen View-Verbindungsserver-Instanz im Dashboard rot angezeigt.

Wenn Sie in der anderen View-Verbindungsserver-Instanz auf die rote Anzeige des Systemzustands klicken, wird SSL-Zertifikat: Ungültig und Status: (leer) angezeigt. Dies weist darauf hin, dass kein gültiges Zertifikat gefunden wurde. Die View-Protokolldatei enthält einen Eintrag des Typs FEHLER mit dem folgenden Fehlertext: Keine passenden Zertifikate im Schlüsselspeicher.

Die View-Protokolldaten befinden sich unter C:\ProgramData\VMware\VDM\logs\log-*.txt in der View-Verbindungsserver-Instanz.

Ursache

Wenn ein Zertifikat nicht ordnungsgemäß auf einem View-Server installiert ist, kann dies einen der folgenden Gründe haben:

- Das Zertifikat befindet sich nicht im Ordner „Persönlich“ des lokalen Windows-Zertifikatspeichers auf dem Computer.
- Der Zertifikatspeicher hat keinen privaten Schlüssel für das Zertifikat.
- Das Zertifikat hat nicht den Anzeigenamen **vdm**.
- Das Zertifikat wurde auf Grundlage einer V3-Zertifikatvorlage für Windows Server 2008 oder höher generiert. View kann keinen privaten Schlüssel erkennen, aber wenn Sie den Windows-Zertifikatspeicher mit dem Zertifikat-Snap-In überprüfen, gibt der Speicher an, dass ein privater Schlüssel vorhanden ist.

Lösung

- Stellen Sie sicher, dass das Zertifikat in den Ordner „Persönlich“ des lokalen Windows-Zertifikatspeichers auf dem Computer importiert wurde.
Siehe [„Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“](#), auf Seite 96.
- Überprüfen Sie, ob das Zertifikat einen privaten Schlüssel enthält.
Siehe [„Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“](#), auf Seite 96.
- Überprüfen Sie, ob das Zertifikat den Anzeigenamen **vdm** hat.
Siehe [„Ändern des Anzeigenamens eines Zertifikats“](#), auf Seite 97.
- Wenn das Zertifikat auf Grundlage einer V3-Zertifikatvorlage generiert wurde, fordern Sie ein gültiges, signiertes Zertifikat von einer Zertifizierungsstelle an, die keine V3-Vorlage verwendet.
Siehe [„Beziehen eines signierten SSL-Zertifikats von einer Zertifizierungsstelle“](#), auf Seite 92.

Erstmaliges Konfigurieren von View

Nachdem Sie die View Server-Software installiert und SSL-Zertifikate für die Server konfiguriert haben, müssen Sie einige zusätzliche Schritte durchführen, um eine funktionierende View-Umgebung einzurichten.

Sie konfigurieren Benutzerkonten für vCenter Server und View Composer, installieren einen View-Lizenzschlüssel, fügen vCenter Server und View Composer Ihrer View-Umgebung hinzu, konfigurieren das PCoIP Secure Gateway und den sicheren Tunnel und ändern optional die Windows Server-Einstellungen so, dass sie Ihre View-Umgebung unterstützen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Konfigurieren von Benutzerkonten für vCenter Server und View Composer“](#), auf Seite 111
- [„Anfängliches Konfigurieren von View-Verbindungsserver“](#), auf Seite 115
- [„Konfigurieren von Horizon Client-Verbindungen“](#), auf Seite 128
- [„Ersetzen von Standardports für View-Dienste“](#), auf Seite 136
- [„Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung“](#), auf Seite 142

Konfigurieren von Benutzerkonten für vCenter Server und View Composer

Um vCenter Server mit View einzusetzen, müssen Sie ein Benutzerkonto mit entsprechenden vCenter Server-Rechten erstellen. Sie können eine vCenter Server-Rolle mit den entsprechenden Rechten erstellen und diese Rolle dem vCenter Server-Benutzerkonto zuweisen.

Wenn Sie View Composer auf einem anderen Computer als vCenter Server installieren, müssen Sie auch ein Benutzerkonto in Active Directory erstellen, das View für die Authentifizierung beim View Composer-Dienst auf dem eigenständigen Computer verwenden kann.

Wenn Sie View Composer verwenden, müssen Sie ein drittes Benutzerkonto in Active Directory erstellen, mit dem View Composer bestimmte Vorgänge in Active Directory ausführen kann. View Composer benötigt dieses Konto, um virtuelle Linked-Clone-Maschinen zur Active Directory-Domäne hinzuzufügen. Siehe [„Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge“](#), auf Seite 34.

Bei der erstmaligen Konfiguration von View erstellen Sie demnach also die folgenden Benutzerkonten in View Administrator:

- Der vCenter Server-Benutzer ermöglicht View und View Composer die Ausführung von Vorgängen in vCenter Server.
- Der eigenständige View Composer Server-Benutzer ermöglicht View die Authentifizierung beim View Composer-Dienst auf einem eigenständigen Computer.

Wenn Sie View Composer auf demselben Computer wie vCenter Server installieren, führt der vCenter Server-Benutzer die beiden vorausgehenden Funktionen aus, und Sie verwenden keinen eigenständigen View Composer Server-Benutzer.

- Der View Composer-Benutzer für AD-Vorgänge ermöglicht View Composer die Ausführung bestimmter Vorgänge in Active Directory.

Verwendungsmöglichkeiten von vCenter Server- und View Composer-Benutzern

Nachdem Sie diese Benutzerkonten erstellt und konfiguriert haben, geben Sie die Benutzernamen in View Administrator an.

- Sie geben einen vCenter Server-Benutzer an, wenn Sie vCenter Server zu View hinzufügen.
- Sie geben einen eigenständigen View Composer Server-Benutzer an, wenn Sie View Composer-Einstellungen konfigurieren und **Eigenständiger View Composer Server** auswählen.
- Sie geben einen View Composer-Benutzer für AD-Vorgänge an, wenn Sie View Composer-Domänen konfigurieren.
- Sie geben den View Composer-Benutzer für AD-Vorgänge an, wenn Sie Linked-Clone-Pools erstellen.

Konfigurieren eines vCenter Server-Benutzers für View und View Composer

Um ein Benutzerkonto zu konfigurieren, mit dem View Vorgänge in vCenter Server ausführen kann, müssen Sie diesem Benutzer eine vCenter Server-Rolle mit den entsprechenden Rechten zuweisen.

Die Liste der Rechte, die Sie zur vCenter Server-Rolle hinzufügen müssen, hängt davon ab, ob Sie View mit oder ohne View Composer verwenden. Mit dem View Composer-Dienst werden Vorgänge in vCenter Server ausgeführt, die neben den Basisrechten zusätzliche Rechte erfordern.

Wenn Sie View Composer auf demselben Computer wie vCenter Server installieren, müssen Sie den vCenter Server-Benutzer als lokalen Systemadministrator auf dem vCenter Server-Computer konfigurieren. Dies ermöglicht View die Authentifizierung beim View Composer-Dienst.

Wenn Sie View Composer auf einem anderen Computer als vCenter Server installieren, müssen Sie den vCenter Server-Benutzer nicht als lokalen Administrator auf dem vCenter Server-Computer konfigurieren. Sie müssen jedoch ein eigenständiges View Composer Server-Benutzerkonto erstellen, das ein lokaler Administrator auf dem View Composer-Computer sein muss.

Voraussetzungen

- Erstellen Sie in Active Directory einen Benutzer in der View-Verbindungsserver-Domäne oder einer vertrauenswürdigen Domäne. Siehe [„Erstellen eines Benutzerkontos für vCenter Server“](#), auf Seite 34.
- Machen Sie sich mit den vCenter Server-Berechtigungen vertraut, die für das Benutzerkonto erforderlich sind. Siehe [„Für den vCenter Server-Benutzer erforderliche Berechtigungen“](#), auf Seite 113.
- Wenn Sie View Composer verwenden, machen Sie sich mit den zusätzlich erforderlichen Berechtigungen vertraut. Siehe [„Erforderliche View Composer-Berechtigungen für den vCenter Server-Benutzer“](#), auf Seite 115.

Vorgehensweise

- 1 Bereiten Sie in vCenter Server eine Rolle mit den erforderlichen Berechtigungen für den Benutzer vor.
 - Sie können die vordefinierte Administratorrolle in vCenter Server verwenden. Diese Rolle kann alle Aufgaben in vCenter Server ausführen.
 - Wenn Sie View Composer verwenden, können Sie eine eingeschränkte Rolle mit den Mindestberechtigungen erstellen, die der View-Verbindungsserver und View Composer zur Durchführung von vCenter Server-Vorgängen benötigen.

Klicken Sie in vSphere Client auf **Home > Rollen > Rolle hinzufügen**, geben Sie einen Rollennamen wie beispielsweise **View Composer-Administrator** ein und wählen Sie Rechte für die Rolle aus.

Diese Rolle muss über alle Berechtigungen verfügen, die sowohl der View-Verbindungsserver als auch View Composer benötigen, um in vCenter Server Vorgänge auszuführen.

- Wenn Sie View ohne View Composer verwenden, können Sie eine noch stärker eingeschränkte Rolle mit den Mindestberechtigungen erstellen, die der View-Verbindungsserver zur Durchführung von vCenter Server-Vorgängen benötigt.

Klicken Sie in vSphere Client auf **Home > Rollen > Rolle hinzufügen**, geben Sie einen Rollennamen wie beispielsweise **View Manager-Administrator** ein und wählen Sie Rechte für die Rolle aus.

- 2 Klicken Sie in vSphere Client mit der rechten Maustaste auf die vCenter Server-Instanz der obersten Bestandslistenebene, klicken Sie auf **Berechtigung hinzufügen** und fügen Sie den vCenter Server-Benutzer hinzu.

HINWEIS Der vCenter Server-Benutzer muss auf vCenter Server-Ebene definiert werden.

- 3 Wählen Sie im Dropdown-Menü die Administratorrolle oder die View Composer- bzw. View Manager-Rolle aus, die Sie erstellt haben, und weisen Sie sie dem vCenter Server-Benutzer zu.
- 4 Wenn Sie View Composer auf demselben Computer wie vCenter Server installieren, fügen Sie das vCenter Server-Benutzerkonto als Mitglied der lokalen Systemadministratorgruppe auf dem vCenter Server-Computer hinzu.

Dieser Schritt ist nicht erforderlich, wenn Sie View Composer auf einem anderen Computer als vCenter Server installieren.

Weiter

Geben Sie in View Administrator den vCenter Server-Benutzer an, wenn Sie vCenter Server zu View hinzufügen. Siehe „[Hinzufügen von vCenter Server-Instanzen zu View](#)“, auf Seite 117.

Für den vCenter Server-Benutzer erforderliche Berechtigungen

Der vCenter Server-Benutzer muss über ausreichende vCenter Server-Berechtigungen verfügen, damit View Vorgänge in vCenter Server durchführen kann. Erstellen Sie für den vCenter Server-Benutzer eine View Manager-Rolle mit den erforderlichen Berechtigungen.

Tabelle 9-1. Für die View Manager-Rolle benötigte Berechtigungen

Berechtigungsgruppe	Zu aktivierende Berechtigungen
Ordner	Ordner erstellen Ordner löschen
Datenspeicher	Speicherplatz zuordnen

Tabelle 9-1. Für die View Manager-Rolle benötigte Berechtigungen (Fortsetzung)

Berechtigungsgruppe	Zu aktivierende Berechtigungen
Virtuelle Maschine	<p>In Konfiguration:</p> <ul style="list-style-type: none"> ■ Gerät hinzufügen oder entfernen ■ Erweitert ■ Geräteeinstellungen ändern <p>In Interaktion:</p> <ul style="list-style-type: none"> ■ Ausschalten ■ Einschalten ■ Zurücksetzen ■ Anhalten ■ Zurücksetzungs- oder Verkleinerungsvorgänge ausführen <p>In Bestandsliste:</p> <ul style="list-style-type: none"> ■ Neue erstellen ■ Aus vorhandener erstellen ■ Entfernen <p>In Bereitstellung:</p> <ul style="list-style-type: none"> ■ Anpassen ■ Vorlage bereitstellen ■ Anpassungsspezifikation lesen ■ Vorlage klonen ■ Virtuelle Maschine klonen
Ressource	Virtuelle Maschine zu Ressourcenpool zuweisen
Global	<p>Als vCenter Server agieren</p> <p>Der vCenter Server-Benutzer erfordert dieses Recht, auch wenn Sie View Storage Accelerator nicht verwenden.</p>
Host	<p>Die folgende Host-Berechtigung ist erforderlich, um die View-Speicherbeschleunigung zu implementieren. Mit dieser Komponente wird das ESXi-Host-Caching ermöglicht. Wenn Sie die View-Speicherbeschleunigung nicht verwenden, benötigt der vCenter Server-Benutzer diese Berechtigung nicht.</p> <p>In Konfiguration:</p> <ul style="list-style-type: none"> ■ Erweiterte Einstellungen
Profilgesteuerter Speicher (Wenn Sie Virtual SAN-Datenspeicher oder virtuelle Volumes verwenden)	(alle)

Erforderliche View Composer-Berechtigungen für den vCenter Server-Benutzer

Zur Unterstützung von View Composer benötigt der vCenter Server-Benutzer neben den zur Unterstützung von View erforderlichen Berechtigungen zusätzliche Berechtigungen. Erstellen Sie für den vCenter Server-Benutzer eine View Composer-Rolle mit den View Manager-Berechtigungen und diesen zusätzlichen Berechtigungen.

Tabelle 9-2. View Composer-Berechtigungen

Berechtigungsgruppe	Zu aktivierende Berechtigungen
Datenspeicher	Speicherplatz zuordnen Datenspeicher durchsuchen Dateioperationen auf unterer Systemebene
Virtuelle Maschine	Bestandsliste (alle) Konfiguration (alle) Snapshot-Verwaltung (alle) In Bereitstellung: <ul style="list-style-type: none"> ■ Virtuelle Maschine klonen ■ Festplattenzugriff zulassen
Ressource	Virtuelle Maschine zu Ressourcenpool zuweisen Die folgende Berechtigung ist erforderlich, um View Composer ausgleichende Operationen durchzuführen. Ausgeschaltete virtuelle Maschine migrieren
Global	Methoden aktivieren Methoden deaktivieren Systemkennzeichen Die folgende Berechtigung ist erforderlich, um die View-Speicherbeschleunigung zu implementieren. Mit dieser Komponente wird das ESXi-Host-Caching ermöglicht. Wenn Sie die View-Speicherbeschleunigung nicht verwenden, benötigt der vCenter Server-Benutzer diese Berechtigung nicht. Agieren als vCenter Server
Netzwerk	(alle)
Profilgesteuerter Speicher	(alle, wenn Sie Virtual SAN-Datenspeicher oder virtuelle Volumes verwenden)

Anfängliches Konfigurieren von View-Verbindungsserver

Nach der Installation des View-Verbindungsservers müssen Sie eine Produktlizenz installieren sowie vCenter Server und View Composer-Dienste zu View hinzufügen. Sie können auch zulassen, dass ESXi-Hosts Speicherplatz auf virtuellen Maschinen mit verknüpften Klonen freigeben, und Sie können ESXi-Hosts so konfigurieren, dass Festplattendaten von virtuellen Maschinen zwischengespeichert werden.

Wenn Sie Sicherheitsserver installieren, werden sie automatisch zu View hinzugefügt und in View Administrator angezeigt.

Horizon Administrator und Horizon-Verbindungsserver

Horizon Administrator bietet eine webbasierte Verwaltungsschnittstelle für Horizon 7.

Der Horizon-Verbindungsserver kann über mehrere Instanzen verfügen, die als Replizierungs- oder Sicherheitsserver dienen. Je nach Ihrer Horizon 7-Bereitstellung erhalten Sie eine eigene Horizon Administrator-Oberfläche mit jeder Instanz eines Verbindungsservers.

Wir empfehlen die folgenden Best Practices für die Verwendung von Horizon Administrator mit einem Verbindungsserver:

- Verwenden Sie den Hostnamen und die IP-Adresse des Verbindungsservers für die Anmeldung bei Horizon Administrator. Verwenden Sie die Horizon Administrator-Oberfläche zur Verwaltung des Verbindungsservers und jedes damit verbundenen Sicherheits- oder Replizierungsservers.
- Stellen Sie in einer Pod-Umgebung sicher, dass alle Administratoren den Hostnamen und die IP-Adresse desselben Verbindungsservers für die Anmeldung bei Horizon Administrator verwenden. Für den Zugriff auf eine Horizon Administrator-Webseite dürfen Sie keinesfalls den Hostnamen und die IP-Adresse des Lastausgleichsdienstes verwenden.

HINWEIS Wenn Sie anstelle von Sicherheitsservern Unified Access Gateway-Appliances benutzen, müssen Sie die Unified Access Gateway-REST-API zur Verwaltung der Unified Access Gateway-Appliances verwenden. Frühere Versionen von Unified Access Gateway wurden als „Access Point“ bezeichnet. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Anmelden an View Administrator

Zum Ausführen anfänglicher Konfigurationsaufgaben müssen Sie sich an View Administrator anmelden.

Voraussetzungen

Vergewissern Sie sich, dass Sie einen von View Administrator unterstützten Webbrowser verwenden. Siehe [„View Administrator-Anforderungen“](#), auf Seite 11.

Vorgehensweise

- 1 Öffnen Sie Ihren Webbrowser und geben Sie die folgende URL ein. Hierbei steht *Server* für den Hostnamen der Verbindungsserver-Instanz.

https://Server/admin

HINWEIS Um auf eine Verbindungsserver-Instanz zuzugreifen, deren Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem SSL-Zertifikat, das für die Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

Ihr Zugriff auf Horizon Administrator hängt von der Art Zertifikat ab, die auf dem Verbindungsserver-Computer konfiguriert ist.

Wenn Sie den Webbrowser auf dem Verbindungsserver-Host öffnen, verwenden Sie für die Verbindung **https://127.0.0.1** anstelle von **https://localhost**. Diese Methode ist sicherer, da mögliche DNS-Angriffe bei der localhost-Auflösung vermieden werden.

Option	Beschreibung
Sie haben ein Zertifikat konfiguriert, das von einer Zertifizierungsstelle für View-Verbindungsserver signiert ist.	Wenn Sie zum ersten Mal eine Verbindung herstellen, zeigt Ihr Webbrowser Horizon Administrator an.
Das standardmäßige selbst signierte Zertifikat, das mit View-Verbindungsserver bereitgestellt wird, ist konfiguriert.	Bei der ersten Verbindungsherstellung zeigt Ihr Webbrowser möglicherweise eine Warnung an, nach der das mit der Adresse verknüpfte Sicherheitszertifikat nicht durch eine vertrauenswürdige Zertifizierungsstelle ausgegeben wurde. Klicken Sie auf Ignorieren , um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren.

- 2 Melden Sie sich als Benutzer mit Anmeldeinformationen an, um auf das View Administrators-Konto zuzugreifen.

Sie geben ein View Administrator-Konto an, wenn Sie eine eigenständige Verbindungsserver-Instanz oder die erste Verbindungsserver-Instanz in einer replizierten Gruppe installieren. Das View Administrator-Konto kann die lokale Administratorengruppe (BUILTIN\Administrators) auf dem Verbindungsserver-Computer oder ein Domänenbenutzer- oder Gruppenkonto sein.

Nachdem Sie sich bei View Administrator angemeldet haben, können Sie **View-Konfiguration > Administratoren** auswählen, um die Liste der Benutzer und Gruppen zu ändern, die die Administratorrolle für View haben.

Installation des Produktlizenzschlüssels

Bevor Sie View-Verbindungsserver verwenden können, müssen Sie einen Produktlizenzschlüssel eingeben.

Bei der ersten Anmeldung zeigt View Administrator die Seite „Product Licensing and Usage“ (Produktlizenzierung und -verwendung) an.

Nachdem Sie den Lizenzschlüssel installiert haben, wird bei der Anmeldung die Dashboard-Seite in View Administrator angezeigt.

Sie müssen keinen Lizenzschlüssel konfigurieren, wenn Sie eine replizierte View-Verbindungsserver-Instanz oder einen Sicherheitsserver installieren. Replizierte Instanzen und Sicherheitsserver verwenden den allgemeinen Lizenzschlüssel, der in der View LDAP-Konfiguration gespeichert ist.

HINWEIS View-Verbindungsserver erfordern einen gültigen Lizenzschlüssel. Ab der View-Version 4.0 umfasst der Produktlizenzschlüssel 25 Zeichen.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Produktlizenzierung und -verwendung** aus.
- 2 Klicken Sie im Bereich **Lizenzierung** auf **Lizenz bearbeiten**.
- 3 Geben Sie die Seriennummer der Lizenz ein und klicken Sie auf **OK**.
- 4 Überprüfen Sie das Ablaufdatum der Lizenz.
- 5 Überprüfen Sie, ob die Lizenzen für Desktops, die Remote-Ausführung von Anwendungen sowie View Composer aktiviert oder deaktiviert sind, je nach der VMware Horizon-Edition, zu deren Verwendung Ihre Produktlizenz Sie berechtigt.

Nicht alle Funktionen von VMware Horizon 7 sind in allen Editionen verfügbar. Einen Funktionsvergleich der einzelnen Editionen finden Sie unter

<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Hinzufügen von vCenter Server-Instanzen zu View

Sie müssen View zur Herstellung von Verbindungen mit den vCenter Server-Instanzen in Ihrer View-Bereitstellung konfigurieren. vCenter Server erstellt und verwaltet die virtuellen Maschinen, die View in Desktop-Pools verwendet.

Wenn Sie vCenter Server-Instanzen in einer Gruppe im verknüpften Modus ausführen, muss jede vCenter Server-Instanz View separat hinzugefügt werden.

View stellt über eine sichere Verbindung (SSL) eine Verbindung mit der vCenter Server-Instanz her.

Voraussetzungen

- Installieren Sie den View-Verbindungsserver-Produktlizenzschlüssel.

- Erstellen Sie einen vCenter Server-Benutzer mit der Berechtigung, Vorgänge in vCenter Server auszuführen, die zur Unterstützung von View erforderlich sind. Wenn Sie View Composer verwenden, müssen Sie dem Benutzer zusätzliche Berechtigungen gewähren.

Siehe „[Konfigurieren eines vCenter Server-Benutzers für View und View Composer](#)“, auf Seite 112.

- Überprüfen Sie, ob auf dem vCenter Server-Host ein TLS/SSL-Serverzertifikat installiert ist. Installieren Sie in einer Produktionsumgebung ein gültiges Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert ist.

In einer Testumgebung können Sie das Standardzertifikat verwenden, das zusammen mit vCenter Server installiert wird. Sie müssen jedoch den Zertifikatfingerabdruck akzeptieren, wenn Sie View zu vCenter Server hinzufügen.

- Überprüfen Sie, dass alle Instanzen von View-Verbindungsserver in der replizierten Gruppe dem Stamm-CA-Zertifikat für das Serverzertifikat vertrauen, das auf dem vCenter Server-Host installiert ist. Überprüfen Sie, ob sich das Stamm-CA-Zertifikat im Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** in den Zertifikatsspeichern der lokalen Windows-Computer auf den View-Verbindungsserver-Hosts befindet. Ist dies nicht der Fall, importieren Sie das Stamm-CA-Zertifikat in die Zertifikatsspeicher der lokalen Windows-Computer.

Siehe „[Importieren eines Stamm- und Zwischenzertifikats in einen Windows-Zertifikatsspeicher](#)“, auf Seite 97.

- Stellen Sie sicher, dass die vCenter Server-Instanz ESXi-Hosts enthält. Wenn in der vCenter Server-Instanz keine Hosts konfiguriert sind, können Sie die Instanz nicht zu View hinzufügen.
- Wenn Sie ein Upgrade auf vSphere 5.5 oder eine höhere Version durchführen, müssen Sie sicherstellen, dass dem Domänenadministratorkonto, das Sie als Benutzer von vCenter Server verwenden, explizit Berechtigungen zur Anmeldung bei vCenter Server über einen lokalen Benutzer von vCenter Server zugewiesen wurden.
- Wenn Sie View im FIPS-Modus verwenden möchten, müssen Sie über Hosts mit vCenter Server 6.0 oder höher und mit ESXi 6.0 oder höher verfügen.

Weitere Informationen finden Sie unter [Kapitel 4, „Installieren von View im FIPS-Modus“](#), auf Seite 29.

- Machen Sie sich mit den Einstellungen vertraut, die die maximalen Grenzwerte für Betriebsvorgänge für vCenter Server und View Composer festlegen. Siehe „[Grenzwerte für parallele Vorgänge für vCenter Server und View Composer](#)“, auf Seite 125 und „[Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen](#)“, auf Seite 126.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
- 3 Geben Sie im Textfeld **Serveradresse** der vCenter Server-Einstellungen den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der vCenter Server-Instanz ein.

Der FQDN umfasst den Hostnamen und den Domännennamen. Beispiel: Im FQDN **myserverhost.companydomain.com** ist **myserverhost** der Hostname und **companydomain.com** die Domäne.

HINWEIS Wenn Sie einen Server unter Verwendung eines DNS-Namens oder einer URL angeben, führt View kein DNS-Lookup durch, um zu überprüfen, ob ein Administrator View diesen Server zuvor unter Verwendung seiner IP-Adresse hinzugefügt hatte. Es entsteht ein Konflikt, wenn eine vCenter Server-Instanz sowohl mit dem DNS-Namen als auch mit der IP-Adresse angegeben wird.

- 4 Geben Sie den Namen des vCenter Server-Benutzers ein.

Beispiel: **domain\user** oder **user@domain.com**

- 5 Geben Sie das Kennwort für den vCenter Server-Benutzer ein.
- 6 (Optional) Geben Sie eine Beschreibung für diese vCenter Server-Instanz ein.
- 7 Geben Sie die TCP-Portnummer ein.
Der Standardport lautet 443.
- 8 Stellen Sie unter „Erweiterte Einstellungen“ die Grenzwerte für gleichzeitige Vorgänge für vCenter Server- und View Composer-Vorgänge ein.
- 9 Klicken Sie auf **Weiter**, um die Seite „View Composer-Einstellungen“ anzuzeigen.

Weiter

Konfigurieren Sie die View Composer-Einstellungen.

- Wenn die vCenter Server-Instanz mit einem signierten SSL-Zertifikat konfiguriert ist und View-Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „View Composer-Einstellungen“ an.
- Wenn die vCenter Server-Instanz mit einem Standardzertifikat konfiguriert ist, müssen Sie zunächst festlegen, ob der Fingerabdruck des vorhandenen Zertifikats akzeptiert werden soll. Siehe [„Akzeptieren des Fingerabdrucks eines standardmäßigen SSL-Zertifikats“](#), auf Seite 126.

Wenn View mehrere vCenter Server-Instanzen verwendet, wiederholen Sie diese Schritte, um die anderen vCenter Server-Instanzen hinzuzufügen.

Konfigurieren von View Composer-Einstellungen

Damit Sie View Composer verwenden können, müssen Sie Einstellungen konfigurieren, die es dem View-Verbindungsserver erlauben, eine Verbindung mit dem View Composer-Dienst herzustellen. View Composer kann auf einem separaten, eigenständigen Computer oder auf demselben Computer wie vCenter Server installiert werden.

VMware empfiehlt eine 1:1-Zuordnung zwischen je einem View Composer-Dienst und einer vCenter Server-Instanz.

Voraussetzungen

- Überprüfen Sie, ob der View-Verbindungsserver zur Verbindungsherstellung mit vCenter Server konfiguriert wurde. Dazu müssen Sie die Seite „vCenter Server-Informationen“ im Assistenten „vCenter Server hinzufügen“ ausfüllen. Siehe [„Hinzufügen von vCenter Server-Instanzen zu View“](#), auf Seite 117.
- Stellen Sie sicher, dass dieser View Composer-Dienst nicht bereits konfiguriert wurde, um eine Verbindung zu einer anderen vCenter Server-Instanz herzustellen.
- Falls Sie View Composer auf einem eigenständigen Computer installiert haben, sollten Sie sicherstellen, dass Sie ein eigenständiges View Composer Server-Benutzerkonto erstellt haben. Dieses Domänenbenutzerkonto muss ein Mitglied der lokalen Administratorgruppe auf dem View Composer-Computer sein.

Vorgehensweise

- 1 Dazu müssen Sie in View Administrator die Seite „vCenter Server-Informationen“ im Assistenten „vCenter Server hinzufügen“ ausfüllen.
 - a Klicken Sie auf **View-Konfiguration > Server**.
 - b Klicken Sie auf der Registerkarte „vCenter Server“ auf **Hinzufügen** und geben Sie die vCenter Server-Einstellungen an.

- 2 Wählen Sie auf der Seite „View Composer-Einstellungen“ die Option **View Composer nicht verwenden**, wenn Sie View Composer nicht verwenden.

Wenn Sie **View Composer nicht verwenden** auswählen, werden die anderen View Composer-Einstellungen inaktiv. Wenn Sie auf **Weiter** klicken, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „Speichereinstellungen“ an. Die Seite „View Composer-Domänen“ wird angezeigt.

- 3 Wenn Sie View Composer verwenden, wählen Sie den Ort des View Composer-Computers aus.

Option	Beschreibung
View Composer wird auf demselben Computer installiert wie vCenter Server.	<p>a Wählen Sie View Composer wurde zusammen mit vCenter Server installiert.</p> <p>b Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des View Composer-Dienstes in vCenter Server angegeben haben. Die standardmäßige Portnummer lautet 18443.</p>
View Composer wird auf einem separaten, eigenständigen Computer installiert.	<p>a Wählen Sie Eigenständiger View Composer Server.</p> <p>b Geben Sie im Textfeld für die View Composer-Serveradresse den vollqualifizierten Domännennamen (FQDN) des View Composer-Computers ein.</p> <p>c Geben Sie den Namen eines Domänenbenutzerkontos ein, das für die Authentifizierung beim View Composer-Dienst verwendet werden kann. Dieses Konto muss ein Mitglied der lokalen Administratorgruppe auf dem eigenständigen View Composer-Computer sein. Beispiel: domain.com\user oder user@domain.com</p> <p>d Geben Sie das Kennwort dieses Domänenbenutzerkontos ein.</p> <p>e Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des View Composer-Dienstes angegeben haben. Die standardmäßige Portnummer lautet 18443.</p>

- 4 Klicken Sie auf **Weiter**, um die Seite „View Composer-Domänen“ anzuzeigen.

Weiter

Konfigurieren Sie die View Composer-Domänen.

- Wenn die View Composer-Instanz mit einem signierten SSL-Zertifikat konfiguriert ist und View-Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „View Composer-Domänen“ an.
- Wenn die View Composer-Instanz mit einem Standardzertifikat konfiguriert ist, müssen Sie zunächst festlegen, ob der Fingerabdruck des vorhandenen Zertifikats akzeptiert werden soll. Siehe [„Akzeptieren des Fingerabdrucks eines standardmäßigen SSL-Zertifikats“](#), auf Seite 126.

Konfigurieren von View Composer-Domänen

Sie müssen eine Active Directory-Domäne konfigurieren, in der View Composer Linked-Clone-Desktops bereitstellt. Es ist möglich, mehrere Domänen für View Composer zu konfigurieren. Nachdem Sie die anfänglichen vCenter Server- und View Composer-Einstellungen zu View hinzugefügt haben, können Sie weitere View Composer-Domänen hinzufügen, indem Sie die vCenter Server-Instanz in View Administrator bearbeiten.

Voraussetzungen

- Ihr Active Directory-Administrator muss einen View Composer-Benutzer für AD-Vorgänge erstellen. Dieser Domänenbenutzer benötigt die Berechtigung zum Hinzufügen und Entfernen virtueller Maschinen in der Active Directory-Domäne, die Ihre Linked-Clones (verknüpften Klone) enthält. Weitere Informationen zu den erforderlichen Berechtigungen für diesen Benutzer finden Sie unter „[Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge](#)“, auf Seite 34.
- Überprüfen Sie in View Administrator, ob die Seiten mit den vCenter Server-Informationen und den View Composer-Einstellungen im Assistenten zum Hinzufügen von vCenter Server-Instanzen ausgefüllt wurden.

Vorgehensweise

- 1 Klicken Sie auf der Seite mit den View Composer-Domänen auf **Hinzufügen**, um den View Composer-Benutzer für die Kontoinformationen der AD-Vorgänge hinzuzufügen.
- 2 Geben Sie den Domänennamen der Active Directory-Domäne ein.
Beispiel: **domain.com**
- 3 Geben Sie den Domänenbenutzernamen (einschließlich des Domänennamens) des View Composer-Benutzers ein.
Beispiel: **domain.com\admin**
- 4 Geben Sie das Kontokennwort ein.
- 5 Klicken Sie auf **OK**.
- 6 Um Domänenbenutzerkonten mit Berechtigungen in weiteren Active Directory-Domänen hinzuzufügen, in denen Sie Linked-Clone-Pools bereitgestellt haben, wiederholen Sie die vorangehenden Schritte.
- 7 Klicken Sie auf **Weiter**, um die Seite mit den Speichereinstellungen anzuzeigen.

Weiter

Aktivieren Sie die Zurückgewinnung von VM-Datenträgerplatz und konfigurieren Sie die View-Speicherbeschleunigung für View.

Zulassen, dass vSphere Speicherplatz auf virtuellen Maschinen mit verknüpften Klonen freigibt

In vSphere 5.1 und höher können Sie die Funktion zur Rückgewinnung von Datenträgerplatz für View aktivieren. Mit Einführung von vSphere 5.1 erstellt View virtuelle Linked-Clone-Maschinen in einem effizienten Festplattenformat, welches es ESXi-Hosts erlaubt, nicht genutzten Festplattenspeicherplatz in den verknüpften Klonen zurückzugewinnen. Dadurch kann der insgesamt erforderliche Speicherplatz für verlinkte Klone reduziert werden.

Wenn Benutzer mit Linked-Clone-Desktops interagieren, nimmt die Größe der Betriebssystemfestplatte der Klone zu und kann schließlich fast so viel Festplattenspeicherplatz belegen wie Full-Clone-Desktops. Durch die Rückgewinnung von Datenträgerplatz verringert sich die Größe der Betriebssystemfestplatten, ohne dass Sie dazu die verknüpften Klone aktualisieren oder neu zusammenstellen müssen. Der Datenträgerplatz kann zurückgewonnen werden, während die virtuellen Maschinen eingeschaltet sind und Benutzer mit ihren Remote-Desktops interagieren.

Die Rückgewinnung von Datenträgerplatz eignet sich insbesondere für Bereitstellungen, die keine speicherplatzsparenden Strategien wie Aktualisierung oder Abmeldung nutzen können. Büroanwender beispielsweise, die Anwenderprogramme auf dedizierten Remote-Desktops installieren, könnten ihre persönlichen Anwendungen verlieren, wenn Remote-Desktops aktualisiert oder neu zusammengestellt würden. Mit der Rückgewinnung von Datenträgerplatz kann View verknüpfte Klone ungefähr in der gleichen verringerten Größe erhalten, die sie bei der ersten Bereitstellung hatten.

Diese Funktion besteht aus zwei Komponenten: speicherplatzsparendes Festplattenformat und Vorgänge zur Rückgewinnung von Speicherplatz.

In einer vSphere 5.1- oder neueren Umgebung erstellt View verknüpfte Klone mit platzsparenden Betriebssystemfestplatten, wenn eine übergeordnete virtuelle Maschine die virtuelle Hardwareversion 9 oder höher aufweist, unabhängig davon, ob Vorgänge zur Rückgewinnung von Datenträgerplatz aktiviert sind oder nicht.

Zum Aktivieren der Vorgänge zur Rückgewinnung von Datenträgerplatz müssen Sie View Administrator verwenden, um die Rückgewinnung von Datenträgerplatz für vCenter Server zu aktivieren und VM-Festplattenspeicher für einzelne Desktop-Pools zurückzugewinnen. Die Einstellung für die Rückgewinnung von Datenträgerplatz für vCenter Server ermöglicht es Ihnen, diese Funktion auf allen Desktop-Pools zu deaktivieren, die von der vCenter Server-Instanz verwaltet werden. Wenn Sie die Funktion für vCenter Server deaktivieren, wird die Einstellung auf Desktop-Pool-Ebene übergangen.

Für die Funktion zur Rückgewinnung von Datenträgerplatz gelten folgende Richtlinien:

- Sie funktioniert nur auf platzsparenden Betriebssystemfestplatten in verknüpften Klonen.
- Dieser Vorgang hat keine Auswirkungen auf persistente View Composer-Festplatten.
- Sie funktioniert nur mit vSphere 5.1 oder höher und nur auf virtuellen Maschinen, die die virtuelle Hardwareversion 9 oder höher aufweisen.
- Sie funktioniert nicht auf Full-Clone-Desktops.
- Sie funktioniert auf virtuellen Maschinen mit SCSI-Controllern. IDE-Controller werden nicht unterstützt.

Die View Composer Array Integration (VCAI) wird nicht in Pools unterstützt, die virtuelle Maschinen mit speicherplatzsparenden Festplatten enthalten. VCAI verwendet die systemeigene NFS-Snapshot-Technologie vStorage APIs for Array Integration (VAAI) zum Klonen virtueller Maschinen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und die ESXi-Hosts, einschließlich aller ESXi-Hosts in einem Cluster, in der Version 5.1 mit ESXi 5.1-Download-Patch ESXi510-201212001 oder höher vorliegen.

Vorgehensweise

- 1 Führen Sie in View Administrator die Schritte auf den Seiten des Assistenten zum Hinzufügen von vCenter Server-Instanzen aus, die der Seite mit den Speichereinstellungen vorangehen.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
 - c Geben Sie die Informationen für vCenter Server an, legen Sie die View Composer-Einstellungen fest und füllen Sie die Seiten für View Composer-Domänen aus.
- 2 Vergewissern Sie sich auf der Seite **Speichereinstellungen**, dass Zurückgewinnung von Datenträgerplatz aktiviert ausgewählt ist.

Die Zurückgewinnung von Datenträgerplatz ist standardmäßig ausgewählt, wenn Sie eine frische Installation von View 5.2 oder höher durchführen. Sie müssen **Zurückgewinnung von Datenträgerplatz aktivieren** auswählen, wenn Sie ein Upgrade auf View 5.2 oder höher von View 5.1 oder einer früheren Version durchführen.

Weiter

Konfigurieren Sie auf der Seite Speichereinstellungen die View-Speicherbeschleunigung.

Um die Konfiguration der Zurückgewinnung von Datenträgerplatz in View abzuschließen, richten Sie die Zurückgewinnung von Datenträgerplatz für Desktop-Pools ein.

Konfigurieren der View-Speicherbeschleunigung für vCenter Server

In vSphere 5.0 und höher können Sie ESXi-Hosts so konfigurieren, dass Festplattendaten von virtuellen Maschinen gespeichert werden. Diese Funktion, die View-Speicherbeschleunigung, verwendet die CBRC-Funktion (Content Based Read Cache) in ESXi-Hosts. Die View-Speicherbeschleunigung verbessert die Leistung von Horizon 7 bei E/A-Überlastungen, die auftreten können, wenn viele virtuelle Maschinen gleichzeitig starten oder Antivirenschans ausführen. Die Funktion ist außerdem nützlich, wenn Administratoren oder Benutzer häufig Anwendungen oder Daten laden. Statt das gesamte Betriebssystem oder die gesamte Anwendung wieder und wieder aus dem Speichersystem zu lesen, kann ein Host gemeinsame Datenblöcke aus dem Cache lesen.

Durch Verringern der E/A-Vorgänge pro Sekunde bei sogenannten „Boot Storms“ senkt die View-Speicherbeschleunigung die Last des Speicher-Arrays. Dadurch wird weniger Speicher-E/A-Bandbreite belegt, so dass die Horizon 7-Bereitstellung unterstützt wird.

Um das Caching auf Ihren ESXi-Hosts zu aktivieren, wählen Sie die Einstellung für die View-Speicherbeschleunigung im vCenter Server-Assistenten in Horizon Administrator wie in dieser Vorgehensweise beschrieben aus.

Stellen Sie sicher, dass die View-Speicherbeschleunigung auch für einzelne Desktop-Pools konfiguriert ist. Damit die View-Speicherbeschleunigung für einen Desktop-Pool genutzt werden kann, muss sie sowohl für vCenter Server als auch für den jeweiligen Desktop-Pool aktiviert werden.

Die View-Speicherbeschleunigung ist für Desktop-Pools standardmäßig aktiviert. Die Funktion kann beim Erstellen oder Bearbeiten eines Pools deaktiviert oder aktiviert werden. Es empfiehlt sich, diese Funktion zu aktivieren, wenn Sie erstmalig einen Desktop-Pool erstellen. Wenn Sie die Funktion aktivieren, indem Sie einen vorhandenen Pool bearbeiten, müssen Sie sicherstellen, dass ein neues Replikat und seine Digest-Festplatten erstellt werden, bevor Linked Clones bereitgestellt werden. Sie können ein neues Replikat erstellen, indem Sie den Pool zu einem neuen Snapshot neu zusammenstellen oder den Pool in einem neuen Datenspeicher neu verteilen. Digest-Dateien können für die virtuellen Maschinen in einem Desktop-Pool nur konfiguriert werden, wenn sie ausgeschaltet sind.

Sie können die View-Speicherbeschleunigung für Desktop-Pools aktivieren, die Linked Clones enthalten, und auch für Pools, die vollständige virtuelle Maschinen enthalten.

Die systemeigene NFS-Snapshot-Technologie (VAAI) wird nicht in Pools unterstützt, die für die View-Speicherbeschleunigung aktiviert sind.

Die View-Speicherbeschleunigung kann nun in Konfigurationen eingesetzt werden, in denen eine mehrstufige Speicherung von Horizon 7-Replikaten verwendet wird und Replikate in einem anderen Datenspeicher gespeichert werden als Linked Clones. Wenngleich bei der Verwendung der View-Speicherbeschleunigung mit der mehrstufigen Speicherung von Horizon 7-Replikaten keine erheblichen Leistungsvorteile erzielt werden, sind bestimmte Vorteile im Hinblick auf die Kapazität möglich, wenn die Replikate in einem separaten Datenspeicher gespeichert werden. Aus diesem Grund wird diese Kombination getestet und unterstützt.

WICHTIG Wenn Sie diese Funktion mit mehreren View-Pods verwenden möchten, die gemeinsam einige ESXi-Hosts nutzen, müssen Sie die View-Speicherbeschleunigung für alle Pools auf den gemeinsam genutzten ESXi-Hosts aktivieren. Sind die Einstellungen für mehrere Pods nicht einheitlich, kann dies zur Instabilität der virtuellen Maschinen auf den gemeinsam genutzten ESXi-Hosts führen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und Ihre ESXi-Hosts in der Version 5.0 oder höher vorliegen. Überprüfen Sie in einem ESXi-Cluster, ob alle Hosts mindestens in der Version 5.0 ausgeführt werden.
 - Stellen Sie sicher, dass dem vCenter Server-Benutzer die Berechtigung **Host > Konfiguration > Erweiterte Einstellungen** in vCenter Server zugewiesen wurde.
- Siehe „[Konfigurieren von Benutzerkonten für vCenter Server und View Composer](#)“, auf Seite 111.

Vorgehensweise

- 1 Führen Sie in Horizon Administrator die Schritte auf den Seiten des Assistenten zum Hinzufügen von vCenter Server-Instanzen aus, die der Seite mit den Speichereinstellungen vorangehen.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
 - c Geben Sie die Informationen für vCenter Server an, legen Sie die View Composer-Einstellungen fest und füllen Sie die Seiten für View Composer-Domänen aus.
- 2 Stellen Sie auf der Seite mit den Speichereinstellungen sicher, dass das Kontrollkästchen **View-Speicherbeschleunigung aktivieren** aktiviert ist.

Dieses Kontrollkästchen ist standardmäßig aktiviert.
- 3 Geben Sie eine standardmäßige Größe für den Host-Cache an.

Diese Größe gilt für alle ESXi-Hosts, die von dieser vCenter Server-Instanz verwaltet werden.

Der Standardwert ist 1.024 MB. Die Cachegröße muss zwischen 100 MB und 2.048 MB betragen.
- 4 Um für einen einzelnen ESXi-Host eine andere Cachegröße anzugeben, wählen Sie einen ESXi-Host aus, und klicken Sie auf **Cachegröße bearbeiten**.
 - a Aktivieren Sie im Dialogfeld „Host-Cache“ das Kontrollkästchen **Standard-Hostzwischen-speichergröße außer Kraft setzen**.
 - b Geben Sie unter **Größe des Host-Caches** einen Wert zwischen 100 MB und 2.048 MB an, und klicken Sie auf **OK**.
- 5 Klicken Sie auf der Seite mit den Speichereinstellungen auf **Weiter**.
- 6 Klicken Sie auf **Fertig stellen**, um die vCenter Server-, View Composer- und Speichereinstellungen zu Horizon 7 hinzuzufügen.

Weiter

Informationen zur Konfiguration des PCoIP Secure Gateway, des sicheren Tunnels und externer URLs für Clientverbindungen finden Sie unter „[Konfigurieren von Horizon Client-Verbindungen](#)“, auf Seite 128.

Um die Einstellungen für die View-Speicherbeschleunigung in Horizon 7 zu vervollständigen, konfigurieren Sie die View-Speicherbeschleunigung für Desktop-Pools. Weitere Informationen finden Sie unter „[Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools](#)“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Grenzwerte für parallele Vorgänge für vCenter Server und View Composer

Wenn Sie vCenter Server zu View hinzufügen oder die vCenter Server-Einstellungen bearbeiten, können Sie mehrere Optionen konfigurieren, die die maximale Anzahl an parallelen Vorgängen festlegen, die von vCenter Server und View Composer ausgeführt werden.

Sie konfigurieren diese Optionen im Bereich „Erweiterte Einstellungen“ auf der Seite „vCenter Server-Informationen“.

Tabelle 9-3. Grenzwerte für parallele Vorgänge für vCenter Server und View Composer

Einstellung	Beschreibung
Maximale Anzahl paralleler vCenter-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl paralleler Anforderungen fest, die ein View-Verbindungsserver zum Bereitstellen und Löschen vollständiger virtueller Maschinen in dieser vCenter Server-Instanz senden kann.</p> <p>Der Standardwert lautet 20.</p> <p>Diese Einstellung gilt nur für vollständige virtuelle Maschinen.</p>
Maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands	<p>Legt die maximale Anzahl an parallelen Betriebsvorgängen fest (Starten, Herunterfahren, Anhalten usw.), die auf virtuellen Maschinen ausgeführt werden können, die in dieser vCenter Server-Instanz von einem View-Verbindungsserver verwaltet werden.</p> <p>Der Standardwert ist 50.</p> <p>Richtlinien zum Berechnen eines Wertes für diese Einstellung finden Sie unter „Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen“, auf Seite 126.</p> <p>Diese Einstellung gilt für vollständige virtuelle Maschinen und verknüpfte Klone.</p>
Maximale parallele View Composer-Wartungsvorgänge	<p>Legt die maximale Anzahl an parallelen View Composer-Vorgängen zur Aktualisierung, Neuzusammenstellung und Neuverteilung fest, die auf den verknüpften Klonen ausgeführt werden können, die von dieser View Composer-Instanz verwaltet werden.</p> <p>Der Standardwert ist 12.</p> <p>Remote-Desktops mit aktiven Sitzungen müssen abgemeldet werden, bevor ein Wartungsvorgang ausgeführt werden kann. Wenn Sie Benutzer zur Abmeldung zwingen, sobald ein Wartungsvorgang beginnt, entspricht die maximale Anzahl paralleler Vorgänge auf Remote-Desktops, die eine Abmeldung erfordern, der Hälfte des konfigurierten Wertes. Wenn Sie für diese Einstellung beispielsweise den Wert 24 konfigurieren und Benutzer zur Abmeldung zwingen, sind maximal 12 parallele Vorgänge auf Remote-Desktops möglich, die Abmeldungen erfordern.</p> <p>Diese Einstellung gilt nur für verknüpfte Klone.</p>
Maximale parallele View Composer-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl an parallelen Erstellungs- und Löschvorgängen fest, die auf verknüpften Klonen ausgeführt werden können, die von dieser View Composer-Instanz verwaltet werden.</p> <p>Der Standardwert ist 8.</p> <p>Diese Einstellung gilt nur für verknüpfte Klone.</p>

Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen

Die Einstellung **Maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands** legt die maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands fest, die auf virtuellen Remote-Desktop-Maschinen in einer vCenter Server-Instanz stattfinden können. Diese Obergrenze ist standardmäßig auf 50 festgelegt. Sie können diesen Wert ändern, um Einschaltzeiten zu Spitzenzeiten zu unterstützen, während derer sich viele Benutzer gleichzeitig bei ihren Desktops anmelden.

Die empfohlene Vorgehensweise besteht darin, während einer Pilotphase den korrekten Wert für diese Einstellung zu ermitteln. Als Planungshilfe lesen Sie „Architekturforschungselemente und Planungsanleitungen“ im Dokument *Planung der View-Architektur*.

Die erforderliche Anzahl paralleler Vorgänge zum Ändern des Betriebszustands basiert auf der Spitzenrate, mit der Desktops eingeschaltet werden, sowie der Zeit, die für das Einschalten, Booten und Verfügbarwerden für eine Verbindung benötigt wird. Im Allgemeinen entspricht der empfohlene Maximalwert für Betriebsvorgänge der Gesamtzeit, die der Desktop zum Starten benötigt, multipliziert mit der Spitzenrate für Einschaltvorgänge.

Der durchschnittliche Desktop benötigt beispielsweise zwei bis drei Minuten zum Starten. Daher sollte die maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands dreimal so hoch wie die Spitzenrate für Einschaltvorgänge sein. Bei einer Standardeinstellung von 50 wird erwartet, dass eine Einschaltzeit von 16 Desktops pro Minute während Spitzenzeiten unterstützt wird.

Das System wartet maximal fünf Minuten auf den Start eines Desktops. Wenn die Startzeit länger ist, können andere Fehler auftreten. Wenn Sie vorsichtig sein möchten, legen Sie eine maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands fest, die fünf Mal höher als die Einschaltzeit während Spitzenzeiten ist. Bei einer vorsichtigen Herangehensweise unterstützt die Standardeinstellung 50 eine Einschaltzeit während Spitzenzeiten von 10 Desktops pro Minute.

Anmeldungen und daher Desktop-Einschaltvorgänge finden üblicherweise auf normal verteilte Weise während eines bestimmten Zeitfensters statt. Sie können die Einschaltzeit während Spitzenzeiten in etwa ermitteln, indem Sie annehmen, dass diese in der Mitte des Zeitfensters auftritt, während der ungefähr 40 Prozent der Einschaltvorgänge in einem Sechstel des Zeitfensters erfolgen. Wenn sich Benutzer beispielsweise zwischen 8:00 und 9:00 Uhr morgens anmelden, beträgt das Zeitfenster eine Stunde, und 40 Prozent dieser Anmeldungen erfolgen in den zehn Minuten zwischen 8:25 und 8:35 Uhr. Wenn es 2.000 Benutzer gibt, von denen 20 Prozent ihre Desktops ausgeschaltet haben, dann erfolgen 40 Prozent der 400 Desktop-Einschaltvorgänge während dieser zehn Minuten. Die Einschaltzeit während Spitzenzeiten beträgt 16 Desktops pro Minute.

Akzeptieren des Fingerabdrucks eines standardmäßigen SSL-Zertifikats

Wenn Sie vCenter Server und View Composer-Instanzen zu View hinzufügen, müssen Sie sicherstellen, dass die SSL-Zertifikate, die für vCenter Server und View Composer-Instanzen verwendet werden, gültig sind und vom View-Verbindungsserver als vertrauenswürdig anerkannt werden. Wenn die mit vCenter Server und View Composer installierten Standardzertifikate immer noch an Ort und Stelle sind, müssen Sie festlegen, ob Sie die Fingerabdrücke dieser Zertifikate akzeptieren wollen.

Wenn ein vCenter Server oder eine View Composer-Instanz mit einem Zertifikat konfiguriert ist, das von einer Zertifizierungsstelle (CA) signiert ist, und das Stammzertifikat vom View-Verbindungsserver als vertrauenswürdig anerkannt wird, müssen Sie den Fingerabdruck des Zertifikats nicht akzeptieren. Es sind keine Schritte erforderlich.

Wenn Sie ein Standardzertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzen, der View-Verbindungsserver das Stammzertifikat jedoch nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatsfingerabdruck akzeptiert wird. Bei einem Fingerabdruck handelt es sich um einen kryptografischen Hash-Wert eines Zertifikats. Anhand des Fingerabdrucks wird rasch ermittelt, ob ein Zertifikat mit einem anderen Zertifikat übereinstimmt (z. B. mit dem zuvor akzeptierten Zertifikat).

HINWEIS Wenn Sie vCenter Server und View Composer auf demselben Windows Server-Host installieren, können sie dasselbe SSL-Zertifikat verwenden, aber Sie müssen das Zertifikat separat für jede Komponente konfigurieren.

Einzelheiten zur Konfiguration von SSL-Zertifikaten finden Sie unter [Kapitel 8, „Konfigurieren von SSL-Zertifikaten für View Servers“](#), auf Seite 89.

Zunächst fügen Sie vCenter Server und View Composer in View Administrator hinzu; verwenden Sie dazu den Assistenten zum Hinzufügen von vCenter Server. Wenn ein Zertifikat nicht als vertrauenswürdig eingestuft wird und Sie den Fingerabdruck nicht akzeptieren, können Sie vCenter Server und View Composer nicht hinzufügen.

Nachdem diese Server hinzugefügt wurden, können Sie sie im Dialogfeld „vCenter Server bearbeiten“ neu konfigurieren.

HINWEIS Ein Zertifikatsfingerabdruck muss außerdem akzeptiert werden, wenn Sie eine Aktualisierung von einer früheren Version durchführen und ein vCenter Server- oder View Composer-Zertifikat als nicht vertrauenswürdig eingestuft wird. Gleiches gilt, wenn Sie ein vertrauenswürdiges Zertifikat durch ein nicht vertrauenswürdiges Zertifikat ersetzen.

Auf dem View Administrator-Dashboard ändert sich die Farbe des Symbols für vCenter Server oder View Composer in Rot und das Dialogfeld „Ungültiges Zertifikat ermittelt“ wird angezeigt. **Klicken Sie auf Überprüfen** und führen Sie die hier beschriebenen Schritte aus.

Gleichermaßen können Sie in View Administrator einen SAML-Authentifikator für die Verwendung durch eine View-Verbindungsserver-Instanz konfigurieren. Wenn der View-Verbindungsserver das SAML-Serverzertifikat nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatsfingerabdruck akzeptiert wird. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie den SAML-Authentifikator in View nicht konfigurieren. Nach der Konfiguration eines SAML-Authentifikators können Sie ihn im Dialogfeld zum Bearbeiten des View-Verbindungsservers neu konfigurieren.

Vorgehensweise

- 1 **Klicken Sie auf** Zertifikat anzeigen, wenn View Administrator ein Dialogfeld Ungültiges Zertifikat ermittelt anzeigt.
- 2 Überprüfen Sie den Zertifikatsfingerabdruck im Fenster mit den Zertifikatsinformationen.
- 3 Untersuchen Sie den Fingerabdruck des Zertifikats, das für die vCenter Server- oder View Composer-Instanz konfiguriert wurde.
 - a Starten Sie auf dem vCenter Server- oder View Composer-Host das MMC-Snap-In und öffnen Sie den Windows-Zertifikatspeicher.
 - b Navigieren Sie zum vCenter Server- oder View Composer-Zertifikat.
 - c Klicken Sie auf die Registerkarte mit den Zertifikatsdetails, um den Zertifikatsfingerabdruck anzuzeigen.

Untersuchen Sie den Zertifikatsfingerabdruck gleichermaßen auf einen SAML-Authentifikator. Führen Sie die vorstehenden Schritte gegebenenfalls auf dem SAML-Authentifikatorhost aus.

- 4 Überprüfen Sie, ob der Fingerabdruck im Fenster mit den Zertifikatsinformationen mit dem Fingerabdruck für die vCenter Server- oder View Composer-Instanz übereinstimmt.

Überprüfen Sie ebenfalls, ob die Fingerabdrücke für einen SAML-Authentifikator übereinstimmen.

- 5 Geben Sie an, ob der Zertifikatsfingerabdruck akzeptiert wird.

Option	Beschreibung
Die Fingerabdrücke stimmen überein.	Klicken Sie auf Akzeptieren , um das Standardzertifikat zu verwenden.
Die Fingerabdrücke stimmen nicht überein.	Klicken Sie auf Ablehnen . Behandeln Sie das Problem der nicht übereinstimmenden Zertifikate. Möglicherweise haben Sie z. B. eine falsche IP-Adresse für vCenter Server oder View Composer angegeben.

Konfigurieren von Horizon Client -Verbindungen

Clientendpunkte kommunizieren mit einem View-Verbindungsserver- oder Sicherheitsserver-Host über sichere Verbindungen.

Die erste Clientverbindung, die für die Benutzerauthentifizierung und für die Auswahl von Remote-Desktops und -anwendungen verwendet wird, wird über HTTPS erstellt, wenn ein Benutzer einen Domännennamen für Horizon Client bereitstellt. Wenn Firewall und Lastausgleichssoftware in Ihrer Netzwerkumgebung ordnungsgemäß konfiguriert sind, wird diese Anforderung an den View-Verbindungsserver- oder Sicherheitsserver-Host gesendet. Diese Verbindung wird zur Benutzerauthentifizierung und Auswahl eines Desktops oder einer Anwendung verwendet, aber die Benutzer haben noch keine Verbindung mit dem Remote-Desktop oder der Remoteanwendung hergestellt.

Wenn Benutzer eine Verbindung mit Remote-Desktops und -anwendungen herstellen, stellt der Client standardmäßig eine zweite Verbindung mit dem View-Verbindungsserver- oder Sicherheitsserver-Host her. Diese Verbindung wird als „Tunnelverbindung“ bezeichnet, da sie einen sicheren Tunnel für die Übertragung von RDP-Daten und anderen Daten über HTTPS bereitstellt.

Wenn Benutzer mit dem PCoIP-Anzeigeprotokoll eine Verbindung mit Remote-Desktops und -anwendungen herstellen, kann der Client auf dem View-Verbindungsserver- oder Sicherheitsserver-Host eine weitere Verbindung mit dem PCoIP Secure Gateway aufbauen. Über das PCoIP Secure Gateway wird sichergestellt, dass nur authentifizierte Benutzer mit Remote-Desktops und -anwendungen über PCoIP kommunizieren können.

Sichere Verbindungen können auch für Benutzer, die mit dem VMware Blast-Anzeigeprotokoll eine Verbindung mit Remote-Desktops und -anwendungen herstellen, und für externe Benutzer, die HTML Access zum Herstellen einer Verbindung mit Remote-Desktops verwenden, bereitgestellt werden. Das Blast Secure Gateway sorgt dafür, dass nur authentifizierte Benutzer mit Remote-Desktops kommunizieren können.

Abhängig vom Typ des verwendeten Clientgeräts werden weitere Kanäle eingerichtet, um Datenverkehr wie USB-Umleitungsdaten an das Clientgerät zu übertragen. Diese Datenkanäle leiten Datenverkehr über den sicheren Tunnel weiter, sofern dieser aktiviert ist.

Wenn der sichere Tunnel und sichere Gateways deaktiviert sind, werden Desktop- und Anwendungssitzungen direkt zwischen dem Clientgerät und der Remote-Maschine eingerichtet, wobei der View-Verbindungsserver- oder der Sicherheitsserver-Host umgangen werden. Dieser Verbindungstyp wird als direkte Verbindung bezeichnet.

Desktop- und Anwendungssitzungen, die direkte Verbindungen verwenden, bleiben auch dann verbunden, wenn der View-Verbindungsserver nicht mehr ausgeführt wird.

In der Regel aktivieren Sie den sicheren Tunnel, das PCoIP Secure Gateway und das Blast Secure Gateway, um sichere Verbindungen für externe Clients bereitzustellen, die über ein WAN eine Verbindung mit einem Sicherheitsserver- oder einem View-Verbindungsserver-Host herstellen. Sie können den sicheren Tunnel und die sicheren Gateways deaktivieren, um internen, mit dem LAN verbundenen Clients das Herstellen von direkten Verbindungen mit Remote-Desktop und -anwendungen zu ermöglichen.

Wenn Sie nur den sicheren Tunnel und nur ein sicheres Gateway aktivieren, verwendet eine Sitzung möglicherweise eine direkte Verbindung für einen Teil des Datenverkehrs, sendet jedoch den anderen Datenverkehr über den View-Verbindungsserver- oder Sicherheitsserver-Host. Entscheidend ist hier der Typ des verwendeten Clients.

SSL ist für alle Clientverbindungen mit Hosts von View-Verbindungsservern oder Sicherheitsservern erforderlich.

Konfigurieren von PCoIP Secure Gateways und sicheren Tunnelverbindungen

Sie können mithilfe von View Administrator die Verwendung des sicheren Tunnels und PCoIP Secure Gateways konfigurieren. Über diese Komponenten wird sichergestellt, dass nur authentifizierte Benutzer mit Remote-Desktops und -Anwendungen kommunizieren können.

Clients, die das PCoIP-Anzeigeprotokoll verwenden, können das PCoIP Secure Gateway nutzen. Clients, die das RDP-Anzeigeprotokoll verwenden, können den sicheren Tunnel nutzen.

Informationen zur Konfiguration des Blast Secure Gateway finden Sie unter [„Konfigurieren des Blast-Sicherheitsgateways“](#), auf Seite 130.

WICHTIG Eine typische Netzwerkkonfiguration, die sichere Verbindungen für externe Clients bereitstellt, umfasst einen Sicherheitsserver. Zum Aktivieren oder Deaktivieren des sicheren Tunnels und des PCoIP Secure Gateway auf einem Sicherheitsserver müssen Sie die View-Verbindungsserver-Instanz bearbeiten, die mit dem Sicherheitsserver kombiniert ist.

In einer Netzwerkkonfiguration, bei der externe Clients sich direkt mit einem View-Verbindungsserver-Host verbinden, aktivieren oder deaktivieren Sie den sicheren Tunnel und ein PCoIP Secure Gateway, indem Sie die entsprechende View-Verbindungsserver-Instanz in View Administrator bearbeiten.

Voraussetzungen

- Wenn Sie beabsichtigen, das PCoIP Secure Gateway zu aktivieren, stellen Sie sicher, dass die View-Verbindungsserver-Instanz und der kombinierte Sicherheitsserver in der Version View 4.6 oder höher vorliegen.
- Wenn Sie einen Sicherheitsserver mit einer View-Verbindungsserver-Instanz kombinieren, auf der Sie das PCoIP Secure Gateway bereits aktiviert haben, stellen Sie sicher, dass der Sicherheitsserver in der Version View 4.6 oder höher vorliegt.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server**.
- 2 Wählen Sie unter „View-Verbindungsserver“ eine View-Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Konfigurieren Sie die Verwendung des sicheren Tunnels.

Option	Beschreibung
Deaktivieren des sicheren Tunnels	Deaktivieren Sie Sichere Tunnelverbindung zum Computer verwenden .
Aktivieren des sicheren Tunnels	Aktivieren Sie Sichere Tunnelverbindung zum Computer verwenden .

Der sichere Tunnel ist standardmäßig aktiviert.

- 4 Konfigurieren Sie die Verwendung des PCoIP Secure Gateway.

Option	Beschreibung
Aktivieren des PCoIP Secure Gateway	Aktivieren Sie PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden.
Deaktivieren des PCoIP Secure Gateway	Deaktivieren Sie PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden.

Das PCoIP Secure Gateway ist standardmäßig deaktiviert.

- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren des Blast-Sicherheitsgateways

Sie können in Horizon Administrator das Blast-Sicherheitsgateway konfigurieren, um einen sicheren Zugriff auf Remote-Desktops und -anwendungen zu ermöglichen. Der Zugriff erfolgt entweder über HTML Access oder über Clientverbindungen, für die das VMware Blast-Anzeigeprotokoll verwendet wird.

Das Blast-Sicherheitsgateway beinhaltet das BEAT-Netzwerkprotokoll (Blast Extreme Adaptive Transport), das sich dynamisch an die jeweiligen Netzwerkbedingungen wie unterschiedliche Geschwindigkeiten und Paketverluste anpasst.

- Horizon Clients können für die Herstellung einer Verbindung mit dem Verbindungsserver, dem Sicherheitsserver oder der Unified Access Gateway-Appliance das BEAT-Netzwerk mit einer ausgezeichneten Netzwerkbedingung verwenden.
- Horizon Clients mit einer typischen Netzwerkbedingung müssen eine Verbindung mit einem Verbindungsserver mit deaktiviertem BSG, einem Sicherheitsserver mit deaktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 herstellen. Wenn Horizon Client eine typische Netzwerkbedingung zur Herstellung einer Verbindung mit einem Verbindungsserver mit aktiviertem BSG, einem Sicherheitsserver mit aktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 verwendet, erkennt der Client automatisch diese Netzwerkbedingung und verwendet das TCP-Netzwerk.
- Horizon Clients mit einer schwachen Netzwerkbedingung müssen eine Verbindung mit der Version 2.9 oder höher einer Unified Access Gateway-Appliance (mit aktiviertem UDP-Tunnelserver) herstellen. Wenn Horizon Client eine schwache Netzwerkbedingung zur Herstellung einer Verbindung mit dem Verbindungsserver mit aktiviertem BSG, mit dem Sicherheitsserver mit aktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 verwendet, erkennt der Client automatisch diese Netzwerkbedingung und verwendet das TCP-Netzwerk.
- Wenn Horizon Clients eine schwache Netzwerkbedingung zur Herstellung einer Verbindung mit einem Verbindungsserver mit deaktiviertem BSG, mit einem Sicherheitsserver mit deaktiviertem BSG oder mit Version 2.9 oder höher einer Unified Access Gateway-Appliance (ohne aktivierten UDP-Tunnelserver) oder mit Version 2.8 einer Unified Access Gateway-Appliance verwenden, erkennt der Client automatisch diese Netzwerkbedingung und verwendet die typische Netzwerkbedingung.

Weitere Informationen finden Sie in der Dokumentation zu Horizon Client unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

HINWEIS Sie können auch Unified Access Gateway-Appliances statt Sicherheitsserver für den sicheren externen Zugriff auf Horizon 7 Server und Desktops verwenden. Wenn Sie Unified Access Gateway-Appliances benutzen, müssen Sie die sicheren Gateways auf den Verbindungsserver-Instanzen deaktivieren und diese Gateways auf den Unified Access Gateway-Appliances aktivieren. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Wenn das Blast-Sicherheitsgateway nicht aktiviert ist, verwenden Client-Webbrowser das VMware Blast Extreme-Protokoll, um direkte Verbindungen mit den virtuellen Remote-Desktop-Computern herzustellen, und umgehen somit das Blast-Sicherheitsgateway.

WICHTIG Eine typische Netzwerkkonfiguration, die sichere Verbindungen für externe Benutzer bereitstellt, umfasst einen Sicherheitsserver. Zum Aktivieren oder Deaktivieren des Blast-Sicherheitsgateways auf einem Sicherheitsserver müssen Sie die Verbindungsserver-Instanz bearbeiten, die mit dem Sicherheitsserver gekoppelt ist. Wenn externe Benutzer sich direkt mit einem Verbindungsserver-Host verbinden, aktivieren oder deaktivieren Sie das Blast-Sicherheitsgateway, indem Sie die Verbindungsserver-Instanz bearbeiten.

Voraussetzungen

Wenn Benutzer Remote-Desktops über VMware Identity Manager auswählen, müssen Sie überprüfen, ob VMware Identity Manager installiert und für die Verwendung mit dem Verbindungsserver konfiguriert ist. Außerdem muss der Verbindungsserver mit einem SAML 2.0-Authentifizierungsserver gekoppelt sein.

Vorgehensweise

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Konfigurieren Sie die Verwendung des Blast-Sicherheitsgateways.

Option	Beschreibung
Aktivieren des Blast Secure Gateway	Aktivieren Sie Blast Secure Gateway für Blast-Verbindungen mit dem Computer verwenden .
Deaktivieren des Blast Secure Gateway	Deaktivieren Sie Blast Secure Gateway für Blast-Verbindungen mit dem Computer verwenden .

Das Blast-Sicherheitsgateway ist standardmäßig aktiviert.

- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren externer URLs für sichere Gateways und Tunnelverbindungen

Zur Verwendung des sicheren Tunnels muss ein Clientsystem auf eine IP-Adresse zugreifen können oder über einen vollqualifizierten Domännennamen verfügen, der in eine IP-Adresse aufgelöst werden kann, so dass der Client eine Verbindung mit einem View-Verbindungsserver- oder Sicherheitsserver-Host herstellen kann.

Um das PCoIP Secure Gateway zu verwenden, stellt ein Client unter Verwendung einer URL eine Verbindung zum View-Verbindungsserver oder zum Sicherheitsserver-Host her. In einer IPv4-Umgebung muss die URL einen Host anhand seiner IP-Adresse identifizieren. In einer IPv6-Umgebung kann die URL einen Host entweder anhand seiner IP-Adresse oder seines FQDN identifizieren.

Zur Verwendung des Blast Secure Gateway muss das Endgerät eines Benutzers auf einen FQDN zugreifen können, den es in eine IP-Adresse auflösen kann, über die der Webbrowser oder Computer des Benutzers den View-Verbindungsserver-Host oder Sicherheitsserver-Host kontaktieren kann.

Verwenden von Tunnelverbindungen von externen Standorten

In der Standardeinstellung kann der View-Verbindungsserver- oder Sicherheitsserver-Host nur über Tunnelclients kontaktiert werden, die sich innerhalb desselben Netzwerks befinden und daher in der Lage sind, den angeforderten Server zu ermitteln.

Viele Organisationen erfordern, dass Benutzer sich von einem externen Standort aus verbinden können. Hierzu wird entweder eine spezifische IP-Adresse oder ein durch den Client auflösbarer Domänenname sowie ein bestimmter Port verwendet. Diese Informationen können der tatsächlichen Adresse und Portnummer des View-Verbindungsserver- oder Sicherheitsserver-Hosts ähneln, dies ist jedoch nicht zwingend erforderlich. Die Informationen werden in Form einer URL für ein Clientsystem bereitgestellt. Beispiel:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

Zur Verwendung solcher Adressen in View müssen Sie den View-Verbindungsserver- oder Sicherheitsserver-Host so konfigurieren, dass er eine externe URL anstelle des Host-FQDN zurückgibt.

Konfigurieren externer URLs

Sie können mehrere externe URLs konfigurieren. Über die erste URL können Clientsysteme Tunnelverbindungen herstellen. Eine zweite URL ermöglicht es dem Client, der PCoIP verwendet, sichere Verbindungen über das PCoIP Secure Gateway herzustellen. In einer IPv4-Umgebung muss die URL einen Host anhand seiner IP-Adresse identifizieren. In einer IPv6-Umgebung kann die URL einen Host entweder anhand seiner IP-Adresse oder seines FQDN identifizieren. Die URL ermöglicht Clients, von einem externen Standort aus eine Verbindung herzustellen.

Mit einer dritten URL können Benutzer mit dem Blast Secure Gateway über Clientgeräte oder über einen Webbrowser eine sichere Verbindung herstellen.

Wenn Ihre Netzwerkkonfiguration Sicherheitsserver umfasst, stellen Sie externe URLs für die Sicherheitsserver bereit. Auf View-Verbindungsserver-Instanzen, die mit den Sicherheitsservern kombiniert sind, werden keine externen URLs benötigt.

Das Vorgehen zum Konfigurieren der externen URLs ist für View-Verbindungsserver-Instanzen und Sicherheitsserver unterschiedlich.

- Für eine View-Verbindungsserver-Instanz legen Sie die externen URLs fest, indem Sie die View-Verbindungsserver-Einstellungen in View Administrator bearbeiten.
- Für einen Sicherheitsserver legen Sie die externen URLs fest, wenn Sie das View-Verbindungsserver-Installationsprogramm ausführen. Sie können mithilfe von View Administrator eine externe URL für einen Sicherheitsserver ändern.

Festlegen der externen URLs für eine View-Verbindungsserver-Instanz

Sie können View Administrator verwenden, um die externen URLs für eine View-Verbindungsserver-Instanz zu konfigurieren.

Bei den externen URLs für den sicheren Tunnel, für PCoIP und für Blast muss es sich um die Adressen handeln, mit denen Clientsysteme diese View-Verbindungsserver-Instanz erreichen.

Voraussetzungen

- Stellen Sie sicher, dass die sicheren Tunnelverbindungen und das PCoIP Secure Gateway für die View-Verbindungsserver-Instanz aktiviert sind. Siehe [„Konfigurieren von PCoIP Secure Gateways und sicheren Tunnelverbindungen“](#), auf Seite 129.
- Zum Festlegen der externen URL für Blast stellen Sie sicher, dass das Blast Secure Gateway für die View-Verbindungsserver-Instanz aktiviert ist. Siehe [„Konfigurieren des Blast-Sicherheitsgateways“](#), auf Seite 130.

Vorgehensweise

- 1 Klicken Sie in View Administrator auf **View-Konfiguration > Server**.
- 2 Wählen Sie auf der Registerkarte für Verbindungsserver die View-Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.

- 3 Geben Sie im Textfeld **Externe URL** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch Clients auflösbaren Hostnamen und die Portnummer enthalten.

Beispiel: `https://myserver.example.com:443`

HINWEIS Um auf eine View-Verbindungsserver-Instanz zuzugreifen, deren Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem SSL-Zertifikat, das für die View-Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

- 4 Geben Sie im Textfeld **PCoIP – Externe URL** die externe URL des PCoIP Secure Gateway ein.

Geben Sie in einer IPv4-Umgebung die externe PCoIP-URL in Form einer IP-Adresse mit der Portnummer 4172 an. In einer IPv6-Umgebung können Sie eine IP-Adresse oder einen vollqualifizierten Domännennamen und die Portnummer 4172 angeben. In beiden Fällen geben Sie keinen Protokollnamen an.

Beispiel für eine IPv4-Umgebung: `10.20.30.40:4172`

Clients müssen die URL verwenden können, um den Sicherheitsserver zu erreichen.

- 5 Geben Sie im Textfeld **Externe Blast-URL** die externe URL des Blast Secure Gateway ein.

Die URL muss das HTTPS-Protokoll, den durch den Client auflösbaren Hostnamen sowie die Portnummer enthalten.

Beispiel: `https://myserver.example.com:8443`

Die URL enthält standardmäßig den FQDN der externen URL des sicheren Tunnels und die standardmäßige Portnummer 8443. Die URL muss den FQDN und die Portnummer enthalten, die ein Clientsystem zur Verbindungsherstellung mit diesem View-Verbindungsserver-Host benötigt.

- 6 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit dieser View-Verbindungsserver-Instanz herstellen können.
- 7 Klicken Sie auf **OK**.

Ändern der externen URLs für einen Sicherheitsserver

Verwenden Sie View Administrator, um die externen URLs für einen Sicherheitsserver zu ändern.

Sie konfigurieren diese externen URLs zum ersten Mal, wenn Sie im Installationsprogramm für View-Verbindungsserver einen Sicherheitsserver installieren.

Bei den externen URLs für den sicheren Tunnel, für PCoIP und für Blast muss es sich um die Adressen handeln, mit denen Clientsysteme diesen Sicherheitsserver erreichen.

Voraussetzungen

- Stellen Sie sicher, dass die sicheren Tunnelverbindungen und das PCoIP Secure Gateway für die View-Verbindungsserver-Instanz aktiviert sind, die mit diesem Sicherheitsserver kombiniert ist. Siehe [„Konfigurieren von PCoIP Secure Gateways und sicheren Tunnelverbindungen“](#), auf Seite 129.
- Um die externe URL für Blast festzulegen, stellen Sie sicher, dass das Blast Secure Gateway für die View-Verbindungsserver-Instanz aktiviert ist, die mit diesem Sicherheitsserver kombiniert ist. Siehe [„Konfigurieren des Blast-Sicherheitsgateways“](#), auf Seite 130.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server**.
- 2 Wählen Sie die Registerkarte „Sicherheitsserver“ aus, wählen Sie den Sicherheitsserver aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie im Textfeld **Externe URL** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch den Client auflösbaren Hostnamen des Sicherheitsservers sowie die Portnummer enthalten.

Beispiel: `https://myserver.example.com:443`

HINWEIS Um auf einen Sicherheitsserver zuzugreifen, dessen Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, mit dem Sie Verbindung aufnehmen, entspricht jedoch nicht dem für den Sicherheitsserver konfigurierten SSL-Zertifikat. Aus diesem Grund wird der Zugriff blockiert oder die Sicherheit des Zugriffs wird reduziert.

- 4 Geben Sie im Textfeld **PCoIP – Externe URL** die externe URL des PCoIP Secure Gateway ein.
 Geben Sie in einer IPv4-Umgebung die externe PCoIP-URL in Form einer IP-Adresse mit der Portnummer 4172 an. In einer IPv6-Umgebung können Sie eine IP-Adresse oder einen Domänennamen und die Portnummer 4172 angeben. In beiden Fällen geben Sie keinen Protokollnamen an.
 Beispiel für eine IPv4-Umgebung: `10.20.30.40:4172`
 Clients müssen die URL verwenden können, um den Sicherheitsserver zu erreichen.
- 5 Geben Sie im Textfeld **Externe Blast-URL** die externe URL des Blast Secure Gateway ein.
 Die URL muss das HTTPS-Protokoll, den durch den Client auflösbaren Hostnamen sowie die Portnummer enthalten.
 Beispiel: `https://myserver.example.com:8443`
 Standardmäßig schließt die URL den FQDN der externen URL für den sicheren Tunnel sowie die standardmäßige Portnummer 8443 ein. Die URL muss den FQDN und die Portnummer enthalten, über die ein Clientsystem diesen Sicherheitsserver erreichen kann.
- 6 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit diesem Sicherheitsserverhost herstellen können.
- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

View Administrator sendet die aktualisierten externen URLs an den Sicherheitsserver. Es ist kein Neustart des Sicherheitsserverdienstes erforderlich, damit die Änderungen wirksam werden.

Bevorzugen von DNS-Namen, wenn der View-Verbindungsserver Adressinformationen zurückgibt

Standardmäßig bevorzugt der View-Verbindungsserver beim Senden der Adressen von Desktop-Maschinen und RDS-Hosts an Clients und Gateways IP-Adressen. Sie können dieses Standardverhalten mit einem View LDAP-Attribut ändern, mit dem der View-Verbindungsserver angewiesen wird, bevorzugt DNS-Namen zu verwenden. In bestimmten Umgebungen erhalten Sie dadurch, dass der View-Verbindungsserver DNS-Namen an Clients und Gateways zurückgibt, zusätzliche Flexibilität beim Entwurf einer Netzwerkinfrastruktur.

HINWEIS Dieses View LDAP-Attribut ersetzt die auf einzelne Desktops bezogenen Funktionen, die in Horizon 6.0.x und früheren Versionen durch die Gruppenrichtlinieneinstellung `Connect using DNS Name` bereitgestellt wurden.

Das View LDAP-Attribut hat Auswirkungen auf Clients, die Horizon Client 3.3 für Windows oder höher, HTML Access 3.5 oder höher und sichere Gateways auf View-Verbindungsserver-Instanzen (nicht auf Sicherheitsservern) ausführen.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogrammes AD-SI-Editor mit Ihrer Windows Server-Betriebssystemversion.

Vorgehensweise

- 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 Domänennamen (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 Legen Sie für das Objekt **CN=Common, OU=Global, OU=Properties** den Wert des Attributs **paeferDNS** auf 1 fest.

Wenn dieses Attribut auf 1 festgelegt wird, gibt der View-Verbindungsserver einen DNS-Namen zurück, sofern ein DNS-Name verfügbar ist und der Empfänger Namensauflösung unterstützt. Andernfalls gibt der View-Verbindungsserver eine IP-Adresse zurück, sofern eine IP-Adresse des richtigen Typs für Ihre Umgebung (IPv4 oder IPv6) verfügbar ist.

Wird dieses Attribut nicht angegeben oder auf 0 festgelegt, gibt der View-Verbindungsserver eine IP-Adresse zurück, sofern eine IP-Adresse des richtigen Typs verfügbar ist. Andernfalls wird ein IP-Adressen-Kompatibilitätsfehler zurückgegeben.

Zulassen von HTML Access über einen Lastausgleichsdienst

View-Verbindungsserver-Instanzen und Sicherheitsserver, die sich direkt hinter einem Lastausgleichsdienst befinden, wie z. B. Access Point, müssen die Adresse kennen, über die Browser eine Verbindung mit dem Lastausgleichsdienst herstellen, wenn Benutzer HTML Access verwenden.

Führen Sie für View-Verbindungsserver-Instanzen oder Sicherheitsserver, die sich direkt hinter einem Gateway befinden, die in „Zulassen von HTML Access über ein Gateway“, auf Seite 136 beschriebenen Schritte aus.

Sie müssen diesen Vorgang für jeden View Server ausführen, der sich hinter einem Lastausgleichsdienst befindet.

Vorgehensweise

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserver-Host.

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

- 2 Fügen Sie die Eigenschaft `balancedHost` hinzu und legen Sie für diese die Adresse des Lastausgleichsdienstes fest.

Wenn die Benutzer z. B. `https://view.example.com` in einen Browser eingeben, um einen der View Server mit Lastausgleichsdienst zu erreichen, dann fügen Sie der Datei `locked.properties` den Eintrag `balancedHost=view.example.com` hinzu.

- 3 Speichern Sie die Datei `locked.properties`.

- 4 Starten Sie den View-Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Zulassen von HTML Access über ein Gateway

View-Verbindungsserver-Instanzen und Sicherheitsserver, die sich direkt hinter einem Gateway wie z. B. Access Point befinden, müssen die Adresse kennen, über die Browser eine Verbindung mit dem Gateway herstellen, wenn Benutzer HTML Access verwenden.

Führen Sie für View-Verbindungsserver-Instanzen oder Sicherheitsserver, die sich hinter einem Lastausgleichsdienst oder einem Gateway mit Lastausgleichsdienst befinden, die in „[Zulassen von HTML Access über einen Lastausgleichsdienst](#)“, auf Seite 135 beschriebenen Schritte aus.

Sie müssen diesen Vorgang für jeden View Server ausführen, der sich hinter einem Gateway befindet.

Vorgehensweise

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserver-Host.

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

- 2 Fügen Sie die Eigenschaft `portalHost` hinzu und legen Sie für diese die Adresse des Gateways fest.

Wenn Browser z. B. mit der Adresse `https://view-gateway.example.com` über das Gateway auf View zugreifen, fügen Sie der Datei `locked.properties` den Eintrag `portalHost=view-gateway.example.com` hinzu.

Falls sich die View-Verbindungsserver-Instanz oder der Sicherheitsserver hinter mehreren Gateways befinden, können Sie die einzelnen Gateways angeben, indem Sie der Eigenschaft `portalHost` eine Zahl anhängen. Beispiel:

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

Sie müssen auch mehrere Eigenschaften `portalHost` angeben, wenn ein Gateway-Computer über mehrere Namen verfügt.

- 3 Speichern Sie die Datei `locked.properties`.
- 4 Starten Sie den View-Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Ersetzen von Standardports für View-Dienste

Während der Installation werden View-Dienste standardmäßig für die Überwachung an bestimmten Netzwerkports eingerichtet. In einigen Organisationen müssen diese Ports geändert werden, um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern. Sie können die Standardports ändern, die vom View-Verbindungsserver, vom Sicherheitsserver, vom PCoIP Secure Gateway und von View Composer-Diensten verwendet werden.

Das Ändern der Ports ist eine optionale Aufgabe bei der Einrichtung. Verwenden Sie die Standardports, wenn diese Änderungen für Ihre Bereitstellung nicht erforderlich sind.

Eine Liste der standardmäßigen TCP- und UDP-Ports, die von View Server-Instanzen verwendet werden, finden Sie unter „View-TCP- und UDP-Ports“ im Dokument *Sicherheit von View*.

Ersetzen der standardmäßigen HTTP-Ports oder NICs für View-Verbindungsserver-Instanzen und Sicherheitsserver

Sie können die standardmäßigen HTTP-Ports oder Netzwerkkarten für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver ersetzen, indem Sie die Datei `locked.properties` auf dem Servercomputer bearbeiten. Möglicherweise müssen Sie diese Aufgaben in Ihrer Organisation ausführen, um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern.

Der standardmäßige SSL-Port ist 443. Der Standardport für Nicht-SSL-Verbindungen lautet 80.

Der in der externen URL für den sicheren Tunnel angegebene Port wird durch Änderungen, die Sie in dieser Vorgehensweise an Ports vornehmen, nicht geändert. Abhängig von Ihrer Netzwerkkonfiguration müssen Sie den Port der externen URL für den sicheren Tunnel möglicherweise ebenfalls ändern.

Wenn der Servercomputer über mehrere Netzwerkkarten verfügt, überwacht er das System standardmäßig an allen Netzwerkkarten. Sie können eine NIC für die Überwachung am konfigurierten Port auswählen, indem Sie die mit dieser NIC verknüpfte IP-Adresse angeben.

Während der Installation konfiguriert View die Windows-Firewall so, dass die erforderlichen Standardports geöffnet werden. Wenn Sie eine Portnummer oder die Netzwerkkarte für die Überwachung ändern, müssen Sie die Windows-Firewall manuell so neu konfigurieren, dass die aktualisierten Ports geöffnet werden. Nur so können Clientgeräte eine Verbindung mit dem Server herstellen.

Wenn Sie die SSL-Portnummer ändern und die HTTP-Umleitung weiterhin funktionieren soll, müssen Sie auch die Portnummer für die HTTP-Umleitung ändern. Siehe [„Ändern der Portnummer für die HTTP-Umleitung an Verbindungsserver“](#), auf Seite 140.

Voraussetzungen

Stellen Sie sicher, dass der in der externen URL für diese View-Verbindungsserver-Instanz oder diesen Sicherheitsserver angegebene Port weiterhin gültig ist, nachdem Sie die Porteneinstellungen in dieser Vorgehensweise geändert haben.

Vorgehensweise

- 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\locked.properties`

Bei den Eigenschaften in der Datei `locked.properties` wird die Groß-/Kleinschreibung beachtet.

- 2 Fügen Sie die Eigenschaft `serverPort` oder `serverPortNonSsl` bzw. beide Eigenschaften zur Datei `locked.properties` hinzu.

Beispiel:

```
serverPort=4443
serverPortNonSsl=8080
```

- 3 (Optional) Wenn der Servercomputer über mehrere Netzwerkkarten verfügt, wählen Sie eine Netzwerkkarte für die Überwachung an den konfigurierten Ports aus.

Fügen Sie die Eigenschaften `serverHost` und `serverHostNonSsl` hinzu, um die IP-Adresse anzugeben, die mit der gewählten NIC verknüpft ist.

Beispiel:

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

Üblicherweise sind sowohl SSL- als auch Nicht-SSL-Listener für die Verwendung derselben NIC konfiguriert. Wenn Sie jedoch die Eigenschaft `serverProtocol=http` nutzen, um SSL für Clientverbindungen zu verlagern, können Sie die Eigenschaft `serverHost` auf eine separate NIC festlegen, um SSL-Verbindungen mit Systemen bereitzustellen, die zum Starten von View Administrator verwendet werden.

Bei Konfiguration von SSL- und Nicht-SSL-Verbindungen für die Verwendung derselben NIC dürfen die SSL- und Nicht-SSL-Ports nicht identisch sein.

- 4 Starten Sie den View-Verbindungs- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Weiter

Konfigurieren Sie die Windows-Firewall bei Bedarf manuell, um die aktualisierten Ports zu öffnen.

Ersetzen der Standard-Ports oder NICs für das PCoIP Secure Gateway auf den View-Verbindungs-Server-Instanzen und den Sicherheitsservern

Sie können die Standard-Ports oder NICs ersetzen, die von einem PCoIP Secure Gateway Service verwendet werden, der auf einer View-Verbindungs-Server-Instanz oder einem Sicherheitsserver läuft. Möglicherweise müssen Sie diese Aufgaben in Ihrer Organisation ausführen, um Organisationsrichtlinien einzuhalten oder Konflikte zu verhindern.

Für TCP- und UDP-Verbindungen mit Clients hört das PCoIP Secure Gateway standardmäßig auf Port 4172. Für UDP-Verbindungen mit Remote-Desktops hört das PCoIP Secure Gateway standardmäßig auf Port 55000.

Der in der PCoIP - Externe URL angegebene Port wird durch Änderungen, die Sie bei dieser Vorgehensweise an Ports vornehmen, nicht geändert. Abhängig von Ihrer Netzwerkkonfiguration, müssen Sie möglicherweise den PCoIP - Externe URL-Port auch ändern.

Wenn der Computer, auf dem das PCoIP Secure Gateway läuft über mehrere Netzwerkkarten verfügt, hört der Computer standardmäßig auf allen Netzwerkkarten. Sie können eine NIC für die Überwachung an den konfigurierten Anschlüssen auswählen, indem Sie die mit dieser NIC verknüpfte IP-Adresse angeben.

Voraussetzungen

Stellen Sie sicher, dass der angegebene Port in der PCoIP - Externe URL auf dieser View-Verbindungs-Server-Instanz oder diesem Sicherheitsserver weiterhin gültig ist, nachdem Sie die Port-Einstellungen mit dieser Vorgehensweise geändert haben.

Vorgehensweise

- 1 Starten Sie den Windows Registrierungs-Editor auf dem View-Verbindungs-Server oder Sicherheitsserver-Computer, auf dem das PCoIP Secure Gateway läuft.
- 2 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.

- 3 Unter diesem Registrierungsschlüssel fügen Sie eine oder mehrere der folgenden Zeichenfolgenwerte (REG_SZ) mit Ihren aktualisierten Port-Nummern ein.

Beispiel:

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

- 4 (Optional) Wenn der Computer, auf dem das PCoIP Secure Gateway läuft, über mehrere Netzwerkkarten verfügt, wählen Sie eine Netzwerkkarte, die an den konfigurierten Ports hört.

Unter dem selben Registrierungsschlüssel fügen Sie die folgenden Zeichenfolgenwerte (REG_SZ) ein, um die IP-Adresse anzugeben, die an den vorgesehenen NIC gebunden ist.

Beispiel:

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

Wenn Sie externe und interne Verbindungen so konfigurieren, dass sie denselben NIC benutzen, dürfen die externen und internen UDP-Ports nicht die selben sein.

- 5 Starten Sie den Dienst „VMware Horizon View PCoIP Secure Gateway“ neu, damit Ihre Änderungen wirksam werden.

Ersetzen des Standardsteuerungsports für das PCoIP Secure Gateway auf den Verbindungsserver-Instanzen und Sicherheitsservern

Sie können den Standardport, der den PCoIP Secure Gateway (PSG)-Dienst steuert, der auf einer Verbindungsserver-Instanz oder einem Sicherheitsserver ausgeführt wird, ersetzen. Sie müssen diese Aufgabe eventuell zur Vermeidung eines Portkonflikts ausführen.

Das PCoIP Secure Gateway überwacht standardmäßig Steuerungsverbindungen auf dem lokalen TCP-Port 50060.

Vorgehensweise

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem Verbindungsserver- oder Sicherheitsservercomputer, auf dem PCoIP Secure Gateway ausgeführt wird.

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

Bei den Eigenschaften in der Datei `locked.properties` wird die Groß-/Kleinschreibung beachtet.

- 2 Fügen Sie die Eigenschaft `psgControlPort` zur Datei `locked.properties` hinzu:

Beispiel:

```
psgControlPort=52060
```

- 3 Starten Sie den Windows-Registrierungs-Editor auf derselben Maschine.
- 4 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.
- 5 Fügen Sie diesem Registrierungsschlüssel den im Folgenden dargestellten Zeichenfolgenwert (REG_SZ) mit Ihrer aktualisierten Portnummer hinzu.

Beispiel:

```
TCPControlPort "52060"
```

HINWEIS Die Portnummer für `TCPControlPort` ist die gleiche wie die Portnummer für `psgControlPort`.

- 6 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Ersetzen des Standard-Ports für View Composer

Das SSL-Zertifikat, das vom View Composer-Dienst verwendet wird, ist standardmäßig an einen bestimmten Port gebunden. Sie können den Standard-Port mit dem Dienstprogramm `SviConfig ChangeCertificateBindingPort` ändern.

Wenn Sie mit dem Dienstprogramm `SviConfig ChangeCertificateBindingPort` einen neuen Port angeben, hebt das Dienstprogramm die Bindung des View Composer-Zertifikats an den aktuellen Port auf und bindet es an den neuen Port.

Während der Installation konfiguriert View Composer die Windows-Firewall so, dass der erforderliche Standard-Port geöffnet wird. Wenn Sie den Port ändern, müssen Sie die Windows-Firewall manuell konfigurieren, um den aktualisierten Port zu öffnen und die Konnektivität mit dem View Composer-Dienst sicherzustellen.

Voraussetzungen

Stellen Sie sicher, dass der von Ihnen angegebene Port verfügbar ist.

Vorgehensweise

- 1 Halten Sie den View Composer-Dienst an.
- 2 Öffnen Sie eine Eingabeaufforderung auf dem Windows Server Host, auf dem View Composer installiert ist.
- 3 Navigieren Sie zur ausführbaren Datei `SviConfig`.

Die Datei befindet sich im Ordner der View Composer-Anwendung. Der Standardpfad lautet `C:\Programme (x86)\VMware\VMware View Composer\sviconfig.exe`.

- 4 Geben Sie den Befehl `SviConfig ChangeCertificateBindingPort` ein.

Beispiel:

```
sviconfig -operation=ChangeCertificateBindingPort
          -Port=port number
```

wobei `-port=port number` der neue Port ist, an den View Composer das Zertifikat bindet. Der Parameter `-port=port number` ist erforderlich.

- 5 Starten Sie den View Composer-Dienst neu, damit die Änderungen wirksam werden.

Weiter

Wenn nötig, konfigurieren Sie die Windows-Firewall auf dem View Composer Server manuell, um den aktualisierten Port zu öffnen.

Ändern der Portnummer für die HTTP-Umleitung an Verbindungsserver

Wenn Sie den standardmäßigen Port 443 auf einem View Server ändern und die HTTP-Umleitung für View-Clients zulassen möchten, die versuchen, sich mit Port 80 zu verbinden, müssen Sie auf dem View Server die Datei `locked.properties` konfigurieren.

HINWEIS Wenn SSL auf ein Zwischengerät verschoben wird, hat dieser Vorgang keinerlei Auswirkungen. Beim Verschieben von SSL auf ein anderes Gerät wird der HTTP-Port auf dem View Server für Clientverbindungen verwendet.

Voraussetzungen

Überprüfen Sie, ob die standardmäßige Portnummer 443 geändert wurde. Bei Verwendung der Standardwerte, die während der Installation konfiguriert werden, müssen Sie diese Schritte nicht ausführen, um die HTTP-Umleitungsregel beizubehalten.

Vorgehensweise

- 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\locked.properties`

Bei den Eigenschaften in der Datei `locked.properties` wird die Groß-/Kleinschreibung beachtet.

- 2 Fügen Sie die folgenden Zeilen zur Datei `locked.properties` hinzu:

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

In den vorstehenden Zeilen entspricht die Variable `Port` der Portnummer, mit der sich Clients verbinden sollen.

Wenn Sie die vorstehenden Zeilen nicht hinzufügen, entspricht `Port` weiterhin Port 443.

- 3 Starten Sie den View-Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Verhindern der HTTP-Umleitung für Client-Verbindungen auf Verbindungsserver

Wenn View-Clients versuchen, über HTTP eine Verbindung mit View Servern herzustellen, findet im Hintergrund eine Umleitung an HTTPS statt. In einigen Bereitstellungen kann es sinnvoll sein, zu verhindern, dass Benutzer die Zeichenfolge `http://` in ihre Webbrowser eingeben können, sodass stattdessen die Verwendung von HTTPS erzwungen wird. Um die HTTP-Umleitung für View-Clients zu verhindern, müssen Sie auf dem View Server die Datei `locked.properties` konfigurieren.

HINWEIS Wenn SSL auf ein Zwischengerät verschoben wird, hat dieser Vorgang keinerlei Auswirkungen. Beim Verschieben von SSL auf ein anderes Gerät wird der HTTP-Port auf dem View Server für Clientverbindungen verwendet.

Vorgehensweise

- 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\locked.properties`

Bei den Eigenschaften in der Datei `locked.properties` wird die Groß-/Kleinschreibung beachtet.

- 2 Fügen Sie die folgenden Zeilen zur Datei `locked.properties` hinzu:

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

- 3 Starten Sie den View-Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Aktivieren des Remote-Zugriffs auf View-Leistungsindikatoren auf Verbindungsservern

View-Leistungsindikatoren sind lokal auf einem Verbindungsserver verfügbar, geben aber den Wert 0 zurück, wenn von einem anderen Computer aus auf sie zugegriffen wird. Um den Remote-Zugriff auf View-Leistungsindikatoren auf Verbindungsservern zu aktivieren, müssen Sie den Framework-Port des Verbindungsservers in der Registrierung konfigurieren.

Vorgehensweise

- 1 Starten Sie den Windows-Registrierungs-Editor.
- 2 Navigieren Sie zum Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager.
- 3 Fügen Sie einen neuen Zeichenfolgenwert (G_SZ), Verwaltungs-Port, hinzu.
- 4 Setzen Sie den Wert für Verwaltungs-Port auf 32111.

Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung

Zur Unterstützung sehr umfangreicher Bereitstellungen von Remote-Desktops können Sie die Windows Server-Computer konfigurieren, auf denen Sie View-Verbindungsserver installieren. Die Größe der Windows-Auslagerungsdatei kann auf jedem Computer angepasst werden.

Auf Computern unter Windows Server 2008 R2 und Windows Server 2012 R2 werden für die kurzlebigen Ports, die TCB-Hash-Tabelle und die Java Virtual Machine-Einstellungen Standardwerte für die Größe festgelegt. Durch diese Anpassungen wird sichergestellt, dass die Computer über angemessene Ressourcen zur ordnungsgemäßen Ausführung mit der erwarteten Benutzerlast verfügen.

Größeneinstellung des Arbeitsspeichers für View-Verbindungsserver

Auf einem View-Verbindungsserver-Computer sind 10 GB Arbeitsspeicher für Bereitstellungen mit 50 oder mehr Remote-Desktops erforderlich. Ein Windows Server-Computer mit mindestens 10 GB Arbeitsspeicher wird automatisch so konfiguriert, dass er ungefähr 2.000 gleichzeitige Tunnelsitzungen unterstützt. Dies ist die maximale Anzahl, die ein View-Verbindungsserver unterstützen kann.

Nur für kleine Proof-of-Concept-Bereitstellungen kann die Größe des Arbeitsspeichers unter 10 GB liegen. Eine Konfiguration mit dem erforderlichen Minimum von 4 GB Arbeitsspeicher unterstützt ungefähr 500 gleichzeitige Tunnelsitzungen. Dies reicht für kleine Proof-of-Concept-Bereitstellungen vollkommen aus.

VMware empfiehlt jedoch, immer mindestens 10 GB Arbeitsspeicher zu konfigurieren, damit Ihre Umgebung auch dann unterstützt wird, wenn weitere Benutzer hinzugefügt werden und die Bereitstellung dadurch wächst. Weichen Sie nur dann von dieser Empfehlung ab, wenn Sie sicher wissen, dass die Umgebung nicht wachsen wird, und wenn kein Arbeitsspeicher zur Verfügung steht.

Wenn Sie einen View-Verbindungsserver mit weniger als 10 GB Arbeitsspeicher installieren, generiert View nach der Installation Warnmeldungen mit Empfehlungen zur Größe des Arbeitsspeichers. Alle 12 Stunden wird ein Ereignis ausgelöst, das Sie darauf hinweist, dass die View-Verbindungsserver-Instanz mit einer geringen Menge an physischem Arbeitsspeicher konfiguriert ist.

Wenn Sie den Arbeitsspeicher eines Computers auf 10 GB erhöhen, um eine größere Bereitstellung zu unterstützen, starten Sie den View-Verbindungsserver neu, um sicherzustellen, dass der JVM-Heap automatisch auf den empfohlenen Wert vergrößert wird. Sie müssen den View-Verbindungsserver nicht neu installieren.

WICHTIG Auf einem 64 Bit-Windows Server-Computer sollte die Größe des JVM-Heaps nicht geändert werden. Eine Änderung dieses Werts kann zu einem instabilen Verhalten von View-Verbindungsserver führen. Auf 64 Bit-Computern legt der View-Verbindungsserver-Dienst die Größe des JVM-Heaps in Abhängigkeit vom physischen Arbeitsspeicher fest.

Weitere Informationen zu den Hardware- und Arbeitsspeicheranforderungen für View-Verbindungsserver finden Sie unter „[Hardwareanforderungen für den Horizon-Verbindungsserver](#)“, auf Seite 10.

Hardware- und Arbeitsspeicherempfehlungen für den Einsatz von View-Verbindungsservern in einer umfangreichen Bereitstellung finden Sie unter „View-Verbindungsserver: Maximalwerte und Konfigurieren von virtuellen Maschinen“ im Dokument *Planung der View-Architektur*.

Konfigurieren der Einstellungen für die Systemauslagerungsdatei

Sie können den virtuellen Arbeitsspeicher auf den Windows Server-Computern optimieren, auf denen Ihre View-Verbindungsserver-Instanzen installiert sind, indem Sie die Einstellungen für die Systemauslagerungsdatei ändern.

Bei der Installation von Windows Server berechnet Windows, basierend auf dem physischen Arbeitsspeicher, eine anfängliche und eine maximale Größe der Auslagerungsdatei. Diese Standardeinstellungen werden auch nach einem Neustart des Computers beibehalten.

Wenn es sich bei dem Windows Server-Computer um eine virtuelle Maschine handelt, können Sie die Arbeitsspeichergröße über vCenter Server ändern. Wenn Windows jedoch die Standardeinstellung verwendet, wird die Größe der Systemauslagerungsdatei nicht an die neue Arbeitsspeichergröße angepasst.

Vorgehensweise

- 1 Navigieren Sie auf dem Windows Server-Computer mit installiertem View-Verbindungsserver zum Dialogfeld **Virtueller Arbeitsspeicher**.

Standardmäßig ist die Einstellung **Benutzerdefinierte Größe** ausgewählt. Es wird eine anfängliche und eine maximale Größe der Auslagerungsdatei angezeigt.

- 2 Klicken Sie auf **Vom System verwaltete Größe**.

Windows berechnet, basierend auf der aktuellen Arbeitsspeicherverwendung und des verfügbaren Arbeitsspeichers, die Größe der Systemauslagerungsdatei fortlaufend neu.

Sie können eine Ereignisdatenbank erstellen, um Informationen zu View-Ereignissen aufzuzeichnen. Wenn Sie einen Syslog-Server verwenden, können Sie den View-Verbindungsserver darüber hinaus so konfigurieren, dass Ereignisse an einen Syslog-Server gesendet werden oder eine Flatfiledatei mit Ereignissen im Syslog-Format erstellt wird.

Dieses Kapitel behandelt die folgenden Themen:

- [„Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse“](#), auf Seite 145
- [„Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung“](#), auf Seite 146
- [„Konfigurieren der Ereignisdatenbank“](#), auf Seite 147
- [„Konfigurieren der Ereignisprotokollierung für Syslog-Server“](#), auf Seite 148

Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse

Sie erstellen eine Ereignisdatenbank, indem Sie sie zu einem vorhandenen Datenbankserver hinzufügen. Anschließend können Sie mithilfe von Reporting-Software für Unternehmen die Ereignisse in der Datenbank analysieren.

Stellen Sie den Datenbankserver für die Ereignisdatenbank auf einem dedizierten Server bereit, sodass die Aktivitäten der Ereignisprotokollierung weder die Bereitstellung noch andere Aktivitäten, die für View-Bereitstellungen wichtig sind, beeinträchtigen.

HINWEIS Sie müssen für diese Datenbank keine ODBC-Datenquelle erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen unterstützten MySQL SQL Server- oder Oracle-Datenbankserver auf einem System verfügen, auf den eine View-Verbindungsserver-Instanz zugreifen kann. Eine Liste der unterstützten Datenbankversionen finden Sie unter [„Datenbankanforderungen für View Composer und die Ereignisdatenbank“](#), auf Seite 13.
- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Erstellen einer Datenbank und eines Benutzers auf dem Datenbankserver verfügen.
- Wenn Sie mit der Erstellung von Datenbanken auf Microsoft SQL Server-Datenbankservern nicht vertraut sind, lesen Sie die Schrittanweisungen unter [„Hinzufügen einer View Composer-Datenbank zu SQL Server“](#), auf Seite 44.
- Wenn Sie mit der Erstellung von Datenbanken auf Oracle-Datenbankservern nicht vertraut sind, lesen Sie die Schrittanweisungen unter [„Hinzufügen einer View Composer-Datenbank zu Oracle 12c oder 11g“](#), auf Seite 48.

Vorgehensweise

- 1 Fügen Sie dem Server eine neue Datenbank hinzu und geben Sie ihr einen beschreibenden Namen, z.B. "ViewEreignisse".

Geben Sie für eine Oracle 12c- oder 11g-Datenbankinstanz eine Oracle-Systemkennung (SID) ein, die Sie beim Konfigurieren der Ereignisdatenbank in View Administrator verwenden. Legen Sie für das Objekt C

- 2 Fügen Sie einen Benutzer für diese Datenbank hinzu, der über Berechtigungen zum Erstellen von Tabellen, Ansichten und – im Falle von Oracle – Trigger und Sequenzen verfügt sowie die Berechtigung zum Ausführen von Lese- und Schreiboperationen für diese Objekte besitzt.

Verwenden Sie für eine Microsoft SQL Server-Datenbank nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode. Verwenden Sie auf jeden Fall die SQL Server-Authentifizierungsmethode.

Die Datenbank wird erstellt, das Schema jedoch nicht. Dieses wird erst erstellt, wenn Sie die Datenbank in View Administrator konfigurieren.

Weiter

Folgen Sie den Anweisungen unter „[Konfigurieren der Ereignisdatenbank](#)“, auf Seite 147.

Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung

Bevor Sie View Administrator zum Konfigurieren einer Ereignisdatenbank auf dem Microsoft SQL Server verwenden können, müssen Sie die richtigen TCP/IP-Eigenschaften konfigurieren und sicherstellen, dass der Server die SQL Server-Authentifizierung nutzt.

Voraussetzungen

- Erstellen einer SQL Server-Datenbank für die Ereignisberichterstellung. Siehe „[Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse](#)“, auf Seite 145.
- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Konfigurieren der Datenbank verfügen.
- Stellen Sie sicher, dass der Datenbankserver die SQL Server-Authentifizierungsmethode nutzt. Verwenden Sie nicht die Windows-Authentifizierung.

Vorgehensweise

- 1 Öffnen Sie den SQL Server-Konfigurations-Manager und erweitern Sie **Netzwerkkonfiguration von SQL Server YYYY**.
- 2 Wählen Sie **Protokolle für Servername**.
- 3 Klicken Sie in der Liste der Protokolle mit der rechten Maustaste auf **TCP/IP** und wählen Sie **Eigenschaften**.
- 4 Setzen Sie die Eigenschaft **Aktiviert** auf **Ja**.
- 5 Stellen Sie sicher, dass ein Port zugewiesen ist, oder weisen Sie ggf. einen Port zu.
Informationen zu statischen und dynamischen Ports sowie ihrer Zuweisung finden Sie in der Online-Hilfe zum SQL Server-Konfigurations-Manager.
- 6 Stellen Sie sicher, dass dieser Port nicht von einer Firewall blockiert ist.

Weiter

Verbinden Sie mittels View Administrator die Datenbank mit View-Verbindungsserver. Folgen Sie den Anweisungen unter „[Konfigurieren der Ereignisdatenbank](#)“, auf Seite 147.

Konfigurieren der Ereignisdatenbank

Die Ereignisdatenbank speichert Informationen zu View-Ereignissen nicht in einer Protokolldatei, sondern in Form von Einträgen in einer Datenbank.

Sie konfigurieren eine Ereignisdatenbank nach der Installation einer View-Verbindungsserver-Instanz. Sie müssen nur einen host in einer View-Verbindungsserver-Gruppe konfigurieren. Die verbleibenden Hosts in der Gruppe werden automatisch konfiguriert.

HINWEIS Für die Sicherheit der Datenbankverbindung zwischen der View-Verbindungsserver-Instanz und einer externen Datenbank ist der Administrator verantwortlich, obwohl Ereignisdatenverkehr auf Informationen über den Zustand der View-Umgebung beschränkt ist. Wenn Sie zusätzliche Sicherheitsmaßnahmen ergreifen möchten, können Sie diesen Kanal durch IPSec oder ein anderes Mittel schützen. Sie können die Datenbank auch lokal auf dem View-Verbindungsserver-Computer bereitstellen.

Sie können die Ereignisse in den Datenbanktabellen unter Verwendung von Microsoft SQL Server oder Oracle-Datenbankberichtstools untersuchen. Weitere Informationen finden Sie im Dokument *Integration von View*.

Sie können auch View-Ereignisse im Format Syslog generieren, sodass Analysesoftware von Drittanbietern auf die Ereignisdaten zugreifen kann. Sie verwenden den Befehl `vdmadmin` mit der Option `-I`, um View-Ereignismeldungen im Syslog-Format in Ereignisprotokolldateien aufzuzeichnen. Siehe „Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option `-I`“ im Dokument *Administration von View*.

Voraussetzungen

Sie benötigen die folgenden Informationen, um eine Ereignisdatenbank zu konfigurieren:

- Den DNS-Namen oder die IP-Adresse des Datenbankservers.
- Typ des Datenbankservers: Microsoft SQL Server oder Oracle.
- Die Portnummer, die für den Zugriff auf den Datenbankserver verwendet wird. Standardmäßig wird Port 1521 für Oracle und Port 1433 für SQL Server verwendet. Wenn es sich beim SQL Server-Datenbankserver um eine benannte Instanz handelt oder Sie SQL Server Express verwenden, müssen Sie möglicherweise die Portnummer ermitteln. Informationen zum Herstellen einer Verbindung mit einer benannten Instanz von SQL Server finden Sie im Microsoft KB-Artikel unter <http://support.microsoft.com/kb/265808>.
- Der Name der Ereignisdatenbank, die Sie auf dem Datenbankserver erstellt haben. Siehe „[Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse](#)“, auf Seite 145.

Wenn Sie die Ereignisdatenbank in View Administrator konfigurieren, müssen Sie für eine Oracle 12c- oder 11g-Datenbank die Oracle-Systemkennung (SID) als Datenbankname verwenden.

- Den Benutzernamen und das Kennwort des Benutzers, den Sie für diese Datenbank erstellt haben. Siehe „[Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse](#)“, auf Seite 145.

Verwenden Sie die SQL Server-Authentifizierung für diesen Benutzer. Verwenden Sie nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode.

- Ein Präfix für die Tabellen in der Ereignisdatenbank, beispielsweise VE_. Das Präfix ermöglicht eine gemeinsame Verwendung der Datenbank durch die View-Installationen.

HINWEIS Die eingegebenen Zeichen müssen für die verwendete Datenbanksoftware zulässig sein. Die Syntax des Präfixes wird nicht überprüft, wenn Sie Daten in das Dialogfeld eingeben. Wenn Sie Zeichen eingeben, die für die verwendete Datenbanksoftware unzulässig sind, tritt ein Fehler auf, wenn View-Verbindungsserver versucht, eine Verbindung mit dem Datenbankserver herzustellen. Dieser Fehler und mögliche andere Fehlermeldungen, die bei einem ungültigen Datenbanknamen auftreten, werden in der Protokolldatei aufgezeichnet.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Ereigniskonfiguration** aus.
- 2 Klicken Sie im Abschnitt **Ereignisdatenbank** auf **Bearbeiten**, geben Sie die erforderlichen Informationen in die dafür vorgesehenen Felder ein und klicken Sie auf **OK**.
- 3 (Optional) Klicken Sie im Fenster „Ereigniseinstellungen“ auf **Bearbeiten**, ändern Sie den Wert für die Anzeigedauer von Ereignissen sowie die Anzahl der Tage zur Klassifizierung von neuen Ereignissen und klicken Sie auf **OK**.

Diese Einstellungen beziehen sich auf den Zeitraum, für den die Ereignisse in der View Administrator-Oberfläche angezeigt werden. Nach Ablauf dieses Zeitraums stehen die Ereignisse nur in den Verlaufsdatenbanktabellen zur Verfügung.

Das Fenster „Datenbankkonfiguration“ zeigt die aktuelle Konfiguration der Ereignisdatenbank an.

- 4 Wählen Sie **Überwachung > Ereignisse** aus, um zu prüfen, ob die Verbindung mit der Ereignisdatenbank erfolgreich hergestellt wurde.

Tritt bei der Verbindungsherstellung ein Fehler auf, wird eine Fehlermeldung angezeigt. Wenn Sie SQL Express oder eine benannte Instanz von SQL Server verwenden, müssen Sie möglicherweise die richtige Portnummer ermitteln, wie in den Voraussetzungen erwähnt.

Im View Administrator-Dashboard wird der Ereignisdatenbankserver in der Anzeige zum Systemkomponentenstatus unterhalb der Überschrift „Berichtsdatenbank“ angezeigt.

Konfigurieren der Ereignisprotokollierung für Syslog-Server

Sie können View-Ereignisse im Syslog-Format generieren, sodass Analysesoftware auf die Ereignisdaten zugreifen kann.

Sie müssen nur einen Host in einer View-Verbindungsserver-Gruppe konfigurieren. Die verbleibenden Hosts in der Gruppe werden automatisch konfiguriert.

Wenn Sie die dateibasierte Protokollierung von Ereignissen aktivieren, werden Ereignisse in einer lokalen Protokolldatei gesammelt. Bei Angabe einer Dateifreigabe werden diese Protokolldateien auf diese Freigabe verschoben.

- Verwenden Sie eine lokale Datei nur für eine schnelle Fehlerbehebung während der Konfiguration (möglicherweise vor der Konfiguration der Ereignisdatenbank), sodass Sie Ereignisse anzeigen können.

Die maximale Größe des lokalen Verzeichnisses für Ereignisprotokolle (einschließlich geschlossene Protokolldateien) beträgt 300 MB. Bei Überschreiten dieser Größe werden die ältesten Dateien gelöscht. Das Standardziel der Syslog-Ausgabe ist %PROGRAMDATA%\VMware\VDM\events\.

- Verwenden Sie einen UNC-Pfad für langfristige Ereignisaufzeichnungen, wenn Sie nicht über einen Syslog-Server verfügen oder wenn Ihr aktueller Syslog-Server Ihre Anforderungen nicht erfüllt.

Alternativ können Sie einen `vdmadmin`-Befehl verwenden, um die dateibasierte Protokollierung von Ereignissen im Syslog-Format zu konfigurieren. Weitere Informationen finden Sie im Thema zum Generieren von View-Ereignisprotokollmeldungen im Syslog-Format unter Verwendung der Option `-I` des Befehls `vdmadmin` im Dokument *Administration von View*.

WICHTIG Syslog-Daten werden innerhalb des Netzwerks ohne softwarebasierte Verschlüsselung übertragen und enthalten möglicherweise vertrauliche Daten (z. B. Benutzernamen). VMware empfiehlt die Implementierung einer Sicherheitsmaßnahme auf Verbindungsebene, z. B. IPsec, um zu verhindern, dass diese Daten im Netzwerk überwacht werden können.

Voraussetzungen

Um einen View-Verbindungsserver so zu konfigurieren, dass Ereignisse im Syslog-Format aufgezeichnet oder an einen Syslog-Server gesendet werden (oder beides), benötigen Sie die folgenden Informationen:

- Wenn ein Syslog-Server das System an einem UDP-Port auf View-Ereignisse überwachen soll, benötigen Sie den DNS-Namen oder die IP-Adresse des Syslog-Servers sowie die UDP-Portnummer. Die standardmäßige UDP-Portnummer lautet 514.
- Wenn Protokolle in einem Flatfileformat erfasst werden sollen, benötigen Sie den UNC-Pfad zur Dateifreigabe und zum Ordner, in dem die Protokolldateien gespeichert werden sollen. Außerdem benötigen Sie den Benutzernamen, den Domännennamen und das Kennwort eines Kontos mit Schreibberechtigungen für die Dateifreigabe.

Vorgehensweise

- 1 Wählen Sie in View Administrator **View-Konfiguration > Ereigniskonfiguration** aus.
- 2 (Optional) Um den View-Verbindungsserver so zu konfigurieren, dass Ereignisse an einen Syslog-Server gesendet werden, klicken Sie im Bereich **Syslog** neben **An Syslog-Server senden** auf **Hinzufügen** und geben Sie den Servernamen oder die IP-Adresse und die UDP-Portnummer an.
- 3 (Optional) Um das Generieren und Speichern von View-Ereignisprotokollmeldungen im Syslog-Format zu aktivieren, aktivieren Sie das Kontrollkästchen **In Datei protokollieren: Aktivieren**

Wenn Sie keinen UNC-Pfad zu einer Dateifreigabe angeben, werden die Protokolldateien lokal gespeichert.

- 4 (Optional) Um die View-Ereignisprotokollmeldungen auf einer Dateifreigabe zu speichern, klicken Sie neben **An Speicherort kopieren** auf **Hinzufügen** und geben Sie den UNC-Pfad zur Dateifreigabe und zum Ordner an, in dem die Protokolldateien gespeichert werden sollen. Geben Sie dabei auch den Benutzernamen, den Domännennamen und das Kennwort eines Kontos mit Schreibberechtigungen für die Dateifreigabe an.

Beispiel für einen UNC-Pfad:

```
\\syslog-server\folder\file
```


Index

A

- Active Directory
 - Konfigurieren von Domänen und Vertrauensbeziehungen **32**
 - Vorbereitung für Smartcard-Authentifizierung **37**
 - Vorbereitung zur Verwendung mit View **31**
- Active Directory-Gruppen, Erstellung für Clientkonten im Kiosk-Modus **33**
- Antivirensoftware, View Composer **56**
- Anzeigenname
 - für SSL-Zertifikate ändern **97**
 - Registrierungseinstellung für das PSG **106**
- Auslagerungsdatei, Größe, View-Verbindungsserver **143**

B

- Benutzerkonten
 - Anforderungen **111**
 - eigenständige View Composer-Instanz **34**
 - Für Instant Clone-Vorgänge **35**
 - vCenter Server **34, 112**
 - View Composer **112**
 - View Composer-AD-Vorgänge **34**
- Betriebsvorgänge, Einstellen von Grenzen für parallele Vorgänge **126**
- Blast Extreme **130**
- Browseranforderungen **11**

C

- CBRC, Konfigurieren für vCenter Server **123**
- Certificate Signing Request (CSR), , *siehe* CSR-Anfrage
- certutil, Befehl **40**
- CSR-Anfrage, mit der Windows-Zertifikatregistrierung erstellen **93**

D

- Datenbanken
 - Erstellung für View Composer **43**
 - View-Ereignisse **145, 147**
- Deinstallieren von View-Komponenten **87**
- direkte Verbindungen, Konfigurieren **129**
- DNS-Auflösung, View Composer **56**
- DNS-Namen, bevorzugen **134**
- Dokumentationsfeedback, Vorgehensweise **7**
- Domänenfilterung **33**

E

- Eingeschränkte Gruppen, Richtlinie, Konfigurieren **36**
- Enterprise NTAAuth-Speicher, Hinzufügen von Stammzertifikaten **40**
- Ereignisdatenbank
 - Erstellung für View **145, 147**
 - SQL Server-Konfiguration **146**
- Ereignisse, gesendet an Syslog-Server **148**
- Erstkonfiguration, Ansicht **111**
- ESX/ESXi-Hosts, View Composer **55**
- Externe URLs
 - Ändern für einen Sicherheitsserver **133**
 - konfigurieren, für View-Verbindungsserver-Instanz **132**
 - Zweck und Format **131**

F

- Fingerabdruck, Akzeptieren für ein Standardzertifikat **126**
- FIPS-Modus
 - Systemanforderungen **30**
 - View-Installation **29**
- Firefox, unterstützte Versionen **11**
- Firewall-Regeln
 - Back-End-Firewall **82**
 - View-Verbindungsserver **81**
- Firewalls, Konfigurieren **59**

G

- Gastbetriebssystem, Softwareanforderungen **15**
- Glossar, Website **7**
- GPOs, Verknüpfung mit einer Horizon-Desktop-OU **37**
- Größeneinstellungen für Windows Server, Vergrößern des JVM-Heaps **142**
- Gruppenrichtlinienobjekte, , *siehe* GPOs

H

- Hardwareanforderungen
 - Horizon-Verbindungsserver **10**
 - PCoIP **17**
 - View Composer, eigenständig **13**
- Horizon Agent, Installationsanforderungen **15**
- Horizon Client für iOS, Stammzertifikat als vertrauenswürdig einstufen **102**
- Horizon Client für Mac, Stammzertifikat als vertrauenswürdig einstufen **101**

Horizon-Clients, Konfigurieren von Verbindungen **128**
 Horizon-Verbindungsserver, Hardwareanforderungen **10**
 Horizon-Verbindungsserver-Installation
 Anforderungen, Übersicht **9**
 Netzwerkkonfiguration **11**
 Unterstützte Betriebssysteme **10**
 Virtualisierungssoftware, Anforderungen **10**
 Host-Caching, für vCenter Server **123**
 HTML Access **135, 136**
 HTML-Zugriff, Konfigurieren **130**
 HTTP
 Ändern des Ports für die HTTP-Umleitung **140**
 Verhindern der HTTP-Umleitung **141**

I

Installation, Unbeaufsichtigte Installation, Optionen für **84**
 Instant Clones, Erstellen eines Domänenadministratorkontos **35**
 Internet Explorer, unterstützte Versionen **11**
 IPsec, Konfigurieren einer Back-End-Firewall **82**
 IPv6-Umgebung
 andere unterstützte Funktionen **26**
 einrichten **23, 29**
 unterstützte Active Directory-Versionen **24**
 unterstützte Authentifizierungstypen **26**
 unterstützte Betriebssysteme für Desktops und RDS-Hosts **25**
 unterstützte Betriebssysteme für View Composer **24**
 unterstützte Betriebssysteme für View-Verbindungsserver **24**
 unterstützte Clients und Browser **25**
 unterstützte Datenbankversionen **24**
 unterstützte Remote-Protokolle **25**
 unterstützte vSphere-Versionen **24**
 View-Installation **23**

K

Kiosk-Modus, Active Directory-Vorbereitung **33**

L

Leistungsindikatoren, Aktivieren des Remote-Zugriffs auf Verbindungsservern **142**
 Lizenzschlüssel, View-Verbindungsserver **117**

M

Maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, Konfigurationsrichtlinien **126**
 Microsoft SQL Server-Datenbanken **13**
 Microsoft Windows Installer
 Eigenschaften für replizierte Instanz von View-Verbindungsserver **72**

Eigenschaften für Sicherheitsserver **79**
 Eigenschaften für View-Verbindungsserver **64**
 View-Komponenten unbeaufsichtigt deinstallieren **87**

MMC, Hinzufügen des Zertifikat-Snap-Ins **95**

N

Neuinstallieren, View-Verbindungsserver **83**

O

OCSP-Antwortdienst, Für die Zertifikatsperrüberprüfung **102**

ODBC

Verbindung mit Oracle 12c oder 11g herstellen **51**

Verbindungsherstellung mit SQL Server **47**

Oracle 11g, Erstellen einer View Composer-Datenbank mit einem Skript **49**

Oracle 11g-Datenbank

Hinzufügen einer ODBC-Datenquelle **51**

Hinzufügen für View Composer **48**

Konfigurieren eines Datenbankbenutzers **50**

Oracle 12c, Erstellen einer View Composer-Datenbank mit einem Skript **49**

Oracle 12c-Datenbank

Hinzufügen einer ODBC-Datenquelle **51**

Hinzufügen für View Composer **48**

Konfigurieren eines Datenbankbenutzers **50**

Oracle-Datenbanken **13**

Organisationseinheiten, , *siehe* OUs

OUs

Erstellen für View-Desktops **33**

Erstellung für Clientkonten im Kiosk-Modus **33**

P

PCoIP, Hardwareanforderungen **17**

PCoIP Secure Gateway

Externe URL **131**

Importieren eines Zertifikats **105**

Konfigurieren eines SSL-Zertifikats **103**

Legacy-Client-Zugriff verhindern **107**

Zertifikatsthemenname **104**

Persona-Verwaltung, Systemanforderungen für eine eigenständige Installation **16**

Port

Ändern für PSG **139**

Ändern für Sicherheitsserver **137**

Ändern für View-Verbindungsserver **137, 139**

Änderung für PCoIP Secure Gateway **138**

Änderung für View Composer **140**

Ports, Ersetzen der Standardports **136**

Professional Services **7**

R

RDP- **19**

- Registrierungsserver **57**
- Remote-Anzeigeprotokolle
 - PCoIP **17**
 - RDP- **19**
- ReplaceCertificate-Option, sviconfig-Dienstprogramm **99**
- Replizierte Instanzen
 - Installieren **66**
 - Netzwerkanforderungen **11**
 - Unbeaufsichtigte Installation **69**
 - Unbeaufsichtigte Installation, Eigenschaften **72**
- Richtlinien
 - Eingeschränkte Gruppen **36**
 - Vertrauenswürdige Stammzertifizierungsstellen **39**
 - Zwischenzertifizierungsstellen **40**
- S**
- schwache Verschlüsselungen in SSL/TLS, Deaktivieren **41**
- Sicherer Tunnel, Externe URL **131**
- Sicherheitsserver
 - Ändern einer externen URL **133**
 - Betriebssystemanforderungen **10**
 - Entfernen von IPSec-Regeln **80**
 - Installationsdatei **74**
 - Konfigurieren einer externen URL **131**
 - Konfigurieren eines Kennworts für die Kombination **73**
 - Unbeaufsichtigte Installation **77**
 - Unbeaufsichtigte Installation, Eigenschaften **79**
 - Vorbereitung für eine Aktualisierung oder Neuinstallation **80**
- Smartcard-Authentifizierung
 - Active Directory-Vorbereitung **37**
 - Benutzerprinzipalnamen (UPNs) für Smartcard-Benutzer **38**
- Softwareanforderungen, Serverkomponenten **9**
- Sparse-Festplatten, Konfigurieren für vCenter Server **122**
- Speicher, Rückgewinnung von Datenträgerplatz **122**
- SQL Server Management Studio, Installieren **44**
- SQL Server-Datenbank
 - Berechtigungen manuell festlegen **45**
 - Hinzufügen einer ODBC-Datenquelle **47**
 - Hinzufügen für View Composer **44**
 - Vorbereiten für Ereignisdatenbank **146**
- SQL Server-Datenbanken **13**
- SSL, Akzeptieren eines Zertifikatsfingerabdrucks **126**
- Stammzertifikat, Importieren in den Windows-Zertifikatspeicher **97**
- Stammzertifikate
 - Hinzufügen zu vertrauenswürdigen Stammzertifizierungsstellen **39, 100**
 - Hinzufügen zum Enterprise NTAAuth-Speicher **40**
- Standardzertifikat, ersetzen **89**
- Support, Online- und Telefonsupport **7**
- sviconfig-Dienstprogramm
 - Konfigurieren von Zertifikaten **99**
 - ReplaceCertificate-Option **99**
- Syslog-Server, Konfigurieren von View-Ereignissen für das Senden an Syslog-Server **148**
- Systemauslagerungsdatei, Größe, Windows Server **143**
- T**
- TCP-Ports, View-Verbindungsserver **81**
- Technischer Support und Schulung **7**
- TLSv1.0 **54, 65**
- U**
- unbeaufsichtigte Installation
 - Replizierte Instanzen **69**
 - Sicherheitsserver **77**
 - View-Verbindungsserver **62**
- Unbeaufsichtigte Installation, Optionen für **84**
- UPNs, Smartcard-Benutzer **38**
- userPrincipalName, Attribut **38**
- V**
- vCenter Server
 - Benutzerkonten **34, 112**
 - Grenzwerte für parallele Vorgänge konfigurieren **125**
 - Installieren des View Composer-Dienstes **52**
 - Konfigurieren für View Composer **55**
 - Konfigurieren von Host-Caching **123**
 - Konfigurieren von Sparse-Festplatten **122**
- vCenter Server-Benutzer
 - vCenter Server-Berechtigungen **113**
 - View Composer-Berechtigungen **115**
- vCenter Server-Instanzen, Hinzufügen in View Administrator **117**
- Vertrauensbeziehungen, konfigurieren, für View-Verbindungsserver **32**
- Vertrauenswürdige Stammzertifizierungsstellen, Richtlinie **39, 100**
- View Administrator
 - Anforderungen **11**
 - Anmelden **116**
 - Übersicht **115**
- View Composer
 - eigenständiges Benutzerkonto **34**
 - Hardwareanforderungen für eigenständigen View Composer **13**

- View Composer-Datenbank
 - Anforderungen **13, 43**
 - ODBC-Datenquelle für Oracle 12c oder 11g **51**
 - ODBC-Datenquelle für SQL Server **47**
 - Oracle 12c und 11g **48**
 - SQL Server **44**
 - View Composer-Infrastruktur
 - Konfigurieren von vSphere **55**
 - optimieren **55**
 - Testen der DNS-Auflösung **56**
 - View Composer-Installation
 - Anforderungen, Übersicht **12**
 - Installationsdatei **52**
 - Übersicht **43**
 - View Composer-Konfiguration
 - Berechtigungen für vCenter Server-Benutzer **115**
 - Domänen **121**
 - Einstellungen in View Administrator **119**
 - Erstellen eines Benutzerkontos **34**
 - Erstellen eines vCenter Server-Benutzers **34, 112**
 - Grenzwerte für parallele Vorgänge **125**
 - SSL-Zertifikate **52**
 - View Composer-Upgrade
 - Anforderungen, Übersicht **12**
 - Betriebssystemanforderungen **12**
 - Kompatibilität mit vCenter Server-Versionen **12**
 - View-Desktops, Konfigurieren direkter Verbindungen **129**
 - View-Speicherbeschleunigung, Konfigurieren für vCenter Server **123**
 - View-Verbindungsserver-Installation
 - Einzelserver **59**
 - Installationsarten **57**
 - Neuinstallation mit Sicherungskonfiguration **83**
 - Produktlizenzschlüssel **117**
 - Replizierte Instanzen **66**
 - Sicherheitsserver **74**
 - Übersicht **57**
 - Unbeaufsichtigt **62**
 - Unbeaufsichtigte Installation, Eigenschaften **64**
 - Voraussetzungen **58**
 - View-Verbindungsserver-Konfiguration anfängliche **115**
 - Clientverbindungen **128**
 - Ereignisdatenbank **145, 147**
 - Ereignisse für Syslog-Server **148**
 - Ersetzen des Standardzertifikats **89**
 - Externe URL **131, 132**
 - Größeneinstellungen für Windows Server **142**
 - Systemauslagerungsdatei, Größe **143**
 - Übersicht **57**
 - Vertrauensbeziehungen **32**
 - VMware Blast Extreme-Anzeigeprotokoll **19**
 - vSphere, Konfigurieren für View Composer **55**
- ## W
- Webbrowseranforderungen **11**
 - Windows Server, Systemauslagerungsdatei, Größe **143**
 - Windows-Zertifikatspeicher
 - Importieren eines Stammzertifikats **97**
 - Importieren eines Zertifikats **96**
 - Konfigurieren von Zertifikaten **94**
 - signiertes Zertifikat erwerben **93**
- ## Z
- Zertifikate
 - Akzeptieren des Fingerabdrucks **126**
 - Anforderungen **89**
 - Anzeigename **97**
 - Bestimmen, wann Zertifikate für View Composer konfiguriert werden **52**
 - Beziehen von einer Zertifizierungsstelle **92**
 - Ersetzen des Standardzertifikats **89**
 - Erstellen neuer Zertifikate **92**
 - Fehlerbehebung auf View Servern **109**
 - Horizon Client für iOS **102**
 - Horizon Client für Mac **101**
 - Import in einen Windows Zertifikatspeicher **94**
 - Konfigurationsübersicht **91**
 - Konfigurieren von Clients, um das Stammzertifikat als vertrauenswürdig einzustufen **100**
 - Richtlinien und Konzepte **90**
 - Signaturen vom Windows-Zertifikatspeicher abrufen **93**
 - vCenter Server-Zertifikate in View Administrator als vertrauenswürdig einstufen **108**
 - View Composer-Zertifikate in View Administrator als vertrauenswürdig einstufen **108**
 - Vorteile der Verwendung **108**
 - Zertifikatssperrliste **102**
 - Zertifikatssperrüberprüfung, Aktivieren **102**
 - Zwischenzertifikate, Hinzufügen zu Zwischenzertifizierungsstellen **40**
 - Zwischenzertifizierungsstellen, Richtlinie **40**