

Horizon 7-Upgrades

MÄRZ 2020

VMware Horizon 7 7.12



vmware®

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

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

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

docfeedback@vmware.com

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

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

Copyright © 2009-2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Horizon 7-Upgrades auf 7.12	5
1 Überblick über das Horizon 7-Upgrade	6
2 Anwenden einer Extended Service Branch	9
3 Upgrade der Client-Anwendung	10
4 Systemanforderungen für Horizon 7 Server-Upgrades	12
Kompatibilitätsmatrix für verschiedene Versionen von Horizon 7-Komponenten	12
View Composer-Anforderungen	13
Unterstützte Betriebssysteme für View Composer	13
Hardwareanforderungen für eigenständigen View Composer	14
Datenbankanforderungen für View Composer und die Ereignisdatenbank	15
Upgrade-Anforderungen für View Composer	15
Horizon-Verbindungsserver – Serveranforderungen	16
Hardwareanforderungen für den Horizon-Verbindungsserver	17
Unterstützte Betriebssysteme für den Horizon-Verbindungsserver	17
Upgrade-Anforderungen für Horizon-Verbindungsserver	18
Anforderungen und Überlegungen für Horizon Agent	19
5 Upgrade von Horizon 7-Serverkomponenten	21
Upgrade für View Composer	21
Vorbereiten von vCenter Server und View Composer für ein Upgrade	22
Upgrade für View Composer	24
Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer	25
Aktivieren der Digest Access Authentication für View Composer	26
Manuelles Upgrade der View Composer-Datenbank	27
Migrieren von View Composer auf eine andere Maschine	30
Aktualisieren des Horizon-Verbindungsservers	37
Vorbereiten des Verbindungsservers für ein Upgrade	38
Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe	39
Aktivieren von TLSv1.0 für vCenter-Verbindungen vom Verbindungsserver	43
Upgrade auf die neueste Version des Verbindungsservers auf einer anderen Maschine	44
Erstellen einer replizierten Gruppe nach dem Zurücksetzen des Verbindungsservers auf einen Snapshot	45
Upgrade von Sicherheitsservern	46
Vorbereiten des Sicherheitsservers für ein Upgrade	46

Upgrade für Sicherheitsserver und die damit kombinierten Verbindungsserver	47
Ersetzen eines Sicherheitsservers durch eine Unified Access Gateway-Appliance	51
Upgrade der Registrierungsserver	52
Upgrade einer Cloud-Pod-Architektur-Umgebung	52
Upgrade von Horizon 7-Servern für das Zulassen von HTML Access	53
Upgrade von vCenter Server	53
Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats	55
Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7	57

6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen 58

7 Upgrade von veröffentlichten und virtuellen Desktops 61

Sicherheitsbezogene Anforderungen für das Desktop-Upgrade	61
Durchführen eines Upgrades von RDS-Hosts, die sitzungsbasierte Desktops bereitstellen	62
Upgrade von View Agent oder Horizon Agent	63
Upgrade von View Composer-Desktop-Pools	66
Upgrade von Instant-Clone-Desktop-Pools	68

8 Aufgaben nach dem Upgrade zum Aktivieren neuer Funktionen für Ihr Horizon-Setup 71

Ändern des Sicherheitsmodus für JMS-Meldungen auf Erweitert	71
Aufgaben für die Aktualisierung von Desktop-Pools zur Verwendung der Speicherplatzrückgewinnung	73
Upgrade-Aufgaben bei Verwendung von VMware vSAN-Datenspeichern	74
Upgrade von einem Non-vSAN-Datenspeicher auf einen vSAN-Datenspeicher	74
Upgrade vom vSAN-Festplattenformat der Version 1	76
Upgrade von Horizon View 5.3.x auf einem vSAN-Datenspeicher	78
Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer	79

9 Separates Upgrade von vSphere-Komponenten in einer Horizon 7-Umgebung 84

Horizon 7-Upgrades auf 7.12

Horizon 7-Upgrades enthält Anleitungen für Upgrades von den letzten Wartungsversionen von VMware Horizon™ 6 (mit View) oder VMware Horizon 6 Version 6.1 oder 6.2 auf VMware Horizon 7. Sie können dieses Handbuch auch bei Upgrades auf Wartungsversionen von Horizon 7 verwenden.

Falls Sie auch ein Upgrade Ihrer Version von VMware vSphere® durchführen, erfahren Sie in dem Handbuch, welche Schritte dieses Upgrades Sie in verschiedenen Phasen des Horizon 7-Upgrades durchführen müssen.

Zielgruppe

Dieses Handbuch richtet sich an Benutzer, die ein Upgrade auf diese neueste Version dieses Produkts durchführen möchten. Dieses Dokument wurde für erfahrene Microsoft Windows- bzw. Linux-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen und Rechenzentrumsoperationen vertraut sind.

Überblick über das Horizon 7-Upgrade

1

Zur Durchführung des Upgrades einer Horizon 7-Unternehmensbereitstellung gehören mehrere allgemeine Aufgaben. Das Upgrade ist ein mehrstufiger Prozess, bei dem Vorgänge in einer bestimmten Reihenfolge durchgeführt werden müssen. Sie aktualisieren View Composer vor dem Upgrade des Horizon Connection Server und den anderen Horizon 7-Servern.

Wichtig Mit Horizon 6 Version 6.2 und höheren Versionen können Sie Horizon 7-Komponenten zur Ausführung im FIPS-Modus installieren. Horizon 7 unterstützt kein Upgrade einer Nicht-FIPS-Installation auf eine FIPS-Installation. Horizon unterstützt das Upgrade von Horizon 6 Version 6.2 im FIPS-Modus auf Horizon 7 im FIPS-Modus. Für eine Neuinstallation finden Sie Erläuterungen unter „Installieren von Horizon 7 im FIPS-Modus“ im Dokument *Horizon 7-Installation*.

Während eines Upgrades unterstützt Horizon 7 keine Bereitstellungs- und Wartungsvorgänge für View Composer. Vorgänge wie die Bereitstellung und Neuerstellung von Linked-Clone-Desktops sind in der Übergangsphase, wenn auf manchen Horizon 7-Servern noch die frühere Version ausgeführt wird, nicht möglich. Sie können diese Vorgänge erst erfolgreich ausführen, wenn die Upgrades aller Verbindungsserver- und View Composer-Instanzen abgeschlossen sind.

Der Upgrade-Prozess muss in einer bestimmten Reihenfolge abgeschlossen werden. Auch innerhalb der einzelnen Schritte muss die Reihenfolge berücksichtigt werden.

Hinweis Dieser Überblick bezieht sich auf Upgrades für Haupt- und Nebenversionen sowie Wartungsversionen.

Wie viele der folgenden Aufgaben durchzuführen sind, hängt von den Horizon 7-Komponenten ab, die Sie in Ihrer Bereitstellung verwenden.

- 1 Führen Sie ein Upgrade der Horizon Client-Software durch, die auf den Clientgeräten der Endbenutzer ausgeführt wird. Siehe [Kapitel 3 Upgrade der Client-Anwendung](#).
- 2 Erstellen Sie Sicherungen auf den physischen Computern oder virtuellen Maschinen, auf denen View Composer und VMware® vCenter Server™ gehostet werden, und halten Sie bestimmte geplante Aufgaben vorübergehend an. Siehe [Vorbereiten von vCenter Server und View Composer für ein Upgrade](#).

Wenn Sie über eine eigenständige View Composer-Installation verfügen, die auf einem anderen Computer als vCenter Server installiert ist, müssen Sie nur eine Sicherung der View Composer-Datenbank und des View Composer-TLS/SSL-Zertifikats erstellen. Wenn Sie auch ein Upgrade für vCenter Server durchführen möchten, können Sie dieses gesondert vornehmen.

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.

- 3 Führen Sie das Upgrade von View Composer auf dem vorhandenen Host durch oder migrieren Sie auf eine neue Maschine. Siehe [Upgrade für View Composer](#).
- 4 Erstellen Sie Sicherungen auf den physischen oder virtuellen Maschinen, auf denen Verbindungsserver-Instanzen gehostet werden, und zeichnen Sie verschiedene Konfigurations- und Systemeinstellungen auf. Siehe [Vorbereiten des Verbindungsservers für ein Upgrade](#).

Verfügen Sie über mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe, erstellen Sie Sicherungen und dokumentieren Sie die Konfigurationseinstellungen für nur eine Instanz der Gruppe. Alle anderen Vorbereitungsaufgaben können Sie immer für jeweils eine Instanz unmittelbar vor dem Upgrade dieser Serverinstanz durchführen.

- 5 Führen Sie ein Upgrade für Verbindungsserver-Instanzen durch, die nicht mit Sicherheitsservern kombiniert sind. Siehe [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#).

In einer typischen Produktionsumgebung mit zwei oder mehr Verbindungsserver-Instanzen, denen ein Lastausgleichsmodul vorgelagert ist, können Sie, wenn Sie die Ausfallzeit minimieren möchten, immer jeweils eine Verbindungsserver-Instanz aus dem Lastausgleichs-Cluster entfernen, wenn Sie das Upgrade durchführen.

Wichtig Nach dem Upgrade einer Verbindungsserver-Instanz auf die neueste Version ist kein Downgrade dieser Instanz auf eine frühere Version mehr möglich. Nach dem Upgrade aller Verbindungsserver-Instanzen in einer replizierten Gruppe können Sie keine weitere Instanz hinzufügen, auf der eine frühere Version ausgeführt wird.

- 6 Wenn Sie Sicherheitsserver verwenden, führen Sie Sicherungen durch und dokumentieren Sie die verschiedenen Konfigurations- und Systemeinstellungen. Siehe [Vorbereiten des Sicherheitsservers für ein Upgrade](#).

Zur Minimierung der Ausfallzeit können Sie diese Vorbereitungsaufgaben immer für jeweils einen Sicherheitsserver unmittelbar vor dem Upgrade dieser Serverinstanz durchführen.

- 7 Wenn Sie Sicherheitsserver verwenden, führen Sie für jeden Sicherheitsserver und die Verbindungsserver-Instanz, mit der dieser kombiniert ist, ein Upgrade durch. Wenn Sie für diese Kombinationen das Upgrade nacheinander durchführen, können Sie durch Entfernen jedes Sicherheitsservers aus der Gruppe mit dem Lastausgleich, durch das Upgrade für die Kombination und das anschließende erneute Hinzufügen des Sicherheitsservers zur Gruppe Ausfallzeiten vermeiden. Siehe [Upgrade für Sicherheitsserver und die damit kombinierten Verbindungsserver](#).
- 8 Führen Sie ein Upgrade der in Active Directory verwendeten Gruppenrichtlinien durch. Siehe [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für Horizon 7](#).

- 9 Wenn Sie gleichzeitig ein Upgrade von VMware vSphere-Komponenten durchführen, aktualisieren Sie auch vCenter Server. Siehe [Upgrade von vCenter Server](#).

Während der Durchführung des Upgrades von vCenter Server wird die Verbindung mit vorhandenen Remote-Desktop- und -Anwendungssitzungen nicht getrennt. Remote-Desktops im Bereitstellungsstatus werden während des vCenter Server-Upgrades nicht eingeschaltet, neue Desktops können nicht gestartet werden und es sind keine View Composer-Vorgänge während des vCenter Server-Upgrades möglich.

- 10 Wenn Sie gleichzeitig ein Upgrade von vSphere durchführen, aktualisieren Sie auch die VMware[®] ESXi[™]-Hosts und die virtuellen Maschinen. Siehe [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#).

Für ESXi-Hosts kann ein Upgrade ohne Ausfallzeit durch Verlagerung der virtuellen Maschinen auf einen anderen Host im Cluster durchgeführt werden, wenn die Hosts für eine Cluster-Umgebung konfiguriert sind.

- 11 Wenn Sie zurzeit Windows-Terminaldienste-Server als Desktop-Quellen verwenden, führen Sie ein Upgrade auf Windows Server 2008 R2 oder höher durch und prüfen Sie, ob die RDS-Host-Rolle bereits installiert ist. Siehe [Durchführen eines Upgrades von RDS-Hosts, die sitzungsbasierte Desktops bereitstellen](#).
- 12 Führen Sie ein Upgrade der Horizon[™] Agent- oder View Agent[™]-Software durch, die auf dem physischen Computer oder der virtuelle Maschine ausgeführt wird, die als Desktop-Quellen, als Full-Clone-Desktops in einem Pool und als einzelne Desktops in einem manuellen Pool verwendet werden. Siehe [Upgrade von View Agent oder Horizon Agent](#).
- 13 Verwenden Sie die neu aktualisierten Quellen von Desktops mit virtuellen Maschinen zum Erstellen aktualisierter Desktop-Pools. Siehe [Upgrade von View Composer-Desktop-Pools](#).
- 14 Erläuterungen zur Cloud-Pod-Architektur-Funktion finden Sie unter [Upgrade einer Cloud-Pod-Architektur-Umgebung](#).

Da bestimmte Befehle mehrere Stadien gleichzeitig aktualisieren können, empfiehlt VMware, sich mit den unumkehrbaren Änderungen der einzelnen Stadien gründlich vertraut zu machen, bevor Sie Ihre Produktionsumgebungen aktualisieren.

Wichtig Der VMware View[®]-Client mit Funktion „Lokaler Modus“ für die Verwendung von Offline-Desktops wurde entfernt. Aus diesem Grund enthält dieser Überblick keine Schritte für das Upgrade von View-Übertragungsserver-Instanzen und View Client mit „Lokaler Modus“. Anstelle der Funktion „Lokaler Modus“ empfiehlt VMware die Verwendung von VMware[®] Mirage[™]. Diese Anwendung ist im Lieferumfang von VMware Horizon 6.0 und höher enthalten. Weitere Informationen finden Sie in den Versionshinweisen zu Horizon 7, die unter <https://docs.vmware.com/de/VMware-Horizon-7/index.html> verfügbar sind.

Anwenden einer Extended Service Branch

2

Ein Extended Service Branch (ESB) ist eine Option, die mit Horizon 7, VMware App Volumes und VMware Dynamic Environment Manager verfügbar ist. Es enthält regelmäßige Service Pack-Updates (SP), zu denen kumulative, kritische Fehlerbehebungen und Sicherheitskorrekturen gehören.

Wenn Sie kein Upgrade auf die neueste Version von Horizon durchführen und Ihre Version beibehalten möchten, können Sie ESBs bereitstellen, um weiterhin frühzeitige Fehler- und Sicherheitskorrekturen zu erhalten. Die SP-Updates enthalten keine neuen Funktionen. Sie können sich daher darauf verlassen, dass Sie für Ihre geschäftskritischen Bereitstellungen weiterhin über eine stabile Horizon-Plattform verfügen.

Einmal pro Jahr sind separate ESBs für den Kern der Horizon-Plattform, VMware App Volumes und VMware Dynamic Environment Manager verfügbar. ESBs werden 24 Monate lang durch drei geplante SP-Updates unterstützt: SP1 wird sechs Monate nach der Erstveröffentlichung freigegeben, SP2 drei Monate nach SP1 und SP3 sechs Monate nach SP2.

Weitere Informationen finden Sie in den häufig gestellten Fragen: Horizon 7, App Volumes, DEM Extended Service Branches (ESB) unter <https://kb.vmware.com/s/article/52845>.

Upgrade der Client-Anwendung

3

Führen Sie ein Upgrade auf die neueste Version von Horizon Client durch und aktualisieren Sie die Firmware auf Thin Client-Geräten, sofern Sie diese verwenden.

Wichtig Für ein Upgrade muss die neue Version des Horizon Client-Installationsprogramms ausgeführt werden, ohne dass zuerst die ältere Version der Client-Anwendung entfernt wird. Wenn Ihre Endbenutzer den Windows-basierten Horizon Client 4.6.0 oder eine ältere Version haben, weisen Sie sie an, die Client-Software zu entfernen, bevor sie das neueste Horizon Client-Installationsprogramm herunterladen und ausführen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.
- Stellen Sie sicher, dass der Client-Desktop, der Laptop, das Tablet oder das Telefon die Horizon Client-Anforderungen an das Betriebssystem und die Hardware erfüllt. Informationen über die Anforderungen des jeweiligen Desktop- oder mobilen Client-Geräts finden Sie im Dokument „Verwenden von Horizon Client“. Besuchen Sie <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

Verfahren

- 1 Weisen Sie Endbenutzer an, ein Upgrade auf die neueste Version von Horizon Client durchzuführen.

Option	Aktion
Horizon Client	<p>Laden Sie die Horizon Client-Installationsprogramme herunter und senden Sie sie an die Endbenutzer oder platzieren Sie die Programme auf einer Website und bitten Sie die Endbenutzer, sie von dort herunterzuladen und auszuführen. Die Installationsprogramme können Sie selbst herunterladen oder lassen Sie Ihre Endbenutzer das Programm von der VMware-Website unter https://www.vmware.com/go/viewclients herunterladen.</p> <p>Bei mobilen Clients können Sie die Endbenutzer auch anweisen, die neueste Horizon Client-Version von Apple App Store, Google Play, Amazon, Windows Store oder ähnlichen Websites herunterzuladen.</p>
VMware Horizon-Webportal für Benutzer	<p>Die Endbenutzer können einen Browser öffnen und zu einer bestimmten Verbindungsserver-Instanz navigieren. Die angezeigte Webseite ist das VMware Horizon-Webportal für Benutzer, das Links zum Herunterladen der Horizon Client-Installationsprogrammdatei enthält.</p> <p>Hinweis Die standardmäßigen Links auf der Webseite verweisen auf die Site zum Horizon Client-Download. Sie können die Standardlinks so abändern, dass Sie auf andere Seiten verweisen. Siehe Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer.</p>
Thin Client	<p>Aktualisieren Sie die Thin Client-Firmware und installieren Sie die neue Horizon Client-Software auf den Clientgeräten der Endbenutzer. Thin Clients und Zero Clients werden von den VMware-Partnern bereitgestellt.</p>

- 2 Fordern Sie die Endbenutzer auf, zu überprüfen, ob sie sich anmelden und eine Verbindung mit ihren Remote-Desktops herstellen können.

Systemanforderungen für Horizon 7 Server-Upgrades

4

Hosts und virtuelle Maschinen in einer Horizon 7-Bereitstellung müssen spezifische Hardware- und Betriebssystemanforderungen erfüllen.

Dieses Kapitel enthält die folgenden Themen:

- [Kompatibilitätsmatrix für verschiedene Versionen von Horizon 7-Komponenten](#)
- [View Composer-Anforderungen](#)
- [Horizon-Verbindungsserver – Serveranforderungen](#)
- [Anforderungen und Überlegungen für Horizon Agent](#)

Kompatibilitätsmatrix für verschiedene Versionen von Horizon 7-Komponenten

Da große Unternehmen Upgrades häufig in mehreren Phasen durchführen müssen, sind Komponenten zumindest während des Aktualisierungsvorgangs aufwärts- und abwärtskompatibel.

Die folgenden Versionen werden für das Upgrade auf Horizon 7 unterstützt:

- Letzte Wartungsversion von Horizon View 5.3
- Letzte Wartungsversion von VMware Horizon 6.0 (mit View)
- Letzte Wartungsversion von VMware Horizon 6 Version 6.1
- Letzte Wartungsversion von VMware Horizon 6 Version 6.2

In den Versionshinweisen für die betreffende Version unter <https://docs.vmware.com/de/VMware-Horizon-7/index.html> ist die letzte Wartungsversion einer Komponente aufgeführt.

Die Kompatibilität des Horizon-Verbindungservers mit Horizon Agents beschränkt sich auf die Interoperabilität während eines Verbindungsserver-Upgrades. Sie müssen Horizon Agents schnellstmöglich aktualisieren, sodass diese mit der Verbindungsserverversion übereinstimmt, die für deren Verwaltung verwendet wird.

In der folgenden Tabelle werden die Komponenten aufgelistet. Außerdem wird angegeben, ob diese Komponenten mit Komponenten anderer Versionen kompatibel sind.

Tabelle 4-1. Kompatibilitätsmatrix für VMware Horizon 7 und frühere Versionen von View-Komponenten

	Verbindungsserver: Frühere Version	Sicherheitsserver: Frühere Version	View Composer: Frühere Version	View Agent: Frühere Version	Horizon Client (Windows): Frühere Version
Verbindungsserver 7.0	Nur während Upgrade	Nur wenn vor Upgrade kombiniert	Nein	Nur während Upgrade	Ja
Sicherheitsserver 7.0 (PCoIP und RDP)	Nein	–	Nein	Nur während Upgrade	Ja
View Composer 7.0	Nur während Upgrade	Nur während Upgrade	–	Nur während Upgrade	–
Horizon Agent 7.0	Nur während des Upgrades (siehe die Ausnahme im Hinweis im Anschluss an diese Tabelle)	Nein	Nein	–	Nur während Upgrade
Horizon Client 4.0	Ja	Ja	Ja	Ja	–

Vorsicht Während eines Upgrades werden keine View Composer-Bereitstellungs- und -Wartungsvorgänge unterstützt. Vorgänge wie die Bereitstellung und Neuerstellung von Linked-Clone-Desktops sind in der Übergangsphase, wenn auf manchen Horizon 7-Servern noch die frühere Version ausgeführt wird, nicht möglich. Sie können diese Vorgänge nur dann erfolgreich ausführen, wenn ein Upgrade aller Instanzen des Verbindungsservers und von View Composer auf die neueste Version durchgeführt wurde.

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.

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

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 4-2. 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
Windows Server 2019	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](#).

Weitere Informationen zur Fehlerbehebung einer View Composer-Installation auf einer virtuellen Maschine mit Windows Server 2016 oder Windows Server 2019 finden Sie im VMware Knowledgebase-Artikel <https://kb.vmware.com/s/article/59633>.

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 4-3. 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

Tabelle 4-3. Hardwareanforderungen für View Composer (Fortsetzung)

Hardwarekomponente	Erforderlich	Empfohlen
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 Horizon Connection Server zu Horizon-Ereignissen erfassen lassen.

Wenn bereits eine Datenbankserverinstanz für vCenter Server vorhanden ist, kann View Composer diese vorhandene Instanz nutzen, wenn es sich um eine in der Interoperabilitätsmatrix für VMware-Produkte unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php genannte Version handelt. 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.

Aktuelle Informationen zu unterstützten Datenbanken finden Sie in den VMware Produkt-Interoperabilitäts-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**.

Upgrade-Anforderungen für View Composer

Für den Vorgang der View Composer-Aktualisierung gibt es spezifische Anforderungen und Einschränkungen.

Um das Installationsprogramm für View Composer auszuführen, müssen Sie Domänenbenutzer mit Administratorrechten auf dem System sein.

Sicherheitsbezogene Anforderungen

- View Composer benötigt ein TLS-Zertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde. 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.

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

Alle Informationen zu den Anforderungen an Sicherheitszertifikate finden Sie im Abschnitt „Konfigurieren von SSL-Zertifikaten für View Server“ im Dokument *Horizon 7 Installation* von .

- Zertifikate für vCenter Server, View Composer und Horizon 7-Server müssen Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) enthalten. Weitere Informationen finden Sie unter „Konfigurieren der Zertifikatsperrüberprüfung für Serverzertifikate“ im Handbuch *Horizon 7 Installation* von .
- Stellen Sie sicher, dass keine auf dem Computer mit View Composer ausgeführten Anwendungen SSL-Bibliotheken von Windows verwenden, die das über das Microsoft Secure Channel (Schannel)-Sicherheitspaket bereitgestellte SSLv2 erfordern. 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. SSLv3, TLSv1.0 und RC4 sind standardmäßig ebenso deaktiviert. Weitere Informationen dazu finden Sie unter „Ältere Protokolle und in View deaktivierte Verschlüsselungen“ im Dokument *Horizon 7-Sicherheit*.
- Um die Sicherheit von View Composer zu erhöhen, deaktivieren Sie die kryptografisch schwachen Verschlüsselungssammlungen auf dem Windows Server-Computer, auf dem der View Composer-Dienst installiert ist. Informationen dazu finden Sie im Dokument *Horizon 7-Installation* unter „Deaktivieren Sie schwache Verschlüsselungen in SSL/TLS“.
- Um fortzufahren, müssen Sie eventuell die Konfiguration des Sicherheitsprotokolls ändern, damit die Kompatibilität mit vSphere gewährleistet ist. Wenn möglich, wenden Sie vor dem Upgrade von View Composer Patches für ESXi und vCenter Server zur Unterstützung von TLSv1.1 und TLSv1.2 an. Ist dies nicht möglich, aktivieren Sie TLSv1.0 auf View Composer erneut, bevor Sie ein Upgrade durchführen. Weitere Informationen finden Sie unter [Aktivieren von TLSv1.0 für vCenter- und ESXi-Verbindungen von View Composer](#).
- Ab Horizon 7 Version 7.0.3 können Sie die Digest Access Authentication für View Composer zur Verbesserung der Sicherheit aktivieren. Weitere Informationen finden Sie unter [Aktivieren der Digest Access Authentication für View Composer](#).

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

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 4-4. 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-Verbindungservers, 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 4-5. 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
Windows Server 2019	64 Bit	Standard Datacenter

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

Upgrade-Anforderungen für Horizon-Verbindungsserver

Für das Horizon-Verbindungsserver-Upgrade gibt es spezifische Anforderungen und Einschränkungen.

- Für Verbindungsserver ist ein gültiger Lizenzschlüssel für diese neueste Version erforderlich.
- Das Domänenbenutzerkonto, das Sie zur Installation der neuen Version von Verbindungsserver verwenden, muss auf dem Verbindungsserver-Host über Administratorrechte verfügen. Der Verbindungsserver-Administrator benötigt Administratoranmeldeinformationen für vCenter Server.
- Wenn Sie das Installationsprogramm ausführen, autorisieren Sie ein Konto für Administratoren. Das Konto kann auch das der lokalen Administratorengruppe, das eines Domänenbenutzers oder ein Gruppenkonto sein. Horizon 7 weist nur diesem Konto vollständige Horizon-Administratorrechte zu, einschließlich der Berechtigung zum Installieren von replizierten Verbindungsserver-Instanzen. Wenn Sie einen Domänenbenutzer oder eine Gruppe angeben, müssen Sie das Konto in Active Directory erstellen, bevor Sie das Installationsprogramm ausführen.
- Wenn Sie den Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Um die verschlüsselte Horizon 7-Sicherungskonfiguration wiederherzustellen, müssen Sie das Kennwort für die Datenwiederherstellung angeben. Das Kennwort muss 1 bis 128 Zeichen umfassen.

Sicherheitsbezogene Anforderungen

- Für Verbindungsserver ist ein TLS-Zertifikat erforderlich, das von einer Zertifizierungsstelle (CA) signiert wurde und von Ihren Clients validiert werden kann. Wenn bei der Installation des Verbindungservers kein Zertifikat vorhanden ist, das von einer Zertifizierungsstelle signiert wurde, wird zwar ein selbstsigniertes Standardzertifikat erstellt, das jedoch so schnell wie möglich ersetzt werden muss. Selbstsignierte Zertifikate werden in Horizon Administrator als ungültig angezeigt.

Außerdem erwarten aktualisierte Clients, dass Informationen zum Zertifikat des Servers beim TLS-Handshake zwischen Client und Server übergeben werden. Oft vertrauen aktualisierte Clients den selbst signierten Zertifikaten nicht.

Alle Informationen zu den Anforderungen an Sicherheitszertifikate finden Sie im Abschnitt „Konfigurieren von TLS-Zertifikaten für Horizon 7 Server“ im Dokument *Horizon 7-Installation*. Weitere Informationen finden Sie außerdem im Dokument *Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7*, in dem das Einrichten von Zwischenservern beschrieben wird, die Aufgaben wie den Lastausgleich und das Verschieben von SSL-Verbindungen durchführen.

Hinweis Falls Ihre ursprünglichen Server bereits über TLS-Zertifikate verfügen, die von einer Zertifizierungsstelle signiert wurden, importiert Horizon 7 Ihr vorhandenes von der Zertifizierungsstelle signiertes Zertifikat während der Aktualisierung in den Windows Server-Zertifikatspeicher.

- Zertifikate für vCenter Server, View Composer und Horizon 7-Server müssen Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) enthalten. Weitere Informationen finden Sie unter „Konfigurieren der Zertifikatsperrüberprüfung für Serverzertifikate“ im Dokument *Horizon 7-Installation*.

Wichtig Wenn Ihr Unternehmen für den Internetzugang Proxy-Einstellungen benutzt, müssen Sie eventuell Ihre Verbindungsserver-Hosts so konfigurieren, dass sie den Proxy verwenden. Dieser Schritt stellt sicher, dass die Server auf Zertifikatsperrüberprüfungsseiten im Internet zugreifen können. Sie können Microsoft NetShell-Befehle verwenden, um die Proxy-Einstellungen in den Verbindungsserver zu importieren. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung bei der Horizon 7 Server-Zertifikatsperrüberprüfung im Dokument *Horizon 7-Verwaltung*.

- Wenn Sie einen Sicherheitsserver mit dieser Instanz von Verbindungsserver kombinieren möchten, 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 Verbindungsserver. Diese erfordern, dass die Windows-Firewall mit erweiterter Sicherheit aktiviert ist.
- Falls in Ihrer Netzwerktopologie eine Firewall zwischen einem Sicherheitsserver und einer Verbindungsserver-Instanz steht, müssen Sie die Firewall so konfigurieren, dass sie IPsec unterstützt. Siehe das Dokument *Horizon 7-Installation*.
- Um fortzufahren, müssen Sie eventuell die Konfiguration des Sicherheitsprotokolls ändern, damit die Kompatibilität mit vSphere gewährleistet ist. Wenn möglich, wenden Sie vor dem Upgrade des Verbindungsservers Patches für ESXi und vCenter Server zur Unterstützung von TLSv1.1 und TLSv1.2 an. Ist dies nicht möglich, aktivieren Sie TLSv1.0 auf dem Verbindungsserver erneut, bevor Sie das Upgrade durchführen. Weitere Informationen finden Sie unter [Aktivieren von TLSv1.0 für vCenter-Verbindungen vom Verbindungsserver](#).
- Wenn Sie Horizon 7-Server mit einer älteren View Agent-Version als 6.2 verwenden, müssen Sie TLSv1.0 für PCoIP-Verbindungen aktivieren. View Agent-Versionen vor View Agent 6.2 unterstützen das Sicherheitsprotokoll TLSv1.0 nur für PCoIP. Bei Horizon 7-Servern, einschließlich Verbindungsservern und Sicherheitsservern, ist TLSv1.0 standardmäßig deaktiviert. Um TLSv1.0 für PCoIP-Verbindungen auf diesen Servern zu aktivieren, folgen Sie den Anweisungen in der VMware-Knowledgebase unter <http://kb.vmware.com/kb/2130798>.

Wenn Sie Verbindungsserver-Instanzen auf weiteren physischen bzw. virtuellen Maschinen neu installieren möchten, finden Sie eine vollständige Liste der entsprechenden Installationsanforderungen im Dokument *Horizon 7-Installation*.

Anforderungen und Überlegungen 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.

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. Erläuterungen 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 *Horizon 7-Installation*-Dokument.

Upgrade von Horizon 7-Serverkomponenten

5

Zu den Serverkomponenten, für die Sie ein Upgrade durchführen müssen, gehören der Horizon Connection Server, replizierte Server und Sicherheitsserver. Abhängig von den optionalen Komponenten, die Sie verwenden, ist möglicherweise auch ein Upgrade von View Composer erforderlich.

Durch die Verteilung der Upgrade-Aufgaben auf mehrere Wartungsfenster können Sie feststellen, ob die einzelnen Phasen erfolgreich verlaufen sind oder ob Probleme auftreten. VMware empfiehlt die Aktualisierung aller Serverkomponenten innerhalb des ersten Wartungsfensters.

Dieses Kapitel enthält die folgenden Themen:

- [Upgrade für View Composer](#)
- [Aktualisieren des Horizon-Verbindungsservers](#)
- [Upgrade von Sicherheitsservern](#)
- [Upgrade der Registrierungsserver](#)
- [Upgrade einer Cloud-Pod-Architektur-Umgebung](#)
- [Upgrade von Horizon 7-Servern für das Zulassen von HTML Access](#)
- [Upgrade von vCenter Server](#)
- [Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats](#)
- [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für Horizon 7](#)

Upgrade für View Composer

Während eines Upgrades unterstützt Horizon 7 keine Bereitstellungs- und Wartungsvorgänge für View Composer. Vorgänge wie die Bereitstellung und Neuerstellung von Linked-Clone-Desktops sind in der Übergangsphase, wenn auf manchen Horizon 7-Servern noch die frühere Version ausgeführt wird, nicht möglich. Sie können diese Vorgänge erst erfolgreich ausführen, wenn die Upgrades aller Horizon Connection Server- und View Composer-Instanzen abgeschlossen sind.

Hinweis Bevor Sie die View Composer 6.2-Funktion zum Erstellen automatisierter Farmen von Linked-Clone-RDS-Hosts verwenden können, müssen Sie ein Upgrade für alle Horizon-Komponenten auf Horizon 6 Version 6.2 oder höher durchführen.

Vorbereiten von vCenter Server und View Composer für ein Upgrade

Da vCenter Server und View Composer oft auf derselben virtuellen oder physischen Maschine installiert werden, müssen einige vorbereitende Aufgaben für beide durchgeführt werden.

Vorbereiten von Upgrades einschließlich vSphere

Wenn Sie zusätzlich zu einem vCenter Server-Upgrade auch ein Upgrade auf die neueste Version von Horizon 7 durchführen, sollten Sie das *VMware vSphere-Upgrade-Handbuch* lesen und die folgenden Aufgaben in der angegebenen Reihenfolge ausführen:

- 1 Prüfen Sie, ob die virtuelle oder physische Maschine die Systemvoraussetzungen für die Version von vCenter Server erfüllt, auf die Sie die Software aktualisieren wollen.
- 2 Stellen Sie sicher, dass die virtuelle bzw. physische Maschine, auf der der aktuelle View Composer installiert ist, die Systemanforderungen für die neue Version erfüllt.

Siehe [Upgrade-Anforderungen für View Composer](#).

- 3 Wenn vCenter Server auf einer virtuellen Maschine installiert ist, erstellen Sie einen Snapshot der virtuellen Maschine.

Anleitungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zum vSphere Client™.

- 4 Wenn der Computernamen mehr als 15 Zeichen umfasst, kürzen Sie den Namen auf höchstens 15 Zeichen.
- 5 Sichern Sie die vCenter Server-Datenbank und die View Composer-Datenbank.

Anweisungen zum Erstellen einer Datenbanksicherung finden Sie in der Dokumentation des Datenbankherstellers.

- 6 Prüfen Sie, ob der Datenbankserver mit der Version von vCenter Server kompatibel ist, die Sie verwenden wollen.

Wenn als Datenbankserver z. B. Oracle 9i verwendet wird, müssen Sie eine Aktualisierung vornehmen.

- 7 Prüfen Sie, ob die Datenbank mit der neuen Version von View Composer kompatibel ist.

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 und Horizon 7-Datenbankereignisse.

- 8 Erstellen Sie eine Kopie des Ordners mit den TLS-Zertifikaten.

Dieser Ordner befindet sich unter %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.

- 9 Dokumentieren Sie die IP-Adresse und den Systemnamen des Computers, auf dem vCenter Server installiert ist.

- 10 Verwenden Sie für alle Linked-Clone- und Instant-Clone-Desktop-Pools Horizon Administrator, um die Bereitstellung neuer virtueller Maschinen zu deaktivieren.

Da View Composer möglicherweise in einem anderen Wartungsfenster als die Desktop-Pools aktualisiert wird, muss die Bereitstellung für alle Linked-Clones verschoben werden, bis das Upgrade für beide Komponenten durchgeführt wurde.

- 11 Wenn bestimmte Linked-Clone- oder Instant-Clone-Desktop-Pools so eingestellt sind, dass die Betriebssystemfestplatte beim Abmelden aktualisiert wird, bearbeiten Sie mithilfe von Horizon Administrator die Einstellungen **Desktop/Pools** für diesen Pool und setzen Sie **Maschine nach Abmeldung löschen oder aktualisieren** auf **Nie**.

Für Linked-Clones verhindert diese Einstellung einen Fehler, wenn View Composer nach dem Upgrade versucht, einen Desktop zu aktualisieren, für den noch kein Horizon Agent-Upgrade durchgeführt wurde.

- 12 Wenn für Linked-Clone- oder Instant-Clone-Desktop-Pools eine Aktualisierung, Neuzusammenstellung oder Image-Übertragung geplant ist, verwenden Sie Horizon Administrator, um diese Aufgaben abzuberechnen.

Vorbereiten reiner View Composer-Upgrades

Wenn Sie ausschließlich View Composer und nicht vCenter Server aktualisieren möchten, müssen Sie die folgenden Aufgaben ausführen:

- 1 Stellen Sie sicher, dass die virtuelle bzw. physische Maschine, auf der der aktuelle View Composer installiert ist, die Systemanforderungen für die neue Version erfüllt.

Siehe [Upgrade-Anforderungen für View Composer](#).

- 2 Wenn View Composer auf einer virtuellen Maschinen installiert ist, erstellen Sie einen Snapshot der virtuellen Maschine.

Anweisungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client.

- 3 Sichern Sie die View Composer-Datenbank.

Anweisungen zum Erstellen einer Datenbanksicherung finden Sie in der Dokumentation des Datenbankherstellers.

- 4 Prüfen Sie, ob die Datenbank mit der neuen Version von View Composer kompatibel ist.

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 und Horizon 7-Datenbankereignisse.

- 5 Dokumentieren Sie die IP-Adresse und den Systemnamen des Computers, auf dem vCenter Server installiert ist.
- 6 Deaktivieren Sie mit Horizon Administrator für alle Linked-Clone-Desktop-Pools die Bereitstellung neuer virtueller Maschinen.

Da View Composer möglicherweise in einem anderen Wartungsfenster als die Desktop-Pools aktualisiert wird, muss die Bereitstellung verschoben werden, bis das Upgrade für beide Komponenten durchgeführt wurde.

- 7 Wenn bestimmte Desktop-Pools so eingestellt sind, dass die Betriebssystemfestplatte beim Abmelden aktualisiert wird, bearbeiten Sie mithilfe von Horizon Administrator die Einstellungen **Desktop/Pools** für diesen Pool und setzen Sie **Maschine nach Abmeldung löschen oder aktualisieren** auf **Nie**.

Diese Einstellung verhindert einen Fehler, wenn View Composer nach dem Upgrade versucht, einen Desktop zu aktualisieren, für den noch kein View Agent-Upgrade durchgeführt wurde.

- 8 Wenn für bestimmte Desktop-Pools eine Aktualisierung oder eine Neuzusammenstellung geplant ist, brechen Sie diese Aufgaben mit Horizon Administrator ab.

Upgrade für View Composer

Während des ersten Wartungsfensters werden Sie View Composer aktualisieren. Vorgänge wie die Bereitstellung und Neuzusammenstellung von Linked-Clone-Desktops werden erst unterstützt, nachdem ein Upgrade aller Horizon 7-Server durchgeführt wurde.

Voraussetzungen

- Legen Sie fest, wann Sie das Upgrade durchführen möchten. Wählen Sie ein verfügbares Desktop-Wartungsfenster. Planen Sie 15 bis 30 Minuten ein.
- Führen Sie die unter [Vorbereiten reiner View Composer-Upgrades](#) aufgeführten Aufgaben aus.
- Prüfen Sie, ob auf dem Server, auf welchem View Composer installiert ist, ein von einer CA signiertes TLS/SSL-Serverzertifikat installiert und konfiguriert ist. Falls View Composer nach dem Upgrade des Horizon Connection Server kein von einer Zertifizierungsstelle signiertes Zertifikat verwendet, wird das standardmäßige selbstsignierte Zertifikat in Horizon Administrator als ungültig angezeigt.
- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.
- Legen Sie fest, ob der Installationsassistent ein Upgrade der View Composer-Datenbank durchführen soll, wenn ein Schema-Upgrade erforderlich ist. Wahlweise können Sie nach Abschluss des Assistenten auch das Befehlszeilendienstprogramm `SviConfig` ausführen, um das Upgrade des Datenbankschemas manuell durchzuführen und ein Protokoll des Upgrades zu erstellen.

Verfahren

- 1 Laden Sie das Installationsprogramm für View Composer auf die virtuellen oder physischen View Composer-Maschinen herunter und führen Sie es dort aus.

Das Installationsprogramm steht auf der VMware-Website zum Download zur Verfügung.

Schrittweise Anleitungen zur Ausführung des Installationsprogramms erhalten Sie im Dokument *Installation von Horizon 7*.

- 2 Geben Sie an, ob der Assistent ein Upgrade des Datenbankschemas durchführen soll, wenn ein Schema-Upgrade erforderlich ist.

Wird ein Dialogfeld mit der Meldung „Database upgrade completed with warnings (Datenbank-Upgrade mit Warnungen abgeschlossen)“ angezeigt, können Sie auf **OK** klicken und diese Meldung einfach ignorieren.

- 3 Wenn Sie vom Assistenten zur Eingabe der View Composer-Portnummer aufgefordert werden, müssen Sie die Portnummer auf 18443 setzen.

Nächste Schritte

Wenn Sie ein manuelles Upgrade des Datenbankschemas durchführen müssen, lesen Sie [Ausführen von SviConfig zum manuellen Aktualisieren der Datenbank](#).

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](#).

Setzen Sie das Horizon 7-Upgrade im nächsten Wartungsfenster fort. Siehe [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#).

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.

Verfahren

- 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.

Aktivieren der Digest Access Authentication für View Composer

Ab Horizon 7 Version 7.0.3 verfügt View Composer zur Unterstützung der Websicherheit Digest Access Authentication über eine grundlegende Authentifizierungsmethode für den Zugriff, die standardmäßig aktiviert ist. Für eine erweiterte Sicherheit können Sie die Methode der Digest Access Authentication für View Composer aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass View Composer 7.0.3 oder höher installiert ist.
- Stellen Sie sicher, dass Sie sich am View Composer-Computer als Administrator anmelden können.
- Stellen Sie sicher, dass der Verbindungsserver 7.0.3 oder höher installiert ist.

Verfahren

- 1 Wechseln Sie zum Verzeichnis, in dem View Composer installiert ist.
- 2 Bearbeiten Sie die Datei SviWebService.exe.config.
- 3 Für die Konfigurationsoption SslPoxBinding legen Sie authenticationScheme="Digest" fest.
- 4 Für die Konfigurationsoption SslBasicAuth legen Sie clientCredentialType="Digest" fest.
- 5 Speichern und schließen Sie die Datei SviWebService.exe.config.
- 6 Bearbeiten Sie die Datei SviConfig.exe.config.
- 7 Für die Konfigurationsoption SslSviBinding legen Sie clientCredentialType="Digest" fest.
- 8 Speichern und schließen Sie die Datei SviConfig.exe.config.

9 Starten Sie den View Composer-Dienst neu.

- a Starten Sie das Tool „Windows-Dienste“, indem Sie an der Eingabeaufforderung `services.msc` eingeben.
- b Klicken Sie in der Liste der Dienste mit der rechten Maustaste auf den Dienst, den Sie neu starten möchten. Klicken Sie beispielsweise mit der rechten Maustaste auf VMware Horizon Composer 7.0.3.
- c Klicken Sie auf **Neu starten**.

Manuelles Upgrade der View Composer-Datenbank

Statt die Datenbank über das View Composer-Installationsprogramm zu aktualisieren, wenn ein Schema-Update erforderlich ist, können Sie die Datenbank auch manuell aktualisieren. Verwenden Sie das SviConfig-Dienstprogramm, wenn Sie den Upgrade-Prozess näher verfolgen müssen oder wenn Upgrade-Aufgaben an IT-Administratoren mit unterschiedlichen Zuständigkeiten verteilt werden müssen.

Wenn Sie View Composer auf eine Version mit einem aktualisierten Datenbankschema aktualisieren, werden Sie vom Installationsprogramm aufgefordert, das Datenbank-Upgrade durch den Assistenten zu bestätigen. Wenn Sie sich gegen den Assistenten des Installationsprogramms entscheiden, müssen Sie das SviConfig-Dienstprogramm verwenden, um die Datenbank zu aktualisieren und die vorhandenen Daten zu migrieren.

Die Verwendung des SviConfig-Befehlszeilendienstprogramms bietet folgende Vorteile:

- Das Dienstprogramm gibt Ergebniscodes zurück und erstellt ein Protokoll des Datenbank-Upgrades, das die Fehlerbehebung bei einem Upgrade-Fehler vereinfacht.
- Sie können die Upgrade-Aufgaben aufteilen. Ein vSphere- oder Horizon 7-Administrator kann das View Composer-Installationsprogramm zum Aktualisieren der Software ausführen. Ein Datenbankadministrator (DBA) kann mithilfe von SviConfig die View Composer-Datenbank aktualisieren.
- Das Software-Upgrade und das Datenbank-Upgrade können innerhalb unterschiedlicher Wartungsfenster stattfinden. Beispielsweise kann Ihr Standort Vorgänge zur Datenbankwartung nur an Wochenenden durchführen, während Softwarewartungsaufgaben während der Woche stattfinden können.

Ausführen von SviConfig zum manuellen Aktualisieren der Datenbank

Mit dem Befehlszeilendienstprogramm SviConfig können Sie die View Composer-Datenbank unabhängig von der View Composer-Software aktualisieren. Dieses Dienstprogramm erstellt außerdem eine Protokolldatei, um die Fehlerbehebung bei Upgrade-Fehlern zu vereinfachen.

Wichtig Nur erfahrene View Composer-Administratoren sollten das Dienstprogramm SviConfig verwenden. Mit diesem Dienstprogramm lassen sich Fehler im Zusammenhang mit dem View Composer-Dienst behandeln.

Voraussetzungen

- Sichern Sie die View Composer-Datenbank. Anleitungen finden Sie in der Dokumentation für Ihren Datenbankserver.
- Überprüfen Sie, ob Sie den Datenbankquellnamen (DSN) für die View Composer-Datenbank kennen.
- Überprüfen Sie, ob Sie den Benutzernamen und das Kennwort für das Datenbank-Administratorkonto für diese Datenbank kennen.

Verfahren

- 1 Öffnen Sie auf der virtuellen bzw. physischen vCenter Server-Maschine eine Windows-Eingabeaufforderung und navigieren Sie zu der ausführbaren Datei SviConfig.

Die Datei befindet sich im Ordner der View Composer-Anwendung. Der Standardpfad lautet C:\Programme (86)\VMware\VMware View Composer\sviconfig.exe.

- 2 Geben Sie den Befehl zum Beenden von VMware View Composer ein.

net stop svid

- 3 Führen Sie den Befehl SviConfig databaseupgrade aus.

```
sviconfig -operation=databaseupgrade
          -DsnName=target_DSN
          -Username=database_administrator_username
```

Beispiel:

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

- 4 Geben Sie bei der entsprechenden Aufforderung das Kennwort ein.

Bei einem erfolgreichen Vorgang werden in der Ausgabe die Upgrade-Schritte angezeigt.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

- 5 Geben Sie den Befehl zum Starten von View Composer ein.

net start svid

Ein vollständiges Protokoll des Upgradeprozesses wird erstellt und in C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log abgelegt.

Nächste Schritte

Wenn das Datenbank-Upgrade fehlschlägt, finden Sie weitere Informationen unter [Fehlerbehebung beim View Composer-Datenbank-Upgrade](#)

Entspricht der Ergebniscode einer anderen Zahl als 0, weist dies auf einen Erfolg hin. Informationen hierzu finden Sie unter [Ergebniscodes für eine manuelle Aktualisierung des Datenbankschemas](#).

Ergebniscodes für eine manuelle Aktualisierung des Datenbankschemas

Wenn Sie ein manuelles Upgrade der View Composer-Datenbank durchführen, zeigt der Befehl `sviconfig databaseupgrade` einen Ergebniscode an.

Tabelle 5-1. Ergebniscodes für den Befehl „databaseupgrade“ zeigt die Ergebniscodes von `sviconfig databaseupgrade`.

Tabelle 5-1. Ergebniscodes für den Befehl „databaseupgrade“

Code	Beschreibung
0	Vorgang erfolgreich abgeschlossen.
1	Angegebener DSN wurde nicht gefunden.
2	Angegebene Anmeldeinformationen für Datenbankadministrator sind ungültig.
3	Treiber für die Datenbank wird nicht unterstützt.
4	Unerwartetes Problem ist aufgetreten und der Befehl konnte nicht abgeschlossen werden.
14	View Composer-Dienst wird von einer anderen Anwendung verwendet. Beenden Sie den Dienst, bevor Sie den Befehl ausführen.
15	Während des Wiederherstellungsvorgangs ist ein Problem aufgetreten. Einzelheiten sind in der angezeigten Protokollausgabe aufgeführt.
17	Upgrade der Datenbankdaten nicht möglich.
18	Verbindung zum Datenbankserver kann nicht hergestellt werden.

Fehlerbehebung beim View Composer-Datenbank-Upgrade

Wenn Sie den View Composer-Dienst mit dem View Composer-Installationsprogramm aktualisieren oder den Befehl `SviConfig databaseupgrade` ausführen, wird bei diesem Vorgang möglicherweise nicht die View Composer-Datenbank aktualisiert.

Problem

Der Vorgang `SviConfig databaseupgrade` zeigt den Fehlercode 17 an, oder das View Composer-Installationsprogramm zeigt eine Warnmeldung an.

Datenbank-Upgrade mit Warnungen abgeschlossen

Ursache

Die Datenbank-Upgrade-Software kontaktiert vCenter Server, um zusätzliche Daten über Desktops abzurufen. Das Datenbank-Upgrade kann fehlschlagen, wenn die Desktops nicht verfügbar sind, der ESXi-Host nicht ausgeführt wird oder vCenter Server nicht zur Verfügung steht.

Lösung

- 1 Weitere Informationen hierzu finden Sie in der View Composer-Protokolldatei SviConfig.
Standardmäßig befindet sich diese Datei unter C:\Benutzer\All Users\VMware\View Composer\vmware-sviconfig.log. Das Upgrade-Skript protokolliert eine Nachricht für jeden Fehler.
- 2 Prüfen Sie die Protokolleinträge, um die Desktops zu ermitteln, die nicht aktualisiert werden konnten.

Option	Aktion
Der Desktop ist vorhanden, jedoch nicht verfügbar.	Stellen Sie die Verfügbarkeit des Desktops wieder her. Je nach der Ursache des Fehlers müssen Sie möglicherweise den ESXi-Host oder vCenter Server neu starten oder eine andere Aktion durchführen.
Der Desktop ist nicht vorhanden.	Ignorieren Sie die Protokollnachricht. Hinweis Ein gelöschter Desktop kann scheinbar in Horizon Administrator vorhanden sein, wenn ein Administrator die virtuelle Desktop-Maschine direkt in vSphere löscht.

- 3 Führen Sie den Befehl SviConfig databaseupgrade erneut aus.

Migrieren von View Composer auf eine andere Maschine

In bestimmten Situationen kann es erforderlich sein, einen VMware Horizon View Composer-Dienst auf eine neue virtuelle Maschine oder einen neuen physischen Computer unter Windows Server zu migrieren. Möglicherweise migrieren Sie View Composer und vCenter Server z. B. auf einen neuen ESXi-Host oder -Cluster, um Ihre Horizon 7-Bereitstellung zu erweitern. Darüber hinaus müssen View Composer und vCenter Server nicht auf derselben Windows Server-Maschine installiert werden.

Sie können View Composer von der vCenter Server-Maschine auf eine eigenständige oder von einer eigenständigen Maschine auf die vCenter Server-Maschine migrieren.

Wichtig Diese Themen befassen sich mit der Migration der neuesten Version von View Composer auf eine andere Maschine. Bevor Sie diese Aufgaben durchführen können, müssen Sie ein Upgrade der früheren Version von View Composer durchführen.

Wenn Ihre aktuelle View Composer-Version auf einer Maschine installiert ist, die die Systemanforderungen für die neue View Composer-Version nicht erfüllt, können Sie diese Schritte nicht ausführen. Nachdem Sie View Composer auf ein System mit einem Windows Server-Betriebssystem migriert haben, das für diese Version unterstützt wird, können Sie ein In-Place-Upgrade auf die neueste Version von View Composer durchführen.

■ [Anleitungen für die Migration von View Composer](#)

Die für die Migration des VMware Horizon View Composer-Diensts durchzuführenden Schritte richten sich danach, ob Sie vorhandene virtuelle Linked-Clone-Maschinen beibehalten möchten.

- **Migrieren von View Composer mit einer vorhandenen Datenbank**

Wenn Sie View Composer auf einen anderen physischen Computer oder eine andere virtuelle Maschine migrieren und beabsichtigen, die aktuellen virtuellen Linked-Clone-Maschinen zu erhalten, muss der neue VMware Horizon View Composer-Dienst die vorhandene View Composer-Datenbank weiterverwenden.

- **Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen**

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie View Composer auf eine neue physische oder virtuelle Maschine migrieren, ohne die RSA-Schlüssel auf die neue Maschine zu migrieren. Der migrierte VMware Horizon View Composer-Dienst kann eine Verbindung zur ursprünglichen View Composer-Datenbank herstellen oder Sie können eine neue Datenbank für View Composer vorbereiten.

- **Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln**

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer zwischen den Maschinen migrieren. Sie migrieren den RSA-Schlüsselcontainer mit dem Tool für die ASP.NET IIS-Registrierung, das zum Lieferumfang von Microsoft .NET Framework gehört.

- **Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst**

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer von der physischen oder virtuellen Quellmaschine, auf der der vorhandene VMware Horizon View Composer-Dienst installiert ist, auf die Maschine migrieren, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Anleitungen für die Migration von View Composer

Die für die Migration des VMware Horizon View Composer-Diensts durchzuführenden Schritte richten sich danach, ob Sie vorhandene virtuelle Linked-Clone-Maschinen beibehalten möchten.

Um die virtuellen Linked-Clone-Maschinen in Ihrer Bereitstellung beizubehalten, muss der VMware Horizon View Composer-Dienst, den Sie auf der neuen virtuellen Maschine oder dem neuen physischen Computer installieren, die vorhandene View Composer-Datenbank weiterhin verwenden. Die View Composer-Datenbank enthält Daten, die für die Erstellung, Bereitstellung, Wartung und Löschung von Linked-Clones erforderlich sind.

Wenn Sie den VMware Horizon View Composer-Dienst migrieren, können Sie auch die View Composer-Datenbank auf einen neuen Computer migrieren.

Unabhängig davon, ob Sie die View Composer-Datenbank migrieren, muss diese auf einem verfügbaren Computer in derselben Domäne wie der neue Computer, auf dem Sie den neuen VMware Horizon View Composer-Dienst installieren, oder in einer vertrauenswürdigen Domäne installiert werden.

View Composer erstellt RSA-Schlüsselpaare zum Ver- und Entschlüsseln der in der View Composer-Datenbank gespeicherten Authentifizierungsinformationen. Damit diese Datenquelle zur neuen Instanz des VMware Horizon View Composer-Dienstes kompatibel ist, müssen Sie zunächst den vom ursprünglichen VMware Horizon View Composer-Dienst erstellten RSA-Schlüsselcontainer migrieren. Importieren Sie den RSA-Schlüsselcontainer auf den Computer, auf dem Sie den neuen Dienst installieren.

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie den Dienst migrieren, ohne die vorhandene View Composer-Datenbank zu verwenden. Sie müssen die RSA-Schlüssel unabhängig davon, ob Sie die vorhandene Datenbank verwenden, nicht migrieren.

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

Migrieren von View Composer mit einer vorhandenen Datenbank

Wenn Sie View Composer auf einen anderen physischen Computer oder eine andere virtuelle Maschine migrieren und beabsichtigen, die aktuellen virtuellen Linked-Clone-Maschinen zu erhalten, muss der neue VMware Horizon View Composer-Dienst die vorhandene View Composer-Datenbank weiterverwenden.

Befolgen Sie die Schritte dieser Vorgehensweise, wenn Sie View Composer in eine der folgenden Richtungen migrieren:

- Von einem vCenter Server-Computer auf einen eigenständigen Computer
- Von einem eigenständigen Computer auf einen vCenter Server
- Von einem eigenständigen Computer auf einen anderen eigenständigen Computer
- Von einem vCenter Server-Computer auf einen anderen vCenter Server-Computer

Wenn Sie den VMware Horizon View Composer-Dienst migrieren, können Sie auch die View Composer-Datenbank auf einen neuen Speicherort migrieren. So müssen Sie beispielsweise die View Composer-Datenbank migrieren, wenn sich die aktuelle Datenbank auf einem vCenter Server-Computer befindet, den Sie ebenfalls migrieren.

Wenn Sie den VMware Horizon View Composer-Dienst auf dem neuen Computer installieren, müssen Sie den Dienst so konfigurieren, dass er eine Verbindung mit der View Composer-Datenbank herstellt.

Voraussetzungen

- Machen Sie sich mit den Migrationsanforderungen von View Composer vertraut. Siehe [Anleitungen für die Migration von View Composer](#).
- Machen Sie sich mit den Schritten zur Migration des RSA-Schlüsselcontainers auf den neuen VMware Horizon View Composer-Dienst vertraut. Siehe [Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln](#) und [Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst](#).

- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Installation des VMware Horizon View Composer-Dienstes vertraut.
- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Konfiguration eines TLS-Zertifikats für View Composer vertraut.
- Machen Sie sich mit der Konfiguration von View Composer in Horizon Administrator vertraut. Lesen Sie die Abschnitte zur Konfiguration der View Composer-Einstellungen und der View Composer-Domänen im Dokument *Horizon 7-Verwaltung*.
- Als Best Practice empfiehlt es sich, dass Sie überprüfen, ob die Quell- und Zielmaschinen, die Sie für die Migration von View Composer verwenden, identisch sind und dieselben Administratoranmeldedaten verwenden. Wenn Sie View Composer von einem eigenständigen Computer auf eine vCenter Server-Maschine migrieren, auf der View Composer bereits installiert ist, schlägt die Konfiguration von View Composer möglicherweise fehl, wenn die auf den beiden Maschinen verwendeten Anmeldedaten unterschiedlich sind.

Verfahren

- 1 Deaktivieren Sie die Bereitstellung virtueller Maschinen auf der vCenter Server-Instanz, die mit dem VMware Horizon View Composer-Dienst verknüpft ist.
 - a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus und klicken Sie auf **Bereitstellung deaktivieren**.
- 2 (Optional) Migrieren Sie die View Composer-Datenbank an einen neuen Ort.
 Wenn Sie diesen Schritt ausführen müssen, fragen Sie den Datenbankadministrator nach Migrationsanweisungen.
- 3 Deinstallieren Sie den VMware Horizon View Composer-Dienst von der aktuellen Maschine.
- 4 Migrieren Sie den RSA-Schlüsselcontainer auf den neuen Computer.
- 5 Installieren Sie den VMware Horizon View Composer-Dienst auf der neuen Maschine.
 Geben Sie während der Installation den DSN der Datenbank ein, die vom ursprünglichen VMware Horizon View Composer-Dienst verwendet wurde. Geben Sie auch den Benutzernamen und das Kennwort des Domänenadministrators an, die für die ODBC-Datenquelle für die Datenbank bereitgestellt wurden.
 Wenn Sie die Datenbank migriert haben, müssen DSN und Datenquelleninformationen auf den neuen Speicherort der Datenbank verweisen. Unabhängig davon, ob Sie die Datenbank migriert haben, muss der neue VMware Horizon View Composer-Dienst Zugriff auf die ursprünglichen Datenbankinformationen über Linked Clones haben.
- 6 Konfigurieren Sie auf der neuen Maschine ein SSL-Serverzertifikat für View Composer.
 Möglicherweise können Sie das Zertifikat kopieren, das auf der ursprünglichen Maschine für View Composer installiert war, oder Sie können ein neues Zertifikat installieren.

7 Konfigurieren Sie in Horizon Administrator die neuen View Composer-Einstellungen.

- a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit diesem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
- c Klicken Sie im Bereich „View Composer Server-Einstellungen“ auf **Bearbeiten** und geben Sie die neuen View Composer-Einstellungen an.

Wenn Sie View Composer mit vCenter Server auf der neuen Maschine installieren, wählen Sie **View Composer wurde zusammen mit vCenter Server installiert** aus.

Wenn Sie View Composer auf einer eigenständigen Maschine installieren, wählen Sie **Eigenständiger View Composer Server** aus und geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der View Composer-Maschine sowie den Benutzernamen und das Kennwort des View Composer-Benutzers an.

- d Klicken Sie im Bereich „Domänen“ auf **Serverinformationen bestätigen** und fügen Sie nach Bedarf View Composer-Domänen hinzu bzw. bearbeiten Sie diese.
- e Klicken Sie auf **OK**.

Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie View Composer auf eine neue physische oder virtuelle Maschine migrieren, ohne die RSA-Schlüssel auf die neue Maschine zu migrieren. Der migrierte VMware Horizon View Composer-Dienst kann eine Verbindung zur ursprünglichen View Composer-Datenbank herstellen oder Sie können eine neue Datenbank für View Composer vorbereiten.

Voraussetzungen

- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Installation des VMware Horizon View Composer-Dienstes vertraut.
- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Konfiguration eines TLS-Zertifikats für View Composer vertraut.
- Machen Sie sich mit den Schritten zum Entfernen von View Composer aus Horizon Administrator vertraut. Lesen Sie den Abschnitt zum Entfernen von View Composer aus Horizon Administrator im Dokument *Horizon 7-Verwaltung*.

Bevor Sie View Composer entfernen können, müssen Sie überprüfen, ob diese Komponente keine virtuellen Linked-Clone-Maschinen mehr verwaltet. Wenn Linked Clones verbleiben, müssen Sie diese löschen.

- Machen Sie sich mit der Konfiguration von View Composer in Horizon Administrator vertraut. Lesen Sie die Abschnitte zur Konfiguration der View Composer-Einstellungen und der View Composer-Domänen im Dokument *Horizon 7-Verwaltung*.

Verfahren

- 1 Entfernen Sie View Composer in Horizon Administrator aus Horizon Administrator.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit dem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
 - c Klicken Sie im Fensterbereich „View Composer Server-Einstellungen“ auf **Bearbeiten**.
 - d Wählen Sie **View Composer nicht verwenden** aus und klicken Sie auf **OK**.
- 2 Deinstallieren Sie den VMware Horizon View Composer-Dienst von der aktuellen Maschine.
- 3 Installieren Sie den VMware Horizon View Composer-Dienst auf der neuen Maschine.
Konfigurieren Sie während der Installation View Composer, um eine Verbindung zum DSN der ursprünglichen oder neuen View Composer-Datenbank herzustellen.
- 4 Konfigurieren Sie auf der neuen Maschine ein TLS-Serverzertifikat für View Composer.
Möglicherweise können Sie das Zertifikat kopieren, das auf der ursprünglichen Maschine für View Composer installiert war, oder Sie können ein neues Zertifikat installieren.
- 5 Konfigurieren Sie in Horizon Administrator die neuen View Composer-Einstellungen.
 - a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit diesem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
 - c Klicken Sie im Fensterbereich „View Composer Server-Einstellungen,“ auf **Bearbeiten**.
 - d Geben Sie die neuen View Composer-Einstellungen an.

Wenn Sie View Composer mit vCenter Server auf der neuen Maschine installieren, wählen Sie **View Composer wurde zusammen mit vCenter Server installiert** aus.

Wenn Sie View Composer auf einer eigenständigen Maschine installieren, wählen Sie **Eigenständiger View Composer Server** aus und geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der View Composer-Maschine sowie den Benutzernamen und das Kennwort des View Composer-Benutzers an.
 - e Klicken Sie im Bereich „Domänen“ auf **Serverinformationen bestätigen** und fügen Sie nach Bedarf View Composer-Domänen hinzu bzw. bearbeiten Sie diese.
 - f Klicken Sie auf **OK**.

Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer zwischen den Maschinen migrieren. Sie migrieren den RSA-Schlüsselcontainer mit dem Tool für die ASP.NET IIS-Registrierung, das zum Lieferumfang von Microsoft .NET Framework gehört.

Voraussetzungen

Laden Sie .NET Framework herunter und lesen Sie die Informationen über das Tool für die ASP.NET IIS-Registrierung. Besuchen Sie <http://www.microsoft.com/net>.

Verfahren

- 1 Installieren Sie .NET Framework auf der physischen oder virtuellen Maschine, auf der der mit der vorhandenen Datenbank verknüpfte VMware Horizon View Composer-Dienst installiert ist.
- 2 Installieren Sie .NET Framework auf der Zielformaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Nächste Schritte

Migrieren Sie den RSA-Schlüsselcontainer auf die Zielformaschine. Siehe [Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst](#).

Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer von der physischen oder virtuellen Quellmaschine, auf der der vorhandene VMware Horizon View Composer-Dienst installiert ist, auf die Maschine migrieren, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Sie müssen diese Schritte ausführen, bevor Sie den neuen VMware Horizon View Composer-Dienst installieren.

Voraussetzungen

Stellen Sie sicher, dass Microsoft .NET Framework und das Tool für die ASP.NET IIS-Registrierung auf den Quell- und Zielformaschinen installiert sind. Siehe [Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln](#).

Verfahren

- 1 Öffnen Sie auf der Quellmaschine mit dem vorhandenen VMware Horizon View Composer-Dienst eine Eingabeaufforderung und navigieren Sie zum Verzeichnis %windir%\Microsoft.NET\Framework\v2.0.xxxxx.

- 2 Geben Sie den Befehl `aspnet_regiis` ein, um das RSA-Schlüsselpaar in einer lokalen Datei zu speichern.

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

Das Tool für die ASP.NET IIS-Registrierung exportiert das RSA-Schlüsselpaar aus privatem und öffentlichem Schlüssel vom Container SviKeyContainer in die Datei `keys.xml` und speichert die Datei lokal.

- 3 Kopieren Sie die Datei `keys.xml` auf die Zielformaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

- 4 Öffnen Sie auf der Zielformaschine eine Eingabeaufforderung und navigieren Sie zum Verzeichnis %windir%\Microsoft.NET\Framework\v2.0xxxxx.
- 5 Geben Sie den Befehl `aspnet_regiis` ein, um die RSA-Schlüsselpaaraten zu migrieren.

`aspnet_regiis -pi "SviKeyContainer" "Pfad\keys.xml" -exp`

Hierbei steht *Pfad* für den Pfad zur exportierten Datei.

Die Option `-exp` erstellt ein exportierbares Schlüsselpaar. Wenn eine künftige Migration erforderlich ist, können die Schlüssel von dieser Maschine exportiert und auf eine andere Maschine importiert werden. Wenn Sie die Schlüssel zuvor auf diese Maschine migriert haben, ohne die Option `-exp` zu verwenden, können Sie die Schlüssel mit der Option `-exp` erneut importieren, sodass Sie sie künftig exportieren können.

Das Registrierungstool importiert das Schlüsselpaar in den lokalen Schlüsselcontainer.

Nächste Schritte

Installieren Sie den neuen VMware Horizon View Composer-Dienst auf der Zielformaschine. Geben Sie die Quellinformationen für die DSN- und ODBC-Daten an, die es View Composer erlauben, eine Verbindung zu den selben Datenbankinformationen herzustellen, die vom ursprünglichen VMware Horizon View Composer-Dienst verwendet wurden. Installationsanleitungen finden Sie unter „Installation von View Composer“ im Dokument *Horizon 7-Installation*.

Führen Sie die Schritte zur Migration von View Composer auf eine neue Maschine aus und verwenden Sie dieselbe Datenbank. Siehe [Migrieren von View Composer mit einer vorhandenen Datenbank](#).

Aktualisieren des Horizon-Verbindungsservers

Wenn in Ihrer Bereitstellung Lastausgleichsdienste zur Verwaltung mehrerer Verbindungsserver-Instanzen verwendet werden, kann ein Upgrade für die Infrastruktur der Verbindungsserver ohne Ausfallzeit durchgeführt werden.

Hinweis Bevor Sie die Funktion zum Klonen eines Desktop-Pools in Horizon 6 Version 6.2 anwenden können, müssen Sie ein Upgrade für alle Verbindungsserver-Instanzen in einem Pod auf Horizon 6 Version 6.2 oder höher durchführen.

Nachdem Sie eine Neuinstallation durchgeführt oder alle Verbindungsserver-Instanzen auf Horizon 7 Version 7.2 aktualisiert haben, können Sie die Verbindungsserver-Instanzen nicht mehr auf eine frühere Version als Horizon 7 Version 7.2 herabstufen, da sich die zum Schutz der LDAP-Daten verwendeten Schlüssel geändert haben.

Um sich die Möglichkeit eines Downgrade der Verbindungsserver-Instanzen auch bei einem Upgrade auf Horizon 7 Version 7.2 zu erhalten, müssen Sie die Verbindungsserver-Instanzen vor Beginn des Upgrades sichern. Wenn Sie die Verbindungsserver-Instanzen herabstufen müssen, müssen Sie alle Verbindungsserver-Instanzen herabstufen und dann die Sicherung auf den letzten Verbindungsserver anwenden, der herabgestuft wurde.

Beim Upgrade von einer Version von Horizon 7 vor Horizon 7 Version 7.8 werden einige Einstellungen für die Benutzerauthentifizierung geändert. Wie sich diese Einstellungen für die Benutzerauthentifizierung auf die Benutzererfahrung auswirken, hängt vom Client ab. Einzelheiten finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>. Bevor Sie die Authentifizierungseinstellungen ändern, müssen Sie sich über die Auswirkungen auf Benutzerfreundlichkeit und Sicherheit im Klaren sein. Einzelheiten finden Sie im Beitrag zu den sicherheitsrelevanten Servereinstellungen für die Benutzerauthentifizierung im Dokument *Horizon 7-Sicherheit*.

Vorbereiten des Verbindungsservers für ein Upgrade

Bevor Sie den Verbindungsserver oder eine der vSphere-Komponenten aktualisieren, von denen Verbindungsserver abhängen, müssen Sie mehrere Aufgaben ausführen, damit diese Upgrades erfolgreich sind.

Aufgaben, die nur für eine Instanz einer replizierten Gruppe ausgeführt werden müssen

Bevor Sie mit der Durchführung des Upgrades von Verbindungsserver-Instanzen beginnen, müssen Sie die nachfolgend aufgeführten Aufgaben nur für eine Instanz durchführen. Da die Instanzen repliziert werden, sind die Einstellungen für eine Instanz mit jenen der anderen Instanzen identisch.

- Wenn der Verbindungsserver auf einer virtuellen Maschine installiert ist, erstellen Sie einen Snapshot der virtuellen Maschine.

Anweisungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client. Wenn Sie irgendwann die Instanz auf diesen Snapshot zurücksetzen müssen und andere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie diese Instanzen erst deinstallieren, bevor Sie den Master auf den Snapshot zurücksetzen. Nach dem Zurücksetzen können Sie die replizierten Instanzen erneut installieren und auf die zurückgesetzte Instanz verweisen.

Sie können den Snapshot „Upgrade-Vorbereitungsphase“ nennen.

- Öffnen Sie Horizon Administrator und dokumentieren Sie alle globalen Einstellungen und die Einstellungen für Desktops und Pools: in den Abschnitten „Desktops“ und „Pools“ im Bestandsbaum und im Abschnitt „Globale Einstellungen“ im View-Konfigurationsbaum.

Erstellen Sie zum Beispiel einen Screenshot der Einstellungen.

- Verwenden Sie das Dienstprogramm `vdmexport.exe`, um die View LDAP-Datenbank zu sichern.

Entsprechende Anweisungen finden Sie im Verwaltungshandbuch für Ihre aktuelle Version des Dokuments *Horizon 7-Verwaltung*.

Aufgaben, die für jede Instanz vor dem Upgrade ausgeführt werden müssen

- Stellen Sie sicher, dass die virtuelle bzw. physische Maschine, auf der die aktuelle Verbindungsserver-Instanz installiert ist, die Systemanforderungen für die neue Version erfüllt.

Siehe [Horizon-Verbindungsserver – Serveranforderungen](#).

- Dokumentieren Sie die IP-Adresse und den Systemnamen des Computers, auf dem der Verbindungsserver installiert ist.
- Stellen Sie fest, ob Ihr Unternehmen Batch-Dateien oder Skripte erstellt hat, die für die View-Datenbank auf der Verbindungsserver-Instanz ausgeführt werden. Ist dies der Fall, dokumentieren Sie deren Namen und Speicherorte.
- Öffnen Sie Horizon Administrator und dokumentieren Sie alle speziellen Einstellungen für diese Instanz.

Wechseln Sie beispielsweise zu **View-Konfiguration > Server > Verbindungsserver**, wählen Sie die Verbindungsserver-Instanz in der Tabelle aus und klicken Sie auf **Bearbeiten**. Sie können einen Screenshot von jeder Registerkarte im Dialogfeld **Verbindungsserver-Einstellungen bearbeiten** erstellen.

Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe

Dieser Vorgang beschreibt die Durchführung eines Upgrades für Verbindungsserver-Instanzen, die nicht mit Sicherheitsservern kombiniert sind. Beispielsweise kann der beschriebene Vorgang auf Verbindungsserver angewendet werden, die für die Herstellung von Verbindungen mit Clients innerhalb der Unternehmensfirewall konfiguriert sind.

Für Verbindungsserver-Instanzen, die mit Sicherheitsservern kombiniert sind, gehen Sie vor wie unter [Upgrade für Sicherheitsserver und die damit kombinierten Verbindungsserver](#) beschrieben.

Der Verbindungsserver muss nach Abschluss des Upgrades nicht neu gestartet werden.

Hinweis In diesem Verfahren wird ein In-Place-Upgrade beschrieben. Weitere Informationen zum Migrieren auf eine andere Maschine finden Sie unter [Upgrade auf die neueste Version des Verbindungsservers auf einer anderen Maschine](#).

Voraussetzungen

- Legen Sie fest, wann Sie das Upgrade durchführen möchten. Wählen Sie ein verfügbares Desktop-Wartungsfenster. Die Dauer des Upgrades hängt von der Anzahl an Verbindungsserver-Instanzen in der Gruppe ab. Planen Sie für jede Instanz 15 bis 30 Minuten ein.
- Wenn Sie View Composer verwenden, überprüfen Sie, ob View Composer aktualisiert wurde. Siehe [Upgrade für View Composer](#). Nachdem Sie den Verbindungsserver aktualisiert haben, müssen Sie View Composer mit Horizon Administrator hinzufügen.
- Machen Sie sich mit den sicherheitsbezogenen Anforderungen von Horizon 7 vertraut und stellen Sie sicher, dass diese Anforderungen erfüllt werden. Siehe [Upgrade-Anforderungen für Horizon-Verbindungsserver](#). Eventuell müssen Sie ein von einer Zertifizierungsstelle signiertes SSL-Serverzertifikat mit Informationen zur Zertifikatsperre installieren, sicherstellen, dass „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist, und alle Backend-Firewalls zur Unterstützung von IPsec konfigurieren.

- Prüfen Sie, ob auf dem Server, auf dem vCenter Server installiert ist, ein von einer Zertifizierungsstelle signiertes SSL-Serverzertifikat installiert und konfiguriert ist. Falls nach dem Upgrade des Verbindungsservers vCenter Server kein von der CA signiertes Serverzertifikat verwendet wird, wird das standardmäßige selbst signierte Zertifikat in Horizon Administrator als ungültig angezeigt, und eine Meldung weist darauf hin, dass vCenter Server nicht verfügbar ist.
- Führen Sie die unter [Vorbereiten des Verbindungsservers für ein Upgrade](#) aufgeführten Aufgaben aus.
- Stellen Sie sicher, dass Sie über eine gültige Lizenz für die neue Version verfügen.

Hinweis Wenn Sie ein Upgrade von 6.0.x oder 6.1.x auf 6.2 durchführen, ist Ihre vorherige Lizenz weiterhin gültig und für das Nutzungsmodell wird **Gleichzeitiger Benutzer** gewählt. Ab Horizon 6 Version 6.2 ist ein neues Lizenzierungsmodell namens **Benannter Benutzer** enthalten, das Sie stattdessen auswählen können. Weitere Informationen finden Sie unter <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.
- Wenn Sie mit dem Dienstprogramm `vdmexport.exe` nicht vertraut sind, drucken Sie die entsprechenden Bedienungsanleitungen im Dokument *Horizon 7-Verwaltung* aus. Mit diesem Dienstprogramm führen Sie im Rahmen des Upgrades eine Sicherung der View LDAP-Datenbank durch.

Es ist nicht erforderlich, Änderungen an der Konfiguration vorhandener Lastausgleichsmodule vorzunehmen.

Verfahren

- 1 Wenn Sie mit einem Lastausgleichsdienst eine Gruppe von Verbindungsserver-Instanzen verwalten, deaktivieren Sie den Server, der die Verbindungsserver-Instanz hostet, für die Sie ein Upgrade durchführen möchten.
 - a Melden Sie sich bei Horizon Administrator an.
 - b Wechseln Sie zu **View-Konfiguration > Server** und klicken Sie auf die Registerkarte **Verbindungsserver**.
 - c Wählen Sie die betreffende Verbindungsserver-Instanz in der Liste aus und klicken Sie auf die Schaltfläche **Deaktivieren** über der Tabelle.
 - d Klicken Sie auf **OK**, um die Deaktivierung des Servers zu bestätigen.

- 2 Laden Sie auf dem Host der Verbindungsserver-Instanz das Installationsprogramm für die neue Version des Verbindungsservers herunter und führen Sie es aus.

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. Vor dem Upgrade müssen Sie keine Dienste beenden. Die Dienste werden vom Installationsprogramm bei Bedarf beendet und neu gestartet. Der VMwareVDMDS-Dienst muss ausgeführt werden, damit das Upgrade der View LDAP-Datenbank durchgeführt werden kann.

Das Installationsprogramm ermittelt, dass bereits eine ältere Version installiert ist und führt ein Upgrade durch. Bei einem Upgrade werden weniger Installationsoptionen als bei einer Neuinstallation angezeigt.

Die View LDAP-Datenbank wird ebenfalls aktualisiert.

Hinweis Vor der Durchführung des Upgrades überprüft das Installationsprogramm den Replikationsstatus, um festzustellen, ob der Server in der Lage ist, mit den anderen Servern der replizierten Gruppe zu kommunizieren und ob der Server LDAP-Aktualisierungen aus den anderen Servern der Gruppe abrufen kann. Schlägt die Statusüberprüfung fehl, wird das Upgrade nicht fortgesetzt.

- 3 Stellen Sie sicher, dass der VMware Horizon-Verbindungsserver-Dienst nach Beendigung des Installationsprogramms neu gestartet wird.
- 4 Melden Sie sich bei Horizon Administrator an und aktivieren Sie die Verbindungsserver-Instanz, für die aktuell ein Upgrade durchgeführt wurde.
 - a Wechseln Sie zu **View-Konfiguration > Server** und klicken Sie auf die Registerkarte **Verbindungsserver**.
 - b Wählen Sie die betreffende Verbindungsserver-Instanz in der Liste aus und klicken Sie auf die Schaltfläche **Aktivieren** über der Tabelle.
 - c In der Spalte „Version“ überprüfen Sie, ob die neue Version dargestellt wird.
- 5 Wählen Sie **View-Konfiguration > Produktlizenzierung und -verwendung** aus, klicken Sie auf **Lizenz bearbeiten**, geben Sie den-Lizenzschlüssel ein und klicken Sie auf **OK**.
- 6 Wenn Sie diese Verbindungsserver-Instanz mit einem Lastausgleichsdienst verwalten, aktivieren Sie den Server, für den aktuell ein Upgrade durchgeführt wurde.
- 7 Stellen Sie sicher, dass Sie sich bei einem Remote-Desktop anmelden können.
- 8 Wiederholen Sie die vorausgehenden Schritte, um ein Upgrade für jede Verbindungsserver-Instanz in der Gruppe durchzuführen.

Wichtig Wenn Sie nicht alle Verbindungsserver-Instanzen in einer replizierten Gruppe aktualisieren, zeigt der Systemzustand im Horizon Administrator-Dashboard eventuell einen Fehlerzustand von Instanzen an. Zu dieser Situation kommt es, wenn verschiedene Versionen verschiedene Arten von Daten liefern. Zur Lösung dieses Problems müssen alle Instanzen in der replizierten Gruppe aktualisiert werden.

- 9 Verwenden Sie das Dienstprogramm `vdmexport.exe`, um die soeben aktualisierte View LDAP-Datenbank zu sichern.

Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren.

- 10 Melden Sie sich bei Horizon Administrator an und überprüfen Sie dort das Dashboard, um sicherzustellen, dass die Symbole für vCenter Server und View Composer grün sind.

Falls eines der Symbole rot ist und das Dialogfeld "Ungültiges Zertifikat festgestellt" erscheint, müssen Sie auf **Überprüfen** klicken und dann entweder wie in "Nächste Schritte" beschrieben den Fingerabdruck des nicht vertrauenswürdigen Zertifikats akzeptieren oder ein gültiges, von einer CA signiertes SSL-Zertifikat installieren.

Informationen zum Ersetzen des Standardzertifikats für vCenter Server finden Sie im Dokument *VMware vSphere – Beispiele und Szenarien*.

- 11 Überprüfen Sie, ob die Dashboard-Symbole für die Verbindungsserver-Instanzen ebenfalls grün dargestellt werden.

Wird für eine Instanz ein rotes Symbol angezeigt, klicken Sie auf diese Instanz, um den Replikationsstatus zu ermitteln. Die Replikation kann aus folgenden Gründen beeinträchtigt sein:

- Eine Firewall blockiert die Kommunikation
- Der VMware VDMDS-Dienst wurde auf der Verbindungsserver-Instanz eventuell angehalten.
- Die VMware VDMS DSA-Optionen blockieren die Replikationen
- Ein Netzwerkfehler ist aufgetreten

Nächste Schritte

Wie Sie ein standardmäßiges oder selbst signiertes Zertifikat von vCenter Server oder View Composer verwenden, erfahren Sie unter [Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats](#).

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

Wenn das Upgrade für eine oder mehrere Verbindungsserver-Instanzen fehlschlägt, finden Sie weitere Informationen unter [Erstellen einer replizierten Gruppe nach dem Zurücksetzen des Verbindungsservers auf einen Snapshot](#).

Wichtig Wenn Sie für JMS-Nachrichten den erweiterten Sicherheitsmodus für Nachrichten verwenden möchten, müssen Sie sicherstellen, dass die Firewalls für Verbindungsserver-Instanzen den Empfang von eingehendem JMS-Datenverkehr auf Port 4002 von Desktops und Sicherheitsservern zulassen. Öffnen Sie außerdem Port 4101, um Verbindungen von anderen Verbindungsserver-Instanzen zuzulassen.

Wenn Sie den Verbindungsserver später auf einem Server neu installieren, für den ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert ist, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

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 5.1 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 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.

Verfahren

- 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 Domännennamen (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 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.

Upgrade auf die neueste Version des Verbindungsservers auf einer anderen Maschine

Im Rahmen des Upgrades können Sie den Verbindungsserver auf eine neue Maschine migrieren.

Voraussetzungen

- Aktualisieren Sie mindestens eine vorhandene Verbindungsserver-Instanz auf die aktuelle Version. Siehe [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#). Während dieses Upgrades wird die vorhandene View LDAP-Version aktualisiert.
- Stellen Sie sicher, dass die neue physische oder virtuelle Maschine den Systemanforderungen zur Installation des Verbindungsservers entspricht. Siehe [Unterstützte Betriebssysteme für den Horizon-Verbindungsserver](#) und [Hardwareanforderungen für den Horizon-Verbindungsserver](#).
- Machen Sie sich mit den sicherheitsbezogenen Anforderungen von Horizon 7 vertraut und stellen Sie sicher, dass diese Anforderungen erfüllt werden. Siehe [Upgrade-Anforderungen für Horizon-Verbindungsserver](#).
- Legen Sie fest, wann Sie das Upgrade durchführen möchten. Wählen Sie ein verfügbares Desktop-Wartungsfenster. Planen Sie für jede Instanz 15 bis 30 Minuten ein.
- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf dem Host verfügen, auf dem Sie das Installationsprogramm ausführen möchten.
- Machen Sie sich mit der Vorgehensweise zur Installation einer replizierten Instanz vertraut. Siehe das Dokument *Horizon 7-Installation*. Als Teil dieser Vorgehensweise installieren Sie eine replizierte Instanz.

Es ist nicht erforderlich, Änderungen an der Konfiguration vorhandener Lastausgleichsmodule vorzunehmen.

Verfahren

- 1 Stellen Sie sicher, dass eine aktualisierte Instanz des Verbindungsservers ausgeführt wird und für die neue Maschine zugänglich ist, auf der Sie den Verbindungsserver installieren möchten.

Bei der Installation des Verbindungsservers auf dem neuen Host werden Sie auf diese vorhandene Instanz verweisen.

- 2 Installieren Sie auf der neuen Maschine eine replizierte Instanz des Verbindungsservers.

Die View LDAP-Version auf der neuen Instanz repliziert die Version der aktualisierten Quellinstanz.

- 3 Deinstallieren Sie gegebenenfalls den Verbindungsserver vom ursprünglichen Host mithilfe des Windows-Dienstprogramms **Software**.

- 4 Wählen Sie in Horizon Administrator die Option **View-Konfiguration > Server > Verbindungsserver** aus und ermitteln Sie auf dieser Registerkarte, ob die deinstallierte Verbindungsserver-Instanz weiterhin in der Liste angezeigt wird.
- 5 Wenn die deinstallierte Verbindungsserver-Instanz noch immer in der Liste aufgeführt wird, entfernen Sie sie mithilfe eines vdmadmin-Befehls.

```
vdmadmin.exe -S -s Servername -r
```

In diesem Beispiel steht *Servername* für den Hostnamen oder die IP-Adresse des Verbindungsserver-Hosts. Weitere Informationen zum Befehlszeilenprogramm vdmadmin finden Sie im Dokument *Horizon 7-Verwaltung*.

Ergebnisse

Eine neue Instanz des Verbindungsservers wird einer Gruppe hinzugefügt, und eine alte Instanz wird entfernt.

Nächste Schritte

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

Führen Sie ein Upgrade der anderen Horizon 7 Server-Komponenten durch.

Wenn Sie den Verbindungsserver später auf einem Server neu installieren, für den ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert ist, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

Erstellen einer replizierten Gruppe nach dem Zurücksetzen des Verbindungsservers auf einen Snapshot

Wenn ein Upgrade fehlschlägt oder es aus einem anderen Grund erforderlich ist, eine virtuelle Maschine, auf der sich der Verbindungsserver befindet, auf einen Snapshot zurückzusetzen, müssen Sie die anderen Verbindungsserver-Instanzen in der Gruppe deinstallieren und die replizierte Gruppe neu erstellen.

Wenn Sie eine virtuelle Verbindungsserver-Maschine auf einen Snapshot zurücksetzen, stimmen die View LDAP-Objekte in der Datenbank dieser virtuellen Maschine nicht mehr mit den View LDAP-Objekten in den Datenbanken der anderen replizierten Instanzen überein. Nach dem Zurücksetzen auf einen Snapshot wird das folgende Ereignis im Windows-Ereignisprotokoll und im VMwareVDMDS-Ereignisprotokoll erfasst (Ereignis-ID 2103): The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure (Die Active Directory Lightweight Directory Services-Datenbank wurde mithilfe eines nicht unterstützten Wiederherstellungsvorgangs wiederhergestellt). Die zurückgesetzte virtuelle Maschine hält die Replikation ihres View LDAP an.

Wenn das Zurücksetzen auf einen Snapshot erforderlich ist, müssen Sie andere Verbindungsserver-Instanzen und das View LDAP auf den entsprechenden virtuellen Maschinen deinstallieren und anschließend Replikatinstanzen neu installieren.

Voraussetzungen

Legen Sie fest, welche Verbindungsserver-Instanz der neue Standard- oder Master-Verbindungsserver sein soll. Dieser Verbindungsserver verfügt über die gewünschten Horizon 7-Konfigurationsdaten.

Verfahren

- 1 Deinstallieren Sie auf allen Verbindungsserver-Instanzen außer auf derjenigen, die als neue Standard-Verbindungsserver-Instanz gewählt wurde, den Verbindungsserver und die View LDAP-Instanz.

Die View LDAP-Instanz trägt den Namen AD LDS Instance VMwareVDMDS.

- 2 Öffnen Sie auf der virtuellen Maschine, auf der sich die Standard-Verbindungsserver-Instanz (oder Master-Verbindungsserver-Instanz) befindet, eine Eingabeaufforderung. Geben Sie darin den folgenden Befehl ein, um sicherzustellen, dass die Replikationsfunktion nicht deaktiviert ist.

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```

- 3 Führen Sie auf den virtuellen Maschinen, auf denen sich die replizierten Verbindungsserver-Instanzen befinden sollen, das Verbindungsserver-Installationsprogramm aus, wählen Sie die Installationsoption **View-Replikatserver** und geben Sie den Hostnamen oder die IP-Adresse der Verbindungsserver-Standardinstanz an.

Ergebnisse

Die replizierte Gruppe von Verbindungsserver-Instanzen wird neu erstellt und deren View LDAP-Objekte stimmen überein.

Upgrade von Sicherheitsservern

Wenn Ihre Bereitstellung einen Lastausgleichsdienst zur Verwaltung mehrerer Sicherheitsserver verwendet, können Sie ein Upgrade der Verbindungsserver-Infrastruktur ohne Ausfallzeit durchführen.

Hinweis Wenn Sie Unified Access Gateway-Appliances anstelle von Sicherheitsservern benutzen möchten, müssen Sie für die Verbindungsserver-Instanzen ein Upgrade auf Horizon 6 Version 6.2 oder höher durchführen, bevor Sie die Unified Access Gateway-Appliances für den Verweis auf Verbindungsserver-Instanzen oder auf den Lastausgleichsdienst, der sich vor den Instanzen befindet, installieren und konfigurieren. Weitere Informationen finden Sie unter [Ersetzen eines Sicherheitsservers durch eine Unified Access Gateway-Appliance](#).

Vorbereiten des Sicherheitsservers für ein Upgrade

Bevor Sie ein Upgrade für Sicherheitsserver durchführen, müssen Sie die nachfolgend beschriebenen Aufgaben zur Erstellung von Backups und zur Erfassung der Konfigurationseinstellungen ausführen.

- Stellen Sie sicher, dass die virtuelle bzw. physische Maschine, auf der der aktuelle Sicherheitsserver installiert ist, die Systemanforderungen für die neue Version erfüllt.

Siehe [Horizon-Verbindungsserver – Serveranforderungen](#).

- Wenn der Sicherheitsserver auf einer virtuellen Maschine installiert ist, erstellen Sie einen Snapshot der virtuellen Maschine.

Anweisungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client. Sie können den Snapshot „Upgrade-Vorbereitungsphase“ nennen.

- Öffnen Sie Horizon Administrator und dokumentieren Sie die Einstellungen für diesen Sicherheitsserver. Wechseln Sie zu **View-Konfiguration > Server** und klicken Sie auf die Registerkarte **Sicherheitsserver**.

Beispielsweise wählen Sie den Sicherheitsserver aus, klicken Sie auf **Bearbeiten** und erstellen Sie einen Screenshot dieser Einstellungen.

- Dokumentieren Sie die IP-Adresse und den Systemnamen des Computers, auf dem der Sicherheitsserver installiert ist.
- Wenn Sie Lastausgleichsmodule für Sicherheitsserver verwenden, dokumentieren Sie die Konfigurationseinstellungen für diese Programme.

Hinweis In diesem Thema wird nicht der Horizon Administrator-Befehl **Auf Aktualisierung oder Neuinstallation vorbereiten** auf der Registerkarte **Sicherheitsserver** behandelt. Dieser Befehl entfernt IPsec-Regeln für den Sicherheitsserver, wodurch die gesamte Kommunikation zwischen dem Sicherheitsserver und der kombinierten Verbindungsserver-Instanz angehalten wird. Sie führen deshalb diesen Befehl während des Upgrade-Vorgangs aus, unmittelbar bevor Sie das Upgrade für den Sicherheitsserver durchführen. Eine Beschreibung dazu finden Sie unter [Upgrade für Sicherheitsserver und die damit kombinierten Verbindungsserver](#).

Upgrade für Sicherheitsserver und die damit kombinierten Verbindungsserver

Wenden Sie diesen Vorgang an, wenn die Verbindungsserver-Instanz, für die ein Upgrade durchgeführt werden soll, mit einem Sicherheitsserver kombiniert ist.

Mit diesem Vorgang lässt sich das Upgrade für einen Sicherheitsserver und die damit kombinierte Verbindungsserver-Instanz durchführen. Erst dann sollte das Upgrade kann für den nächsten Sicherheitsserver und die damit kombinierte Verbindungsserver-Instanz fortgesetzt werden. Mit dieser Vorgehensweise kommt es zu keiner Ausfallzeit. Wenn die Instanz nicht mit einem Sicherheitsserver kombiniert ist, gehen Sie vor, wie unter [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#) erläutert.

Zu den ersten Schritten dieses Vorgangs gehört das Upgrade der Verbindungsserver-Instanz. Nach dem Upgrade des Verbindungsservers, aber noch vor dem Sicherheitsserver-Upgrade, beschreibt ein Schritt das Entfernen der IPsec-Regeln für den Sicherheitsserver. Wenn Sie die IPsec-Regeln für einen aktiven Sicherheitsserver entfernen, verlieren Sie so lange die gesamte Kommunikation mit dem Sicherheitsserver, bis Sie den Sicherheitsserver wieder installieren.

Standardmäßig wird die Kommunikation zwischen einem Sicherheitsserver und der dazugehörigen Verbindungsserver-Instanz durch IPsec-Regeln gesteuert. Wenn die vorhandenen IPsec-Regeln vor dem Upgrade oder der Neuinstallation nicht entfernt werden, können der Sicherheitsserver und der Verbindungsserver nicht kombiniert werden und es können keine neuen IPsec-Regeln nach dem Upgrade eingerichtet werden.

Voraussetzungen

- Legen Sie fest, wann Sie das Upgrade durchführen möchten. Wählen Sie ein verfügbares Desktop-Wartungsfenster. Planen Sie 15 bis 30 Minuten für jeden Sicherheitsserver und die Verbindungsserver-Instanz ein, mit der der Sicherheitsserver kombiniert ist.
- Wenn Sie View Composer verwenden, überprüfen Sie, ob View Composer aktualisiert wurde. Siehe [Upgrade für View Composer](#). Nachdem Sie den Verbindungsserver aktualisiert haben, müssen Sie View Composer mit Horizon Administrator hinzufügen.
- Machen Sie sich mit den sicherheitsbezogenen Anforderungen von Horizon 7 vertraut und stellen Sie sicher, dass diese Anforderungen erfüllt werden. Siehe [Upgrade-Anforderungen für Horizon-Verbindungsserver](#). Eventuell müssen Sie ein von einer Zertifizierungsstelle signiertes TLS-Serverzertifikat mit Informationen zur Zertifikatsperre installieren, sicherstellen, dass „Windows-Firewall mit erweiterter Sicherheit“ **aktiviert** ist, und alle Back-End-Firewalls zur Unterstützung von IPsec konfigurieren.
- Stellen Sie sicher, dass die virtuellen bzw. physischen Maschinen, auf denen der aktuelle Sicherheitsserver und die Verbindungsserver-Instanzen installiert sind, die Systemanforderungen erfüllen.

Siehe [Horizon-Verbindungsserver – Serveranforderungen](#).

- Führen Sie die unter [Vorbereiten des Verbindungservers für ein Upgrade](#) aufgeführten Aufgaben aus.
- Stellen Sie sicher, dass Sie über eine Lizenz für die neue Version verfügen.
- Stellen Sie sicher, dass Sie über ein Benutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.
- Stellen Sie sicher, dass der Computer, auf dem Sie den Sicherheitsserver installieren möchten, auf die mit dem Sicherheitsserver zu koppelnde Verbindungsserver-Instanz zugreifen kann.

Hinweis Nach einem Verbindungsserver-Upgrade auf Horizon 7 Version 7.5 müssen Sicherheitsserver mit deaktiviertem IPsec erneut installiert werden. Wenn die IP-Adresse eines Sicherheitsservers geändert wird, muss er erneut installiert werden. Das Koppeln von Sicherheitsservern funktioniert nicht ordnungsgemäß, wenn der Sicherheitsserver sich hinter der dynamischen NAT befindet.

Verfahren

- 1 Wenn Sie mit einem Lastausgleichsdienst Sicherheitsserver verwalten, die mit Verbindungsserver-Instanzen gekoppelt sind, deaktivieren Sie den Sicherheitsserver, der mit der Verbindungsserver-Instanz gekoppelt ist, für die Sie ein Upgrade durchführen möchten.

- 2 Führen Sie ein Upgrade für die Verbindungsserver-Instanz durch, die mit diesem Sicherheitsserver kombiniert ist.

Folgen Sie den Schritten 2 bis 6 von [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#).

- 3 Entfernen Sie die IPsec-Regeln für den Sicherheitsserver, der mit der Verbindungsserver-Instanz kombiniert ist, für die das Upgrade durchgeführt wurde.
 - a Klicken Sie in Horizon Administrator auf **View-Konfiguration > Server**.
 - b 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.

- c 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.

- 4 Konfigurieren Sie mit der aktuellen Version von Horizon Administrator ein Sicherheitsserverkennwort für die Kombination. Informationen finden Sie im Abschnitt zur Konfiguration eines Sicherheitsserverkennworts für die Kombination im Dokument *Horizon 7-Installation*.
- 5 Laden Sie auf dem Host des Sicherheitsservers das Installationsprogramm für die neueste Version des Verbindungsservers herunter und führen Sie es aus.

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. Das Installationsprogramm ermittelt, dass bereits eine ältere Version installiert ist und führt ein Upgrade durch. Bei einem Upgrade werden weniger Installationsoptionen als bei einer Neuinstallation angezeigt.

Sie werden aufgefordert, das Kennwort für die Paarbildung mit dem Sicherheitsserver anzugeben.

Sie werden möglicherweise aufgefordert, ein Meldungsfeld wegzuklicken, das Sie darüber informiert, dass der Sicherheitsserver-Dienst gestoppt wurde. Der Installateur hält den Dienst in Vorbereitung auf die Aktualisierung an.

- 6 Wenn der Installationsassistent abgeschlossen ist, prüfen Sie, ob der VMware Horizon View-Sicherheitsserver-Dienst gestartet wurde.
- 7 Wenn Sie diesen Sicherheitsserver mit einem Lastausgleichsmodul verwalten, fügen Sie diesen Server wieder der Gruppe mit dem Lastausgleich hinzu.
- 8 Melden Sie sich bei Horizon Administrator an, wählen Sie den Sicherheitsserver im Dashboard aus und prüfen Sie, ob dessen Version die neueste ist.
- 9 Stellen Sie sicher, dass Sie sich bei einem Remote-Desktop anmelden können.

- 10** Wechseln Sie in Horizon Administrator zur Registerkarte **View-Konfiguration > Server > Sicherheitsserver** und entfernen Sie dann alle Duplikate von Sicherheitsservern aus der Liste.

Der automatische Paarbildungsmechanismus für Sicherheitsserver kann doppelte Einträge in der Liste **Sicherheitsserver** erzeugen, wenn der vollständige Systemname nicht dem Namen entspricht, der dem Sicherheitsserver bei seiner ursprünglichen Erstellung zugewiesen wurde.

- 11** Verwenden Sie das Dienstprogramm `vdmexport.exe`, um die soeben aktualisierte View LDAP-Datenbank zu sichern.

Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren.

- 12** Melden Sie sich bei Horizon Administrator an und überprüfen Sie dort das Dashboard, um sicherzustellen, dass die Symbole für vCenter Server und View Composer grün sind.

Falls eines der Symbole rot ist und das Dialogfeld "Ungültiges Zertifikat festgestellt" erscheint, müssen Sie auf **Überprüfen** klicken und dann entweder wie in "Nächste Schritte" beschrieben den Fingerabdruck des nicht vertrauenswürdigen Zertifikats akzeptieren oder ein gültiges, von einer CA signiertes SSL-Zertifikat installieren.

Informationen zum Ersetzen des Standardzertifikats für vCenter Server finden Sie im Dokument *VMware vSphere – Beispiele und Szenarien*.

- 13** Überprüfen Sie, ob die Dashboard-Symbole für die Verbindungsserver-Instanzen ebenfalls grün dargestellt werden.

Wird für eine Instanz ein rotes Symbol angezeigt, klicken Sie auf diese Instanz, um den Replikationsstatus zu ermitteln. Die Replikation kann aus folgenden Gründen beeinträchtigt sein:

- Eine Firewall blockiert die Kommunikation
- Der VMware VDMDS-Dienst wurde auf der Verbindungsserver-Instanz eventuell angehalten.
- Die VMware VDMS DSA-Optionen blockieren die Replikationen
- Ein Netzwerkfehler ist aufgetreten

Nächste Schritte

Wie Sie ein standardmäßiges oder selbst signiertes Zertifikat von vCenter Server oder View Composer verwenden, erfahren Sie unter [Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats](#).

Wenn das Upgrade für eine oder mehrere Verbindungsserver-Instanzen fehlschlägt, finden Sie weitere Informationen unter [Erstellen einer replizierten Gruppe nach dem Zurücksetzen des Verbindungsservers auf einen Snapshot](#).

Wichtig Wenn Sie für JMS-Nachrichten den erweiterten Sicherheitsmodus für Nachrichten verwenden möchten, müssen Sie sicherstellen, dass die Firewalls für Verbindungsserver-Instanzen den Empfang von eingehendem JMS-Datenverkehr auf Port 4002 von Desktops und Sicherheitsservern zulassen. Öffnen Sie außerdem Port 4101, um Verbindungen von anderen Verbindungsserver-Instanzen zuzulassen.

Wenn Sie den Verbindungsserver später auf einem Server neu installieren, für den ein Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert ist, stoppen Sie das Datenerfassungs-Set und starten Sie es dann erneut.

Ersetzen eines Sicherheitsservers durch eine Unified Access Gateway-Appliance

Sie können einen Sicherheitsserver durch eine Unified Access Gateway-Appliance ersetzen.

Voraussetzungen

Wenn Sie Unified Access Gateway-Appliances anstelle von Sicherheitsservern benutzen möchten, müssen Sie für die Verbindungsserver-Instanzen ein Upgrade auf Horizon 6 Version 6.2 oder höher durchführen, bevor Sie die Unified Access Gateway-Appliances für den Verweis auf Verbindungsserver-Instanzen oder auf den Lastausgleichsdienst, der sich vor den Instanzen befindet, installieren und konfigurieren.

Verfahren

- 1 Deinstallieren Sie die Software des Sicherheitsservers.
- 2 Entfernen Sie die IPsec-Konfiguration für den Sicherheitsserver. Weitere Informationen finden Sie unter *Entfernen von IPsec-Regeln für Sicherheitsserver* im Dokument *Horizon 7-Installation*.
- 3 Entfernen Sie den LDAP-Eintrag des Sicherheitsservers. Weitere Informationen finden Sie unter *Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option -S* im Dokument *Horizon 7-Verwaltung*.
- 4 Registrieren Sie in Horizon Administrator die Unified Access Gateway-Appliance.
- 5 Klicken Sie in der Netzwerkfirewall zwischen Unified Access Gateway und Verbindungsserver, entfernen Sie Firewallregeln, die mit dem entfernten Sicherheitsserver verknüpft sind, und fügen Sie Firewallregeln hinzu, die mit dem eingehenden Unified Access Gateway verknüpft sind. Das Unified Access Gateway muss mit dem Verbindungsserver über den TCP-Port 443 kommunizieren.

Die Back-End-Firewallregeln vom Sicherheitsserver zum Verbindungsserver lauten folgendermaßen:

Quelle	Standardport	Protokoll	Ziel	Standardports	Hinweise
Sicherheitsserver	UDP 500	ISAKMP	Verbindungsserver	UDP 500	IPsec-Phase-1-Aushandlung
Sicherheitsserver	UDP 4500	NAT-T	Verbindungsserver	UDP 4500	Gekapselter AJP13-Datenverkehr bei der Verwendung von NAT
Sicherheitsserver		ESP	Verbindungsserver		Gekapselter AJP13-Datenverkehr, wenn keine NAT-Ausnahme erforderlich ist. ESP ist IP-Protokoll 50. Portnummern werden nicht angegeben.
Sicherheitsserver		AJP13	Verbindungsserver	TCP 8009	AJP13-Datenverkehr ohne IPsec und während Kopplung

Quelle	Standardport	Protokoll	Ziel	Standardports	Hinweise
Sicherheitsserver		JMS	Verbindungsserver	TCP 4001	Nachrichtenkanal für Schlüsselaushandlung
Sicherheitsserver		JMS-TLS	Verbindungsserver	TCP 4002	Nachrichtenkanal für Verwaltung

6 Konfigurieren und starten Sie die Unified Access Gateway-Appliance.

Weitere Informationen finden Sie im Dokument *Bereitstellen und Konfigurieren von VMware Unified Access Gateway* unter <https://docs.vmware.com/de/Unified-Access-Gateway/index.html>.

Upgrade der Registrierungsserver

Sie können ein Upgrade eines Registrierungsservers durchführen, indem Sie die neueste Version des Verbindungsserver-Installationsprogramms auf der virtuellen Maschine ausführen, auf der bereits eine frühere Version eines Registrierungsservers installiert ist. Sie können auch die frühere Version eines Registrierungsservers deinstallieren und die neueste Version installieren, indem Sie die neueste Version des Verbindungsserver-Installationsprogramms ausführen und die Option „Horizon 7-Registrierungsserver“ auswählen.

Ein Registrierungsserver ist zustandslos. Die mit True SSO verknüpfte Konfiguration wird auf dem Registrierungsserver nicht beibehalten. Der Registrierungsserver empfängt die True SSO-Konfiguration vom Verbindungsserver, wenn der Registrierungsserver ausgeführt wird und der Verbindungsserver erfolgreich eine Verbindung mit dem Registrierungsserver hergestellt hat.

Hinweis Nach dem Upgrade müssen Sie das/die Paarbildungszertifikat(e) vom Verbindungsserver nicht manuell erneut in den Windows-Zertifikatspeicher des Registrierungsservers importieren. Das/Die zuvor manuell importierte(n) Paarbildungszertifikat(e) wird/werden im Rahmen des Deinstallations- oder Upgrade-Vorgangs nicht entfernt. Wenn der Registrierungsserver nach einem Upgrade ausgeführt wird, kann der Verbindungsserver erfolgreich eine Verbindung herstellen, und das/die zuvor importierte(n) Paarbildungszertifikat(e) wird/werden wieder verwendet.

Upgrade einer Cloud-Pod-Architektur-Umgebung

Die Funktion Cloud-Pod-Architektur verwendet Standard-Horizon 7-Komponenten für eine Datencenter-übergreifende Verwaltung. Mit der Funktion Cloud-Pod-Architektur können Sie mehrere Pods verbinden, sodass eine einzelne große Umgebung für das Brokering und die Verwaltung von Desktops und Anwendungen entsteht. Ein Pod besteht aus mehreren Verbindungsserver-Instanzen, einem gemeinsamen Speicher, einem Datenbankserver sowie den vSphere- und Netzwerkinfrastrukturen, die erforderlich sind, um Desktop- und Anwendungspools zu hosten.

Verwenden Sie das folgende Verfahren für die Aktualisierung einer Cloud-Pod-Architektur-Umgebung.

- 1 Führen Sie für alle Verbindungsserver-Instanzen in einem Pod ein Upgrade durch und folgen Sie dabei der üblichen Vorgehensweise für das Durchführen eines Upgrades für eine einzelne Verbindungsserver-Instanz.

- 2 Wiederholen Sie den vorhergehenden Schritt für die anderen Pods im Pod-Verbund und führen Sie das Upgrade für jeden Pod einzeln durch.

Während des Upgrade-Vorgangs können einige Verbindungsserver-Instanzen die aktuelle Version von Horizon 7 und andere eine ältere Version verwenden. Obwohl eine solche Umgebung mit gemischten Versionen ab Horizon 7 Version 7.4 unterstützt wird, können die neuen Funktionen in einer gemischten Umgebung nicht angewendet werden. Beispielsweise ist eine neue Funktion, die in Horizon Administrator auf einem Server erscheint, für den ein Upgrade durchgeführt wurde, in Horizon Administrator auf einem Server, für den kein Upgrade durchgeführt wurde, nicht sichtbar.

Informationen zum Entwerfen und Einrichten einer Cloud-Pod-Architektur-Umgebung finden Sie unter *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

Upgrade von Horizon 7-Servern für das Zulassen von HTML Access

Bei einem Upgrade von Verbindungsserver-Instanzen oder Sicherheitsservern hinter einem Lastausgleichsdienst oder hinter einem Gateway wie Unified Access Gateway müssen Sie für die weitere Verwendung von HTML Access Änderungen an der Konfiguration durchführen.

Weitere Informationen dazu finden Sie unter „Zulassen von HTML Access über einen Lastausgleichsdienst“ und „Zulassen von HTML Access über ein Gateway“ im Dokument *Horizon 7-Installation*.

Upgrade von vCenter Server

Führen Sie ein vCenter Server-Upgrade im Rahmen des Wartungsfensters durch, in dem Sie auch andere Horizon 7 Serverkomponenten aktualisieren. Bevor Sie ein Upgrade für vCenter Server durchführen, müssen Sie zunächst einige Horizon 7-Daten sichern. Falls View Composer nach der Aktualisierung auf dem gleichen Server ausgeführt wird, müssen Sie den View Composer-Dienst neu starten.

Hinweis Im Verlauf eines vCenter Server-Upgrades wird die Verbindung mit vorhandenen Remote-Desktop- und -Anwendungssitzungen nicht getrennt. Die folgende Funktionalität ist aber während eines vCenter Server-Upgrades nicht verfügbar:

- Remote-Desktops im Bereitstellungsstatus werden nicht eingeschaltet.
 - Neue Desktops können nicht gestartet werden.
 - Es sind keine View Composer-Vorgänge möglich.
-

Voraussetzungen

- Legen Sie fest, wann Sie das Upgrade durchführen möchten. Wählen Sie ein verfügbares Desktop-Wartungsfenster. Informationen zur Dauer des Upgrades finden Sie im *VMware vSphere-Upgrade-Handbuch*.
- Sichern Sie die vCenter Server-Datenbank und die View Composer-Datenbank.

- Sichern Sie die View LDAP-Datenbank von einer Verbindungsserver-Instanz. Verwenden Sie hierzu das Dienstprogramm `vdmexport.exe`.

Die Anweisungen dazu finden Sie im *Horizon 7-Verwaltung*-Dokument. Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten aus nur einer Instanz exportieren.

- Führen Sie die Aufgaben aus, die in Abschnitt [Vorbereiten von Upgrades einschließlich vSphere](#) beschrieben sind.
- Prüfen Sie, ob auf dem Server, auf dem vCenter Server installiert ist, ein von einer Zertifizierungsstelle signiertes TLS-Serverzertifikat installiert und konfiguriert ist. Falls nach dem Upgrade des Verbindungsservers vCenter Server kein von der CA signiertes Serverzertifikat verwendet wird, wird das standardmäßige selbst signierte Zertifikat in Horizon Administrator als ungültig angezeigt, und eine Meldung weist darauf hin, dass vCenter Server nicht verfügbar ist.
- Führen Sie die im *VMware vSphere-Upgrade-Leitfaden* aufgeführten Vorarbeiten durch. Nehmen Sie hierfür die Ausgabe des Leitfadens zu Hilfe, die für die Version von vSphere gilt, auf die Sie ein Upgrade durchführen möchten.
- Informationen dazu, wie Sie ein Upgrade von vCenter Server durchführen, während Instant Clones verwendet werden, finden Sie im VMware-Knowledgebase(KB)-Artikel <https://kb.vmware.com/s/article/52573>.

Verfahren

- 1 Führen Sie das Upgrade von vCenter Server wie im *VMware vSphere-Upgrade-Handbuch* beschrieben durch.

Wichtig Wenn Ihre Cluster vSAN-Datenspeicher enthalten, finden Sie weitere Informationen im Kapitel zum Upgrade des vSAN-Clusters im Dokument *Verwalten von VMware vSAN*. Dieses Kapitel enthält ein Thema zum Upgrade von vCenter Server.

- 2 Starten Sie, falls View Composer auf dem gleichen Host installiert ist, den View Composer-Dienst neu.
- 3 Melden Sie sich bei Horizon Administrator an und überprüfen Sie das Dashboard, um sicherzustellen, dass die Symbole für vCenter Server und View Composer grün sind.

Falls eines der Symbole rot ist und das Dialogfeld "Ungültiges Zertifikat festgestellt" erscheint, müssen Sie auf **Überprüfen** klicken und dann entweder wie in "Nächste Schritte" beschrieben den Fingerabdruck des nicht vertrauenswürdigen Zertifikats akzeptieren oder ein gültiges, von einer CA signiertes SSL-Zertifikat installieren.

Informationen zum Ersetzen des Standardzertifikats für vCenter Server finden Sie im Dokument *VMware vSphere – Beispiele und Szenarien*.

Nächste Schritte

Wie Sie ein standardmäßiges oder selbstsigniertes Zertifikat von vCenter Server oder View Composer verwenden, erfahren Sie unter [Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats](#).

Nachdem Sie die Aktualisierung der Horizon 7 Serverkomponenten ausgeführt haben, fahren Sie mit der Aktualisierung von Horizon 7 fort.

- Wenn Sie gleichzeitig auch vSphere-Komponenten aktualisieren, finden Sie weitere Informationen unter [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#).
- Falls Sie nur ein Upgrade von Horizon 7-Komponenten durchführen, lesen Sie [Upgrade von View Agent oder Horizon Agent](#).

Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats

Wenn Sie vCenter Server- und View Composer-Instanzen zu Horizon 7 hinzufügen, müssen Sie sicherstellen, dass die TLS-Zertifikate, die für vCenter Server- und View Composer-Instanzen verwendet werden, gültig sind und vom 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 vCenter Server oder eine View Composer-Instanz mit einem Zertifikat konfiguriert ist, das von einer Zertifizierungsstelle (CA) signiert ist, und das Stammzertifikat vom 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 Verbindungsserver das Stammzertifikat jedoch nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatfingerabdruck 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 TLS-Zertifikat verwenden, aber Sie müssen das Zertifikat separat für jede Komponente konfigurieren.

Einzelheiten zur Konfiguration von TLS-Zertifikaten finden Sie unter „Konfigurieren von TLS-Zertifikaten für View Server“ im Dokument *Horizon 7-Installation*.

Als Erstes fügen Sie vCenter Server und View Composer in Horizon Administrator hinzu. Verwenden Sie dazu den Assistenten „vCenter Server hinzufügen“. 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 Zertifikatfingerabdruck 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 Horizon 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 in Horizon Administrator auf **View-Konfiguration > Server** und bearbeiten Sie den vCenter Server-Eintrag für den View Composer-Dienst. Klicken Sie dann in den vCenter Server-Einstellungen auf **Bearbeiten** und folgen Sie den Eingabeaufforderungen, um das selbstsignierte Zertifikat zu überprüfen und zu akzeptieren.

Gleichermaßen können Sie in Horizon Administrator einen SAML-Authentifikator für die Verwendung durch eine Verbindungsserver-Instanz konfigurieren. Wenn der Verbindungsserver das SAML-Serverzertifikat nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatfingerabdruck akzeptiert wird. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie den SAML-Authentifikator in Horizon 7 nicht konfigurieren. Nach der Konfiguration eines SAML-Authentifikators können Sie ihn im Dialogfeld zum Bearbeiten des Verbindungsservers neu konfigurieren.

Verfahren

- 1 Klicken Sie auf **Zertifikat anzeigen**, wenn Horizon Administrator das Dialogfeld „Ungültiges Zertifikat ermittelt“ anzeigt.
- 2 Überprüfen Sie den Zertifikatfingerabdruck 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 Zertifikatfingerabdruck anzuzeigen.

Untersuchen Sie den Zertifikatfingerabdruck gleichermaßen auf einen SAML-Authentifikator. Führen Sie die vorstehenden Schritte gegebenenfalls auf dem SAML-Authentifikatorhost aus.

- 4 Überprüfen Sie, ob der Fingerabdruck im Fenster der Zertifikatsinformationen mit dem Fingerabdruck für die vCenter Server- oder die View Composer-Instanz übereinstimmt.

Überprüfen Sie ebenfalls, ob die Fingerabdrücke für einen SAML-Authentifikator übereinstimmen.

5 Geben Sie an, ob der Zertifikatfingerabdruck 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.

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

Horizon 7 bietet verschiedene komponentenspezifische administrative ADMX-Vorlagendateien für Gruppenrichtlinien. Sie können Remote-Desktops und -anwendungen optimieren und schützen, indem Sie die Richtlinieneinstellungen in den ADMX-Vorlagendateien einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in der Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip verfügbar, wobei x.x.x für die Version und yyyyyyy für die Build-Nummer steht. Sie können die Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Für ein Upgrade von Gruppenrichtlinien verwenden Sie den Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server, um die neue Version der Vorlagendateien hinzuzufügen.

Die Horizon 7-ADMX-Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Die Richtlinien für die Computerkonfiguration gelten für alle Remote-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.
- Die Richtlinien für die Benutzerkonfiguration gelten für alle Benutzer, unabhängig davon, mit welchem Remote-Desktop oder mit welcher Remoteanwendung sie sich verbinden. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

Microsoft Windows wendet Richtlinien beim Start eines Desktops und bei der Benutzeranmeldung an.

Upgrade von ESXi-Hosts und ihren virtuellen Maschinen

6

Das Aktualisieren von ESXi-Hosts und virtuellen Maschinen ist die zeitaufwendigste Aufgabe dieser mittleren Phase eines Horizon 7-Upgrades.

Dieses Verfahren bietet einen Überblick über die Aufgaben, die Sie während des zweiten und während der nachfolgenden Wartungsfenster durchführen müssen. Für einen Teil dieser Aufgaben benötigen Sie möglicherweise die schrittweisen Anleitungen aus dem *VMware vSphere-Upgrade-Leitfaden* und dem Dokument *Horizon 7-Verwaltung*.

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.

Wichtig In der folgenden Tabelle wird beschrieben, welche Horizon 7-Funktionen von bestimmten Versionen virtueller Hardware abhängen und deshalb möglicherweise ein Upgrade der virtuellen Maschine erfordern.

Tabelle 6-1. Erforderliche Versionen virtueller Hardware für bestimmte Funktionen

Funktion	Version der virtuellen Hardware	Entsprechende vSphere-Version
Platzsparendes Datenträgerformat für Linked-Clone-Pools	9 oder höher	vSphere 5.1 oder höher
VMware [®] vSAN [®] -Datenspeicher, erste Version	10 oder höher	vSphere 5.5 Update 1 oder höher
VMware vSAN-Datenspeicher, zweite Version	11 oder höher	vSphere 6.0 oder höher
VMware-VVOL-Datenspeicher	11 oder höher	vSphere 6.0 oder höher
Systemeigene NFS-Snapshot-Technologie (VAAI)	9 oder höher	vSphere 5.1 oder höher
Virtual Shared Graphics Acceleration (vSGA)	8 oder höher	vSphere 5.0 oder höher
Virtual Dedicated Graphics Acceleration (vDGA)	9 oder höher	vSphere 5.1 oder höher
NVIDIA GRID vGPU-Grafikbeschleunigung	11 oder höher	vSphere 6.0 oder höher

Voraussetzungen

- Führen Sie die unter [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#) beschriebenen Schritte aus.

- Führen Sie die vorbereitenden Aufgaben des ESXi-Upgrades aus, die im *VMware vSphere-Upgrade-Handbuch* aufgelistet sind.

Verfahren

- 1 Führen Sie Cluster für Cluster ein Upgrade für die ESXi-Hosts aus.

Anleitungen finden Sie im *VMware vSphere-Upgrade-Handbuch*. Wenn Ihre Cluster vSAN-Datenspeicher enthalten, finden Sie weitere Informationen im Kapitel zum Upgrade des vSAN-Clusters im Dokument *Verwalten von VMware vSAN*. Dieses Kapitel enthält ein Thema zum Upgrade von ESXi-Hosts.

Sind viele Cluster vorhanden, kann dieser Schritt mehrere Wartungsfenster in Anspruch nehmen. Für ESXi-Host-Upgrades sind möglicherweise die folgenden Aufgaben auszuführen:

- a Verschieben Sie die virtuellen Maschinen mit VMware vSphere® vMotion® vom ESXi-Host auf einen anderen.
- b Versetzen Sie den Host in den Wartungsmodus.
- c Führen Sie das Upgrade durch.
- d Verschieben Sie die virtuellen Maschinen mit vMotion zurück auf den Host.
- e Führen Sie die nach dem Upgrade erforderlichen Aufgaben für ESXi-Hosts aus.

Jeder Host muss zu einem Cluster gehören, wie in den Voraussetzungen erwähnt.

- 2 Wenn ein aktualisierter Host die Verbindung mit vCenter Server nicht automatisch wiederherstellt, verwenden Sie vSphere Client, um die Verbindung des Hosts mit vCenter Server wiederherzustellen.
- 3 Wenn Sie View Composer verwenden, starten Sie den View Composer-Dienst auf dem ESXi-Host neu, nachdem ein Upgrade aller vCenter Server-Hosts durchgeführt wurde.
- 4 (Optional) Führen Sie ein Upgrade von VMware® Tools™ und der virtuellen Maschinen auf allen übergeordneten virtuellen Maschinen, Vorlagen virtueller Maschinen und virtuellen Maschinen durch, die Horizon 7-Serverkomponenten, z. B. Verbindungsserver-Instanzen, hosten.

- a Planen Sie Ausfallzeiten ein. Weitere Informationen hierzu finden Sie im *VMware vSphere - Upgrade-Handbuch*.

- b Aktualisieren Sie VMware Tools und führen Sie ein Upgrade der Hardware für virtuelle Maschinen durch, die als Quellen für Remote-Desktops verwendet werden sollen.

Schrittweise Anleitungen für die Verwendung von VMware vSphere® Update Manager™ finden Sie im Kapitel zum Upgrade von virtuellen Maschinen im Dokument *Verwaltung virtueller VMware vSphere-Maschinen*.

Wenn Sie VMware vSphere Update Manager verwenden, können Sie zunächst VMware Tools und dann die Version der virtuellen Hardware für alle virtuellen Maschinen in einem bestimmten Ordner in der entsprechenden Reihenfolge aktualisieren. Siehe *VMware vSphere-Upgrade-Handbuch*.

- 5 (Optional) Führen Sie, falls Sie Full-Clone-Desktops verwenden, auf jeder virtuellen Maschine ein Upgrade von VMware Tools und der Hardware für die virtuellen Maschinen durch, die als Quellen für Remote-Desktops verwendet werden sollen.

Schrittweise Anleitungen dafür, wenn Sie VMware vSphere® Update Manager™ nicht verwenden möchten, finden Sie im Kapitel zum Upgrade von virtuellen Maschinen im Dokument *Verwaltung virtueller VMware vSphere-Maschinen*.

Wenn Sie vSphere Update Manager verwenden, können Sie zunächst die VMware Tools und dann die virtuelle Hardwareversion in der richtigen Reihenfolge für alle virtuellen Maschinen in einem bestimmten Ordner aktualisieren. Siehe *VMware vSphere-Upgrade-Handbuch*.

Nächste Schritte

Führen Sie ein Upgrade für die Agent-Software durch. Siehe [Upgrade von View Agent oder Horizon Agent](#).

Upgrade von veröffentlichten und virtuellen Desktops

7

Aktualisieren Sie veröffentlichte Desktops, virtuelle Desktops und den Horizon Agent, der unter den Betriebssystemen von virtuellen oder veröffentlichten Desktops und Microsoft RDS-Hosts ausgeführt wird.

Wichtig Dieses Kapitel enthält keine Informationen zur Durchführung eines Upgrades für Horizon Agent auf einer virtuellen Linux-Maschine. Informationen dazu finden Sie unter *Einrichten von Horizon 7 for Linux-Desktops*.

Dieses Kapitel enthält die folgenden Themen:

- [Sicherheitsbezogene Anforderungen für das Desktop-Upgrade](#)
- [Durchführen eines Upgrades von RDS-Hosts, die sitzungsbasierte Desktops bereitstellen](#)
- [Upgrade von View Agent oder Horizon Agent](#)
- [Upgrade von View Composer-Desktop-Pools](#)
- [Upgrade von Instant-Clone-Desktop-Pools](#)

Sicherheitsbezogene Anforderungen für das Desktop-Upgrade

RC4, SSLv3 und TLSv1.0 sind in Horizon 7-Komponenten standardmäßig deaktiviert. Zur erneuten Aktivierung von RC4, SSLv3 oder TLSv1.0 auf einem virtuellen Desktop oder einem veröffentlichten Desktop finden Sie Erläuterungen unter „Ältere Protokolle und in Horizon 7 deaktivierte Verschlüsselungen“ im Dokument *Horizon 7-Sicherheit*.

Alle Informationen zu den Sicherheitsfunktionen von View Agent, Horizon Agent und Horizon Client finden Sie im Dokument *Horizon Client und Agent-Sicherheit*.

Durchführen eines Upgrades von RDS-Hosts, die sitzungsbasierte Desktops bereitstellen

Auf RDS-Hosts mit Windows Server 2008 R2 oder einem höheren Betriebssystem können Sie die View Agent- oder Horizon Agent-Software aktualisieren und die Pool-Einstellungen bearbeiten, sodass der RDS-Host Remote-Desktops und Windows-basierte Remoteanwendungen bereitstellen kann.

Bei VMware Horizon 6.0 und höher können Sie mithilfe von Microsoft-RDS-Hosts nicht nur Remote-Desktops, sondern auch Remoteanwendungen bereitstellen. Mit dieser zusätzlichen Funktionalität wird der zuvor ausgeblendete Serverfarmname in Horizon Administrator angezeigt.

Voraussetzungen

- Stellen Sie sicher, dass mindestens eine Horizon-Verbindungsserver-Instanz in der replizierten Gruppe aktualisiert wurde. Der Verbindungsserver muss zuerst aktualisiert werden, damit der sichere JMS-Kombinationsmechanismus mit Horizon Agent arbeiten kann.
- Prüfen Sie, ob Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 R2 auf dem RDS-Host ausgeführt wird, der zurzeit Remote-Desktops hostet. Windows Server 2008 (Terminaldienste) wurde für frühere Versionen von Horizon 7 unterstützt, ist jedoch kein unterstütztes Betriebssystem für diese Version. Wenn Sie nicht über ein unterstütztes Windows Server-Betriebssystem verfügen, müssen Sie kein Upgrade, sondern eine Neuinstallation durchführen. Eine Liste der unterstützten Betriebssysteme finden Sie unter [Anforderungen und Überlegungen für Horizon Agent](#).
- Prüfen Sie, ob die RDS-Host-Rolle im Betriebssystem installiert ist. Siehe die Prozedur „Installieren von Remote-Desktop-Diensten auf Windows Server 2008 R2“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Machen Sie sich mit der Vorgehensweise zum Ausführen des Horizon Agent-Installationsprogramms vertraut. Siehe die Prozedur „Installieren von Horizon Agent auf einem RDS-Host“ in *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*. Dieses Dokument kann durch Klicken auf die Schaltfläche **Hilfe** in Horizon Administrator aufgerufen werden.
- Stellen Sie sicher, dass Sie von allen Remote-Desktops und Remoteanwendungen abgemeldet sind.
- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.

Verfahren

- 1 Bearbeiten Sie in Horizon Administrator die Desktop-Pool-Einstellungen für den Pool, um diesen zu deaktivieren.

Wechseln Sie zu **Katalog > Desktop-Pools**, wählen Sie den Pool aus und klicken Sie auf **Bearbeiten**.

- 2 Laden Sie auf dem RDS-Host das Installationsprogramm für die neue Horizon Agent-Version herunter und installieren Sie es.

Das Installationsprogramm steht auf der VMware-Website zum Download zur Verfügung.

- 3 Bearbeiten Sie die Farmeinstellungen in Horizon Administrator und legen Sie das Standardanzeigeprotokoll auf **PCoIP** oder **VMware Blast** fest.

Wechseln Sie zu **Ressourcen > Farmen**, wählen Sie die Farm aus und klicken Sie auf **Bearbeiten**.

Sie können auch eine Einstellung verwenden, die dem Endbenutzer gestattet, das Protokoll zu wählen. Für Remoteanwendungen muss als Protokoll PCoIP oder VMware Blast verwendet werden. Remoteanwendungen werden mit RDP nicht unterstützt.

- 4 Bearbeiten Sie in Horizon Administrator die Desktop-Pool-Einstellungen für den Pool, um diesen zu aktivieren.

Ergebnisse

Der Host kann nun zusätzlich zu Remote-Desktops Remoteanwendungen bereitstellen. Wenn Sie in Horizon Administrator zu **Katalog > Desktop-Pools** wechseln, wird angezeigt, dass der Typ des Pools **RDS-Desktop-Pool** ist. Wenn Sie zu **Ressourcen > Farmen** wechseln, wird eine Farm-ID in der Liste angezeigt, die der Pool-ID entspricht.

Nächste Schritte

Aktualisieren Sie die Clients. Siehe [Kapitel 3 Upgrade der Client-Anwendung](#).

Upgrade von View Agent oder Horizon Agent

Die Strategie zum Aktualisieren der Agent-Software hängt vom Typ der Desktop-Quelle ab.

Hinweis Zum Upgrade des Betriebssystems für einen Desktop auf einer virtuellen Maschine von Windows 8 auf Windows 8.1 müssen Sie Horizon Agent deinstallieren, das Betriebssystem von Windows 8 auf Windows 8.1 aktualisieren und dann Horizon Agent neu installieren. Alternativ können Sie eine neue Installation von Windows 8.1 durchführen und dann Horizon Agent installieren.

Diese Vorgehensweise bietet einen Überblick über die Aufgaben, die Sie für das Upgrade der Agent-Software in virtuellen Maschinen benötigen, die als Desktop-Quellen verwendet werden. Um einige dieser Aufgaben auszuführen, benötigen Sie eventuell die schrittweisen Anleitungen in der vSphere Client-Onlinehilfe oder in *Einrichten von virtuellen Desktops in Horizon 7*. Dieses Dokument kann durch Klicken auf die Schaltfläche **Hilfe** in Horizon Administrator aufgerufen werden. Weitere Informationen zum Upgrade der Agent-Software auf einem Terminaldienste-Host oder Microsoft-RDS-Host finden Sie unter [Durchführen eines Upgrades von RDS-Hosts, die sitzungsbasierte Desktops bereitstellen](#). Zum Upgrade der Agent-Software auf einer virtuellen Linux-Maschine finden Sie Erläuterungen im Dokument *Einrichten von Horizon 7 for Linux-Desktops*.

Wenn Sie Instant Clones bereitstellen möchten, können Sie mit diesem Vorgang eine übergeordnete virtuelle Maschine für einen Instant-Clone-Desktop-Pool anlegen. Wenn Sie für Horizon Agent ein Upgrade auf einer übergeordneten virtuellen Maschine durchführen, wählen Sie einfach die entsprechende Option für einen Instant-Clone-Desktop-Pool.

Wichtig Das Horizon Agent-Installationsprogramm umfasst nunmehr alle Komponenten, die zuvor im Remote Experience Agent enthalten waren, der zum VMware Horizon™ View™ Feature-Pack gehörte. Zum Upgrade von Funktionen, die mit dem Remote Experience Agent installiert wurden, können Sie das Horizon Agent-Installationsprogramm ausführen. Dieses Installationsprogramm entfernt den Remote Experience Agent, bevor das Upgrade ausgeführt wird. Wenn Sie den Remote Experience Agent manuell entfernen möchten, müssen Sie dies tun, bevor Sie das Installationsprogramm für die neue Horizon Agent-Version ausführen.

Voraussetzungen

- Stellen Sie sicher, dass alle Verbindungsserver-Instanzen in der replizierten Gruppe aktualisiert wurden. Alle Verbindungsserver-Instanzen müssen zuerst aktualisiert werden, damit der sichere JMS-Paarbildungsmechanismus mit Horizon Agent arbeiten kann.
- Wenn Sie ESXi-Hosts und virtuelle Maschinen aktualisieren, führen Sie das Verfahren aus, das in [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#) beschrieben wird.
- Stellen Sie sicher, dass Sie über ein Domänenbenutzerkonto mit Administratorrechten auf den Hosts verfügen, auf denen Sie das Installationsprogramm ausführen und das Upgrade installieren möchten.

Verfahren

- 1 Wenn Sie Instant Clones oder View Composer-Linked-Clones bereitstellen möchten, führen Sie für die Agent-Software ein Upgrade auf einer übergeordneten virtuellen Maschine durch und erstellen Sie einen Desktop-Pool für Testzwecke.

- a Laden Sie die neue Version des Horizon Agent-Installationsprogramms auf eine übergeordnete virtuelle Maschine herunter und führen Sie es dort aus.

Das Installationsprogramm steht auf der VMware-Website zum Download zur Verfügung.

- b Erstellen Sie einen kleinen Desktop-Pool von dieser virtuellen Maschine.
 - c Testen Sie einen Desktop einer virtuellen Maschine aus dem Desktop-Pool, um sicherzustellen, dass alle Anwendungsfälle ordnungsgemäß ausgeführt werden können.

Erstellen Sie beispielsweise einen Desktop-Pool, der einen Desktop auf einer virtuellen Maschine umfasst, und prüfen Sie, ob Sie sich über Horizon Client bei diesem Desktop anmelden können.

Schrittweise Anweisungen zur Ausführung des Horizon Agent-Installationsprogramms und zur Erstellung von Desktop-Pools erhalten Sie in *Einrichten von virtuellen Desktops in Horizon 7*. Dieses Dokument kann durch Klicken auf die Schaltfläche **Hilfe** in Horizon Administrator aufgerufen werden.

Wichtig Wenn Sie ein Upgrade von View 5.1.x oder früher durchführen, Sysprep verwenden und Ihre Endbenutzer USB-Geräte mit Ihren Remote-Desktops verbinden, müssen Sie das in der VMware-Knowledgebase beschriebene Verfahren unter <http://kb.vmware.com/kb/2051801> durchführen. Ansonsten funktioniert die USB-Umleitungsfunktion nach dem Upgrade der Agent-Software möglicherweise nicht.

- 2 Laden Sie das Installationsprogramm für die neue Version von Horizon Agent auf die anderen übergeordneten virtuellen Maschinen oder Vorlagen virtueller Maschinen herunter und führen Sie es dort aus.

Schrittweise Anweisungen zur Ausführung des Horizon Agent-Installationsprogramms und zur Erstellung von Desktop-Pools erhalten Sie in *Einrichten von virtuellen Desktops in Horizon 7*. Dieses Dokument kann durch Klicken auf die Schaltfläche **Hilfe** in Horizon Administrator aufgerufen werden.

- 3 Wenn Sie Instant-Clone- oder View Composer-Linked-Clone-Desktop-Pools anlegen möchten, erstellen Sie einen Snapshot jeder übergeordneten virtuellen Maschine, für die ein Upgrade durchgeführt wurde.

Mit diesem Snapshot können Sie einen Instant-Clone- oder Linked-Clone-Desktop-Pool anlegen oder einen vorhandenen Linked-Clone-Desktop-Pool neu zusammenstellen.

Anweisungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client.

- 4 Wenn Sie Desktops auf Grundlage vollständiger Klone oder andere virtuelle Maschinen verwenden, die Sie als einzelne Desktops oder als Teil eines manuellen Pools hinzugefügt haben, aktualisieren Sie die Agent-Software mithilfe eines beliebigen Drittanbieter-Tools, das Sie für gewöhnlich für Software-Upgrades einsetzen.
- 5 Bei automatisierten und manuellen Windows 7- und Windows 8-Pools, die keine Instant-Clone- oder Linked-Clone-Pools sind, müssen Sie zum Aktivieren der Funktion für das 3D-Rendern den Pool bearbeiten und die Desktops der virtuellen Maschinen ein- und ausschalten.

a Konfigurieren Sie folgende Pool-Einstellungen:

- Legen Sie für den Pool die Verwendung des PCoIP-Anzeigeprotokolls oder des VMware Blast-Anzeigeprotokolls fest.
- Setzen Sie die Option **Benutzern die Wahl des Protokolls erlauben** auf **Nein**.
- Aktivieren Sie die Funktion **3D-Renderer**.

b Schalten Sie jede virtuelle Maschine einzeln aus und dann wieder ein.

Wenn Sie statt des Aus- und Einschaltens die virtuelle Maschine nur neu starten, werden die Einstellungen nicht übernommen.

- 6 Wenn Sie physische PCs oder virtuelle Maschinen als Microsoft RDS-Hosts verwenden, um Remote-Desktops oder -Anwendungen bereitzustellen, laden Sie das Installationsprogramm für die neue Horizon Agent-Version auf diese physischen Maschinen herunter und führen Sie es dort aus.

Das Installationsprogramm steht auf der VMware-Website zum Download zur Verfügung.

Wichtig Bei der Ausführung des Installationsprogramms auf dem RDS-Host einer virtuellen Maschine ist die **View Composer Agent**-Komponente nicht ausgewählt. Wählen Sie diese Komponente nicht während eines Upgrade-Vorgangs aus. Wenn Sie diese Komponente zur Erstellung einer automatisierten Farm verwenden möchten (eine neue Funktion in Horizon 6 Version 6.2), müssen Sie die vorherige Version der Agent-Software deinstallieren und anschließend die neue Version mit ausgewählter **View Composer Agent**-Komponente installieren.

- 7 Wenn Sie physische PCs als Desktop-Quellen verwenden, laden Sie das Installationsprogramm für die neue Horizon Agent-Version auf diese physischen Maschinen herunter und führen Sie es dort aus.

Das Installationsprogramm steht auf der VMware-Website zum Download zur Verfügung.

Wichtig Wenn Sie auf Windows Server-Betriebssystemen, die für die Desktop-Verwendung konfiguriert sind, den Installationsmodus von Horizon Agent während des Upgrades nicht ändern möchten, wählen Sie **Desktop-Modus** im Horizon Agent-Installationsprogramm aus und fahren Sie fort. Wenn Sie den Modus ändern möchten, wählen Sie **RDS-Modus** aus und folgen Sie den Anweisungen des Installationsprogramms, um mit dem Upgrade fortzufahren.

- 8 Überprüfen Sie anhand einer noch nicht aktualisierten Horizon Client-Instanz, dass Sie sich mit der alten Client-Software bei den aktualisierten Remote-Desktop-Quellen anmelden können.

Nächste Schritte

Wenn Sie View Composer-Desktop-Pools verwenden, stellen Sie die Pools neu zusammen oder erstellen Sie sie neu. Siehe [Upgrade von View Composer-Desktop-Pools](#).

Aktualisieren Sie die Clients. Siehe [Kapitel 3 Upgrade der Client-Anwendung](#).

Upgrade von View Composer-Desktop-Pools

Zur letzten Phase eines Horizon-Upgrades gehört das Aktualisieren der View Composer-Desktop-Pools.

Zum Aktualisieren von Pools, die mit View Composer erstellt wurden, müssen Sie einen Snapshot verwenden, der nach dem Upgrade von Horizon Agent auf einer übergeordneten virtuellen Maschine erstellt wurde.

Wichtig Wenn Sie View Composer-Linked-Clones verwenden und die Funktion zur Rückgewinnung von Speicherplatz nutzen möchten, die auf virtuellen Maschinen ab vSphere 5.1 oder höher verfügbar ist, müssen Sie zusätzlich zu den Schritten in diesem Verfahren bestimmte Einstellungen in View LDAP und in Horizon Administrator konfigurieren. Für eine vollständige Liste der Aufgaben siehe [Aufgaben für die Aktualisierung von Desktop-Pools zur Verwendung der Speicherplatzrückgewinnung](#).

Hinweis Wenn Sie zudem auch ein Upgrade der Version der virtuellen Hardware durchführen (z. B. ein Upgrade auf die mit vSphere 5 und neueren Versionen bereitgestellte virtuelle Hardware-Version 8), wird der Snapshot der aktualisierten übergeordneten virtuellen Maschine zur Aktualisierung der virtuellen Hardware-Version der restlichen virtuellen Maschinen im Linked-Clone-Pool verwendet.

Ein auf diese Weise erfolgreiches Upgrade von einer virtuellen Hardware-Version (oder Kompatibilitätsstufe) auf eine höhere Version wird unterstützt. Sie können jedoch keine Neuzusammenstellung für Linked Clones in eine Hardware-Version durchführen, die niedriger ist als die aktuelle Version. So können beispielsweise Klone mit der Hardwareversion 8 nicht in einer übergeordneten virtuellen Maschine neu zusammengestellt werden, die über die Hardware-Version 7 verfügt.

Voraussetzungen

- Führen Sie die unter [Upgrade für View Composer](#) beschriebenen Schritte aus.
- Führen Sie die unter [Upgrade von Verbindungsserver-Instanzen in einer replizierten Gruppe](#) beschriebenen Schritte aus.
- Wenn Sie außerdem ESXi-Hosts und virtuelle Maschinen aktualisieren, führen Sie das Verfahren aus, das unter [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#) beschrieben wird. Informationen zu den vSphere-Versionen, die für verschiedene neue Funktionen erforderlich sind, finden Sie unter [Tabelle 6-1. Erforderliche Versionen virtueller Hardware für bestimmte Funktionen](#).
- Führen Sie die unter [Upgrade von View Agent oder Horizon Agent](#) beschriebenen Schritte aus, um den Agenten in der übergeordneten virtuellen Maschine zu aktualisieren.

Wichtig Wenn Sie ein Upgrade von View 5.1.x oder früher durchführen, Sysprep verwenden und Ihre Endbenutzer USB-Geräte mit Ihren Remote-Desktops verbinden, müssen Sie das in der VMware-Knowledgebase beschriebene Verfahren unter <http://kb.vmware.com/kb/2051801> durchführen. Ansonsten funktioniert die USB-Umleitungsfunktion nach dem Upgrade der Agent-Software möglicherweise nicht.

- Planen Sie die Wartungsfenster sorgfältig, damit die Leistung des Speicher-Arrays und der ESXi-Hosts durch das Neuerstellen und Neuzusammenstellen von Desktop-Pools nicht beeinträchtigt wird.

Verfahren

- 1 Wenn Sie die Bereitstellung neuer virtueller Maschinen bei der Vorbereitung auf das Upgrade deaktiviert haben, aktivieren Sie die Bereitstellungsoption wieder.
- 2 Um die Funktion für das 3D-Rendern zu aktivieren, bearbeiten Sie den Pool und konfigurieren die folgenden Einstellungen:
 - Legen Sie für den Pool die Verwendung des PCoIP-Anzeigeprotokolls oder des VMware Blast-Anzeigeprotokolls fest.
 - Setzen Sie die Option **Benutzern die Wahl des Protokolls erlauben** auf **Nein**.
 - Aktivieren Sie die Funktion **3D-Rendering**.
- 3 Um die Funktion für die Rückgewinnung von Speicherplatz zu aktivieren, die auf virtuellen Maschinen mit vSphere 5.1 verfügbar ist, wählen Sie in den Pool-Einstellungen unter **Erweiterter Speicher** die Option **VM-Datenträgerplatz zurückgewinnen**, und stellen Sie den Schwellenwert für die Rückgewinnung von Speicherplatz auf 1 GB ein.
- 4 Um die View-Speicherbeschleunigung zu aktivieren, die auf virtuellen Maschinen mit vSphere 5.0 oder höher verfügbar ist, stellen Sie in den Pool-Einstellungen im Abschnitt **Erweiterter Speicher** sicher, dass das Kontrollkästchen **View-Speicherbeschleunigung verwenden** aktiviert ist.

Die View-Speicherbeschleunigung kann die Leistung während der Anhäufung von Startvorgängen und Anti-Virus-Scan-E/A-Vorgängen verbessern, indem ESXi-Hosts gestattet wird, gemeinsame VM-Festplattendaten zwischenspeichern.

Wichtig Diese Funktion ist standardmäßig aktiviert. Die View-Speicherbeschleunigung erfordert 1 GB RAM pro ESXi-Host.

- 5 Verwenden Sie den nach dem Upgrade der übergeordneten virtuellen Maschine erstellten Snapshot, um Desktop-Pools neu zusammenzustellen.
- 6 Wenn Sie die Einstellung **Betriebssystemfestplatte beim Abmelden aktualisieren** bei der Vorbereitung auf das Upgrade auf **Nie** gesetzt haben, setzen Sie diese Einstellung zurück, um die entsprechende Aktualisierungsrichtlinie festzulegen.
- 7 Wenn Sie Aktualisierungs- oder Neuzusammenstellungsaufgaben für Desktop-Pools abgebrochen haben, planen Sie die Aufgaben erneut.

Nächste Schritte

Aktualisieren Sie die Clients. Siehe [Kapitel 3 Upgrade der Client-Anwendung](#).

Führen Sie die im Abschnitt [Kapitel 8 Aufgaben nach dem Upgrade zum Aktivieren neuer Funktionen für Ihr Horizon-Setup](#) beschriebenen Aufgaben aus, die Ihre Konfiguration betreffen.

Upgrade von Instant-Clone-Desktop-Pools

Wenn Sie vCenter Server für die Verwendung von vSphere 6.7 aktualisieren, müssen Sie auch die Instant-Clone-Desktop-Pools aktualisieren.

Voraussetzungen

- Stellen Sie sicher, dass die Systemvoraussetzungen für ein Upgrade auf Horizon 7 Version 7.5 oder höher erfüllt sind.
- Führen Sie die unter [Aktualisieren des Horizon-Verbindungsservers](#) beschriebenen Schritte aus.
- Führen Sie die unter [Upgrade von View Agent oder Horizon Agent](#) beschriebenen Schritte aus, um den Agenten in der übergeordneten VM zu aktualisieren.
- Führen Sie die im *VMware vSphere-Upgrade-Handbuch* aufgeführten Vorarbeiten durch. Nehmen Sie hierfür die Ausgabe des Handbuchs zu Hilfe, die für die Version von vSphere gilt, auf die Sie ein Upgrade durchführen möchten.

Hinweis Wenn Sie vCenter Server auf vSphere 6.7 aktualisieren, müssen alle oder einige der ESXi-Hosts im Cluster auf vSphere 6.7 aktualisiert werden. Andernfalls werden die Instant-Clone-Desktop-Pools nicht ordnungsgemäß bereitgestellt.

- Identifizieren Sie die ESXi-Hosts, die Sie aktualisieren möchten, und stellen Sie sicher, dass für vorhandene Desktop-Pools noch ausreichend viele Hosts online bleiben.

Verfahren

- 1 Erstellen Sie einen Snapshot der übergeordneten VM, auf der Sie Horizon Agent auf Horizon 7 Version 7.5 oder höher aktualisieren wollen. Dieser Snapshot ist das Master-Image für Instant-Clones.
- 2 Legen Sie für den Storage DRS-Migrationsschwellenwert (Distributed Resource Scheduler) im Cluster „3“ fest.
- 3 Deaktivieren Sie die Instant-Clone-Desktop-Pools.
- 4 Aktualisieren Sie vCenter Server auf vSphere 6.7.
- 5 Wählen Sie eine der folgenden Optionen aus, um die Hosts, die Sie aktualisieren möchten, in den Wartungsmodus zu versetzen.
 - Versetzen Sie den Host direkt im vSphere Web Client in den Wartungsmodus. Aktualisieren Sie dann den Host auf vSphere 6.7. Verwenden Sie nach Abschluss des Upgrades den vSphere Web Client, um den Wartungsmodus zu beenden.
 - Verwenden Sie das Dienstprogramm `icmaint.cmd`, um einen Host mit der Option **ON** für die Wartung zu kennzeichnen. Wenn Sie einen Host für die Wartung kennzeichnen, werden die Master-Images, die die übergeordneten VMs in vCenter Server sind, vom ESXi-Host gelöscht. Versetzen Sie den Host in den Wartungsmodus und führen Sie das Upgrade auf vSphere 6.7 ESXi durch. Beenden Sie nach Abschluss des Upgrades den Wartungsmodus des Hosts. Verwenden Sie `icmaint.cmd`, um die Kennzeichnung des Hosts für die Wartung mit der Option **OFF** aufzuheben.

Hinweis Sie müssen mindestens einen Host aktualisieren, damit Sie die Bereitstellung von Desktop-Pools fortsetzen können. Anschließend müssen Sie alle anderen Hosts aktualisieren.

- 6 Aktivieren Sie die Instant-Clone-Desktop-Pools.
- 7 Führen Sie für jeden Instant-Clone-Desktop-Pool, der den neuen Snapshot verwendet, eine Image-Übertragung durch.

Für die Bereitstellung werden nur Hosts verwendet, die auf vSphere 6.7 ESXi aktualisiert wurden. Die während der Image-Übertragung erstellten Instant-Clones können auf andere Hosts migriert werden, die noch nicht auf vSphere 6.7 aktualisiert wurden.

- 8 Stellen Sie sicher, dass alle Hosts im Cluster auf vSphere 6.7 aktualisiert wurden.
- 9 Wenn Sie die übergeordnete virtuelle Maschine von einer früheren Version aktualisieren, damit sie mit ESXi 6.7 und höher (VM-Version 14) kompatibel ist, aktualisieren Sie die VMware Tools auf der übergeordneten virtuellen Maschine. Sie müssen einen neuen Snapshot der übergeordneten virtuellen Maschine erstellen, der das Master-Image für Instant-Clones ist, und eine Image-Übertragung an alle Instant-Clone-Desktop-Pools durchführen, die die vorherige Version dieses Master-Images verwenden.
- 10 Wenn der verteilte virtuelle Switch (vDS) aktualisiert wird, schalten Sie die übergeordnete virtuelle Maschine ein und stellen Sie sicher, dass keine Netzwerkprobleme vorliegen. Nach einem vDS-Upgrade müssen Sie einen neuen Snapshot der übergeordneten VM erstellen und eine Image-Übertragung an alle Instant-Clone-Desktop-Pools durchführen.

Aufgaben nach dem Upgrade zum Aktivieren neuer Funktionen für Ihr Horizon-Setup

8

Nachdem Sie das Upgrade der Server, virtuellen Maschinen und Agent-Software für Desktop- und Anwendungspools durchgeführt haben, können Sie Ihr Setup konfigurieren, um bestimmte neue Funktionen zu nutzen.

Zusätzlich zu den in den Themen in diesem Kapitel beschriebenen Aufgaben können Sie, falls zutreffend, Horizon Administrator zum Bearbeiten erweiterter Speicheroptionen für Desktop-Pools und zum Ändern des Geltungsbereichs der transparenten gemeinsamen Nutzung von Seiten verwenden. Die gemeinsame Arbeitsspeichernutzung ist aus Sicherheitsgründen zwischen virtuellen Maschinen auf einem ESXi-Host standardmäßig nicht zulässig. Weitere Informationen finden Sie im Thema „Ändern der Einstellungen in einem vorhandenen Desktop-Pool“ im Dokument *Horizon 7-Verwaltung*.

Dieses Kapitel enthält die folgenden Themen:

- [Ändern des Sicherheitsmodus für JMS-Meldungen auf Erweitert](#)
- [Aufgaben für die Aktualisierung von Desktop-Pools zur Verwendung der Speicherplatzrückgewinnung](#)
- [Upgrade-Aufgaben bei Verwendung von VMware vSAN-Datenspeichern](#)
- [Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer](#)

Ändern des Sicherheitsmodus für JMS-Meldungen auf Erweitert

Bei einem Upgrade wird die vorhandene Einstellung des Sicherheitsmodus für JMS-Meldungen für die vorhergehende Version beibehalten. Ab Horizon 6 Version 6.1 können Sie diese Einstellung mit Horizon Administrator in **Erweitert** ändern.

Im Folgenden wird beschrieben, wie Sie mit Horizon Administrator den Sicherheitsmodus für Meldungen in **Erweitert** ändern und wie Sie den Änderungsfortschritt bei allen Horizon-Komponenten überwachen. Sie können auch das `vdmutil`-Befehlszeilenprogramm verwenden, um den Modus und den Überwachungsfortschritt zu ändern. Siehe das Dokument *Horizon 7-Verwaltung*.

Hinweis Mit Horizon 6 Version 6.2 und höheren Versionen können Sie Access Point-Appliances anstelle von Horizon-Sicherheitsservern benutzen. Access Point verwendet ein HTTP(S)-Protokoll für die Kommunikation mit dem Verbindungsserver. JMS, IPsec und AJP13 werden nicht verwendet.

Wenn Sie Access Point-Appliances anstelle von Horizon-Sicherheitsservern benutzen möchten, müssen Sie für die Verbindungsserver-Instanzen ein Upgrade auf Version 6.2 oder höher durchführen, bevor Sie die Access Point-Appliances zum Verweis auf Verbindungsserver-Instanzen oder auf den Lastausgleichsdienst, der sich vor den Instanzen befindet, installieren und konfigurieren. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Voraussetzungen

Stellen Sie sicher, dass Sie alle Horizon Connection Server-Instanzen, Sicherheitsserver und Horizon-Desktops auf Horizon 6, Version 6.1 oder eine neuere Version aktualisiert haben. View-Komponenten, die älter als Horizon 6 Version 6.1 sind, können nicht mit einer Verbindungsserver 6.1-Instanz kommunizieren, die den erweiterten Modus verwendet.

Verfahren

- 1 Konfigurieren Sie Back-End-Firewall-Regeln, damit Sicherheitsserver JMS-Datenverkehr auf Port 4002 an Verbindungsserver-Instanzen senden können.
- 2 Gehen Sie in Horizon Administrator zu **View-Konfiguration > Globale Einstellungen** und legen Sie auf der Registerkarte **Sicherheit** den **Sicherheitsmodus für Meldungen** auf **Erweitert** fest.
- 3 Starten Sie manuell den VMware Horizon Message Bus-Komponenten-Dienst auf allen Verbindungsserver-Hosts im Pod neu oder starten Sie die Verbindungsserver-Instanzen neu.

Nach dem Neustart der Dienste konfigurieren die Verbindungsserver-Instanzen den Sicherheitsmodus für Nachrichten auf allen Desktops und Sicherheitsservern neu, indem sie den Modus auf **Erweitert** ändern.

- 4 Um den Fortschritt in Horizon Administrator zu überwachen, navigieren Sie zu **View-Konfiguration > Globale Einstellungen**.

Auf der Registerkarte **Sicherheit** wird für die Option **Erweiterter Sicherheitsstatus** der Eintrag **Erweitert** angezeigt, wenn alle Komponenten auf den erweiterten Modus umgestellt wurden.

Ergebnisse

Wenn Server mit Clients kommunizieren, konfigurieren Server Clients für die Verwendung des erweiterten Sicherheitsmodus für Meldungen.

Aufgaben für die Aktualisierung von Desktop-Pools zur Verwendung der Speicherplatzrückgewinnung

Ab vSphere 5.1 erstellt Horizon 7 virtuelle Linked-Clone-Maschinen in einem effizienten Festplattenformat, mit dem ESXi-Hosts nicht genutzten Festplattenspeicherplatz in den Linked Clones zurückgewinnen können. Das Upgrade von Pools, um diese Funktion zu nutzen, beinhaltet das Ändern von Einstellungen in vCenter Server, View LDAP und Pool-Einstellungen und dann eine Neuzusammenstellung des Pools.

Hinweis Die Funktion zur Speicherplatzrückgewinnung wird nicht unterstützt, wenn die VM-Desktops auf vSAN- oder VVOL-Datenspeichern gehostet werden.

Obwohl die Funktion zur Speicherplatzrückgewinnung die Speicherplatzmenge reduziert, die für eine virtuelle Maschine verwendet wird, kann nur Speicherplatz zurückgewonnen werden, der nicht verwendet wird. Dieses Merkmal kann keinen Speicherplatz von virtuellen Maschinen zurückgewinnen, die nicht optimiert wurden. Um ein Betriebssystem-Image zu optimieren, können Sie Windows-Dienste deaktivieren, beispielsweise den Indizierungsdienst, den Defragmentierungsdienst und Wiederherstellungspunkte. Weitere Informationen finden Sie unter „Optimieren der Leistung des Windows-Gastbetriebssystems“, „Optimieren der Leistung des Windows 7- und 8-Gastbetriebssystems“ und „Optimieren von Windows 7 und 8 für Linked-Clone-Desktops“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Wichtig Da dieses Verfahren die Neuzusammenstellung des Desktop-Pools beinhaltet, gehen alle Änderungen verloren, die Endbenutzer an der Festplatte des Betriebssystems vorgenommen haben.

- 1 Wenn alle vCenter Server-Instanzen und ESXi-Hosts für den Pool nicht die Version VMware vSphere 5.1 oder höher aufweisen, aktualisieren Sie sie auf Version 5.1 oder höher.

Anleitungen finden Sie im *VMware vSphere-Upgrade-Handbuch*.

- 2 Wenn alle virtuellen Desktop-Maschinen im Pool keine virtuellen Maschinen der Version VMware vSphere 5.1 (virtuelle Hardware-Version 9) oder höher sind, aktualisieren Sie sie.

- In der übergeordneten virtuellen Maschine aktualisieren Sie VMware Tools auf die neueste Version von VMware vSphere 5.1 oder eine spätere Version und die virtuelle Maschine auf die neueste Version, welche die virtuelle Hardware-Version 9 oder höher sein muss.

Anleitungen finden Sie im *VMware vSphere-Upgrade-Handbuch*.

- Erstellen Sie einen Snapshot der übergeordneten virtuellen Maschine. Anweisungen zum Erstellen von Snapshots finden Sie in der Online-Hilfe zu vSphere Client.
- Verwenden Sie den Snapshot der übergeordneten virtuellen Maschine, die Sie gerade erstellt haben, um den Desktop-Pool neu zusammenzustellen. Für Anweisungen zur Neuzusammenstellung von Pools klicken Sie auf die Schaltfläche **Hilfe** in Horizon Administrator.

Die Neuzusammenstellung des Pools von einem Snapshot einer aktualisierten virtuellen Maschine ist nur ein Upgrade-Verfahren, um alle virtuellen Maschinen in einen Linked-Clone-Pool zu aktualisieren. Sie können auch ein Upgrade der virtuellen Maschinen nacheinander durchführen.

- 3 Aktualisieren des Diskformats für die virtuellen Maschinen.
 - Verwenden Sie ADSIEdit auf dem Verbindungsserver-Host, um zu der Servergruppe zu navigieren, die dem Pool entspricht. Ändern Sie den Wert im Feld **pae-UseSeSparseFormat** von **0** auf **1**.
 - Stellen Sie den Desktop-Pool neu zusammen.
- 4 Verwenden Sie Horizon Administrator zur Bearbeitung der vCenter Server-Einstellungen, navigieren Sie zur Registerkarte **Speicher** und wählen Sie **VM-Datenträgerplatz zurückgewinnen** aus.

Für Anweisungen zur Bearbeitung der Servereinstellungen klicken Sie auf die Schaltfläche **Hilfe** im Horizon Administrator.
- 5 Verwenden Sie Horizon Administrator zur Bearbeitung der Pooleinstellungen, navigieren Sie zum Abschnitt **Erweiterter Speicher**, wählen Sie **VM-Datenträgerplatz zurückgewinnen** aus und stellen Sie den Schwellenwert für die Rückgewinnung von Speicherplatz auf 1 GB.

Upgrade-Aufgaben bei Verwendung von VMware vSAN-Datenspeichern

Ab vSphere 5.5 Update 1 können Sie die vSAN-Funktion für Hochleistungsspeicher und die richtlinienbasierte Verwaltung verwenden.

Bei Verwendung von vSAN werden die lokal angeschlossenen physischen Speicherfestplatten, die in einem Cluster mit vSphere-Hosts zur Verfügung stehen, in einem virtuellen Datenspeicher zusammengefasst. Sie geben diesen Datenspeicher bei der Erstellung eines Desktop-Pools an. Die verschiedenen Komponenten, wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Dateien des Betriebssystems, werden auf den passenden Solid-State-Laufwerken (SSDs) oder direkt angeschlossenen Festplatten (HDDs) abgelegt.

Horizon 7 definiert die Speicheranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, in Abhängigkeit von den verwendeten Pool-Einstellungen. Der Speicher wird gemäß den zugewiesenen Richtlinien bereitgestellt und automatisch konfiguriert.

Hinweis Die Funktion zur Speicherplatzrückgewinnung wird nicht unterstützt, wenn die virtuellen Desktop-Maschinen auf vSAN-Datenspeichern gehostet werden.

Upgrade von einem Non-vSAN-Datenspeicher auf einen vSAN-Datenspeicher

Für ein Upgrade von Pools zur Verwendung von VMware vSAN-Datenspeichern müssen Sie eine Pool-Einstellung ändern und dann eine Neuverteilung des Pools durchführen.

Die in diesem Verfahren beschriebenen Aufgaben erklären das Upgrade von einem Non-vSAN-Datenspeicher auf einen vSAN-Datenspeicher. Upgrades von vSAN-Datenspeichern auf Clustern unter vSphere 5.5 oder älteren Versionen (eine technische Vorschaufunktion) werden nicht unterstützt.

Wichtig Da dieses Verfahren die Neuzusammenstellung des Desktop-Pools beinhaltet, gehen alle Änderungen verloren, die Endbenutzer an der Festplatte des Betriebssystems vorgenommen haben.

Voraussetzungen

- Stellen Sie sicher, dass alle ESXi-Hosts in dem Cluster, der für den Pool verwendet wird, auf Version 5.5 Update 1 oder höher aktualisiert werden und dass sie die Systemanforderungen für die vSAN-Funktion erfüllen. VMware empfiehlt ein Upgrade auf vSphere 6.0 oder höher, da die in vSphere 6.0 und höher verfügbare vSAN-Funktion im Vergleich zu der Funktion aus vSphere 5.5 Update 1 viele Leistungsverbesserungen enthält. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf.

Informationen zu Upgrades finden Sie unter [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#) und im *VMware vSphere-Upgrade-Handbuch*. Informationen zu den vSAN-Anforderungen und -Upgrades finden Sie im Dokument *Verwaltung von VMware vSAN*.

- Stellen Sie in vCenter Server sicher, dass der Composer-Rolle die folgenden Rechte zugewiesen sind:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Verfahren

- 1 Verwenden Sie vCenter Server 5.5 Update 1 oder höher, um vSAN für den vSphere-Cluster zu aktivieren.

Weitere Informationen finden Sie im Dokument zu *vSphere Storage*.

- 2 Aktualisieren Sie den Desktop-Pool auf die neueste Version, wie unter [Upgrade von View Composer-Desktop-Pools](#) beschrieben.

Dazu müssen Sie die neueste Version von Horizon Agent auf der übergeordneten virtuellen Maschine installieren und einen Snapshot erstellen.

- 3 Stellen Sie den Pool auf dem Non-vSAN-Datenspeicher neu zusammen und verwenden Sie dabei den gerade erstellten Snapshot der übergeordneten virtuellen Maschine.

Klicken Sie für eine Anleitung für die Neuzusammenstellung von Pools auf die Schaltfläche **Hilfe** in Horizon Administrator.

- 4 Bearbeiten Sie die Pool-Einstellungen des neu aktualisierten Desktop-Pools, um die Pool-Einstellung **VMware Virtual SAN verwenden** zu aktivieren sowie den Datenspeicher von einem Non-vSAN-Datenspeicher in einen vSAN-Datenspeicher zu ändern, und führen Sie den Befehl **Neu verteilen** aus.

Wenn Sie Anleitungen zum Bearbeiten der Servereinstellungen und zum Verwenden des Befehls **Neu verteilen** benötigen, klicken Sie in Horizon Administrator auf die Schaltfläche **Hilfe**.

Upgrade vom vSAN-Festplattenformat der Version 1

Nach dem Upgrade von VMware vSphere 5.5 Update 1 auf vSphere 6.0 oder höher müssen Sie auch ein Upgrade für das vSAN-Festplattenformat durchführen.

VMware empfiehlt ein Upgrade auf vSphere 6.0 oder höher, da die in vSphere 6.0 und höher verfügbare vSAN-Funktion im Vergleich zu der Funktion aus vSphere 5.5 Update 1 viele Leistungsverbesserungen enthält. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf.

Wichtig In diesem Verfahren wird ein Upgrade-Vorgang für vSAN beschrieben, falls Sie aktuell Desktop-Pools auf vSAN-Datenspeichern verwenden, die in vSphere 5.5 Update 1 oder einem späteren Update verfügbar sind. Wenn Ihre Desktop-Pools aktuell keine vSAN-Datenspeicher verwenden, finden Sie weitere Informationen unter [Upgrade von einem Non-vSAN-Datenspeicher auf einen vSAN-Datenspeicher](#).

Das Upgrade eines VMware vSAN-Datenspeichers besteht aus mehreren Phasen und beinhaltet das Upgrade der vSphere-Software auf jedem ESXi-Host und das anschließende Upgrade des Festplattenformats (jeweils für eine Festplattengruppe). Ein komplettes Kapitel des vSphere 6-Dokuments *Verwaltung von VMware vSAN* befasst sich mit dem Upgrade-Vorgang. Die Schritte im folgenden Verfahren beschreiben die Reihenfolge, in der die Aufgaben auf der ESXi-Host-Ebene, in vCenter Server und auf der Desktop-Pool-Ebene in View Administrator ausgeführt werden müssen.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Desktop-Pools View Agent 6.0 oder höher verwenden. Wenn Ihre virtuellen Maschinen View Agent 5.3.x auf vSAN-Datenspeichern verwenden, finden Sie weitere Informationen unter [Upgrade von Horizon View 5.3.x auf einem vSAN-Datenspeicher](#).
- Stellen Sie in vCenter Server sicher, dass der Composer-Rolle die folgenden Rechte zugewiesen sind:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

- Machen Sie sich mit dem Upgrade-Vorgang für vSAN vertraut. Lesen Sie hierzu das Kapitel zum Upgrade von vSAN im Dokument *Verwaltung von VMware vSAN* unter <https://docs.vmware.com/de/VMware-vSAN/index.html>.

Verfahren

- 1 Führen Sie ein Upgrade von vCenter Server und Ihren ESXi-Hosts auf vSphere 6 oder höher durch, wie im Kapitel zum Upgrade des vSAN-Clusters im Dokument *Verwaltung von VMware vSAN* beschrieben, das Sie im vSphere 6.0-Dokumentationscenter finden.

Zu diesem Zeitpunkt verwendet der Desktop-Pool weiterhin das vSAN-Festplattenformat 1, und für die virtuellen Maschinen und für VMware Tools wurde noch kein Upgrade auf Version 11 der virtuellen Hardware von vSphere 6.0 durchgeführt.

- 2 Aktualisieren Sie den Desktop-Pool auf die neueste Version, wie unter [Upgrade von View Agent oder Horizon Agent](#) und [Upgrade von View Composer-Desktop-Pools](#) beschrieben.

Dies beinhaltet das Installieren der neuesten Version von Horizon Agent auf der übergeordneten virtuellen Maschine, der VM-Vorlage oder den virtuellen Full-Clone-Maschinen im Pool. Für Linked-Clone-Pools beinhaltet dies außerdem das Erstellen eines Snapshots und die Neuzusammenstellung des Pools.

Auf den virtuellen Maschinen im Desktop-Pool ist nun View Agent 6.1 oder höher installiert, und die virtuellen Maschinen befinden sich weiterhin auf vSAN-Datenspeichern, die in vSphere 5.5 Update 1 verfügbar sind. Der Desktop-Pool verwendet zu diesem Zeitpunkt das vSAN-Festplattenformat 1.

- 3 Führen Sie ein Upgrade für das vSAN-Festplattenformat von Version 1 auf Version 2 durch.

Ausführliche Anweisungen finden Sie unter „Upgrade des vSAN-Festplattenformats“ im Upgrade-Kapitel des Dokuments *Verwaltung von VMware vSAN*, verfügbar unter <https://docs.vmware.com/de/VMware-vSAN/index.html>.

Für dieses Upgrade können Sie das RVC-Befehlszeilentool oder, wenn Sie über vSphere 6 Update 1 verfügen, den vSphere Web Client verwenden. Ruby vSphere Console (RVC) ist eine Ruby-basierte Befehlszeilenkonsole für VMware ESXi-Hosts und vCenter Server. RVC ist im Lieferumfang der Windows- und Linux-Versionen von vCenter Server enthalten. Ausführliche Informationen zur Verwendung der RVC-Befehle finden Sie in der *RVC-Befehlszeilenreferenz*.

- 4 Nachdem das Upgrade der Festplatten für alle ESXi-Hosts im Cluster, auf der übergeordneten virtuellen Maschine, der VM-Vorlage oder auf virtuellen Full-Clone-Maschinen im Pool durchgeführt wurde, führen Sie die folgenden Aufgaben in der angegebenen Reihenfolge aus.
 - a Wenn sich die übergeordnete virtuelle Maschine in einem vSAN-Datenspeicher befindet, löschen Sie alle Snapshots.

Die virtuelle Maschine kann das neue Snapshot-Format des vSAN-Festplattenformats 2 erst verwenden, nachdem alle vorherigen redoLog-basierten Snapshots gelöscht wurden. Wenn sich die virtuelle Maschine nicht in einem vSAN-Datenspeicher befindet, brauchen Sie die Snapshots nicht zu löschen.
 - b Führen Sie ein Upgrade der VM-Hardware auf Version 11 sowie ein Upgrade von VMware Tools durch.
- 5 Erstellen Sie für Linked-Clone-Pools einen neuen Snapshot und stellen Sie den Desktop-Pool mithilfe des neuen Snapshots neu zusammen.

Ergebnisse

Der Desktop-Pool verwendet nun das vSAN-Festplattenformat 2.

Upgrade von Horizon View 5.3.x auf einem vSAN-Datenspeicher

Mit Horizon 6.0 wurden einige neue Standard-Speicherrichtlinien für vSAN eingeführt. Diese Richtlinien werden nicht automatisch auf vorhandene Desktops virtueller Maschinen angewendet, die durch Horizon 7 5.3.x auf vSAN erstellt wurden, nachdem der Desktop-Pool aktualisiert wurde.

Wenn Sie ein Upgrade von Horizon 7 5.3.x durchführen, wird die Pool-Einstellung **VMware Virtual SAN verwenden** außerdem auch dann nicht automatisch aktiviert, wenn der Pool auf einem vSAN-Datenspeicher vorhanden ist. Es stehen die folgenden Upgrade-Optionen zur Verfügung:

- Wenn Sie VMware vSphere 5.5 Update 1 nach dem Upgrade weiterhin verwenden, verwenden Sie die standardmäßigen Speicherrichtlinien aus Horizon 7 5.3.x. Wenn Sie diese Option auswählen, bearbeiten Sie die Pool-Einstellungen, sodass **VMware Virtual SAN verwenden** aktiviert wird.
- Verwenden Sie das in diesem Thema beschriebene Verfahren, sodass der Desktop-Pool die neuen standardmäßigen Speicherrichtlinien verwendet. Dieses Verfahren beinhaltet die Neuverteilung des Desktop-Pools auf einen Non-vSAN-Datenspeicher und das anschließende Upgrade sowie die Neuverteilung zurück in den vSAN-Datenspeicher.

Wichtig Die beschriebenen Aufgaben in diesem Vorgehen erklären das Upgrade des Desktop-Pools Horizon 7 5.3.x, indem ein vSAN-Datenspeicher auf einem VMware vSphere 5.5 Update 1-Cluster verwendet wird. Upgrades von vSAN-Datenspeichern auf Clustern unter VMware vSphere 5.5 oder älteren Versionen (eine technische Vorschaufunktion) werden nicht unterstützt.

Da dieses Verfahren die Neuzusammenstellung des Desktop-Pools beinhaltet, gehen außerdem alle Änderungen verloren, die Endbenutzer an der Festplatte des Betriebssystems vorgenommen haben.

Voraussetzungen

- Stellen Sie sicher, dass es sich bei allen virtuellen Maschinen im Pool um VMware vSphere 5.5 Update 1 oder höhere virtuelle Maschinen handelt. VMware empfiehlt ein Upgrade auf VMware vSphere 6.0 oder höher, da die in vSphere 6.0 und höher verfügbare vSAN-Funktion im Vergleich zu der Funktion aus vSphere 5.5 Update 1 viele Leistungsverbesserungen enthält. In vSphere 6.0 weist diese Funktion auch eine umfassendere HCL-Unterstützung (Hardware Compatibility, Hardwarekompatibilität) auf.

Informationen zu Upgrades finden Sie in [Kapitel 6 Upgrade von ESXi-Hosts und ihren virtuellen Maschinen](#) und im *VMware vSphere-Upgrade-Handbuch*. Informationen zu den vSAN-Anforderungen und -Upgrades finden Sie im Dokument *Verwaltung von VMware vSAN*.

- Stellen Sie in vCenter Server sicher, dass der Composer-Rolle die folgenden Rechte zugewiesen sind:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Verfahren

- 1 Bearbeiten Sie die Pool-Einstellungen des Desktop-Pools, um den Datenspeicher von einem vSAN-Datenspeicher in einen Non-vSAN-Datenspeicher zu ändern, und führen Sie den Befehl **Neu verteilen** aus.

Wenn Sie Anleitungen zum Bearbeiten der Servereinstellungen und zum Verwenden des Befehls **Neu verteilen** benötigen, klicken Sie in View Administrator auf die Schaltfläche **Hilfe**.

- 2 Aktualisieren Sie den Desktop-Pool auf die neueste Version, wie unter [Upgrade von View Composer-Desktop-Pools](#) beschrieben.

Dazu müssen Sie die neueste Version von Horizon Agent auf der übergeordneten virtuellen Maschine installieren und einen Snapshot erstellen.

- 3 Stellen Sie den Pool auf dem Non-vSAN-Datenspeicher neu zusammen und verwenden Sie dabei den gerade erstellten Snapshot der übergeordneten virtuellen Maschine.

Für Anweisungen zur Neuzusammenstellung der Pools klicken Sie auf die Schaltfläche **Hilfe** im View Administrator.

- 4 Bearbeiten Sie die Pool-Einstellungen des aktualisierten Desktop-Pools, um den Datenspeicher von einem Non-vSAN-Datenspeicher in einen vSAN-Datenspeicher zu ändern, und führen Sie den Befehl **Neu verteilen** aus.

Nächste Schritte

Wenn Sie für Ihre virtuellen Maschinen ein Upgrade auf VMware vSphere 6.0 durchgeführt haben, finden Sie unter [Upgrade vom vSAN-Festplattenformat der Version 1](#) weitere Informationen zum Upgrade auf vSAN 2 statt auf vSAN 1.

Konfigurieren der VMware Horizon-Webportalseite für Endbenutzer

Sie können die VMware Horizon-Webportalseite so konfigurieren, dass das Symbol zum Herunterladen von Horizon Client oder das Symbol für die Herstellung einer Verbindung mit einem Remote-Desktop über HTML Access sowie andere Verknüpfungen angezeigt oder ausgeblendet werden.

Standardmäßig werden auf der VMware Horizon-Webportalseite ein Symbol für den Download und die Installation von Horizon Client sowie ein Symbol für die Verbindungsherstellung über HTML Access angezeigt. Die Standardwerte, die in der Datei `portal-links-html-access.properties` definiert sind, bestimmen den Download-Link, der auf der VMware Horizon-Webportalseite angezeigt wird.

In manchen Fällen sollen die Links auf der VMware Horizon-Webportalseite möglicherweise auf einen internen Webserver verweisen oder Sie möchten bestimmte Clientversionen auf Ihrem eigenen Server verfügbar machen. Sie können die VMware Horizon-Webportalseite dann so konfigurieren, dass diese auf eine andere Download-URL verweist. Dazu müssen Sie den Inhalt der Datei `portal-links-html-access.properties` ändern. Wenn diese Datei nicht verfügbar oder leer ist und die Datei `oslinks.properties` vorhanden ist, wird der Link für die Installationsdatei in der Datei `oslinks.properties` festgelegt.

Die Datei `oslinks.properties` wird im Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\broker\webapps\portal\WEB-INF installiert. Wenn diese Datei während der HTML Access-Sitzung nicht vorhanden ist, leitet der Download-Link die Benutzer standardmäßig zu <https://www.vmware.com/go/viewclients> weiter. Die Datei enthält die folgenden Standardwerte.

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

In der Datei `portal-links-html-access.properties` oder in der Datei `oslinks.properties` können Sie Installationslinks für bestimmte Clientbetriebssysteme definieren. Wenn Sie z. B. mit einem macOS-System die VMware Horizon-Webportalseite besuchen, wird der Link zum Installationsprogramm für Horizon Client für Mac angezeigt. Für Windows- oder Linux-Clients können Sie separate Links für die 32-Bit- und 64-Bit-Installationsprogramme erstellen.

Verfahren

- 1 Verwenden Sie auf dem Verbindungsserver-Host einen Texteditor, um die Datei `portal-links-html-access.properties` im Verzeichnis *CommonAppDataFolder*\VMware\VDM\portal\portal-links-html-access.properties zu öffnen.

Auf Windows Server 2008-Betriebssystemen entspricht das Verzeichnis *CommonAppDataFolder* dem Ordner `C:\ProgramData`. Zur Anzeige des Ordners `C:\ProgramData` in Windows Explorer aktivieren Sie im Dialogfeld mit den Ordneroptionen die Anzeige ausgeblendeter Ordner.

Wenn die Datei `portal-links-html-access.properties` nicht vorhanden ist, jedoch die Datei `oslinks.properties`, öffnen Sie die Datei *<Installationsverzeichnis>*\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties zur Änderung der URLs für das Herunterladen bestimmter Installationsdateien.

2 Bearbeiten Sie die Konfigurationseigenschaften.

Standardmäßig sind das Installationsprogramm-Symbol und das HTML Access-Symbol aktiviert und ein Link verweist auf die Client-Downloadseite auf der VMware-Website. Wenn Sie ein Symbol deaktivieren möchten, stellen Sie die Eigenschaft auf `false` ein. Dadurch wird das Symbol aus der Webseite entfernt.

Hinweis Die Datei `oslinks.properties` kann ausschließlich zur Konfiguration der Links zu bestimmten Installationsdateien verwendet werden.

Option	Eigenschafteneinstellung
HTML Access deaktivieren	<code>enable.webclient=false</code> Wenn für diese Option „false“ festgelegt ist, aber für die Option <code>enable.download</code> der Wert „true“ gesetzt ist, wird der Benutzer zu einer Webseite geleitet, von der das native Installationsprogramm für Horizon Client heruntergeladen werden kann. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.“
Herunterladen von Horizon Client deaktivieren	<code>enable.download=false</code> Wenn für diese Option „false“ festgelegt ist, aber für die Option <code>enable.webclient</code> der Wert „true“ gesetzt ist, wird der Benutzer zur Anmeldeseite für HTML Access geleitet. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.“
Ändern der URL für die Webseite zum Herunterladen von Horizon Client	<code>link.download=https://url-of-web-server</code> Verwenden Sie diese Eigenschaft, wenn Sie Ihre eigene Webseite erstellen möchten.

Option	Eigenschafteneinstellung
Create links for specific installers (Links für bestimmte Installationsprogramme erstellen)	<p>In den folgenden Beispielen werden vollständige URLs angezeigt. Wenn Sie die Installationsdateien im Verzeichnis Downloads ablegen, das sich im Verzeichnis C:\Programme\VMware\VMware View\Server\broker\webapps\ des Verbindungsserver-Hosts befindet, können Sie relative URLs verwenden, wie im nächsten Schritt beschrieben.</p> <ul style="list-style-type: none"> ■ Allgemeiner Link zum Herunterladen des Installationsprogramms: <pre>link.download=https://server/downloads</pre> ■ 32-Bit-Windows-Installationsprogramm: <pre>link.win32=https://Server/downloads/VMware-Horizon-Client-x86-Build-Nr..exe</pre> ■ 64-Bit-Windows-Installationsprogramm: <pre>link.win64=https://Server/downloads/VMware-Horizon-Client-x86_64-Build-Nr..exe</pre> ■ Windows Phone-Installationsprogramm: <pre>link.winmobile=https://Server/downloads/VMware-Horizon-Client-Build-Nr..appx</pre> ■ 32-Bit-Linux-Installationsprogramm: <pre>link.linux32=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x86.bundle</pre> ■ 64-Bit-Linux-Installationsprogramm: <pre>link.linux64=https://Server/downloads/VMware-Horizon-Client-Build-Nr..x64.bundle</pre> ■ Mac OS X-Installationsprogramm: <pre>link.mac=https://Server/downloads/VMware-Horizon-Client-Build-Nr..dmg</pre> ■ iOS-Installationsprogramm: <pre>link.ios=https://Server/downloads/VMware-Horizon-Client-iPhoneOS-Build-Nr..ipa</pre> ■ Android-Installationsprogramm: <pre>link.android=https://Server/downloads/VMware-Horizon-Client-AndroidOS-Build-Nr..apk</pre> ■ Chrome OS-Installationsprogramm: <pre>link.chromeos=https://Server/downloads/VMware-Horizon-Client-ChromeOS-Build-Nr..apk</pre>
Ändern der URL für den Hilfe-Link auf der Anmeldeseite	<pre>link.help</pre> <p>Dieser Link verweist standardmäßig auf ein Hilfesystem, das auf der VMware-Website verwaltet wird. Der Hilfe-Link wird auf der Anmeldeseite unten angezeigt.</p>

- 3 Damit Benutzer die Installationsprogramme von einem anderen Speicherort als der VMware-Website herunterladen, legen Sie die Installationsdateien auf dem HTTP-Server ab, auf dem sich auch die Installationsdateien befinden.

Dieser Speicherort muss mit den URLs übereinstimmen, die Sie im vorherigen Schritt in der Datei `portal-links-html-access.properties` oder in der Datei `oslinks.properties` angegeben haben. Um die Dateien beispielsweise in einem Verzeichnis „downloads“ auf dem Verbindungsserver-Host zu speichern, verwenden Sie den folgenden Pfad.

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Die Links zu den Installationsdateien können dann relative URLs im Format `/downloads/client-installer-file-name` enthalten.

- 4 Starten Sie den Horizon-Webkomponentendienst neu.

Separates Upgrade von vSphere-Komponenten in einer Horizon 7-Umgebung

9

Wenn Sie das Upgrade von vSphere-Komponenten separat vom Upgrade von Horizon 7-Komponenten durchführen, müssen Sie einige Horizon 7-Daten sichern und Horizon 7-Software neu installieren.

Anstatt ein integriertes Upgrade von Horizon 7- und vSphere-Komponenten durchzuführen, können Sie auch zuerst alle Horizon 7- und dann alle vSphere-Komponenten, oder umgekehrt, aktualisieren. Sie können auch ausschließlich vSphere-Komponenten aktualisieren, wenn eine neue Version oder ein neues Update von vSphere erhältlich ist.

Wenn Sie für vSphere-Komponenten ein von Horizon 7-Komponenten getrenntes Upgrade durchführen, müssen Sie die folgenden zusätzlichen Aufgaben ausführen:

- 1 Sichern Sie vor einem Upgrade von vCenter Server die vCenter Server-Datenbank und die View Composer-Datenbank.
- 2 Sichern Sie vor einem vCenter Server-Upgrade die Horizon LDAP-Datenbank über eine Horizon Connection Server-Instanz. Verwenden Sie hierzu das Dienstprogramm `vdmexport.exe`.

Die Anweisungen dazu finden Sie im *Horizon 7-Verwaltung*-Dokument. Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten aus nur einer Instanz exportieren.

- 3 Wenn Sie View Composer verwenden, nachdem Sie ein Upgrade für alle ESXi-Hosts durchgeführt haben, die von einer bestimmten vCenter Server-Instanz verwaltet werden, starten Sie den View Composer-Dienst auf dem jeweiligen Host neu.
- 4 Nachdem Sie VMware Tools in virtuellen Maschinen aktualisiert haben, die als Remote-Desktops verwendet werden, müssen Sie Horizon Agent neu installieren.

Durch die Neuinstallation von Horizon Agent wird sichergestellt, dass die Treiber der virtuellen Maschine mit den anderen Horizon 7-Komponenten kompatibel bleiben.

Schrittweise Anweisungen zur Ausführung des Horizon Agent-Installationsprogramms erhalten Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.