

vSphere-Upgrade

Update 2

Geändert am 11. August 2020

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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

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

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 © 2009-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Grundlegende Informationen zum vSphere-Upgrade 8

Aktualisierte Informationen 9

1 Einführung in das vSphere-Upgrade 11

vCenter Server-Komponenten und -Dienste 12

Unterschiede zwischen vSphere 6.0 und vSphere 5.x 14

Bereitstellungsmodelle für vCenter Server 16

vSphere-Upgrade-Vorgang 20

Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades 22

Upgrade auf den vSphere-Lizenzdienst 27

Unterschiede zwischen vSphere-Upgrades und -Updates 28

Auswirkungen von vCenter Single Sign On auf Upgrades 28

Übersicht über vSphere-Sicherheitszertifikate 31

Erweiterter verknüpfter Modus – Überblick 32

Beispiele von Upgrade-Pfaden für vCenter Server 33

2 Upgrade-Anforderungen 38

vCenter Server-Upgrade-Kompatibilität 38

Anforderungen für vCenter Server für Windows 40

Pre-Upgrade Checker von vCenter Server für Windows 40

Speichieranforderungen für vCenter Server für Windows 41

Hardwareanforderungen für vCenter Server für Windows 42

Softwareanforderungen für vCenter Server für Windows 43

Datenbankanforderungen für vCenter Server für Windows 43

Anforderungen für die vCenter Server Appliance 44

Hardwareanforderungen für vCenter Server Appliance 44

Speichieranforderungen für die vCenter Server Appliance 45

Im Lieferumfang der vCenter Server Appliance enthaltene Software 46

Softwareanforderungen für vCenter Server Appliance 46

Datenbankanforderungen für die vCenter Server Appliance 46

Erforderliche Ports für vCenter Server und Platform Services Controller 47

Konfigurationshinweise für die vCenter Server-Datenbank 52

Anforderungen für ESXi 53

Hardwareanforderungen für ESXi 54

Unterstützte Remotemanagement-Servermodelle und Firmware-Versionen 56

Empfehlungen für verbesserte ESXi-Leistung 56

Ein- und ausgehende Firewall-Ports für ESXi-Hosts	58
DNS-Anforderungen für vSphere	61
Softwareanforderungen für den vSphere Web Client	62
Softwareanforderungen für das Client-Integrations-Plug-In	62
vSphere Client-Anforderungen	63
vSphere-Client-Hardwareanforderungen	63
Softwareanforderungen des vSphere Clients	64
TCP- und UDP-Ports für den vSphere Client	64
Erforderlicher freier Speicherplatz für die Systemprotokollierung	65

3 Vor dem Upgrade von vCenter Server 67

Überprüfen der grundlegenden Kompatibilität vor dem Upgrade von vCenter Server	67
Vorbereiten der vCenter Server-Datenbanken	68
Vorbereiten der Oracle-Datenbank vor dem Upgrade auf vCenter Server 6.0	69
Vorbereiten der Microsoft SQL Server-Datenbank vor dem Upgrade auf vCenter Server 6.0	70
Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen	73
Vorbereiten der PostgreSQL-Datenbank vor dem Upgrade auf vCenter Server 6.0	74
Datenbankberechtigungsanforderungen für vCenter Server	75
Überprüfen, dass vCenter Server mit der lokalen Datenbank kommunizieren kann	78
Überprüfen der Netzwerkvoraussetzungen vor dem Upgrade	79
Überprüfen des Lastausgleichsdiensts vor dem Upgrade von vCenter Server	80
Vorbereiten der ESXi-Hosts für das Upgrade von vCenter Server	81
Host-Upgrades und Zertifikate	82
Ändern des Zertifikatmodus	83
Überprüfen der Vorbereitungen für das Upgrade von vCenter Server	83
Synchronisieren der Systemuhren im vSphere-Netzwerk	85
Ausfallzeiten während des vCenter Server-Upgrades	86
Verwenden eines Benutzerkontos zur Ausführung von vCenter Server	87
Erforderliche Informationen für das Upgrade von vCenter Server für Windows	87
Erforderliche Informationen für das Upgrade der vCenter Server Appliance	89

4 Upgrade und Update von vCenter Server für Windows 92

Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows	92
Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0	94
Herunterladen des Installationsprogramms für vCenter Server für Windows Installer	97
Upgrade von vCenter Single Sign-On 5.1 für die externe Bereitstellung	97
Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung	101
Upgrade von vCenter Server 5.0	104
Upgrade von vCenter Server 5.1 für Windows	107

Upgrade von vCenter Server 5.5 für Windows 110

Aktualisieren von Java-Komponenten und vCenter Server tc Server mit VIMPatch 113

5 Aktualisieren und Patchen der vCenter Server Appliance und Platform Services Controller-Appliance 115

Upgrade der vCenter Server Appliance 116

Informationen zum Upgrade-Vorgang von vCenter Server Appliance 117

Herunterladen des Installationsprogramms der vCenter Server Appliance 119

Installieren des Client-Integrations-Plug-Ins 119

Upgrade von vCenter Server Appliance mit eingebetteter vCenter Single Sign-On-Instanz 120

Upgrade von vCenter Server Appliance mit externer vCenter Single Sign-On-Instanz 126

Patchen der vCenter Server Appliance und Platform Services Controller-Appliance 131

Patchen der vCenter Server Appliance mit der Appliance-Verwaltungsschnittstelle 132

Patchen der vCenter Server Appliance mit der Appliance-Shell 136

6 Nach dem Upgrade auf vCenter Server 145

Abschließen der Komponentenkonfiguration nach dem Upgrade für vCenter Server 146

Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade 147

Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy 148

Aktualisieren des vSphere-Clients 150

Konfigurieren von VMware vCenter Server - tc Server-Einstellungen im vCenter Server 151

Festlegen der maximalen Anzahl von Datenbankverbindungen nach einem vCenter Server-Upgrade 153

Einrichten des vCenter Server-Administratorbenutzers 154

Authentifizieren für die vCenter Server-Umgebung 154

Identitätsquellen für vCenter Server mit vCenter Single Sign On 155

Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien 156

Neuverweisen von vCenter Server auf einen anderen externen Platform Services Controller 157

Neukonfigurieren einer eigenständigen vCenter Server-Instanz mit einem eingebetteten Platform Services Controller auf eine vCenter Server-Instanz mit einem externen Platform Services Controller 159

Neukonfigurieren mehrerer beigetretener Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller auf vCenter Server mit einem externen Platform Services Controller 163

Sicherstellen, dass alle Dienste der eingebetteten Platform Services Controller-Instanzen ausgeführt werden 165

Konfigurieren der Replizierungsvereinbarung zwischen allen externen Platform Services Controller-Instanzen 166

Neukonfigurieren aller vCenter Server-Instanzen und Neuverweisen von einer eingebetteten auf eine externe Platform Services Controller-Instanz 169

7 Upgrade von Update Manager 173

Upgrade von Update Manager-Server 174

8 Vor dem Upgrade von Hosts 177

- Empfohlene Vorgehensweisen für Upgrades von ESXi 177
- Upgrade-Optionen für ESXi 6.0 178
- Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern 180
- Verwenden von manuell zugewiesenen IP-Adressen für Upgrades, die mit vSphere Update Manager durchgeführt werden 181
- Medienoptionen für das Starten des ESXi-Installationsprogramms 181
 - Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD 182
 - Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades 182
 - Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts 184
 - Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript 186
 - Starten des ESXi-Installationsprogramms per PXE-Startvorgang 187
 - Installieren und Starten von ESXi mit Software FCoE 197
- Verwenden von Anwendungen für die Remoteverwaltung 197
- Herunterladen des ESXi-Installationsprogramms 197

9 Upgrade der Hosts wird durchgeführt 198

- Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades 198
 - Konfigurieren von Host- und Clustereinstellungen 199
 - Durchführen eines koordinierten Upgrades von Hosts mithilfe von vSphere Update Manager 201
- Installieren oder Upgraden von Hosts mithilfe eines Skripts 221
 - Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts 222
 - Startoptionen 223
 - Grundlegendes zu Installations- und Upgrade-Skripts 224
 - Installieren oder Durchführen eines Upgrades von ESXi von einer CD oder DVD mithilfe eines Skripts 236
 - Installieren oder Durchführen eines Upgrades von ESXi von einem USB-Flash-Laufwerk mithilfe eines Skripts 237
 - Ausführen einer Skriptinstallation oder eines Upgrades von ESXi durch Starten des Installationsprogramms per PXE-Startvorgang 239
- Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts 239
 - Erneute Bereitstellung von Hosts 240
 - Erneute Bereitstellung von Hosts mit einfachen Neustartvorgängen 240
 - Erneutes Bereitstellen eines Hosts mit einem neuen Image-Profil 241
 - Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts 242
 - Testen und Reparieren der Regelübereinstimmung 243
- Aktualisieren von Hosts mithilfe von esxcli-Befehlen 245
 - VIBs, Image-Profile und Software-Depots 245
 - Grundlegende Informationen zu Akzeptanzebenen für VIBs und Hosts 246

Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss.	249
Versetzen eines Hosts in den Wartungsmodus	250
Aktualisieren eines Hosts mit individuellen VIBs	251
Upgrade oder Update eines Hosts mit Image-Profilen	253
Aktualisieren von ESXi-Hosts mit ZIP-Dateien	256
Entfernen von VIBs von einem Host	257
Hinzufügen von Erweiterungen von Drittanbietern zu Hosts mit einem esxcli-Befehl	259
Durchführen einer esxcli-Testinstallation oder eines esxcli-Test-Upgrades	259
Anzeigen der installierten VIBs und Profile, die nach dem nächsten Hostneustart aktiv werden	260
Anzeigen des Image-Profiles und der Akzeptanzebene des Hosts	260
Interaktives Upgrade von Hosts	261

10 Nach dem Upgrade von ESXi-Hosts 263

Grundlegendes zum ESXi-Testmodus und -Lizenzmodus	263
Anwenden von Lizenzen nach einem Upgrade auf ESXi 6.0	264
Erforderlicher freier Speicherplatz für die Systemprotokollierung	264
Konfiguration von Syslog auf ESXi-Hosts	265

11 Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools 267

12 Fehlerbehebung eines vSphere-Upgrades 268

Erfassen von Protokollen für die Fehlerbehebung bei einer vCenter Server-Installation oder einem Upgrade	269
Erfassen von Installationsprotokollen mithilfe des Installationsassistenten	269
Manuelles Abrufen der Installationsprotokolle	269
Erfassen von Installationsprotokollen für die vCenter Server Appliance	270
Erfassen der Upgradeprotokolle für die Datenbank	271
Erfassen von Protokollen zur Fehlerbehebung bei ESXi-Hosts	271
Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden	272
Wiederherstellen von vCenter Server-Diensten bei einem fehlgeschlagenen Upgrade	275
Fehler bei VMware Component Manager während des Starts nach dem Upgrade von vCenter Server Appliance	275
Eine Microsoft SQL-Datenbank, bei der ein nicht unterstützter Kompatibilitätsmodus festgelegt ist, sorgt dafür, dass das Installieren oder das Upgrade von vCenter Server fehlschlägt	276

Grundlegende Informationen zum vSphere-Upgrade

vSphere-Upgrade beschreibt, wie Sie ein Upgrade von VMware vSphere™ auf die aktuelle Version durchführen.

Informationen zur Umstellung auf die aktuelle vSphere-Version mithilfe einer Neuinstallation, bei der die bestehenden Konfigurationen nicht übernommen werden, finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.

Zielgruppe

vSphere-Upgrade ist für alle bestimmt, die ein Upgrade von früheren vSphere-Versionen vornehmen. Diese Themen sind für erfahrene Microsoft Windows- oder Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datencentervorgängen vertraut sind.

Aktualisierte Informationen

Dieses Handbuch zum *vSphere-Upgrade* wird mit jeder Version des Produkts oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für das *vSphere-Upgrade-Handbuch*.

Revision	Beschreibung
2. APR 2021	VMware hat das My VMware-Portal in „VMware Customer Connect“ umbenannt. Die Dokumentation <i>vSphere-Upgrade</i> wurde aktualisiert, um diese Namensänderung zu berücksichtigen.
11. August 2020	Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip in unserer Kunden-, Partner- und internen Community zu fördern, ersetzen einen Teil der Terminologie in unseren Inhalten. Wir haben diesen Leitfaden aktualisiert, um Instanzen einer nicht inklusiven Sprache zu entfernen.
DE-001989-08	Port 5480 wurde im Abschnitt Erforderliche Ports für vCenter Server und Platform Services Controller hinzugefügt.
DE-001989-07	UDP wurde aus Port 22 im Abschnitt Erforderliche Ports für vCenter Server und Platform Services Controller entfernt.
DE-001989-06	<ul style="list-style-type: none">■ Die Informationen zu Port 514 wurden unter Erforderliche Ports für vCenter Server und Platform Services Controller aktualisiert.■ Das Thema Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades wurde aktualisiert, um die nicht erforderliche Speicherplatzanforderung „/boot partition“ zu entfernen.
DE-001989-05	<ul style="list-style-type: none">■ Der Abschnitt Grundlegende Informationen zur Datei „boot.cfg“ wurde aktualisiert. Es wurde ein Verweis auf ein Beispiel hinzugefügt.■ In TCP- und UDP-Ports für den vSphere Client wurde Port 903 entfernt.■ Neuverweisen von vCenter Server auf einen anderen externen Platform Services Controller wurde aktualisiert, um die Informationen im Zusammenhang mit dem Aufgabenkontext und den Voraussetzungen zu optimieren.
DE-001989-04	<ul style="list-style-type: none">■ Hardwareanforderungen für vCenter Server für Windows und Hardwareanforderungen für vCenter Server Appliance wurden aktualisiert und besagen nun, dass die Hardwareanforderungen für vCenter Server mit einem eingebetteten Platform Services Controller und vCenter Server mit einem externen Platform Services Controller dieselben sind.■ Neukonfigurieren aller vCenter Server-Instanzen und Neuverweisen von einer eingebetteten auf eine externe Platform Services Controller-Instanz wurde aktualisiert, und es wurde ein Schritt zum Erstellen einer direkten Replizierungsvereinbarung, sofern nicht vorhanden, zwischen den eingebetteten und den externen Platform Services Controller-Instanzen hinzugefügt.

Revision	Beschreibung
DE-001989-03	<ul style="list-style-type: none"> ■ In Erforderliche Ports für vCenter Server und Platform Services Controller wurden die Informationen zu Port 22 aktualisiert. ■ Die Themen Upgrade von vCenter Server Appliance mit eingebetteter vCenter Single Sign-On-Instanz und Upgrade von vCenter Server Appliance mit externer vCenter Single Sign-On-Instanz enthalten nun Voraussetzungen für die Ports, die während des Upgrade-Vorgangs der Appliance offen sein müssen. ■ Installieren des Client-Integrations-Plug-Ins wurde aktualisiert, um die Informationen zum Speicherort der ausführbaren Datei zu verbessern. ■ In Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades wurden die Voraussetzungen und Schritte aktualisiert.
DE-001989-02	<ul style="list-style-type: none"> ■ In Erforderliche Ports für vCenter Server und Platform Services Controller wurden die Informationen zu den Ports 389, 636, 11711 und 11712 aktualisiert. ■ In Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript und Startoptionen wurden kleine Überarbeitungen der Beispiele durchgeführt.
DE-001989-01	<ul style="list-style-type: none"> ■ Die Informationen zur Anzahl der vCenter Server-Instanzen in Auswirkungen von vCenter Single Sign On auf Upgrades wurden aktualisiert. ■ Das Thema Neukonfigurieren einer eigenständigen vCenter Server-Instanz mit einem eingebetteten Platform Services Controller auf eine vCenter Server-Instanz mit einem externen Platform Services Controller wurde aktualisiert, und das Thema Neukonfigurieren mehrerer beigetretener Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller auf vCenter Server mit einem externen Platform Services Controller wurde hinzugefügt, um die Informationen zum Neukonfigurieren eines eigenständigen Instanz und mehreren Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller zu verbessern. ■ Das Thema Konfigurieren von VMware vCenter Server - tc Server-Einstellungen im vCenter Server wurde aktualisiert, um den APJ-Port 8009 zu entfernen, welcher nicht mehr benötigt wird.
DE-001989-00	Erstversion.

Einführung in das vSphere-Upgrade

1

In vSphere 6.0 gibt es viele Möglichkeiten für das Upgrade Ihrer vSphere-Bereitstellung. Für ein erfolgreiches Upgrade von vSphere müssen Sie sich mit den Upgrade-Optionen, den Konfigurationsdetails, die den Upgrade-Vorgang beeinflussen, sowie mit der Abfolge der Schritte auskennen.

Die zwei Hauptkomponenten von vSphere sind VMware ESXi™ und VMware vCenter Server™. {ESXi ist die Virtualisierungsplattform, auf der virtuelle Maschinen erstellt und ausgeführt werden. vCenter Server ist ein Dienst, der als zentraler Administrator für ESXi-Hosts agiert, die in einem Netzwerk verbunden sind. Das vCenter Server-System ermöglicht Ihnen den Zusammenschluss und die Verwaltung der Ressourcen von mehreren Hosts.

Sie können ein Upgrade des vCenter Server-Systems auf einer Windows-VM oder einem physischen Server vornehmen oder aber vCenter Server Appliance upgraden. vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung des vCenter Server-Systems und der vCenter Server-Komponenten optimiert ist.

Ab vSphere 6.0 sind alle zum Ausführen von vCenter Server und vCenter Server-Komponenten erforderlichen Dienste in Form von Platform Services Controller zusammengefasst. In Abhängigkeit von den Details Ihrer vorhandenen vCenter Server-Konfiguration können Sie ein Upgrade auf das vCenter Server-System mit einem eingebetteten oder externen Platform Services Controller durchführen. Weitere Informationen zu den Upgrade-Optionen für vCenter Server 6.0 finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#) und [Informationen zum Upgrade-Vorgang von vCenter Server Appliance](#).

Informationen zur Unterstützung des ESXi-Upgrades finden Sie unter [Upgrade-Optionen für ESXi 6.0](#).

Bei einem Upgrade auf vSphere 6.0 müssen Sie alle Schritte in der angegebenen Reihenfolge ausführen, um Datenverlust zu vermeiden und Ausfallzeiten auf ein Minimum zu reduzieren. Sie können den Upgrade-Vorgang für jede Komponente nur in eine Richtung durchführen. Beispielsweise können Sie nach einem Upgrade auf vCenter Server 6.0 nicht zu vCenter Server 5.x zurückkehren. Mit Sicherungen und etwas Planung können Sie jedoch Ihre ursprünglichen Softwaredatensätze wiederherstellen. Informationen zur allgemeinen Abfolge des vSphere-Upgrades finden Sie unter [vSphere-Upgrade-Vorgang](#).

Dieses Kapitel enthält die folgenden Themen:

- [vCenter Server-Komponenten und -Dienste](#)

- Unterschiede zwischen vSphere 6.0 und vSphere 5.x
- Bereitstellungsmodelle für vCenter Server
- vSphere-Upgrade-Vorgang
- Auswirkungen von vCenter Single Sign On auf Upgrades
- Übersicht über vSphere-Sicherheitszertifikate
- Erweiterter verknüpfter Modus – Überblick
- Beispiele von Upgrade-Pfaden für vCenter Server

vCenter Server-Komponenten und -Dienste

vCenter Server bietet eine zentrale Plattform, um virtuelle Maschinen und Hosts zu verwalten und zu betreiben, um Ressourcen für sie bereitzustellen und ihre Leistung zu bewerten.

Wenn Sie auf vCenter Server mit einem eingebetteten Platform Services Controller oder auf die vCenter Server Appliance mit einem eingebetteten Platform Services Controller aktualisieren, werden vCenter Server, die vCenter Server-Komponenten und die beim Platform Services Controller enthaltenen Dienste auf demselben System bereitgestellt.

Wenn Sie auf vCenter Server mit einem externen Platform Services Controller aktualisieren oder die vCenter Server Appliance mit einem externen Platform Services Controller bereitstellen, werden vCenter Server und die vCenter Server-Komponenten auf einem bestimmten System und die beim Platform Services Controller enthaltenen Dienste auf einem anderen System bereitgestellt.

Die folgenden Komponenten sind in den Installationen von vCenter Server und vCenter Server Appliance enthalten:

- Die VMware Platform Services Controller-Gruppe von Infrastrukturdiensten beinhaltet vCenter Single Sign On, Lizenzdienst, Lookup Service und die VMware-Zertifizierungsstelle.
- Die vCenter Server-Gruppe von Diensten beinhaltet vCenter Server, vSphere Web Client, Inventory Service, vSphere Auto Deploy, vSphere ESXi Dump Collector, VMware vSphere Syslog Collector unter Windows und den VMware Syslog-Dienst für die vCenter Server Appliance.

Mit VMware Platform Services Controller installierte Dienste

vCenter Single Sign On

Der vCenter Single Sign On-Authentifizierungsdienst bietet sichere Authentifizierungsdienste für die vSphere-Softwarekomponenten. Bei Verwendung von vCenter Single Sign On kommunizieren die vSphere-Softwarekomponenten über einen sicheren Token-Austauschmechanismus miteinander, anstatt dass jede Komponente einen Benutzer über einen Verzeichnisdienst wie Active Directory separat authentifizieren muss. vCenter Single Sign On erstellt eine interne Sicherheitsdomäne (zum Beispiel „vsphere.local“), in der die vSphere-Lösungen und -Komponenten bei der Installation oder beim Upgrade registriert

werden, wodurch eine Infrastrukturressource bereitgestellt wird. vCenter Single Sign On kann Benutzer über seine eigenen internen Benutzer und Gruppen authentifizieren oder eine Verbindung mit vertrauenswürdigen externen Verzeichnisdiensten wie Microsoft Active Directory herstellen. Authentifizierten Benutzern können dann registrierte lösungsbasierte Berechtigungen oder Rollen in einer vSphere-Umgebung zugewiesen werden.

vCenter Single Sign On ist für vCenter Server 5.1.x und höher verfügbar und erforderlich.

vSphere-Lizenzdienst

Der vSphere-Lizenzdienst stellt übliche Lizenzbestands- und -verwaltungsfunktionen für alle vCenter Server-Systeme bereit, die mit einem Platform Services Controller bzw. mehreren miteinander verknüpften Platform Services Controller-Instanzen verbunden sind.

VMware-Zertifizierungsstelle

Die VMware-Zertifizierungsstelle (VMCA) stellt für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Diese Bereitstellung findet statt, wenn der ESXi-Host explizit oder im Zuge der Installation des ESXi-Hosts zu vCenter Server hinzugefügt wird. Alle ESXi-Zertifikate werden lokal auf dem Host gespeichert.

Mit vCenter Server installierte Dienste

Diese zusätzlichen Komponenten werden bei der Installation von vCenter Server automatisch installiert. Die Komponenten können nicht separat installiert werden, weil es keine eigenen Installationsprogramme dafür gibt.

vCenter Inventory Service

Inventory Service speichert vCenter Server-Konfigurations- und Bestandslistendaten. Somit können Sie Bestandslistenobjekte in vCenter Server-Instanzen durchsuchen und auf sie zugreifen.

PostgreSQL

Eine gebündelte Version der VMware-Verteilung der PostgreSQL-Datenbank für vSphere und vCloud Hybrid-Dienste.

vSphere Web Client

Über den vSphere Web Client können Sie mithilfe eines Webbrowsers eine Verbindung mit vCenter Server-Instanzen herstellen, um Ihre vSphere-Infrastruktur zu verwalten.

vSphere ESXi Dump Collector

Das vCenter Server-Support-Tool. ESXi kann so konfiguriert werden, dass der VMkernel-Arbeitsspeicher auf einem Netzwerkspeicher anstatt einer Festplatte gespeichert wird, wenn ein kritischer Fehler im System auftritt. Der vSphere ESXi-Dump Collector sammelt solche Speicher-Dumps im Netzwerk.

VMware vSphere Syslog Collector

Das Support-Tool von vCenter Server unter Windows, das die Netzwerkprotokollierung aktiviert und die Protokolle von mehreren Hosts kombiniert. Sie können mit dem vSphere Syslog Collector ESXi-Systemprotokolle an einen Server im Netzwerk statt an eine lokale Festplatte weiterleiten. Die empfohlene maximale Anzahl unterstützter Hosts, von denen Protokolle erfasst werden, beträgt 30. Informationen zum Konfigurieren von vSphere Syslog Collector finden Sie unter <http://kb.vmware.com/kb/2021652>.

VMware Syslog-Dienst

Das Support-Tool von vCenter Server Appliance, das eine einheitliche Architektur für die Systemprotokollierung, die Netzwerkprotokollierung und das Erfassen von Protokollen von mehreren Hosts bietet. Sie können mit dem VMware Syslog-Dienst ESXi-Systemprotokolle an einen Server im Netzwerk statt an eine lokale Festplatte weiterleiten. Die empfohlene maximale Anzahl unterstützter Hosts, von denen Protokolle erfasst werden, beträgt 30. Informationen zum Konfigurieren des VMware Syslog-Diensts finden Sie unter *vCenter Server Appliance-Konfiguration*.

vSphere Auto Deploy

Das vCenter Server-Support-Tool, das Hunderte von physischen Hosts mit ESXi-Software bereitstellen kann. Sie können angeben, welches Image bereitgestellt werden soll und welche Hosts mit dem Image bereitgestellt werden sollen. Optional können Sie die Hostprofile, die auf die Hosts angewendet werden sollen, und einen vCenter Server-Speicherort (Ordner oder Cluster) für jeden Host angeben.

Unterschiede zwischen vSphere 6.0 und vSphere 5.x

Einige Änderungen von vSphere 5.x zu vSphere 6.0 haben Auswirkungen auf den Upgrade-Vorgang für vCenter Server. Eine vollständige Aufstellung der neuen Funktionen in vSphere 6.0 finden Sie in den Versionshinweisen für Version 6.0.

Einführung in den VMware Platform Services Controller

Der VMware Platform Services Controller enthält gemeinsam genutzte Infrastrukturdienste wie etwa vCenter Single Sign-On, VMware Certificate Authority

Sie können eine Platform Services Controller-Instanz auf derselben virtuellen Maschine (VM) bzw. demselben physischen Server wie vCenter Server bereitstellen, wobei es sich um vCenter Server mit einer eingebetteten Platform Services Controller-Instanz handelt. Darüber hinaus können Sie eine Platform Services Controller-Instanz auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server bereitstellen, wobei es sich um vCenter Server mit einer externen Platform Services Controller-Instanz handelt. Weitere Informationen hierzu finden Sie unter [Bereitstellungsmodelle für vCenter Server](#).

Erweiterter verknüpfter Modus

Der verknüpfte Modus wird ab vSphere 6.0 unterschiedlich implementiert. Sie müssen vCenter Server-Instanzen nicht mehr zu Gruppen im verknüpften Modus hinzufügen. Sie haben Zugriff auf die Replizierungsfunktionalität des verknüpften Modus in vSphere 5.5,

indem Sie mehrere vCenter Server-Instanzen für denselben Platform Services Controller registrieren oder Platform Services Controller-Instanzen derselben vCenter Single Sign-On-Domäne hinzufügen.

Um High Availability zwischen den vCenter Server-Instanzen in einer einzelnen vCenter Single Sign-On-Domäne zu ermöglichen, müssen die vCenter Server-Instanzen denselben Site-Namen verwenden.

Im Gegensatz zum ursprünglichen verknüpften Modus wird der erweiterte verknüpfte Modus sowohl für vCenter Server unter Windows als auch vCenter Server Appliance zur Verfügung gestellt und unterstützt.

Bereitstellung der vCenter Server-Komponentendienste

Ab vSphere 6.0 werden vCenter Server-Komponentendienste in der vCenter Server- oder der Platform Services Controller-Dienstgruppe bereitgestellt. Bei gemeinsam genutzten vSphere-Diensten ist für vCenter Server 6.0 kein separates Upgrade mehr möglich.

Die vCenter Server-Upgrade-Software übernimmt bei Bedarf die Migration, das Upgrade und die Konfiguration vorhandener vCenter Server 5.1- oder vCenter Server 5.5-Dienste, wobei einzeln bereitgestellte vCenter Server 5.0- oder vCenter Server 5.1-Dienste während des Upgrades zur entsprechenden Dienstgruppe migriert werden.

- Anmeldedaten, Zertifikate und Ports für vCenter Single Sign-On sind nun Bestandteil der Platform Services Controller-Instanz.
- Tagging-Daten und Lizenzen sind Bestandteil der Platform Services Controller-Instanz.
- Andere Dienste sind Bestandteil der vCenter Server-Instanz. Weitere Informationen finden Sie unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#).
- Nun können Sie den zu verwendenden Zielordner für die Upgrade-Software auswählen.

Weitere Informationen zur Bereitstellung von Diensten finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#).

Ersetzung des einfachen Upgrade-Prozesses

Das Upgrade auf vCenter Server 6.0 mit einer eingebetteten Platform Services Controller-Instanz ersetzt den einfachen Upgrade-Vorgang von vCenter Server 5.1 oder vCenter Server 5.5. Beim Upgrade-Vorgang werden Ihre vCenter Server 5.1- oder vCenter Server 5.5-Dienste zu einer vCenter Server 6.0-Bereitstellung mit einer eingebetteten Platform Services Controller-Instanz migriert.

Ersetzung des benutzerdefinierten Upgrade-Prozesses

Das Upgrade auf vCenter Server 6.0 mit einer externen Platform Services Controller-Instanz ersetzt den benutzerdefinierten oder separaten Upgrade-Vorgang von vCenter Server 5.1 oder 5.5. Beim Upgrade Ihrer benutzerdefinierten oder verteilten vCenter Server 5.1- oder 5.5-Instanz werden alle vCenter Server 5.1- oder 5.5-Dienste, die separat von vCenter Server

bereitgestellt wurden, in den Upgrade-Vorgang einbezogen. Für diese Dienste muss kein separates Upgrade durchgeführt werden.

Während des Upgrades auf vCenter Server 6.0 mit einer externen Platform Services Controller-Bereitstellung werden alle vCenter Server 5.1- oder 5.5-Dienste, die auf einer anderen VM oder einem anderen physischen Server als vCenter Server bereitgestellt wurden, auf dieselbe VM oder denselben physischen Server wie die vCenter Server-Instanz migriert. vCenter Server-Komponenten können nicht mehr einzeln bereitgestellt werden. Weitere Informationen zur Migration von Diensten während des Upgrades finden Sie unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#).

Keine Änderung des Bereitstellungsmodells für Platform Services Controller während des Upgrades

Während des Upgrades auf vCenter Server 6.0 kann das Bereitstellungsmodell nicht geändert werden. Wenn Sie beispielsweise vCenter Server mit einer eingebetteten Platform Services Controller-Instanz bereitstellen, können Sie nicht auf vCenter Server mit einer externen Platform Services Controller-Instanz umstellen. Sie können nur die Platform Services Controller-Instanz entfernen.

Nach dem Upgrade können Sie Ihre Bereitstellung von vCenter Server aktualisieren, indem Sie erneut auf die Verbindungen zwischen vCenter Server und Platform Services Controller verweisen. Darüber hinaus können Sie eine eingebettete Bereitstellung von Platform Services Controller in eine externe Bereitstellung von Platform Services Controller konvertieren.

Datenbankänderungen

Die eingebettete Microsoft SQL Server Express-Datenbank von vCenter Server 5.x wird beim Upgrade auf vCenter Server 6.0 durch eine eingebettete PostgreSQL-Datenbank ersetzt. Die maximale Bestandsgröße, die für Microsoft SQL Server Express galt, gilt auch für PostgreSQL.

VMware vSphere Syslog Collector

Für vCenter Server 6.0 für Windows ist vSphere Syslog Collector in der vCenter Server-Dienstgruppe enthalten. Die Funktionsweise ist gegenüber vCenter Server 5.5 unverändert. Sie wird jedoch nicht mehr für vCenter Server Appliance 6.0 verwendet.

VMware Syslog-Dienst

Für vCenter Server Appliance 6.0 handelt es sich beim vSphere Syslog-Dienst um ein Support-Tool für die Protokollierung, das in der vCenter Server-Dienstgruppe enthalten ist. Siehe [vCenter Server-Komponenten und -Dienste](#).

Bereitstellungsmodelle für vCenter Server

Sie können vCenter Server auf einer virtuellen Maschine oder einem physischen Server unter Microsoft Windows Server 2008 SP2 oder höher installieren oder die vCenter Server Appliance

bereitstellen. Die vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist.

vSphere 6.0 führt vCenter Server mit einem eingebetteten Platform Services Controller und vCenter Server mit einem externen Platform Services Controller ein.

Wichtig Diese Dokumentation enthält Informationen zu den grundlegenden Bereitstellungsmodellen. Informationen zu den empfohlenen Topologien finden Sie unter [Aufstellung der empfohlenen Topologien für vSphere 6.0.x](#).

vCenter Server mit einem eingebetteten Platform Services Controller

Alle mit dem Platform Services Controller gebündelten Dienste werden auf derselben virtuellen Maschine oder demselben physischen Server wie vCenter Server bereitgestellt.

vCenter Server mit einem externen Platform Services Controller

Die mit dem Platform Services Controller und vCenter Server gebündelten Dienste werden auf verschiedenen virtuellen Maschinen oder physischen Servern bereitgestellt.

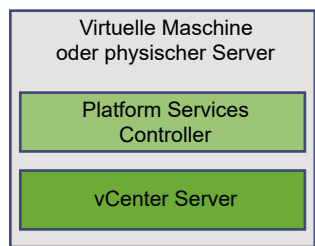
Sie müssen zuerst den Platform Services Controller auf einer virtuellen Maschine bzw. einem physischen Server und anschließend vCenter Server auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server bereitstellen.

Hinweis Nach der Bereitstellung von vCenter Server mit eingebettetem Platform Services Controller können Sie Ihre Topologie neu konfigurieren und auf vCenter Server mit externem Platform Services Controller umstellen. Dieser Vorgang ist unumkehrbar und Sie können nicht wieder auf vCenter Server mit eingebettetem Platform Services Controller zurücksetzen. Die vCenter Server-Instanz können Sie nur auf einen externen Platform Services Controller neu verweisen, für den die Replizierung der Infrastrukturdaten innerhalb derselben Domäne konfiguriert ist.

vCenter Server mit einem eingebetteten Platform Services Controller

vCenter Server und der Platform Services Controller werden auf einer einzelnen virtuellen Maschine bzw. einem einzelnen physischen Server bereitgestellt.

Abbildung 1-1. vCenter Server mit eingebettetem Platform Services Controller



Das Installieren von vCenter Server mit einem eingebetteten Platform Services Controller hat die folgenden Vorteile:

- Die Verbindung zwischen vCenter Server und dem Platform Services Controller erfolgt nicht über das Netzwerk und vCenter Server ist nicht für Ausfälle wegen Verbindungs- und Namensauflösungsproblemen zwischen vCenter Server und dem Platform Services Controller anfällig.
- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie weniger Windows-Lizenzen.
- Sie brauchen weniger virtuelle Maschinen oder physische Server zu verwalten.
- Sie benötigen keinen Lastausgleichsdienst zum Verteilen der Last auf dem Platform Services Controller.

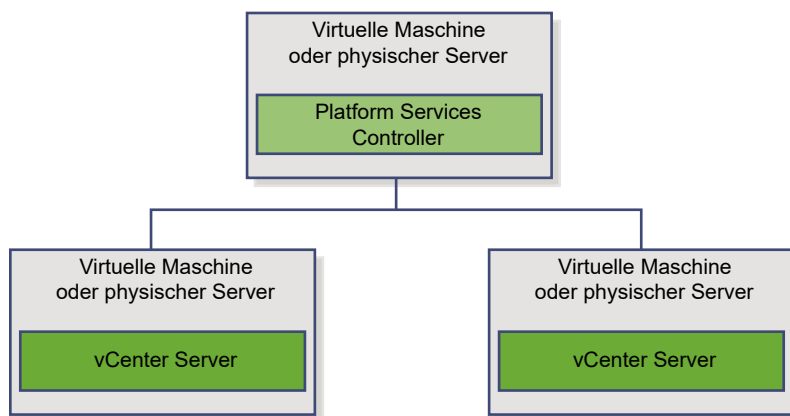
Die Installation mit einem eingebetteten Platform Services Controller hat die folgenden Nachteile:

- Es gibt einen Platform Services Controller für jedes Produkt, also möglicherweise mehr, als erforderlich sind. Dadurch werden mehr Ressourcen verbraucht.
- Das Modell ist für kleinere Umgebungen geeignet.

vCenter Server mit einem externen Platform Services Controller

vCenter Server und der Platform Services Controller werden auf einer separaten virtuellen Maschine bzw. einem separaten physischen Server bereitgestellt. Der Platform Services Controller kann in mehreren vCenter Server-Instanzen gleichzeitig verwendet werden. Sie können einen Platform Services Controller und dann mehrere vCenter Server-Instanzen installieren und diese dann beim Platform Services Controller registrieren. Sie können dann einen anderen Platform Services Controller installieren, ihn so konfigurieren, dass Daten vom ersten Platform Services Controller repliziert werden, und dann vCenter Server-Instanzen installieren und diese beim zweiten Platform Services Controller registrieren.

Abbildung 1-2. vCenter Server mit einem externen Platform Services Controller



Die Installation von vCenter Server mit einem externen Platform Services Controller hat die folgenden Vorteile:

- Ein geringerer Ressourcenverbrauch durch die kombinierten Dienste in den Platform Services Controller-Instanzen verringert den Speicherplatz- und Wartungsbedarf.
- Ihre Umgebung kann aus mehr vCenter Server-Instanzen bestehen.

Die Installation von vCenter Server mit einem externen Platform Services Controller hat die folgenden Nachteile:

- Die Verbindung zwischen vCenter Server und dem Platform Services Controller erfolgt über das Netzwerk und ist für Verbindungs- und Namensauflösungsprobleme anfällig.
- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie mehr Microsoft Windows-Lizenzen.
- Sie müssen mehr virtuelle Maschinen oder physische Server verwalten.

Umgebung mit gemischten Betriebssystemen

Eine unter Windows installierte vCenter Server-Instanz kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Eine vCenter Server Appliance kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Sowohl vCenter Server als auch die vCenter Server Appliance können bei demselben Platform Services Controller innerhalb einer Domäne registriert werden.

Abbildung 1-3. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einem externen Platform Services Controller unter Windows

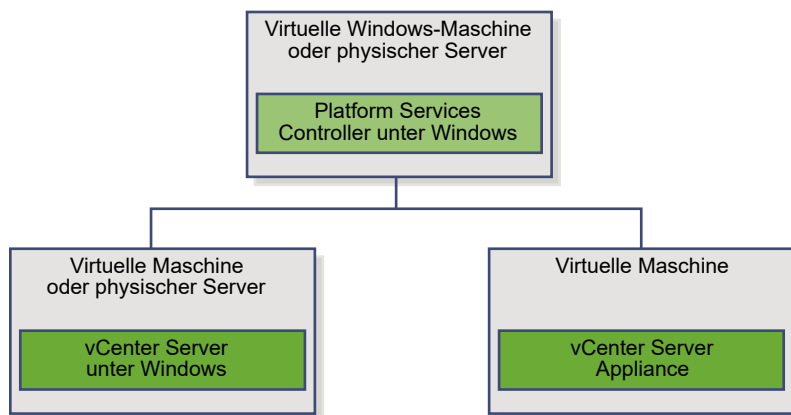
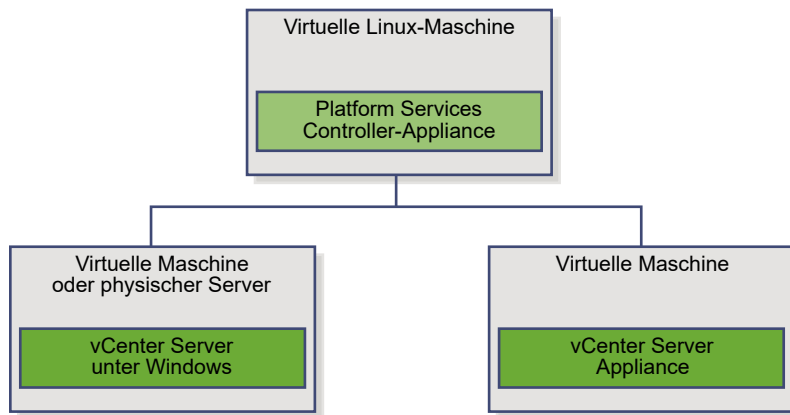


Abbildung 1-4. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einer externen Platform Services Controller-Appliance



Mit vielen Platform Services Controller-Instanzen, die ihre Infrastrukturdaten replizieren, können Sie die Hochverfügbarkeit Ihres Systems sicherstellen.

Wenn ein externer Platform Services Controller, bei dem Ihre vCenter Server-Instanz oder vCenter Server Appliance anfangs registriert wurde, nicht mehr antwortet, können Sie Ihren vCenter Server oder die vCenter Server Appliance neu auf einen anderen externen Platform Services Controller in der Domäne verweisen. Weitere Informationen finden Sie unter [Neuverweisen von vCenter Server auf einen anderen externen Platform Services Controller](#).

vSphere-Upgrade-Vorgang

vSphere ist ein ausgereiftes Produkt mit mehreren Komponenten, für die ein Upgrade durchgeführt werden muss. Für ein erfolgreiches vSphere-Upgrade sollten Sie mit der Abfolge der Arbeitsschritte vertraut sein.

Das Upgrade von vSphere umfasst folgende Aufgaben:

- 1 Lesen Sie die vSphere-Versionshinweise.
- 2 Stellen Sie sicher, dass Ihr System die vSphere-Hardware- und Softwareanforderungen erfüllt. Siehe [Kapitel 2 Upgrade-Anforderungen](#).
- 3 Vergewissern Sie sich, dass Sie Ihre Konfiguration gesichert haben.
- 4 Wenn Ihr vSphere-System VMware-Lösungen oder Plug-Ins enthält, stellen Sie sicher, dass sie zu der Version von vCenter Server oder vCenter Server Appliance, auf die Sie ein Upgrade durchführen, kompatibel sind. Weitere Informationen hierzu finden Sie in der *VMware-Produkt-Interoperabilitätstabelle* unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- 5 Upgrade von vCenter Server.

Sie können vCenter Server-Instanzen mit externen Platform Services Controller-Instanzen im erweiterten verknüpften Modus verbinden.

Wichtig Sie können zwar einer vCenter Single Sign On-Domäne beitreten, aber Sie sollten vCenter Server mit eingebettetem Platform Services Controller als eigenständige Installation in Betracht ziehen und nicht für die Replizierung von Infrastrukturdaten verwenden.

Gleichzeitige Upgrades werden nicht unterstützt und die Upgrade-Reihenfolge spielt eine Rolle. Wenn mehrere vCenter Server-Instanzen oder -Dienste vorhanden sind, die nicht auf demselben physischen Server oder derselben virtuellen Maschine (VM) wie die vCenter Server-Instanz installiert sind, finden Sie weitere Informationen unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#) und [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).

Führen Sie ein Upgrade von vCenter Server auf einer Windows-VM oder einem physischen Server oder ein Upgrade von vCenter Server Appliance durch. Informationen zum Upgrade-Workflow für vCenter Server für Windows finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#). Informationen zum Workflow für vCenter Server Appliance finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server Appliance](#).

- a Stellen Sie sicher, dass Ihr System die Hardware- und Softwareanforderungen für das Upgrade von vCenter Server erfüllt. Siehe [Anforderungen für vCenter Server für Windows](#) oder [Anforderungen für die vCenter Server Appliance](#).
- b Bereiten Sie Ihre Umgebung auf das Upgrade vor. Siehe [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- c Erstellen Sie ein Arbeitsblatt mit den erforderlichen Informationen für das Upgrade. Siehe [Erforderliche Informationen für das Upgrade von vCenter Server für Windows](#) oder [Erforderliche Informationen für das Upgrade der vCenter Server Appliance](#).
- d Upgrade von vCenter Server. Siehe [Kapitel 4 Upgrade und Update von vCenter Server für Windows](#) oder [Kapitel 5 Aktualisieren und Patchen der vCenter Server Appliance und Platform Services Controller-Appliance](#).

Für vCenter Server 5.0 können Sie ein Upgrade auf eine eingebettete oder eine externe Platform Services Controller-Bereitstellung durchführen. Für Upgrades von vCenter Server 5.1 oder 5.5 hängt das Ergebnis der Bereitstellung nach dem Upgrade von der Erstbereitstellung ab. Weitere Informationen zu den Bereitstellungsdetails und deren Auswirkungen auf Upgrades finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#), [Upgrade der vCenter Server Appliance](#), [Patchen der vCenter Server Appliance und Platform Services Controller-Appliance](#) und [Beispiele von Upgrade-Pfaden für vCenter Server](#).

- 6 Führen Sie nach dem Upgrade von vCenter Server die Aufgaben nach dem Upgrade aus. In Abhängigkeit von den Konfigurationsdetails vor dem Upgrade müssen Sie möglicherweise Neukonfigurationsaufgaben ausführen. Siehe [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

- 7 Wenn Sie vSphere Update Manager verwenden, führen Sie ein Upgrade von vSphere Update Manager durch. Siehe [Kapitel 7 Upgrade von Update Manager](#).
- 8 Führen Sie das Upgrade der ESXi-Hosts durch.
 - a Lesen Sie die Best Practices für das Upgrade und stellen Sie sicher, dass Ihr System die Upgrade-Anforderungen erfüllt. Siehe [Empfohlene Vorgehensweisen für Upgrades von ESXi](#) und [Anforderungen für ESXi](#).
 - b Legen Sie die zu verwendende ESXi-Upgrade-Option fest. Siehe [Upgrade-Optionen für ESXi 6.0](#).
 - c Legen Sie den Speicherort und die Startposition des ESXi-Installationsprogramms fest. Siehe [Medienoptionen für das Starten des ESXi-Installationsprogramms](#). Wenn Sie das Installationsprogramm über PXE starten, überprüfen Sie, ob Ihre Netzwerk-PXE-Infrastruktur ordnungsgemäß eingerichtet ist. Siehe [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#).
 - d Führen Sie ein Upgrade von ESXi durch.
 - [Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades](#)
 - [Installieren oder Upgraden von Hosts mithilfe eines Skripts](#)
 - [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#)
 - [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#)
 - [Interaktives Upgrade von Hosts](#)
- 9 Nach dem Upgrade von ESXi-Hosts müssen Sie die Hosts erneut mit vCenter Server verbinden und die Lizenzen erneut anwenden. Siehe [Kapitel 10 Nach dem Upgrade von ESXi-Hosts](#).
- 10 Ziehen Sie es in Erwägung, einen Syslog-Server für die Remoteprotokollierung einzurichten, um ausreichend Speicherplatz für Protokolldateien zu gewährleisten. Die Einrichtung der Protokollierung auf einem Remotehost ist besonders wichtig für Hosts, die über begrenzten lokalen Speicher verfügen. Siehe [Erforderlicher freier Speicherplatz für die Systemprotokollierung](#) und [Konfiguration von Syslog auf ESXi-Hosts](#).
- 11 Führen Sie ein Upgrade Ihrer virtuellen Maschinen und virtuellen Appliances manuell durch oder verwenden Sie vSphere Update Manager für ein koordiniertes Upgrade. Siehe [Kapitel 11 Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools](#).

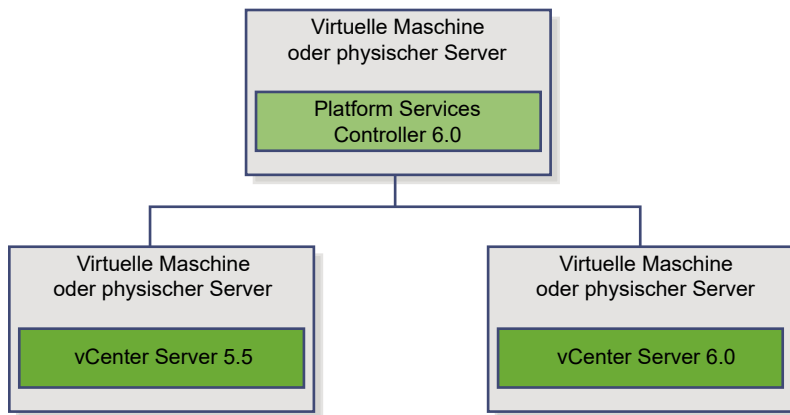
Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades

Sie können für eine vCenter Single Sign-On-Instanz, die auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als vCenter Server bereitgestellt wurde, ein Upgrade auf einen extern bereitgestellten Platform Services Controller 6.0 durchführen, während die vCenter Server-Instanzen, die ihn verwenden, bei Version 5.5 verbleiben.

Wenn Sie für eine extern bereitgestellte vCenter Single Sign-On-Instanz ein Upgrade auf einen extern bereitgestellten Platform Services Controller 6.0 durchführen, sind die vCenter Server 5.5-Instanzen, die die vCenter Single Sign-On-Instanz verwendeten, nicht davon betroffen. Die vCenter Server 5.5-Instanzen verwenden ohne Probleme oder erforderliche Neukonfiguration weiter den aktualisierten Platform Services Controller wie vor dem Upgrade. vCenter Server 5.5-Instanzen sind weiterhin für vSphere Web Client 5.5 sichtbar, obwohl vCenter Server 6.0-Instanzen für vSphere Web Client 5.5 nicht sichtbar sind.

Das Verhalten von im Übergang befindlichen gemischten Versionsumgebungen ist für vCenter Single Sign-On-Instanzen, die in vCenter Server 5.5 für Windows-Umgebungen und in vCenter Server Appliance-Umgebungen bereitgestellt werden, identisch.

Abbildung 1-5. Gemischte Versionsumgebung



Hinweis Gemischte Versionsumgebungen werden für Produktionsumgebungen nicht unterstützt. Sie werden nur für den Zeitraum des Übergangs zwischen vCenter Server-Versionen empfohlen.

Wenn Sie eine externe vCenter Single Sign-On-Instanz und mindestens eine Instanz von vCenter Server auf Version 6.0 aktualisieren, andere Instanzen von vCenter Server aber auf Version 5.5 belassen, führt dies zu folgenden Ergebnissen:

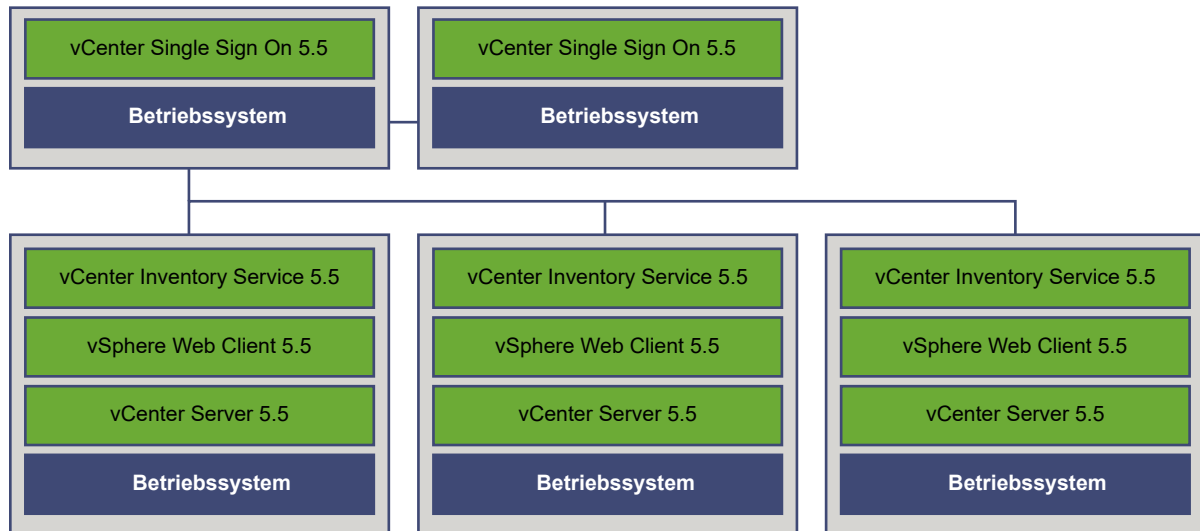
- Der verknüpfte Modus funktioniert nicht mehr.
- vCenter Server 5.5-Instanzen verwenden ohne Probleme oder erforderliche Neukonfiguration weiter den aktualisierten Platform Services Controller wie vor dem Upgrade.
- In einer gemischten vCenter Server-Versionsumgebung mit Version 5.5 und 6.0 zeigt eine vSphere Web Client 6.0-Instanz vCenter Server 5.5-Instanzen.
- vSphere Web Client 5.5 zeigt nur vCenter Server-Instanzen, keine 6.0-Instanzen.

Wenn Sie alle vCenter Server 5.5-Instanzen auf Version 6.0 und die verteilte vCenter Single Sign-On-Instanz auf einen externen Platform Services Controller aktualisieren, ist keine der vCenter Server-Instanzen davon betroffen. Sie verwenden ohne Probleme oder erforderliche Schritte weiter den Platform Services Controller wie vor dem Upgrade.

Der einzige Schritt, der für eine gemischte Umgebung mit Version 5.5 und 6.0 nach dem Upgrade erforderlich ist, ist ein Neustart der vSphere Web Client-Legacy-Instanzen, wenn sie zum Anzeigen von noch nicht aktualisierten vCenter Server 5.5-Instanzen verwendet werden.

Abbildung 1-6. Beispiel für eine Bereitstellung vor Beginn des Upgrades

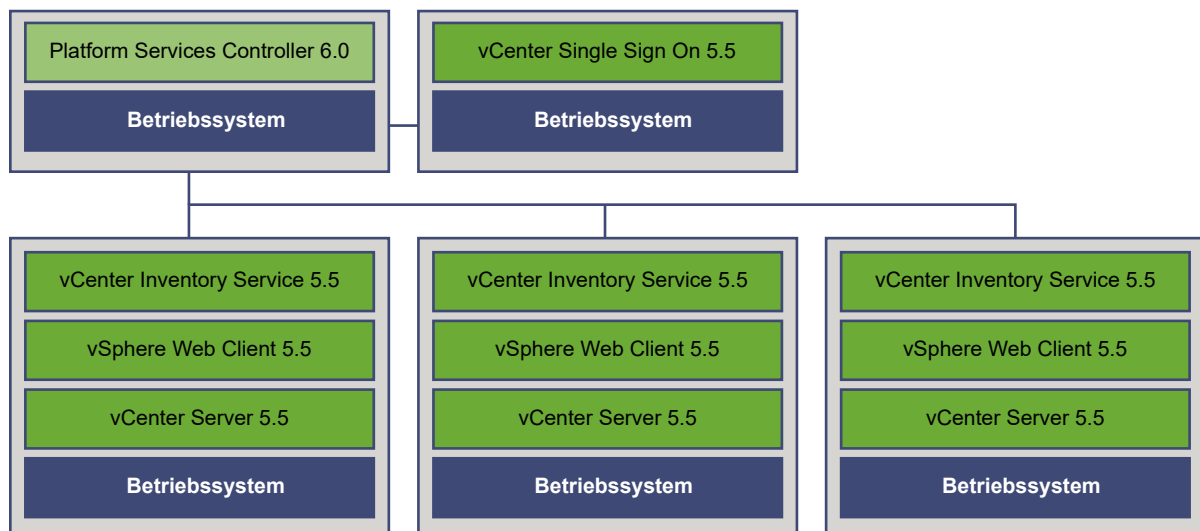
Vorübergehende Upgrade-Umgebung: Ausgangskonfiguration



Beispielsweise muss bei einer Bereitstellung mit drei vCenter Server 5.5-Instanzen und zwei externen vCenter Single Sign-On-Instanzen für jede Instanz einzeln ein Upgrade auf Version 6.0 durchgeführt werden.

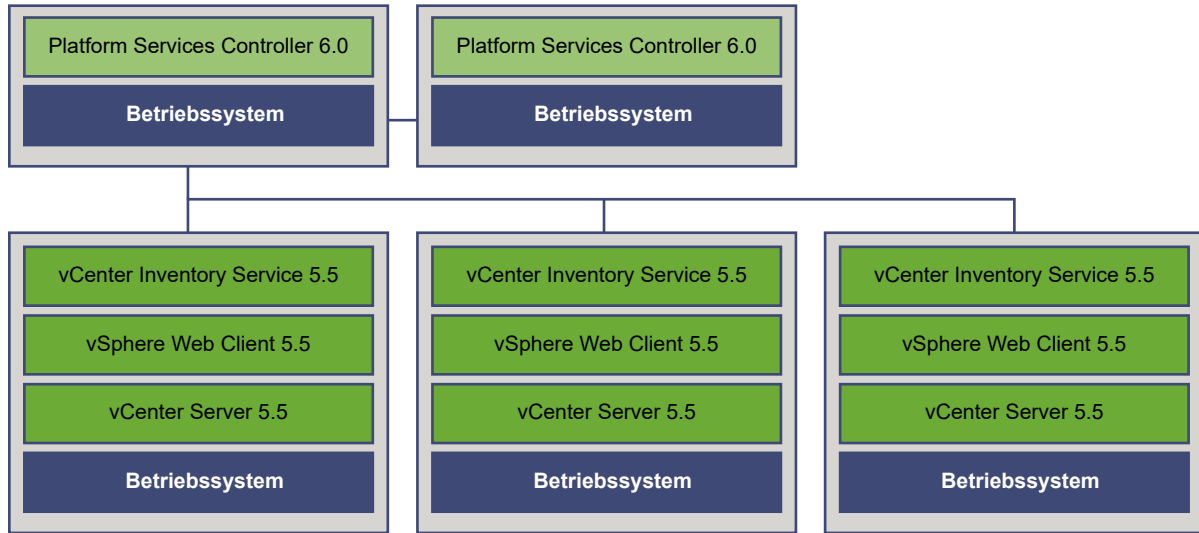
Abbildung 1-7. Beispiel für eine in Schritt 1 des Übergangs befindliche Bereitstellung

Vorübergehende Upgrade-Umgebung: Schritt 1



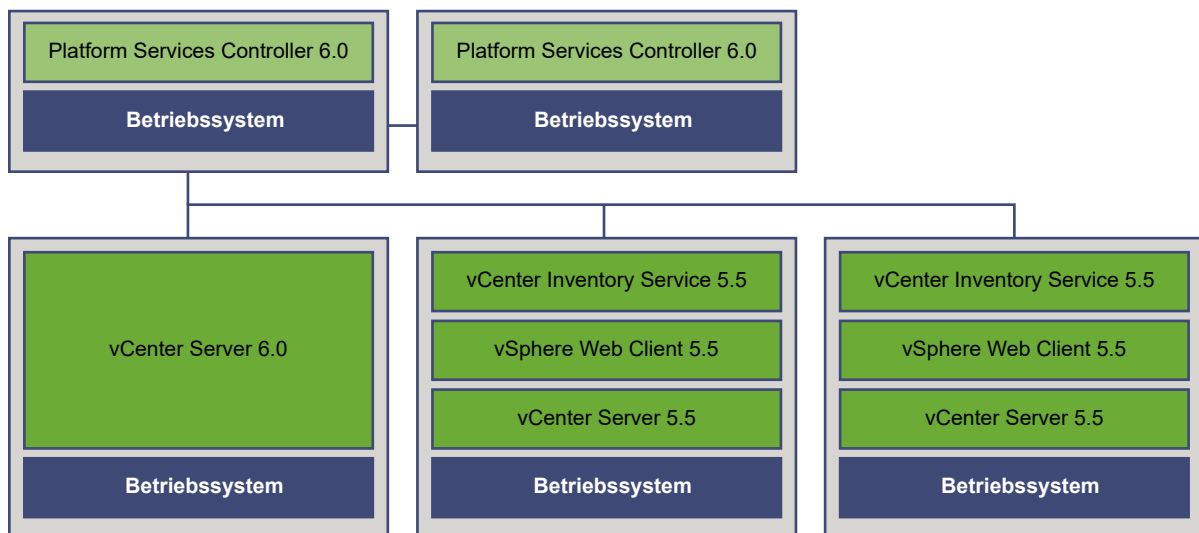
Das Upgrade der ersten externen vCenter Single Sign-On-Instanz auf einen externen Platform Services Controller hat keine Auswirkungen auf die vCenter Server 5.5-Instanzen, außer dass der verknüpfte Modus nicht mehr funktioniert.

Abbildung 1-8. Beispiel für eine in Schritt 2 des Übergangs befindliche Bereitstellung

Vorübergehende Upgrade-Umgebung: Schritt 2

Das Upgrade der zweiten externen vCenter Single Sign-On-Instanz auf einen externen Platform Services Controller hat keine Auswirkungen auf das Verhalten der vCenter Server 5.5-Instanzen.

Abbildung 1-9. Beispiel für eine in Schritt 3 des Übergangs befindliche Bereitstellung

Vorübergehende Upgrade-Umgebung: Schritt 3

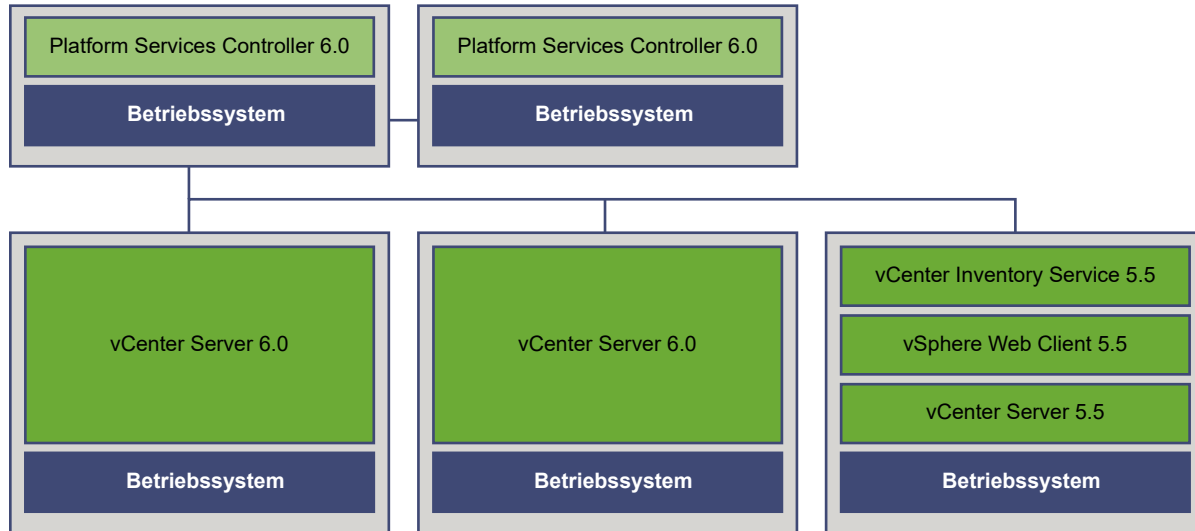
Nach dem Upgrade der ersten vCenter Server-Instanz auf Version 6.0 gibt es Änderungen an der Konnektivität zwischen den vCenter Server-Instanzen.

- Die beiden verbleibenden vSphere Web Client 5.5-Instanzen können die aktualisierte vCenter Server 6.0-Instanz nicht mehr anzeigen, nachdem sie zur Platform Services Controller-Instanz hinzugefügt wurde.
- Die vSphere Web Client 5.5-Instanzen können weiterhin die vCenter Server 5.5-Instanzen anzeigen, nachdem die vSphere Web Client 5.5-Instanzen neu gestartet wurden.

- Die vSphere Web Client 6.0-Instanz, die Bestandteil der aktualisierten vCenter Server 6.0-Instanz ist, kann die vCenter Server 5.5- und vCenter Server 6.0-Instanzen anzeigen.

Abbildung 1-10. Beispiel für eine in Schritt 4 des Übergangs befindliche Bereitstellung

Vorübergehende Upgrade-Umgebung: Schritt 4

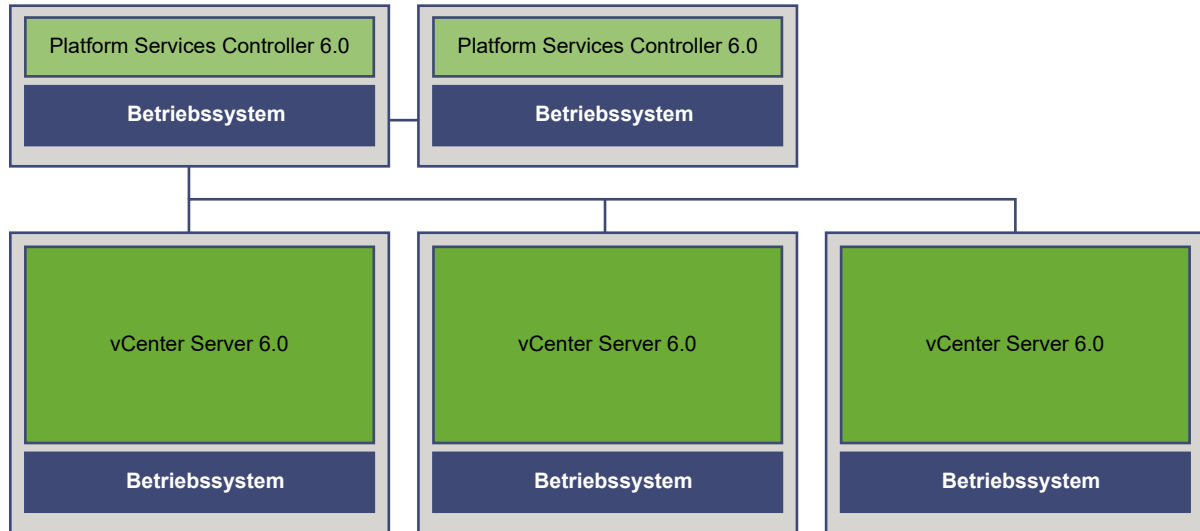


Nach dem Upgrade der zweiten vCenter Server-Instanz auf Version 6.0 gibt es weitere Änderungen an der Konnektivität zwischen den vCenter Server-Instanzen:

- Der verknüpfte Modus wird zwischen den aktualisierten vCenter Server 6.0-Instanzen durch den erweiterten verknüpften Modus ersetzt, nachdem sie zum Plattform Services Controller hinzugefügt wurden.
- Die verbleibende vSphere Web Client 5.5-Instanz kann die vCenter Server 6.0-Instanzen nicht mehr anzeigen.
- Die vSphere Web Client 5.5-Instanz kann weiterhin die vCenter Server 5.5-Instanz anzeigen, nachdem die vSphere Web Client 5.5-Instanz neu gestartet wurden.
- Die vSphere Web Client 6.0-Instanzen, die Bestandteil der aktualisierten vCenter Server 6.0-Instanzen sind, können die vCenter Server 5.5- und vCenter Server 6.0-Instanzen anzeigen.

Abbildung 1-11. Beispiel für eine in Schritt 5 des Übergangs befindliche Bereitstellung mit abgeschlossenem Upgrade

Vorübergehende Upgrade-Umgebung: Schritt 5



Nach dem Upgrade der dritten und letzten vCenter Server-Instanz auf Version 6.0 sind alle vCenter Server-Instanzen mit vCenter Server 6.0-Funktionalität verbunden.

- Der verknüpfte Modus wird zwischen allen vCenter Server 6.0-Instanzen durch den erweiterten verknüpften Modus ersetzt, nachdem sie zum Platform Services Controller hinzugefügt wurden.
- Die vSphere Web Client 6.0-Instanzen können alle vCenter Server 6.0-Instanzen anzeigen.



Im Übergang von vCenter Server 5.5 zu Version 6.0 befindliche Umgebungen (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_orp6ck9v/uiConfId/49694343/)

Upgrade auf den vSphere-Lizenzdienst

In vSphere 5.x befinden sich die Lizenzverwaltungs- und Berichtsfunktionen auf einzelnen vCenter Server-Systemen. In vSphere 6.0 wird der Lizenzdienst eingeführt, der im Platform Services Controller enthalten ist. Der Lizenzdienst stellt übliche Lizenzbestands- und -verwaltungsfunktionen für vCenter Server-Systeme bereit, die bei einem Platform Services Controller bzw. bei mehreren Platform Services Controller in einer gemeinsamen vCenter Single Sign-On-Domäne registriert sind.

Während des Upgrades der vCenter Server-Systeme, die mit einem Platform Services Controller verbunden sind, werden deren Lizenzierungsdaten an den Lizenzdienst übertragen. Zu den Lizenzierungsdaten zählen die verfügbaren Lizenzen und Lizenzzuweisungen für Hosts, vCenter Server-Systeme, Virtual SAN-Cluster und andere, zusammen mit vSphere verwendete Produkte.

Nachdem das Upgrade der vCenter Server-Systeme abgeschlossen ist, werden im Lizenzdienst die verfügbaren Lizenzen gespeichert und die Lizenzzuweisungen für die gesamte vSphere-Umgebung verwaltet. Wenn Ihre vSphere-Umgebung aus mehreren, in einer vCenter Single Sign On-Domäne zusammengefassten Platform Services Controller-Instanzen besteht, enthält der Lizenzdienst in jedem Platform Services Controller ein Replikat der Lizenzierungsdaten für die gesamte Umgebung.

Weitere Informationen zum Lizenzdienst und der Verwaltung von Lizenzen in vSphere finden Sie unter *vCenter Server und Hostverwaltung*.

Unterschiede zwischen vSphere-Upgrades und -Updates

Bei vSphere-Produkten wird zwischen Upgrades, mit denen größere Änderungen an der Software vorgenommen werden, und Updates, mit denen kleinere Änderungen an der Software vorgenommen werden, unterschieden.

VMware-Produktversionen sind mit zwei Ziffern nummeriert, z. B. „vSphere 6.0“. Eine Version, bei der sich die Ziffern ändern, z. B. von 5.5 in 6.0 oder von 5.1 in 5.5, beinhaltet größere Änderungen an der Software und erfordert ein Upgrade der vorherigen Version. Eine Version, die kleinere Änderungen beinhaltet und lediglich ein Update erforderlich macht, wird durch eine Update-Nummer gekennzeichnet, z. B. vSphere 6.0 Update 1.

Wenn Sie ein Upgrade eines ESXi-Hosts vornehmen, werden bestimmte Host-Konfigurationsinformationen in der aktualisierten Version beibehalten. Der aktualisierte Host kann nach dem Neustart einer vCenter Server-Instanz beitreten, die auf dieselbe Stufe aktualisiert wurde. Da Updates und Patches keine größeren Änderungen an der Software umfassen, bleibt die Konfiguration des Hosts davon unberührt. Nähere Informationen finden Sie unter [Upgrade oder Update eines Hosts mit Image-Profilen](#).

Auswirkungen von vCenter Single Sign On auf Upgrades

Wenn Sie ein Upgrade einer einfachen Installationsumgebung (Simple Install) auf eine eingebettete Bereitstellung von vCenter Server 6 durchführen, erfolgt das Upgrade nahtlos. Beim Upgrade einer benutzerdefinierten Installation ist der vCenter Single Sign On-Dienst nach dem Upgrade Bestandteil des Platform Services Controller. Welche Benutzer sich nach der Durchführung eines Upgrades bei vCenter Server anmelden können, hängt von der Version, von der aus Sie das Upgrade durchführen, und von der Bereitstellungskonfiguration ab.

Im Rahmen des Upgrades können Sie festlegen, dass anstelle von „vsphere.local“ ein anderer vCenter Single Sign On-Domänenname verwendet wird.

Upgrade-Pfade

Das Ergebnis des Upgrades ist abhängig von den ausgewählten Installationsoptionen und vom Bereitstellungsmodell, auf das Sie upgraden.

Tabelle 1-1. Upgrade-Pfade

Quelle	Ergebnis
vSphere 5.5 und früher – einfache Installation	vCenter Server mit eingebettetem Platform Services Controller.
vSphere 5.5 und früher – benutzerdefinierte Installation	<p>Wenn sich vCenter Single Sign On auf einem anderen Knoten als vCenter Server befand, erhalten Sie eine Umgebung mit einem externen Platform Services Controller.</p> <p>Wenn sich vCenter Single Sign On auf demselben Knoten wie vCenter Server befand, andere Dienste jedoch auf anderen Knoten, erhalten Sie eine Umgebung mit einem eingebetteten Platform Services Controller.</p> <p>Wenn in der benutzerdefinierten Installation mehrere replizierte vCenter Single Sign On-Server vorhanden waren, erhalten Sie eine Umgebung mit mehreren replizierten Platform Services Controller-Instanzen.</p>

Benutzer, die sich nach dem Upgrade einer einfachen Installation anmelden können

Wenn Sie ein Upgrade einer Umgebung durchführen, die Sie mit der einfachen Installationsoption bereitgestellt haben, erhalten Sie stets eine Installation mit einem eingebetteten Platform Services Controller. Welche Benutzer sich anmelden dürfen, hängt davon ab, ob in der Quellumgebung vCenter Single Sign On vorhanden ist.

Tabelle 1-2. Anmelderechte nach dem Upgrade der einfachen Installationsumgebung

Quellversion	Anmeldezugriff für	Notizen
vSphere 5.0	Benutzer des lokalen Betriebssystems administrator@vsphere.local	Möglicherweise werden Sie bei der Installation aufgefordert, die Administratoranmeldedaten des Root-Ordners in der vSphere-Bestandslistenhierarchie anzugeben. Wenn Ihre vorherige Installation Active Directory-Benutzer unterstützt hat, können Sie die Active Directory-Domäne als Identitätsquelle hinzufügen.
vSphere 5.1	Benutzer des lokalen Betriebssystems administrator@vsphere.local Admin@SystemDomain	Ab vSphere 5.5 unterstützt vCenter Single Sign On nur eine einzige standardmäßige Identitätsquelle. Die standardmäßige Identitätsquelle können Sie festlegen. Informationen finden Sie in der Dokumentation <i>vSphere-Sicherheit</i> . Benutzer in einer Nicht-Standarddomäne können bei der Anmeldung die Domäne angeben (<i>DOMÄNE\Benutzer</i> oder <i>Benutzer@DOMÄNE</i>).
vSphere 5.5	„administrator@vsphere.local“ oder der Administrator der Domäne, die Sie während des Upgrades angegeben haben. Alle Benutzer aus allen Identitätsquellen können sich wie bisher anmelden.	

Bei einem Upgrade von vSphere 5.0, das vCenter Single Sign On nicht beinhaltet, auf eine Version, die vCenter Single Sign On beinhaltet, spielen die Benutzer in einem Verzeichnisdienst wie etwa Active Directory eine wesentlich wichtigere Rolle als Benutzer des lokalen Betriebssystems. Somit ist es nicht immer möglich oder sogar unerwünscht, lokale Betriebssystembenutzer als authentifizierte Nutzer beizubehalten.

Benutzer, die sich nach dem Upgrade einer benutzerdefinierten Installation anmelden können

Wenn Sie ein Upgrade einer Umgebung durchführen, die Sie mit der benutzerdefinierten Installationsoption bereitgestellt haben, hängt das Ergebnis von den ausgewählten Optionen ab:

- Wenn sich vCenter Single Sign On auf demselben Knoten wie das vCenter Server-System befand, erhalten Sie eine Installation mit einem eingebetteten Platform Services Controller.

- Wenn sich vCenter Single Sign On auf einem anderen Knoten als das vCenter Server-System befand, erhalten Sie eine Installation mit einem externen Platform Services Controller.
- Bei einem Upgrade von vSphere 5.0 können Sie im Rahmen des Upgrade-Vorgangs einen externen oder eingebetteten Platform Services Controller auswählen.

Die Anmelderechte nach dem Upgrade hängen von mehreren Faktoren ab.

Tabelle 1-3. Anmelderechte nach dem Upgrade der benutzerdefinierten Installationsumgebung

Quellversion	Anmeldezugriff für	Notizen
vSphere 5.0	<p>vCenter Single Sign On erkennt Benutzer des lokalen Betriebssystems für die Maschine, auf der der Platform Services Controller installiert ist, jedoch nicht für die Maschine, auf der vCenter Server installiert ist.</p> <p>Hinweis Die Verwendung von Benutzern des lokalen Betriebssystems für die Administration wird nicht empfohlen, insbesondere für Verbundumgebungen.</p> <p>„administrator@vsphere.local“ kann sich bei vCenter Single Sign On und jeder vCenter Server-Instanz als Administratorbenutzer anmelden.</p>	<p>Wenn Ihre Installation der Version 5.0 zuvor Active Directory-Benutzer unterstützt hat, haben diese Benutzer nach dem Upgrade keinen Zugriff mehr. Die Active Directory-Domäne können Sie als Identitätsquelle hinzufügen.</p>
vSphere 5.1 oder vSphere 5.5	<p>vCenter Single Sign On erkennt Benutzer des lokalen Betriebssystems für die Maschine, auf der der Platform Services Controller installiert ist, jedoch nicht für die Maschine, auf der vCenter Server installiert ist.</p> <p>Hinweis Die Verwendung von Benutzern des lokalen Betriebssystems für die Administration wird nicht empfohlen, insbesondere für Verbundumgebungen.</p> <p>„administrator@vsphere.local“ kann sich bei vCenter Single Sign On und jeder vCenter Server-Instanz als Administratorbenutzer anmelden.</p> <p>Für Upgrades von vSphere 5.1 verfügt „Admin@SystemDomain“ über dieselben Rechte wie „administrator@vsphere.local“.</p>	<p>Ab vSphere 5.5 unterstützt vCenter Single Sign On nur eine einzige standardmäßige Identitätsquelle.</p> <p>Die standardmäßige Identitätsquelle können Sie festlegen.</p> <p>Informationen finden Sie in der Dokumentation <i>vSphere-Sicherheit</i>.</p> <p>Benutzer in einer Nicht-Standarddomäne können bei der Anmeldung die Domäne angeben (<i>DOMÄNE\Benutzer</i> oder <i>Benutzer@DOMÄNE</i>).</p>

Übersicht über vSphere-Sicherheitszertifikate

ESXi-Hosts und vCenter Server kommunizieren auf sichere Weise über SSL, um Vertraulichkeit, Integrität der Daten und Authentifizierung zu gewährleisten.

In vSphere 6.0 stellt die VMware-Zertifizierungsstelle (VMCA) für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Diese Bereitstellung findet statt, wenn der ESXi-Host explizit oder als Teil der Installation des ESXi-Hosts zu vCenter Server hinzugefügt wird. Alle ESXi-Zertifikate werden lokal auf dem Host gespeichert.

Sie können auch benutzerdefinierte Zertifikate mit einer anderen Root-Zertifizierungsstelle (CA) verwenden. Informationen zum Verwalten von Zertifikaten für ESXi-Hosts finden Sie in der Dokumentation *vSphere-Sicherheit*.

Alle Zertifikate für vCenter Server und die vCenter Server-Dienste werden im VMware-Zertifikatsspeicher (VMware Endpoint Certificate Store, VECS) gespeichert.

Sie können das VMCA-Zertifikat für vCenter Server durch ein anderes von einer Zertifizierungsstelle signiertes Zertifikat ersetzen. Wenn Sie ein Drittanbieterzertifikat verwenden möchten, installieren Sie den Platform Services Controller, fügen Sie VMCA das neue von einer Zertifizierungsstelle signierte Rootzertifikat hinzu und installieren Sie dann vCenter Server. Informationen zum Verwalten von vCenter Server-Zertifikaten finden Sie in der Dokumentation *vSphere-Sicherheit*.

Erweiterter verknüpfter Modus – Überblick

Mit dem erweiterten verknüpften Modus werden mehrere vCenter Server-Systeme mithilfe von einer oder mehreren Platform Services Controller-Instanzen miteinander verbunden.

Mit dem erweiterten verknüpften Modus können Sie alle verknüpften vCenter Server-Systeme anzeigen und durchsuchen sowie Rollen, Berechtigungen, Lizenzen, Richtlinien und Tags replizieren.

Bei der Installation von vCenter Server oder der Bereitstellung der vCenter Server Appliance mit einem externen Platform Services Controller müssen Sie zunächst den Platform Services Controller installieren. Während der Installation des Platform Services Controller können Sie wählen, ob Sie eine neue vCenter Single Sign On-Domäne erstellen oder einer vorhandenen Domäne beitreten möchten. Sie können einer vorhandenen vCenter Single Sign On-Domäne beitreten, wenn Sie einen Platform Services Controller schon installiert oder bereitgestellt und eine vCenter Single Sign On-Domäne erstellt haben. Wenn Sie einer vorhandenen vCenter Single Sign On-Domäne beitreten, werden die Daten zwischen dem vorhandenen Platform Services Controller und dem neuen Platform Services Controller repliziert, und die Infrastrukturdaten werden zwischen den zwei Platform Services Controller-Instanzen ebenfalls repliziert.

Mit dem erweiterten verknüpften Modus können Sie nicht nur vCenter Server-Systeme unter Windows, sondern auch viele vCenter Server Appliance-Instanzen miteinander verbinden. Sie können außerdem eine Umgebung einrichten, in der mehrere vCenter Server-Systeme und vCenter Server Appliance-Instanzen miteinander verknüpft sind.

Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, müssen Sie zuerst den Platform Services Controller auf einer virtuellen Maschine bzw. einem physischen Server und anschließend vCenter Server auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server bereitstellen. Beim Installieren von vCenter Server müssen Sie den externen Platform Services Controller auswählen. Stellen Sie sicher, dass der Platform Services Controller, den Sie auswählen, ein externer eigenständiger Platform Services Controller ist. Die

Auswahl eines vorhandenen Platform Services Controller, der Teil einer eingebetteten Installation ist, wird nicht unterstützt und dies kann nach der Bereitstellung nicht neu konfiguriert werden. Informationen zu den empfohlenen Topologien finden Sie unter <http://kb.vmware.com/kb/2108548>.

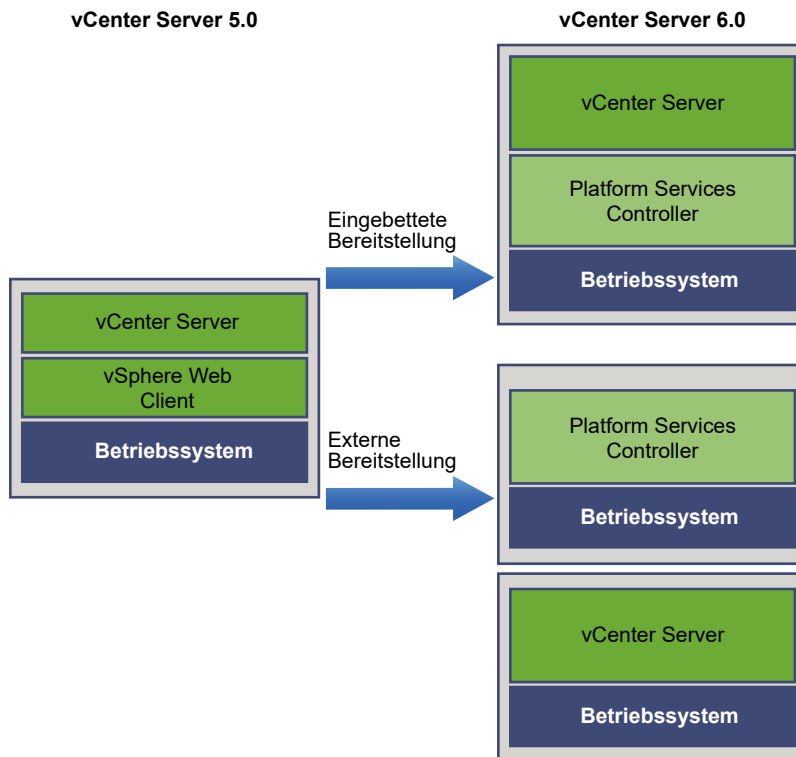
Beispiele von Upgrade-Pfaden für vCenter Server

Welche Optionen Ihnen für das Upgrade und die Konfiguration von vCenter Server 6.0 zur Verfügung stehen, hängt von Ihrer zugrunde liegenden Konfiguration von vCenter Server 5.x ab.

Die beispielhaften Upgrade-Pfade zeigen einige gängige Startkonfigurationen vor dem Upgrade von vCenter Server und die entsprechenden Konfigurationsergebnisse nach dem vCenter Server-Upgrade.

Wenn Sie derzeit mit vCenter Server 5.0 arbeiten, haben Sie keine gemeinsam genutzten Dienste konfiguriert. Sie haben die Wahl zwischen dem Upgrade auf vCenter Server mit eingebettetem Platform Services Controller oder dem Upgrade auf vCenter Server mit externem Platform Services Controller.

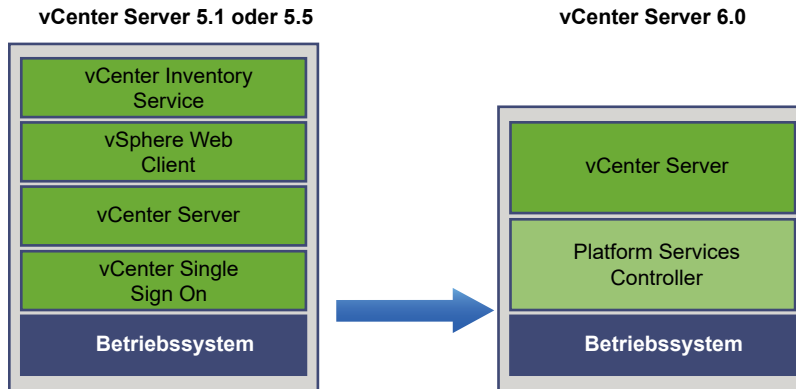
Abbildung 1-12. vCenter Server 5.0 – Bereitstellungsoptionen beim Upgrade



Bei einer einfachen Installation mit allen vCenter Server 5.1-/5.5-Komponenten auf demselben System aktualisiert die vCenter Server 6.0-Software Ihr System auf vCenter Server mit einer eingebetteten Platform Services Controller-Instanz. Dabei werden gemeinsam genutzte vCenter Server-Dienste wie vCenter Single Sign-On in der Platform Services Controller-Instanz

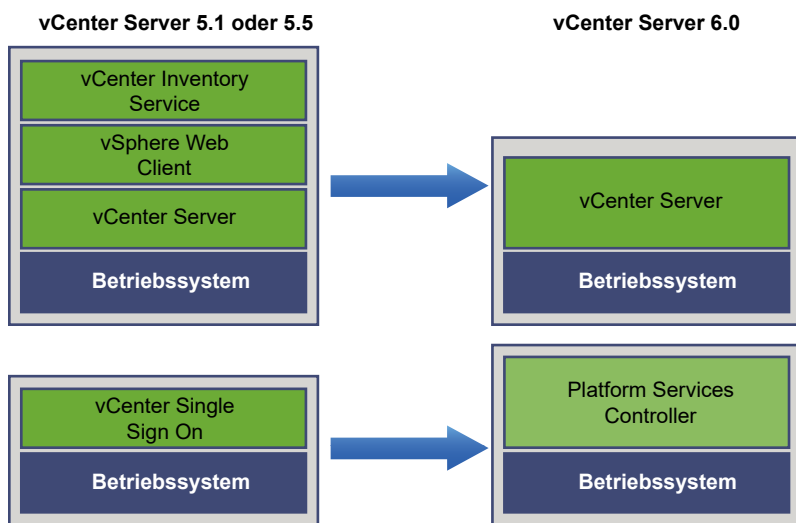
aktualisiert. Die übrigen vCenter Server-Komponenten wie vSphere Web Client oder Inventory Service werden als Teil der Dienstgruppe von vCenter Server auf Version 6.0 aktualisiert. vCenter Server und alle zugehörigen Dienste werden in der entsprechenden Reihenfolge auf dieselbe Version aktualisiert.

Abbildung 1-13. vCenter Server 5.1 oder 5.5 mit eingebettetem vCenter Single Sign-On vor und nach dem Upgrade



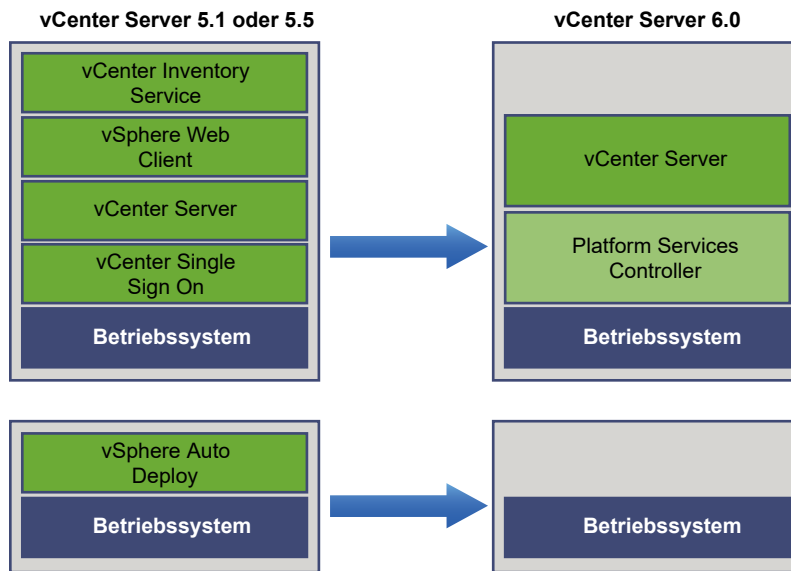
Bei einer benutzerdefinierten vCenter Server 5.1-/5.5-Umgebung mit extern bereitgestelltem vCenter Single Sign-On aktualisiert die vCenter Server 6.0-Software Ihre Bereitstellung auf vCenter Server mit einer externen Platform Services Controller-Instanz.

Abbildung 1-14. vCenter Server 5.1 oder 5.5 mit extern bereitgestelltem vCenter Single Sign-On vor und nach dem Upgrade



Wenn Ihre Konfiguration einen vSphere Auto Deploy-Server enthält, wird dieser beim Upgrade der zugehörigen vCenter Server-Instanz aktualisiert. Sie können keinen vSphere Auto Deploy-Server verwenden, der in einer früheren Version des Produkts in Verbindung mit vCenter Server 6.0 enthalten war. Wenn Ihr vSphere Auto Deploy-Server auf einem Remotesystem ausgeführt wird, wird er während des Upgrade-Vorgangs aktualisiert und auf dasselbe System migriert wie vCenter Server.

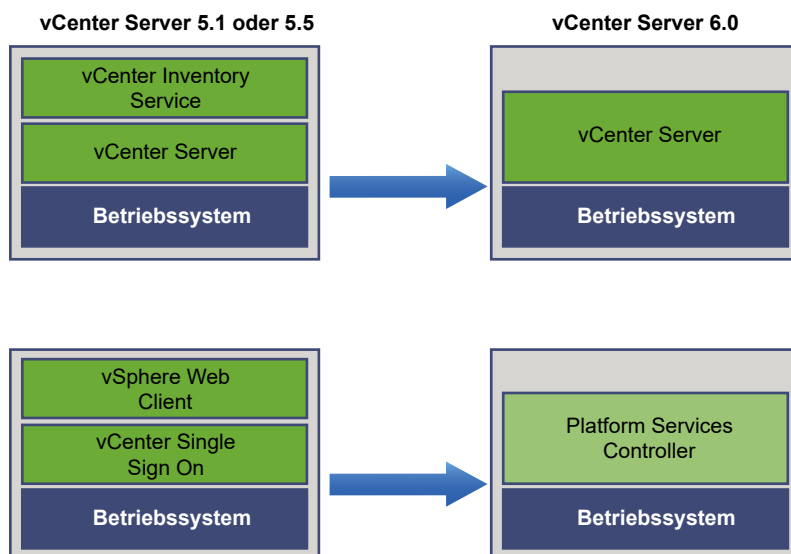
Abbildung 1-15. vCenter Server 5.1 oder 5.5 mit remotem vSphere Auto Deploy-Server vor und nach dem Upgrade



Wenn Ihr vCenter Server z. B. Teil der vCenter Server Appliance ist und Sie den vSphere Auto Deploy-Server auf einem Windows-Rechner installiert haben, wird beim Upgrade der vSphere Auto Deploy-Server an denselben Speicherort wie Ihre vCenter Server Appliance migriert. Alle Einstellungen werden ebenfalls an den neuen Speicherort verschoben. Sie müssen jedoch Ihre ESXi-Hosts neu konfigurieren, damit sie auf den neuen vSphere Auto Deploy-Speicherort verweisen. Siehe [Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade](#).

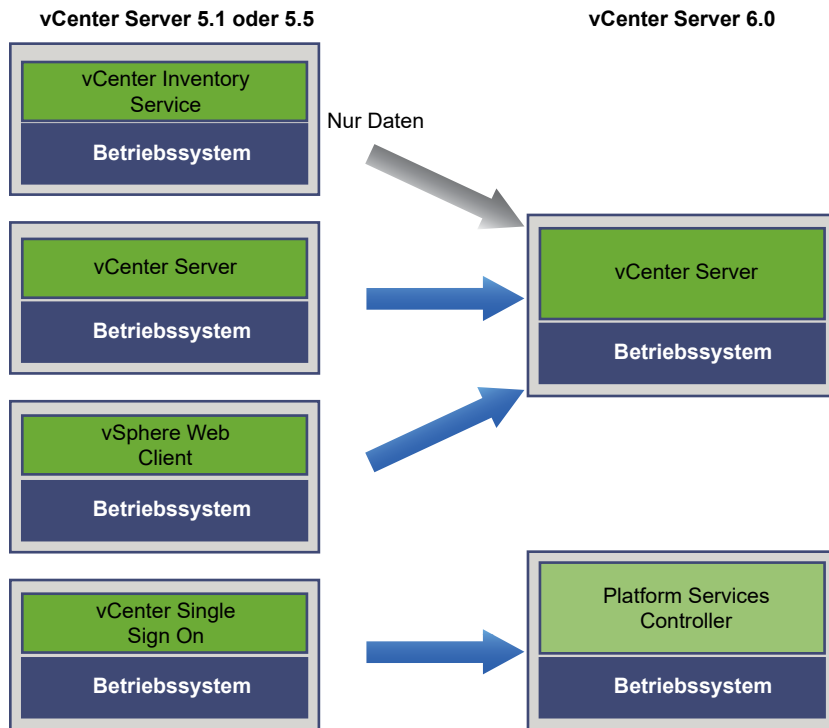
Wenn Ihre Konfiguration einen vSphere Web Client umfasst, wird dieser zusammen mit der vCenter Server-Instanz, bei der er registriert ist, aktualisiert und in denselben Speicherort migriert wie die vCenter Server-Instanz.

Abbildung 1-16. vCenter Server 5.1 oder 5.5 mit remotem vSphere Web Client und vCenter Single Sign On vor und nach dem Upgrade



Nach dem Upgrade auf vCenter Server 6.0 bleibt nur die vCenter Single Sign-On-Instanz als Teil der Platform Services Controller-Instanz remote bereitgestellt. Wenn alle vCenter Server-Komponenten remote bereitgestellt werden, werden alle während des Upgrades an den vCenter Server-Speicherort migriert, mit Ausnahme von vCenter Single Sign-On. Wenn die Inventory Service-Daten in den Speicherort von vCenter Server migriert werden, wird die Legacy-Version nicht mehr genutzt und muss manuell deinstalliert werden. Siehe [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#).

Abbildung 1-17. vCenter Server 5.1 oder 5.5 mit ausschließlich remoten Komponenten vor und nach dem Upgrade



Wenn Sie mehrere Systeme für die Hochverfügbarkeit konfiguriert haben, erlaubt vCenter Server beim Upgrade die Einbindung Ihrer gemeinsam genutzten Dienste in eine externe Konfiguration des Platform Services Controller.

Wenn Ihre Konfiguration aus mehreren Standorten mit Replizierung besteht, ermöglicht vCenter Server beim Upgrade die Einbindung Ihrer gemeinsam genutzten Dienste in eine externe Konfiguration des Platform Services Controller.



Upgrade von vCenter Server 5.0 auf 6.0

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ih7nmi18/uiConfId/49694343/)



Upgrade des vCenter Server von 5.1 oder 5.5 auf 6.0

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vs0qr73b/uiConfId/49694343/)

Weitere Informationen zu im Übergang befindlichen gemischten Versionsumgebungen finden Sie unter [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#)

Upgrade-Anforderungen

2

Für das Upgrade von vCenter Server- und ESXi-Instanzen müssen Ihre Systeme bestimmte Anforderungen erfüllen.

Dieses Kapitel enthält die folgenden Themen:

- [vCenter Server-Upgrade-Kompatibilität](#)
- [Anforderungen für vCenter Server für Windows](#)
- [Anforderungen für die vCenter Server Appliance](#)
- [Erforderliche Ports für vCenter Server und Platform Services Controller](#)
- [Konfigurationshinweise für die vCenter Server-Datenbank](#)
- [Anforderungen für ESXi](#)
- [DNS-Anforderungen für vSphere](#)
- [Softwareanforderungen für den vSphere Web Client](#)
- [Softwareanforderungen für das Client-Integrations-Plug-In](#)
- [vSphere Client-Anforderungen](#)
- [Erforderlicher freier Speicherplatz für die Systemprotokollierung](#)

vCenter Server-Upgrade-Kompatibilität

Das Upgrade auf vCenter Server 6.0 wirkt sich auf andere Softwarekomponenten des Datacenters aus.

Im Abschnitt [Tabelle 2-1. Upgrade von vCenter Server und zugehörigen VMware-Produkten und -Komponenten](#) finden Sie eine Übersicht, welche Auswirkungen das Upgrade von vCenter Server auf Ihre Datacenter-Komponenten haben kann.

vCenter Server 6.0 kann ESXi 5.x-Hosts im selben Cluster mit ESXi 6.0-Hosts verwalten, aber keine ESX 4.x- oder ESXi 4.x-Hosts.

Ein Upgrade auf vCenter Server 6.0 von vCenter Server 4.x oder einer früheren Version ist nicht möglich. Sie müssen zuerst ein Upgrade auf vCenter Server 5.x durchführen.

Tabelle 2-1. Upgrade von vCenter Server und zugehörigen VMware-Produkten und -Komponenten

Produkt oder Komponente	Kompatibilität
vCenter Server	Stellen Sie sicher, dass der Upgrade-Pfad von Ihrer aktuellen Version von vCenter Server auf die geplante Upgrade-Version unterstützt wird. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php .
vCenter Server-Datenbank	<p>Stellen Sie sicher, dass Ihre Datenbank von der vCenter Server-Version, auf die Sie ein Upgrade durchführen möchten, unterstützt wird. Falls nötig, führen Sie ein Upgrade der Datenbank durch. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.</p> <p>Hinweis vCenter Server Appliance für vCenter Server 6.0 verwendet PostgreSQL für die eingebettete Datenbank. Im Falle von externen Datenbanken unterstützt vCenter Server Appliance nur Oracle-Datenbanken der gleichen Versionen, die in der VMware-Produkt-Interoperabilitätsmatrix für die Version von vCenter Server, auf die Sie ein Upgrade durchführen, angezeigt werden.</p>
vSphere Web Client	Stellen Sie sicher, dass Ihr vSphere Web Client mit der vCenter Server-Version kompatibel ist, auf die Sie ein Upgrade durchführen möchten. Um eine optimale Leistung und optimale Kompatibilität zu erzielen, führen Sie ein Upgrade Ihres vSphere Web Clients auf die gleiche vCenter Server-Version durch. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php .
ESX- und ESXi-Hosts	Stellen Sie sicher, dass Ihr ESX- und ESXi-Host mit der vCenter Server-Version kompatibel ist, auf die Sie ein Upgrade durchführen möchten. Aktualisieren Sie sie bei Bedarf. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php .
Virtual Machine File System (VMFS)-Volumes von VMware	Sie können vorhandene VMFS3-Datenspeicher weiter verwenden, aber keine neuen VMFS3-Datenspeicher erstellen. Führen Sie für vorhandene VMFS3-Datenspeicher ein Upgrade auf VMFS5 durch. Informationen zum Upgrade Ihrer VMFS-Volumes finden Sie im Dokument <i>vSphere-Speicher</i> .
virtuelle Maschinen	Die Upgrade-Optionen hängen von Ihrer aktuellen Version ab. Weitere Informationen hierzu finden Sie unter Kapitel 11 Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools .
VMware Tools	Die Upgrade-Optionen hängen von Ihrer aktuellen Version ab. Weitere Informationen über das Durchführen eines Upgrades von VMware Tools finden Sie unter Kapitel 11 Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools .
Auto Deploy	Um Kompatibilität und optimale Leistung sicherzustellen, verwenden Sie beim Upgrade auf vCenter Server 6.0 Auto Deploy, um für ESXi-Hosts ein Upgrade auf dieselbe Version durchzuführen.

Anforderungen für vCenter Server für Windows

Für das Upgrade von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server unter Windows muss Ihr System bestimmte Hardware- und Softwareanforderungen erfüllen.

- Synchronisieren Sie die Systemuhren auf allen Systemen, auf denen die vCenter Server 5.x-Dienste ausgeführt werden. Siehe [Synchronisieren der Systemuhren im vSphere-Netzwerk](#).
- Stellen Sie sicher, dass die Systemnetzwerknamen der Systeme, auf denen vCenter Server 5.x-Dienste ausgeführt werden, gültig sind und von anderen Systemen im Netzwerk aus erreichbar sind.
- Stellen Sie sicher, dass der Hostname der virtuellen Maschine bzw. des physischen Servers, auf der/dem Sie vCenter Server installieren oder upgraden, mit den RFC 1123-Richtlinien übereinstimmt.
- Wenn Ihr vCenter Server-Dienst in einem anderen Benutzerkonto als dem lokalen Systemkonto ausgeführt wird, stellen Sie sicher, dass das Benutzerkonto, in dem der vCenter Server-Dienst ausgeführt wird, über die folgenden Berechtigungen verfügt:
 - **Mitglied der Gruppe „Administratoren“**
 - **Anmelden als Dienst**
 - **Agieren als Teil des Betriebssystems (wenn der Benutzer ein Domänenbenutzer ist)**
- Vergewissern Sie sich, dass das Konto LOCAL SERVICE über Leseberechtigung sowohl für den Ordner, in dem vCenter Server installiert ist, als auch für die HKLM-Registrierung verfügt.
- Stellen Sie sicher, dass die Verbindung zwischen der virtuellen Maschine bzw. dem physischen Server und dem Domänencontroller funktioniert.

Pre-Upgrade Checker von vCenter Server für Windows

Bei einem Upgrade von vCenter Server und dem Platform Services Controller führt das Installationsprogramm eine Prüfung vor dem Upgrade durch, um sicherzustellen, dass ausreichend Speicherplatz auf der virtuellen Maschine bzw. auf dem physischen Server verfügbar ist, wo vCenter Server aktualisiert werden soll, und dass auf die ggf. vorhandene externe Datenbank zugegriffen werden kann.

Wenn Sie vCenter Server mit einem eingebetteten Platform Services Controller oder aber mit einem externen Platform Services Controller bereitstellen, wird vCenter Single Sign On im Rahmen des Platform Services Controller installiert. Zum Zeitpunkt des Upgrades bietet das Installationsprogramm die Möglichkeit, einer vorhandenen vCenter Single Sign On-Serverdomäne beizutreten. Wenn Sie die Informationen zum anderen vCenter Single Sign On-Dienst eingeben, überprüft das Installationsprogramm mithilfe des Administratorkontos den Hostnamen und das Kennwort, um sicherzustellen, dass die für den vCenter Single Sign On-Server eingegebenen Informationen authentifiziert werden können, bevor das Upgrade fortgesetzt wird.

Der Pre-Upgrade Checker überprüft die folgenden Aspekte der Umgebung:

- Windows-Version
- Mindestanforderungen an den Prozessor
- Mindestanforderungen an den Arbeitsspeicher
- Mindestanforderungen an den Festplattenspeicher
- Berechtigungen für das ausgewählte Installations- und Datenverzeichnis
- Verfügbarkeit interner und externer Ports
- Version der externen Datenbank
- Konnektivität zur externen Datenbank
- Administratorrechte auf der Windows-Maschine
- Sämtliche eingegebene Anmeldedaten
- vCenter Server 5.x-Dienste

Informationen zu den Mindestspeicheranforderungen erhalten Sie unter [Speicheranforderungen für vCenter Server für Windows](#). Informationen zu den Mindesthardwareanforderungen erhalten Sie unter [Hardwareanforderungen für vCenter Server für Windows](#).

Speicheranforderungen für vCenter Server für Windows

Beim Upgrade von vCenter Server muss Ihr System Mindestspeicheranforderungen erfüllen.

Die Speicheranforderungen pro Ordner hängen von den vCenter Server 5.x-Diensten, die auf dem System bereitgestellt sind, vom Upgrade-Bereitstellungsmodell und der Größe Ihrer vSphere 5.x-Bestandsliste ab. Das Installationsprogramm berechnet während des Upgrades die Speicheranforderung dynamisch und prüft vor Beginn des Upgrade-Prozesses, ob ausreichend Festplattenspeicherplatz verfügbar ist.

Während der Installation können Sie einen anderen Ordner als den Standardordner `C:\Programme\VMware` auswählen, um vCenter Server und den Platform Services Controller zu installieren. Sie können auch einen anderen Ordner als den Standardordner `C:\ProgramData\VMware\vCenterServer\` zum Speichern von Daten auswählen. Die folgende Tabelle enthält die absoluten Mindestanforderungen an den Festplattenspeicher für die verschiedenen Bereitstellungsmodelle. Die Anforderungen hängen von den installierten vCenter Server 5.x-Diensten und der Größe der vSphere 5.x-Bestandsliste ab.

Tabelle 2-2. Mindestspeicheranforderungen für vCenter Server abhängig vom Bereitstellungsmodell

Standardordner	vCenter Server mit einem eingebetteten Platform Services Controller	vCenter Server mit einem externen Platform Services Controller	Externer Platform Services Controller
Programme	6 GB	6 GB	1 GB
ProgramData	8 GB	8 GB	2 GB
Systemordner (Zwischenspeicher für das MSI-Installationsprogramm)	3 GB	3 GB	1 GB

Hardwareanforderungen für vCenter Server für Windows

Bei der Installation von vCenter Server auf einer virtuellen Maschine oder einem physischen Server unter Microsoft Windows muss Ihr System bestimmte Hardwareanforderungen erfüllen.

Sie können vCenter Server und den Platform Services Controller auf derselben virtuellen Maschine oder demselben physischen Server oder auf verschiedenen virtuellen Maschinen bzw. physischen Servern installieren. Wenn Sie vCenter Server mit einem eingebetteten Platform Services Controller installieren, installieren Sie vCenter Server und den Platform Services Controller auf derselben virtuellen Maschine bzw. demselben physischen Server. Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, installieren Sie zunächst den Platform Services Controller, der alle erforderlichen Dienste auf einer virtuellen Maschine bzw. einem physischen Server enthält, und anschließend installieren Sie vCenter Server und die vCenter Server-Komponenten auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server.

Hinweis Die Installation von vCenter Server auf einem Netzlaufwerk oder USB-Flash-Laufwerk wird nicht unterstützt.

Tabelle 2-3. Empfohlene Mindestanforderungen an die Hardware für die Installation von vCenter Server und Platform Services Controller auf Windows

	Platform Services Controller	vCenter Server mit einem eingebetteten oder externen Platform Services Controller für eine sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	vCenter Server mit einem eingebetteten oder externen Platform Services Controller für eine kleine Umgebung (bis zu 100 Hosts, 1000 virtuelle Maschinen)	vCenter Server mit einem eingebetteten oder externen Platform Services Controller für eine mittlere Umgebung (bis zu 400 Hosts, 4.000 virtuelle Maschinen)	vCenter Server mit einem eingebetteten oder externen Platform Services Controller für eine große Umgebung (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen)
Anzahl der CPUs	2	2	4	8	16
Arbeitsspeicher	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

Informationen zu Hardwareanforderungen für Ihre Datenbank finden Sie in der Datenbankdokumentation. Die Datenbankanforderungen gelten zusätzlich zu den Anforderungen von vCenter Server, sofern die Datenbank und vCenter Server auf derselben Maschine ausgeführt werden.

Softwareanforderungen für vCenter Server für Windows

Stellen Sie sicher, dass vCenter Server von Ihrem Betriebssystem unterstützt wird.

vCenter Server erfordert ein 64-Bit-Betriebssystem sowie den 64-Bit-System-DSN zum Herstellen einer Verbindung mit der externen Datenbank.vCenter Server

Windows Server 2008 SP2 ist die älteste Windows Server-Version, die von vCenter Server unterstützt wird. Auf dem Windows-Server müssen die neuesten Updates und Patches installiert sein. Eine vollständige Aufstellung der unterstützten Betriebssysteme finden Sie unter <http://kb.vmware.com/kb/2091273>.

Datenbankanforderungen für vCenter Server für Windows

vCenter Server benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten.

Für jede vCenter Server-Instanz ist eine eigene Datenbank erforderlich. Für Umgebungen mit bis zu 20 Hosts und bis zu 200 virtuellen Maschinen können Sie die mitgelieferte PostgreSQL-Datenbank verwenden, die das vCenter Server-Installationsprogramm während der Installation von vCenter Server für Sie installieren und einrichten kann. Eine größere Installation erfordert eine für die Größe der Umgebung unterstützte externe Datenbank.

Beim Installieren oder Upgraden von vCenter Server müssen Sie die eingebettete Datenbank installieren oder einen Verweis auf eine vorhandene unterstützte Datenbank für das vCenter Server-System angeben. vCenter Server unterstützt Oracle- und Microsoft SQL Server-Datenbanken. Informationen zu unterstützten Datenbankserverversionen finden Sie in der VMware-Produkt-Interoperabilitätstabelle unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Anforderungen für die vCenter Server Appliance

Für die vCenter Server Appliance kann ein Upgrade auf einem ESXi-Host der Version 5.0 oder höher durchgeführt werden. Ihr System muss auch bestimmte Software- und Hardwareanforderungen erfüllen.

Wenn Sie vollqualifizierte Domännennamen verwenden, stellen Sie sicher, dass die Maschine, die Sie zum Bereitstellen der vCenter Server Appliance verwenden, und der ESXi-Host sich auf demselben DNS-Server befinden.

Bevor Sie die vCenter Server Appliance bereitstellen, sollten Sie die Systemuhren aller virtuellen Maschinen im vSphere-Netzwerk synchronisieren. Nicht synchronisierte Systemuhren können Authentifizierungsprobleme und einen Fehlschlag der Installation verursachen bzw. das Starten der vCenter Server-Dienste verhindern. Siehe [Synchronisieren der Systemuhren im vSphere-Netzwerk](#).

Hardwareanforderungen für vCenter Server Appliance

Bei der Bereitstellung der vCenter Server Appliance können Sie eine für die Größe Ihrer vSphere-Umgebung geeignete Appliance bereitstellen. Die gewählte Option bestimmt die Anzahl der CPUs und den Umfang des Arbeitsspeichers für die Appliance.

Die Hardwareanforderungen wie beispielsweise die Anzahl der CPUs und der Arbeitsspeicher hängen von der Größe Ihrer vSphere-Bestandsliste ab.

Tabelle 2-4. Hardwareanforderungen für VMware vCenter Server Appliance und Platform Services Controller Appliance

Ressourcen	Platform Services Controller Appliance	vCenter Server Appliance mit einem eingebetteten oder externen Platform Services Controller für eine sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	vCenter Server Appliance mit einem eingebetteten oder externen Platform Services Controller für eine kleine Umgebung (bis zu 100 Hosts, 1.000 virtuelle Maschinen)	vCenter Server Appliance mit einem eingebetteten oder externen Platform Services Controller für eine mittlere Umgebung (bis zu 400 Hosts, 4.000 virtuelle Maschinen)	vCenter Server Appliance mit einem eingebetteten oder externen Platform Services Controller für eine große Umgebung (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen)
Anzahl der CPUs	2	2	4	8	16
Arbeitsspeicher	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

Speicheranforderungen für die vCenter Server Appliance

Bei der Bereitstellung der vCenter Server Appliance muss der Host, auf dem Sie die Appliance bereitstellen, Mindestspeicheranforderungen erfüllen. Der erforderliche Speicher ist nicht nur von der Größe der vSphere-Umgebung abhängig, sondern auch vom Festplattenbereitstellungsmodus.

Die Speicheranforderungen hängen vom gewählten Bereitstellungsmodell ab.

Tabelle 2-5. Mindestspeicheranforderungen für vCenter Server abhängig vom Bereitstellungsmodell

	vCenter Server Appliance mit einem eingebetteten Platform Services Controller	vCenter Server Appliance mit einem externen Platform Services Controller	Externe Platform Services Controller-Appliance
Sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	120 GB	86 GB	30 GB
Kleine Umgebung (bis zu 100 Hosts, 1.000 virtuelle Maschinen)	150 GB	108 GB	30 GB
Mittlere Umgebung (bis zu 400 Hosts, 4000 virtuelle Maschinen)	300 GB	220 GB	30 GB
Große Umgebung (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen)	450 GB	280 GB	30 GB

Im Lieferumfang der vCenter Server Appliance enthaltene Software

Die vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung von vCenter Server und zugehörigen Diensten optimiert ist.

Das vCenter Server Appliance-Paket enthält die folgende Software:

- SUSE Linux Enterprise Server 11 Update 3 für VMware, 64-Bit-Edition
- PostgreSQL
- vCenter Server 6.0 und vCenter Server 6.0-Komponenten.

Softwareanforderungen für vCenter Server Appliance

Für die VMware vCenter Server Appliance kann nur auf Hosts unter ESXi Version 5.0 oder höher ein Upgrade durchgeführt werden.

Das Upgrade der vCenter Server Appliance kann nur über das Client-Integrations-Plug-In erfolgen. Dabei handelt es sich um ein HTML-Installationsprogramm für Windows, mit dem Sie eine direkte Verbindung mit einem ESXi 5.0.x-, ESXi 5.1.x-, ESXi 5.5.x- oder ESXi 6.0-Host herstellen und die vCenter Server Appliance auf dem Host bereitstellen können.

Wichtig Sie können die vCenter Server Appliance nicht mit dem vSphere Client oder vSphere Web Client bereitstellen. Bei der Bereitstellung der vCenter Server Appliance müssen Sie verschiedene Informationen eingeben, wie z. B. die Kennwörter des Betriebssystems und von vCenter Single Sign-On. Wenn Sie versuchen, die Appliance mit dem vSphere Client oder vSphere Web Client bereitzustellen, werden Sie nicht zur Eingabe dieser Informationen aufgefordert und die Bereitstellung schlägt fehl.

Datenbankanforderungen für die vCenter Server Appliance

Die vCenter Server Appliance benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten.

Für jede vCenter Server Appliance-Instanz ist eine eigene Datenbank erforderlich. Sie können die PostgreSQL-Datenbank verwenden, die im Lieferumfang der vCenter Server Appliance enthalten ist und bis zu 1000 Hosts und bis zu 10.000 virtuelle Maschinen unterstützt.

Für externe Datenbanken unterstützt die vCenter Server Appliance nur Oracle-Datenbanken. Diese Oracle-Datenbanken weisen die gleichen Versionen, die in der VMware-Produkt-Interoperabilitätsmatrix für die Version der vCenter Server-Instanz, die Sie installieren, angezeigt werden. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Wenn Sie mit einer externen Datenbank arbeiten möchten, müssen Sie ein 64-Bit-DSN erstellen, damit vCenter Server eine Verbindung mit der Oracle-Datenbank herstellen kann.

Erforderliche Ports für vCenter Server und Platform Services Controller

Das vCenter Server-System unter Windows und in der Appliance muss in der Lage sein, Daten an jeden verwalteten Host zu senden und Daten vom vSphere Web Client und von den Platform Services Controller-Diensten zu empfangen. Die Quell- und Zielhosts müssen Daten untereinander austauschen können, um Migrations- und Bereitstellungsaktivitäten zwischen verwalteten Hosts zu ermöglichen.

Wenn ein Port verwendet wird oder gesperrt ist, zeigt das Installationsprogramm für vCenter Server eine Fehlermeldung an. Sie müssen eine andere Portnummer verwenden, um mit der Installation fortfahren zu können. Es gibt interne Ports, die nur für den Datenaustausch zwischen Prozessen verwendet werden.

Für die Kommunikation verwendet VMware festgelegte Ports. Zudem überwachen die verwalteten Hosts die festgelegten Ports auf Daten von vCenter Server. Wenn zwischen diesen Elementen eine Firewall vorhanden ist, öffnet das Installationsprogramm die Ports während der Installation bzw. des Upgrades. Für benutzerdefinierte Firewalls müssen die erforderlichen Ports manuell geöffnet werden. Wenn sich eine Firewall zwischen zwei von verwalteten Hosts befindet und Sie Quell- oder Zielaktivitäten wie z. B. eine Migration oder einen Klonvorgang ausführen möchten, muss der verwaltete Host Daten empfangen können.

Hinweis Unter Microsoft Windows Server 2008 oder höher ist die Firewall standardmäßig aktiviert.

Tabelle 2-6. Erforderliche Ports zur Kommunikation zwischen Komponenten

Port	Protokoll	Beschreibung	Erforderlich für	Erforderlich für Knoten-zu-Knoten-Kommunikation
22	TCP	<p>System-Port für SSHD.</p> <p>Wichtig Dieser Port muss während des Upgrades der Appliance offen sein. Während des Upgrades wird eine SSH-Verbindung zur Übertragung der Daten aus der vorhandenen in die neue Appliance eingerichtet.</p>	<p>Appliance-Bereitstellungen von</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	Nein
80	TCP	<p>vCenter Server benötigt Port 80 für direkte HTTP-Verbindungen. Port 80 leitet Anforderungen an HTTPS-Port 443 weiter. Diese Umleitung ist nützlich, falls Sie versehentlich http://server anstelle von https://server verwenden.</p> <p>WS-Management (Port 443 muss ebenfalls offen sein).</p> <p>Wenn Sie eine Microsoft SQL-Datenbank verwenden, die auf derselben virtuellen Maschine oder demselben physischen Server wie vCenter Server gespeichert ist, wird Port 80 vom SQL Reporting-Dienst verwendet. Bei der Installation bzw. dem Upgrade von vCenter Server werden Sie vom Installationsprogramm aufgefordert, den HTTP-Port für vCenter Server zu ändern. Ändern Sie den HTTP-Port für vCenter Server in einen benutzerdefinierten Wert, um eine erfolgreiche Installation bzw. ein erfolgreiches Upgrade sicherzustellen.</p> <p>Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server und Platform Services Controller auf Windows ändern.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	Nein
88	TCP	<p>Active Directory-Server Dieser Port muss für den Host zu Active Directory beitreten geöffnet sein. Wenn Sie natives Active Directory verwenden, muss der Port in vCenter Server und Platform Services Controller geöffnet sein.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von Platform Services Controller</p>	Nein

Tabelle 2-6. Erforderliche Ports zur Kommunikation zwischen Komponenten (Fortsetzung)

Port	Protokoll	Beschreibung	Erforderlich für	Erforderlich für Knoten-zu-Knoten-Kommunikation
389	TCP/UDP	<p>Sowohl auf der lokalen als auch auf allen Remote-Instanzen von vCenter Server muss dieser Port geöffnet sein. Dies ist die LDAP-Portnummer für die Verzeichnisdienste der vCenter Server-Gruppe. Wenn auf diesem Port ein anderer Dienst ausgeführt wird, ist es in manchen Fällen empfehlenswert, diesen zu löschen oder einen anderen Port zuzuweisen. Sie können den LDAP-Dienst auf jedem Port zwischen 1025 und 65535 ausführen.</p> <p>Sofern diese Instanz als das Microsoft Windows Active Directory dient, ändern Sie die Portnummer von 389 in die Nummer eines verfügbaren Ports zwischen 1025 und 65535.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von Platform Services Controller</p>	<ul style="list-style-type: none"> ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu Platform Services Controller
443	TCP	<p>Der Standardport, den das vCenter Server-System zum Überwachen von Verbindungen vom vSphere Web Client verwendet. Öffnen Sie Port 443 in der Firewall, um dem vCenter Server-System den Empfang von Daten vom vSphere Web Client zu ermöglichen.</p> <p>Das vCenter Server-System verwendet Port 443 auch zur Überwachung der Datenübertragung zwischen SDK-Clients.</p> <p>Dieser Port wird auch für die folgenden Dienste verwendet:</p> <ul style="list-style-type: none"> ■ WS-Management (Port 80 muss offen sein) ■ Verbindungen von Netzwerkverwaltungs-Clients von Drittanbietern mit vCenter Server ■ Zugriff von Netzwerkverwaltungs-Client von Drittanbietern auf Hosts <p>Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server und Platform Services Controller auf Windows ändern.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	<ul style="list-style-type: none"> ■ vCenter Server zu vCenter Server ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu vCenter Server

Tabelle 2-6. Erforderliche Ports zur Kommunikation zwischen Komponenten (Fortsetzung)

Port	Protokoll	Beschreibung	Erforderlich für	Erforderlich für Knoten-zu-Knoten-Kommunikation
514	TCP/UDP	<p>Port für vSphere Syslog Collector für vCenter Server unter Windows und Port für vSphere Syslog-Dienst für vCenter Server Appliance</p> <hr/> <p>Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server und Platform Services Controller auf Windows ändern.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	Nein
636	TCP	LDAPS von vCenter Single Sign-On	Windows-Installationen und Appliance-Bereitstellungen von Platform Services Controller	vCenter Server zu Platform Services Controller
902	TCP/UDP	<p>Der Standardport, den das vCenter Server-System zum Senden von Daten an verwaltete Hosts verwendet. Verwaltete Hosts senden außerdem regelmäßig Taktsignale über den UDP-Port 902 an das vCenter Server-System. Dieser Port darf nicht durch Firewalls zwischen dem Server und den Hosts bzw. zwischen Hosts blockiert werden.</p> <p>Port 902 darf nicht zwischen dem vSphere Client und den Hosts blockiert werden. Der vSphere Client verwendet diesen Port zum Anzeigen der Konsolen von virtuellen Maschinen.</p> <hr/> <p>Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server auf Windows ändern.</p>	Windows-Installationen und Appliance-Bereitstellungen von vCenter Server	Nein
1514	TCP/UDP	<p>TLS-Port für vSphere Syslog Collector für vCenter Server unter Windows und TLS-Port für vSphere Syslog-Dienst für vCenter Server Appliance</p> <hr/> <p>Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server und Platform Services Controller auf Windows ändern.</p>	<p>Windows-Installationen und Appliance-Bereitstellungen von</p> <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	Nein

Tabelle 2-6. Erforderliche Ports zur Kommunikation zwischen Komponenten (Fortsetzung)

Port	Protokoll	Beschreibung	Erforderlich für	Erforderlich für Knoten-zu-Knoten-Kommunikation
2012	TCP	RPC des Schnittstellen- Steuerelements für vCenter Single Sign-On	Windows- Installationen und Appliance- Bereitstellungen von Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu vCenter Server ■ Platform Services Controller zu Platform Services Controller
2014	TCP	RPC-Port für alle APIs von VMCA (VMware Certificate Authority) Wichtig Sie können diese Portnummer bei den Installationen von Platform Services Controller auf Windows ändern.	Windows- Installationen und Appliance- Bereitstellungen von Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu vCenter Server
2020	TCP/UDP	Verwaltung des Authentifizierungsframeworks Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server und Platform Services Controller auf Windows ändern.	Windows- Installationen und Appliance- Bereitstellungen von <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	<ul style="list-style-type: none"> ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu vCenter Server
5480	TCP	Appliance-Verwaltungsschnittstelle Offener Endpoint, der alle HTTPS-, XMLRPC- und JSON-RPC- Anforderungen über HTTPS bedient.	Appliance- Bereitstellungen von <ul style="list-style-type: none"> ■ vCenter Server ■ Platform Services Controller 	Nein
6500	TCP/UDP	ESXi Dump Collector-Port Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server auf Windows ändern.	Windows- Installationen und Appliance- Bereitstellungen von vCenter Server	Nein
6501	TCP	Auto Deploy-Dienst Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server auf Windows ändern.	Windows- Installationen und Appliance- Bereitstellungen von vCenter Server	Nein

Tabelle 2-6. Erforderliche Ports zur Kommunikation zwischen Komponenten (Fortsetzung)

Port	Protokoll	Beschreibung	Erforderlich für	Erforderlich für Knoten-zu-Knoten-Kommunikation
6502	TCP	Auto Deploy-Verwaltung Wichtig Sie können diese Portnummer bei den Installationen von vCenter Server auf Windows ändern.	Windows-Installationen und Appliance-Bereitstellungen von vCenter Server	Nein
7444	TCP	Secure Token Service	Windows-Installationen und Appliance-Bereitstellungen von Platform Services Controller	<ul style="list-style-type: none"> ■ vCenter Server zu Platform Services Controller ■ Platform Services Controller zu vCenter Server
9443	TCP	vSphere Web Client HTTPS	Windows-Installationen und Appliance-Bereitstellungen von vCenter Server	Nein
11711	TCP	LDAP von vCenter Single Sign-On	-	Ausschließlich für Abwärtskompatibilität mit vSphere 5.5. vCenter Single Sign-On 5.5 zu Platform Services Controller 6.0
11712	TCP	LDAPS von vCenter Single Sign-On	-	Ausschließlich für Abwärtskompatibilität mit vSphere 5.5. vCenter Single Sign-On 5.5 zu Platform Services Controller 6.0

Wenn das vCenter Server-System einen anderen Port zum Empfangen von vSphere Web Client-Daten verwenden soll, lesen Sie die Dokumentation *vCenter Server und Hostverwaltung*.

Weitere Informationen zur Firewall-Konfiguration finden Sie in der Dokumentation *vSphere-Sicherheit*.

Konfigurationshinweise für die vCenter Server-Datenbank

Vergewissern Sie sich, sobald Sie einen Datenbanktyp ausgewählt haben, dass Sie mit allen speziellen Konfigurationsanforderungen vertraut sind.

[Tabelle 2-7. Konfigurationshinweise für von vCenter Server unterstützte Datenbanken](#) ist keine vollständige Liste der für vCenter Server und vCenter Server Appliance unterstützten Datenbanken. Weitere Informationen zu bestimmten Datenbankversionen und Service Pack-Konfigurationen, die von vCenter Server unterstützt werden, finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#). Die vCenter Server Appliance unterstützt die gleichen Oracle-Datenbankversionen wie vCenter Server. Nur besondere Datenbankkonfigurationshinweise, die in den Produktinteroperabilitätstabellen nicht aufgeführt sind, werden in [Tabelle 2-7. Konfigurationshinweise für von vCenter Server unterstützte Datenbanken](#) bereitgestellt.

Hinweis vSphere Update Manager benötigt ebenfalls eine Datenbank. Verwenden Sie für vCenter Server und vSphere Update Manager getrennte Datenbanken.

vCenter Server-Datenbanken erfordern einen UTF-Codesatz.

Tabelle 2-7. Konfigurationshinweise für von vCenter Server unterstützte Datenbanken

Datenbanktyp	Konfigurationshinweise
PostgreSQL	<p>Für vCenter Server 6.0 ist die mitgelieferte PostgreSQL-Datenbank für Umgebungen mit bis zu 20 Hosts und bis zu 200 virtuellen Maschinen geeignet. Für die vCenter Server Appliance können Sie die eingebettete PostgreSQL-Datenbank für Umgebungen mit bis zu 1000 Hosts und bis zu 10.000 virtuellen Maschinen verwenden.</p> <p>Wichtig Wenn Sie die eingebettete PostgreSQL-Datenbank verwenden, wird bei der Deinstallation von vCenter Server unter Windows auch die eingebettete Datenbank deinstalliert, und alle Daten gehen verloren.</p> <p>Beim Upgrade von vCenter Server 5.x auf vCenter Server 6.0 wird die mitgelieferte Microsoft SQL Server Express-Datenbank zu PostgreSQL migriert.</p>
Microsoft SQL Server 2008 R2 SP2 oder höher	<p>Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat.</p> <p>Hinweis vCenter Server Appliance unterstützt diese Datenbank nicht.</p>
Microsoft SQL Server 2012	<p>Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat.</p> <p>Hinweis vCenter Server Appliance unterstützt diese Datenbank nicht.</p>
Microsoft SQL Server 2014	<p>Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat.</p> <p>Hinweis vCenter Server Appliance unterstützt diese Datenbank nicht.</p>
Oracle 11g und Oracle 12c	<p>Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat.</p> <p>Wenden Sie nach Abschluss der Installation von vCenter Server den neuesten Patch auf den Oracle-Client und -Server an.</p>

Anforderungen für ESXi

Für die Installation von ESXi oder das Upgrade auf ESXi 6.0 muss Ihr System bestimmte Hardware- und Softwareanforderungen erfüllen.

Hardwareanforderungen für ESXi

Stellen Sie sicher, dass der Host die Mindestanforderungen an die Hardwarekonfiguration erfüllt, die von ESXi 6.0 unterstützt werden.

Hardware- und Systemressourcen

Für die Installation bzw. das Upgrade von ESXi 6.0 müssen Ihre Hardware- und Systemressourcen die folgenden Anforderungen erfüllen:

- Unterstützte Serverplattform. Eine Liste der unterstützten Plattformen finden Sie im *VMware-Kompatibilitätshandbuch* unter <http://www.vmware.com/resources/compatibility>.
- Für ESXi 6.0 ist eine Hostmaschine mit mindestens zwei CPU-Kernen erforderlich.
- ESXi 6.0 unterstützt 64-Bit-x86-Prozessoren, die nach September 2006 veröffentlicht wurden. Hierzu zählt ein breites Spektrum von Prozessoren mit mehreren Kernen. Eine vollständige Liste der unterstützten Prozessoren finden Sie im *VMware-Kompatibilitätshandbuch* unter <http://www.vmware.com/resources/compatibility>.
- Für ESXi 6.0 muss das NX/XD-Bit für die CPU im BIOS aktiviert sein.
- ESXi benötigt mindestens 4 GB an physischem Arbeitsspeicher. Es wird empfohlen, mindestens 8 GB RAM zum Ausführen virtueller Maschinen in typischen Produktionsumgebungen bereitzustellen.
- Um virtuelle 64-Bit-Maschinen zu unterstützen, muss auf x64-CPU die Unterstützung für die Hardwarevirtualisierung (Intel VT-x oder AMD RVI) aktiviert sein.
- Ein oder mehr Gigabit oder schnellere Ethernet-Controller. Eine Liste mit unterstützten Netzwerkadaptermodellen finden Sie im *VMware-Kompatibilitätshandbuch* unter <http://www.vmware.com/resources/compatibility>.
- SCSI-Festplatte oder lokale (nicht im Netzwerk befindliche) RAID-LUN mit nicht partitioniertem Bereich für die virtuelle Maschinen.
- Serial ATA (SATA) – eine über unterstützte SAS-Controller oder unterstützte On-Board-SATA-Controller verbundene Festplatte. SATA-Festplatten werden als remote betrachtet, nicht lokal. Diese Festplatten werden nicht standardmäßig als Scratch-Partition verwendet, da sie als remote betrachtet werden.

Hinweis Sie können auf einem ESXi 6.0-Host kein SATA-CD-ROM-Gerät mit einer virtuellen Maschine verbinden. Zur Verwendung des SATA-CD-ROM-Laufwerks müssen Sie den IDE-Emulationsmodus einsetzen.

Speichersysteme

Eine Liste aller unterstützten Speichersysteme finden Sie im *VMware-Kompatibilitätshandbuch* unter <http://www.vmware.com/resources/compatibility>. Informationen zu Software-Fibre-Channel über Ethernet (FCoE) finden Sie unter [Installieren und Starten von ESXi mit Software FCoE](#).

Startanforderungen für ESXi

vSphere 6.0 unterstützt das Starten von ESXi-Hosts von der Unified Extensible Firmware Interface (UEFI) aus. Mithilfe von UEFI können Sie Systeme von Festplatten, CD-ROM-Laufwerken oder USB-Medien aus starten. Das Starten oder Bereitstellen über das Netzwerk mit VMware Auto Deploy erfordert die Legacy-BIOS-Firmware und steht mit UEFI nicht zur Verfügung.

ESXi kann von einer Festplatte größer als 2 TB starten, vorausgesetzt, dass die System-Firmware und die Firmware auf allen von Ihnen verwendeten Erweiterungskarten unterstützt werden. Informationen finden Sie in der Dokumentation des Anbieters.

Hinweis Das Ändern des Boot-Typs von Legacy-BIOS in UEFI, nachdem Sie ESXi 6.0 installiert haben, kann dazu führen, dass der Host nicht gestartet werden kann. In diesem Fall zeigt der Host eine Fehlermeldung ähnlich der folgenden an: `Keine VMware-Startbank`. Das Ändern des Host-Boot-Typs zwischen Legacy-BIOS und UEFI wird nicht unterstützt, nachdem Sie ESXi 6.0 installiert haben.

Speicheranforderungen für die Installation von ESXi 6.0 bzw. das Upgrade auf ESXi 6.0

Zum Installieren von ESXi 6.0 bzw. das Upgrade auf ESXi 6.0 ist ein Startgerät mit mindestens 1 GB Speicherplatz erforderlich. Beim Starten von einer lokalen Festplatte oder einer SAN/iSCSI LUN ist eine 5,2-GB-Festplatte erforderlich, damit das VMFS-Volume und eine 4-GB-Scratch-Partition auf dem Startgerät erstellt werden können. Wenn eine kleinere Festplatte oder LUN verwendet wird, versucht das Installationsprogramm, einen Scratch-Bereich auf einer anderen lokalen Festplatte zuzuteilen. Wenn keine lokale Festplatte gefunden wird, wird die Scratch-Partition `/scratch` auf der ESXi-Host-Ramdisk erstellt, die mit `/tmp/scratch` verknüpft ist. Sie können `/scratch` neu konfigurieren, um eine separate Festplatte oder LUN zu verwenden. Um eine bestmögliche Leistung zu erzielen und den Arbeitsspeicher zu optimieren, sollten Sie `/scratch` nicht auf der ESXi-Host-Ramdisk belassen.

Zum Neukonfigurieren von `/scratch` finden Sie weitere Informationen unter dem Thema „Festlegen der Scratch-Partition vom vSphere Web Client aus“ in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

Aufgrund der E/A-Empfindlichkeit von USB- und SD-Geräten erstellt das Installationsprogramm keine Scratch-Partition auf diesen Geräten. Beim Installieren oder Upgraden auf USB- bzw. SD-Geräten versucht das Installationsprogramm, einen Scratch-Bereich auf einer verfügbaren lokalen Festplatte oder einem lokalen Datenspeicher zuzuteilen. Wenn keine lokale Festplatte bzw. kein lokaler Datenspeicher gefunden wird, wird `/scratch` auf der Ramdisk abgelegt. Nach der Installation bzw. nach dem Upgrade sollten Sie `/scratch` neu konfigurieren, um einen dauerhaften Datenspeicher zu verwenden. Ein USB/SD-Gerät mit 1 GB reicht zwar für die Minimalinstallation aus, aber Sie sollten ein Gerät mit mindestens 4 GB verwenden. Der zusätzliche Speicher wird für eine erweiterte Coredump-Partition auf dem USB/SD-Gerät verwendet. Verwenden Sie ein qualitativ hochwertiges USB-Flash-Laufwerk mit mindestens 16 GB, sodass

die zusätzlichen Flashzellen die Lebensdauer des Startmediums verlängern können, aber qualitativ hochwertige Laufwerke mit mindestens 4 GB reichen für die erweiterte Coredump-Partition aus. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel <http://kb.vmware.com/kb/2004784>.

Bei Auto Deploy-Installationen versucht das Installationsprogramm, einen Scratch-Bereich auf einer verfügbaren lokalen Festplatte oder einem lokalen Datenspeicher zuzuteilen. Wenn keine lokale Festplatte bzw. kein lokaler Datenspeicher gefunden wird, wird `/scratch` auf der Ramdisk abgelegt. Sie sollten `/scratch` neu konfigurieren, um nach der Installation einen dauerhaften Datenspeicher zu verwenden.

Bei Umgebungen, die von einem SAN starten oder Auto Deploy verwenden, ist es nicht erforderlich, eine separate LUN für jeden ESXi-Host zuzuteilen. Sie können die Scratch-Bereiche für viele ESXi-Hosts zusammen auf einer einzelnen LUN unterbringen. Die Anzahl der Hosts, die einer einzelnen LUN zugewiesen sind, sollten anhand der LUN-Größe und dem E/A-Verhalten der virtuellen Maschinen abgewogen werden.

Unterstützte Remotemanagement-Servermodelle und Firmware-Versionen

Sie können Remotemanagement-Anwendungen für die Installation bzw. das Upgrade von ESXi oder für die Remoteverwaltung von Hosts verwenden.

Tabelle 2-8. Unterstützte Remotemanagement-Servermodelle und Mindest-Firmware-Versionen

Remotemanagement-Servermodell	Firmware-Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20, 1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
IBM RSA 2	1.03, 1.2	1.6.0_22

Empfehlungen für verbesserte ESXi-Leistung

Installieren oder upgraden Sie ESXi zur Verbesserung der Leistung auf einem leistungsfähigen System mit mehr als dem erforderlichen Mindestwert an RAM und mit mehreren physischen Festplatten.

Weitere Informationen zu den ESXi-Systemanforderungen finden Sie unter [Hardwareanforderungen für ESXi](#). Weitere Informationen finden Sie auch in den technischen Dokumenten zur Leistung von vSphere <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-perfbest-practices-vsphere6-0-white-paper.pdf>.

Tabelle 2-9. Empfehlungen zur Leistungssteigerung

Systemelement	Empfehlung
RAM	<p>ESXi-Hosts benötigen mehr RAM-Speicher als übliche Server. Stellen Sie mindestens 8 GB RAM bereit, um alle Vorteile der ESXi-Funktionen optimal nutzen und virtuelle Maschinen in typischen Produktionsumgebungen ausführen zu können. Ein ESXi-Host muss über ausreichend RAM verfügen, um mehrere virtuelle Maschinen gleichzeitig auszuführen. Die folgenden Beispiele sollen Ihnen bei der Berechnung des RAM helfen, der von den virtuellen Maschinen benötigt wird, die auf dem ESXi-Host ausgeführt werden.</p> <p>Der Betrieb von vier virtuellen Maschinen mit Red Hat Enterprise Linux oder Windows XP erfordert mindestens 3 GB RAM für die Baseline-Leistung. Darin enthalten sind etwa 1024 MB für die virtuelle Maschinen, 256 MB Minimum für jedes Betriebssystem, wie von den Anbietern empfohlen.</p> <p>Die Ausführung dieser vier virtuelle Maschinen mit jeweils 512 MB RAM hat zur Folge, dass der ESXi-Host ungefähr 4 GB RAM haben muss, worin 2048 MB für die virtuelle Maschinen enthalten sind.</p> <p>Für diese Berechnungen wurde keine mögliche Einsparung von Arbeitsspeicher durch variable Overhead-Speicherkapazität für die einzelnen virtuelle Maschinen berücksichtigt. Siehe <i>vSphere-Ressourcenverwaltung</i>.</p>
Dedizierte schnelle Ethernet-Adapter für virtuelle Maschinen	<p>Verwenden Sie für Verwaltungsnetzwerke und Netzwerke virtueller Maschinen verschiedene physische Netzwerkkarten. Dedizierte Gigabit-Ethernet-Karten für virtuelle Maschinen, z.B. Intel PRO/1000-Adapter, verbessern den Durchsatz zu virtuelle Maschinen bei hohem Netzwerkdatenverkehr.</p>
Festplattenspeicherort	<p>Alle von den virtuelle Maschinen verwendeten Daten sollten sich auf physischen, den virtuelle Maschinen speziell zugeteilten Festplatten befinden. Sie können die Leistung steigern, wenn Sie Ihre virtuelle Maschinen nicht auf der Festplatte ablegen, die das ESXi-Boot-Image enthält. Verwenden Sie physische Festplatten, die groß genug sind, um Festplatten-Images aufzunehmen, die von allen virtuelle Maschinen verwendet werden.</p>

Tabelle 2-9. Empfehlungen zur Leistungssteigerung (Fortsetzung)

Systemelement	Empfehlung
VMFS5-Partitionierung	<p>Das ESXi-Installationsprogramm erstellt die anfänglichen VMFS-Volumes automatisch auf der ersten leeren gefundenen lokalen Festplatte. Verwenden Sie zum Hinzufügen von Festplatten oder zum Ändern der ursprünglichen Konfiguration den vSphere Web Client. Dadurch wird gewährleistet, dass die Startsektoren der Partitionen für 64 KB ausgerichtet sind, wodurch eine Verbesserung der Speicherleistung erzielt werden kann.</p> <p>Hinweis In reinen SAS-Umgebungen kann es vorkommen, dass das Installationsprogramm die Festplatten nicht formatiert. Bei manchen SAS-Festplatten ist es nicht möglich festzustellen, ob die Festplatten lokal oder remote sind. Nach der Installation können Sie den vSphere Web Client zum Einrichten von VMFS verwenden.</p>
Prozessoren	Die ESXi-Leistung kann durch schnellere Prozessoren gesteigert werden. Für bestimmte Workloads verbessern größere Caches die Leistung von ESXi.
Hardwarekompatibilität	Verwenden Sie auf Ihrem Server Geräte, die von ESXi 6.0-Treibern unterstützt werden. Weitere Informationen finden Sie im <i>Hardware-Kompatibilitätshandbuch</i> unter http://www.vmware.com/resources/compatibility .

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Im vSphere Web Client können Sie für jeden Dienst die Firewall öffnen oder schließen oder den Datenverkehr aus bestimmten IP-Adressen durchlassen.

Die folgende Tabelle enthält die Firewalls für die üblicherweise installierten Dienste. Wenn Sie andere VIBs auf Ihrem Host installieren, stehen Ihnen möglicherweise weitere Dienste und Firewall-Ports zur Verfügung.

Tabelle 2-10. Eingehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-Server	5988 (TCP)	Server für CIM (Common Information Model)
Sicherer CIM-Server	5989 (TCP)	Sicherer Server für CIM
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	546 (TCP, UDP)	DHCP-Client für IPv6

Tabelle 2-10. Eingehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.
Virtual SAN-Clusterbildungsdienst	12345, 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst für Virtual SAN. Verwendet UDP-basiertes IP-Multicast zur Bestimmung von Clustermitgliedern und Verteilung von Virtual SAN-Metadaten an alle Clustermitglieder. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
DHCP-Client	68 (UDP)	DHCP-Client für IPv4
DNS-Client	53 (UDP)	DNS-Client
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Datenverkehr zwischen Hosts für vSphere Fault Tolerance (FT)
NSX Distributed Logical Router-Dienst	6999 (UDP)	NSX Virtual Distributed Logical Router-Dienst. Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein. In früheren Produktversionen wurde dieser Dienst als „NSX Distributed Logical Router“ bezeichnet.
Virtual SAN-Transport	2233 (TCP)	Zuverlässiger Datagramm-Transport für Virtual SAN. Verwendet TCP und dient der Virtual SAN-Speicher-E/A. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
SNMP-Server	161 (UDP)	Ermöglicht dem Host die Verbindung mit einem SNMP-Server.
SSH-Server	22 (TCP)	Erforderlich für SSH-Zugriff.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
vSphere Web Client	902, 443 (TCP)	Client-Verbindungen

Tabelle 2-10. Eingehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
vsanvp	8080 (TCP)	VSAN-VASA-Anbieter-Provider. Wird vom Speicherverwaltungsdienst (Storage Management Service, SMS) im Umfang von vCenter für den Zugriff auf Daten zu Virtual SAN-Speicherprofilen, Funktionen und Compliance genutzt. Wenn deaktiviert, kann das Virtual SAN Storage Profile Based Management (SPBM) nicht genutzt werden.
vSphere Web Access	80 (TCP)	Begrüßungsseite mit Downloadlinks für verschiedene Schnittstellen

Tabelle 2-11. Ausgehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	547 (TCP, UDP)	DHCP-Client für IPv6
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.
HBR	44046, 31031 (TCP)	Wird von vSphere Replication und VMware Site Recovery Manager für den laufenden Replizierungsdatenverkehr verwendet.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.
WOL	9 (UDP)	Verwendet von „Wake on LAN“.
Virtual SAN-Clusterbildungsdienst	12345 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst, verwendet von Virtual SAN
DHCP-Client	68 (UDP)	DHCP-Client
DNS-Client	53 (TCP, UDP)	DNS-Client
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Unterstützt VMware Fault Tolerance.
Software-iSCSI-Client	3260 (TCP)	Unterstützt Software-iSCSI.

Tabelle 2-11. Ausgehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
NSX Distributed Logical Router-Dienst	6999 (UDP)	Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein.
rabbitmqproxy	5671 (TCP)	Ein auf dem ESXi-Host ausgeführter Proxy, der Hostanwendungen innerhalb von virtuellen Maschinen die Kommunikation mit den AMQP-Brokern in der vCenter-Netzwerkdomäne ermöglicht. Die virtuelle Maschine muss sich nicht im Netzwerk befinden, d. h., es ist keine Netzwerkkarte erforderlich. Der Proxy verbindet sich mit den Brokern in der vCenter-Netzwerkdomäne. Die IP-Adressen der ausgehenden Verbindungen müssen daher mindestens die aktuell oder zukünftig verwendeten Broker enthalten. Bei einer Erweiterung können zusätzliche Broker hinzugefügt werden.
Virtual SAN-Transport	2233 (TCP)	Wird für den RDT-Datenverkehr (Unicast-Peer-to-Peer-Kommunikation) zwischen Virtual SAN-Knoten verwendet.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server-Agent
vsanvp	8080 (TCP)	Wird für Virtual SAN-Anbieter-Provider-Datenverkehr verwendet.

DNS-Anforderungen für vSphere

Sie installieren oder upgraden vCenter Server, wie alle anderen Netzwerkservers auch, auf einem Computer mit einer festen IP-Adresse und einem bekannten DNS-Namen, damit Clients einen verlässlichen Zugriff auf den Dienst haben.

Weisen Sie dem Windows-Server, der das vCenter Server-System hosten soll, eine statische IP-Adresse und einen Hostnamen zu. Diese IP-Adresse muss eine gültige (interne) Registrierung für das DNS (Domain Name System) haben. Wenn Sie vCenter Server und den Platform Services Controller installieren, müssen Sie den vollqualifizierten Domännennamen (FQDN) oder die statische IP-Adresse der Hostmaschine, auf der Sie die Installation bzw. das Upgrade durchführen, angeben. Es wird empfohlen, den FQDN zu verwenden.

Bei der Bereitstellung der vCenter Server Appliance können Sie der Appliance eine statische IP-Adresse zuweisen. Dadurch stellen Sie sicher, dass bei einem Neustart des Systems die IP-Adresse der vCenter Server Appliance unverändert bleibt.

Stellen Sie sicher, dass das DNS-Reverse-Lookup einen FQDN zurückgibt, wenn dieser mit der IP-Adresse der Hostmaschine abgefragt wird, auf der vCenter Server installiert ist. Bei der Installation bzw. beim Upgrade von vCenter Server schlägt die Installation bzw. das Upgrade der Webserverkomponente, die den vSphere Web Client unterstützt, fehl, wenn das Installationsprogramm den vollqualifizierten Domänennamen der Hostmaschine von vCenter Server nicht über die IP-Adresse abrufen kann. Das Reverse-Lookup wird unter Verwendung von PTR Records implementiert.

Wenn Sie DHCP anstelle einer statischen IP-Adresse für vCenter Server verwenden, stellen Sie sicher, dass der vCenter Server-Computernamen im DNS (Domain Name Service) aktualisiert ist. Ist der Ping-Test mit dem Computernamen erfolgreich, wurde der Name im DNS aktualisiert.

Stellen Sie sicher, dass die Verwaltungsschnittstelle des ESXi-Hosts von der vCenter Server-Instanz und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat. Stellen Sie sicher, dass der vCenter Server von allen ESXi-Hosts und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat.

Softwareanforderungen für den vSphere Web Client

Stellen Sie sicher, dass Ihr Browser vSphere Web Client unterstützt.

Für vSphere Web Client 6.0 ist Adobe Flash Player 16 oder höher erforderlich. Die neueste Adobe Flash Player-Version für Linux-Systeme ist 11.2. Deshalb kann der vSphere Web Client nicht auf Linux-Plattformen ausgeführt werden.

VMware unterstützt die folgenden getesteten Gastbetriebssysteme und Browserversionen für vSphere Web Client: Verwenden Sie Google Chrome für bestmögliche Leistung.

Tabelle 2-12. Unterstützte Gastbetriebssysteme und Browsermindestversionen für den vSphere Web Client

Betriebssystem	Browser
Windows	Microsoft Internet Explorer 10.0.19 oder höher. Mozilla Firefox 34 und höher. Google Chrome 39 und höher.
Mac OS	Mozilla Firefox 34 und höher. Google Chrome 39 und höher.

Softwareanforderungen für das Client-Integrations-Plug-In

Wenn Sie das Client-Integrations-Plug-In unabhängig vom vSphere Web Client installieren möchten, sodass Sie sich mit einem ESXi-Host verbinden und die vCenter Server Appliance bereitstellen oder aktualisieren können, stellen Sie sicher, dass Ihr Browser das Client-Integrations-Plug-In unterstützt.

Bevor Sie das Client-Integrations-Plug-In verwenden können, prüfen Sie, ob Sie einen der unterstützten Webbrowser haben.

Tabelle 2-13. Unterstützte Webbrowser

Browser	Unterstützte Versionen
Microsoft Internet Explorer	Version 10 oder 11
Mozilla Firefox	Version 30 oder höher
Google Chrome	Version 35 oder höher

vSphere Client-Anforderungen

Sie können den vSphere Client zum Verwalten eines einzelnen ESXi-Hosts installieren. Das Windows-System, auf dem Sie vSphere Client installieren, muss bestimmte Hardware- und Softwareanforderungen erfüllen.

vSphere-Client-Hardwareanforderungen

Stellen Sie sicher, dass die vSphere-Client-Hardware die Mindestanforderungen erfüllt.

Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client

Tabelle 2-14. Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client

vSphere-Client-Hardware	Anforderungen und Empfehlungen
CPU	1 CPU
Prozessor	500 MHz oder schnellerer Intel- oder AMD-Prozessor (1 GHz empfohlen)
Arbeitsspeicher	500 MB (1 GB empfohlen)

Tabelle 2-14. Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client (Fortsetzung)

vSphere-Client-Hardware	Anforderungen und Empfehlungen
Festplattenspeicher	<p>1,5 GB freier Festplattenspeicher für eine Komplettinstallation mit den folgenden Komponenten:</p> <ul style="list-style-type: none"> ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# <p>Entfernen Sie alle vorherigen Versionen von Microsoft Visual J# von dem System, auf dem Sie den vSphere-Client installieren möchten.</p> <ul style="list-style-type: none"> ■ vSphere Client <p>Wenn keine der Komponenten bereits installiert sind, werden 400 MB an freien Speicherplatz auf dem Laufwerk benötigt, auf dem sich das %temp%-Verzeichnis befindet.</p> <p>Wenn alle Komponenten bereits installiert sind, werden 300 MB an freiem Speicherplatz auf dem Laufwerk benötigt, auf dem sich das Verzeichnis%temp% befindet, und 450 MB sind für vSphere-Client erforderlich.</p>
Netzwerk	Gigabit-Verbindung empfohlen

Softwareanforderungen des vSphere Clients

Stellen Sie sicher, dass vSphere Client von Ihrem Betriebssystem unterstützt wird.

Eine vollständige aktuelle Liste der unterstützten Betriebssysteme für den vSphere Client finden Sie unter [Unterstützte Hostbetriebssysteme für die vSphere Client \(Windows\)-Installation](#).

Der vSphere-Client benötigt das Microsoft .NET 3.5 SP1 Framework. Falls dieses nicht auf Ihrem System installiert ist, wird es vom vSphere-Client-Installationsprogramm installiert. Für die .NET 3.5 SP1-Installation wird möglicherweise eine Internetverbindung zum Herunterladen zusätzlicher Dateien benötigt.

TCP- und UDP-Ports für den vSphere Client

Der Zugriff auf ESXi-Hosts und andere Netzwerkkomponenten erfolgt über vorab festgelegte TCP- und UDP-Ports. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

Die Tabelle enthält eine Auflistung von TCP- und UDP-Ports mit dem jeweiligen Zweck und Typ. Bei der Installation standardmäßig geöffnete Ports werden angegeben (Standard).

Tabelle 2-15. TCP- und UDP-Ports

Port	Zweck	Art des Datenverkehrs
443 (Standard)	HTTPS-Zugriff vSphere Client zugriff auf vCenter Server vSphere Client-Zugriff auf ESXi-Hosts vSphere Client-Zugriff auf vSphere Update Manager	Eingehendes TCP zum ESXi-Host
902 (Standard)	vSphere Client-Zugriff auf die Konsolen virtueller Maschinen	Eingehendes TCP zum ESXi-Host, ausgehendes TCP aus dem ESXi-Host, ausgehendes UDP aus dem ESXi-Host

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Wenn Sie Auto Deploy für die Installation Ihres ESXi 6.0-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volume eingerichtet haben, müssen Sie möglicherweise die aktuellen Einstellungen für die Protokollgröße und die Rotation ändern, um sicherzustellen, dass ausreichend Speicherplatz für die Systemprotokollierung verfügbar ist.

Alle vSphere-Komponenten verwenden diese Infrastruktur. Die Standardwerte für die Protokollkapazität in dieser Infrastruktur variieren je nach verfügbarem Speicherplatz und je nach Konfiguration der Systemprotokollierung. Hosts, die mit Auto Deploy bereitgestellt werden, speichern Protokolle auf einer RAM-Festplatte. Der verfügbare Speicherplatz für Protokolle ist daher gering.

Wenn Ihr Host mit Auto Deploy bereitgestellt wurde, stehen Ihnen für die Konfiguration des Protokollspeichers folgende Möglichkeiten zur Verfügung:

- Leiten Sie die Protokolle über das Netzwerk zu einem Remote-Controller um.
- Leiten Sie die Protokolle zu einem NAS- oder NFS-Speicher um.

Wenn Sie Protokolle an einen nicht standardmäßigen Speicher umleiten, zum Beispiel an einen NAS- oder NFS-Speicher, können Sie die Größe und Rotation der auf der Festplatte installierten Hosts ebenfalls neu konfigurieren.

Sie müssen den Protokollspeicher für ESXi-Hosts nicht neu konfigurieren, die die Standardkonfiguration verwenden, bei der Protokolle in einem Scratch-Verzeichnis auf dem VMFS-Volume gespeichert werden. Für diese Hosts konfiguriert ESXi 6.0 die Protokolle in optimaler Abstimmung mit Ihrer Installation und bietet ausreichend Speicherplatz für Protokollnachrichten.

Tabelle 2-16. Empfohlene Mindestgröße und Rotationskonfiguration für hostd-, vpxa- und fdm-Protokolle

Protokoll	Maximale Protokolldateigröße	Anzahl der beizubehaltenden Rotationen	Mindestens erforderlicher Festplattenspeicher
Verwaltungs-Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA-Agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

Informationen zum Einrichten und Konfigurieren des Syslog-Protokolls und eines Syslog-Servers und zum Installieren von vSphere Syslog Collector finden Sie in der Dokumentation zu *Installations- und Einrichtungshandbuch für vSphere*.

Vor dem Upgrade von vCenter Server

3

Stellen Sie sicher, dass Ihr System für das Upgrade von vCenter Server vorbereitet ist, indem Sie die Kompatibilität überprüfen und erforderliche Aufgaben für die Datenbank oder für das Netzwerk oder sonstige vorbereitenden Aufgaben ausführen.

Dieses Kapitel enthält die folgenden Themen:

- Überprüfen der grundlegenden Kompatibilität vor dem Upgrade von vCenter Server
- Vorbereiten der vCenter Server-Datenbanken
- Überprüfen der Netzwerkvoraussetzungen vor dem Upgrade
- Überprüfen des Lastausgleichsdiensts vor dem Upgrade von vCenter Server
- Vorbereiten der ESXi-Hosts für das Upgrade von vCenter Server
- Überprüfen der Vorbereitungen für das Upgrade von vCenter Server
- Erforderliche Informationen für das Upgrade von vCenter Server für Windows
- Erforderliche Informationen für das Upgrade der vCenter Server Appliance

Überprüfen der grundlegenden Kompatibilität vor dem Upgrade von vCenter Server

Prüfen Sie vor dem Upgrade von vCenter Server, ob alle Komponenten die grundlegenden Kompatibilitätsanforderungen erfüllen.

Wenn Sie das Betriebssystem eines vCenter Single Sign On 5.1-Systems zum Erfüllen der Betriebssystemanforderungen von Windows 2003 auf Windows 2008 aktualisieren, können Symptome ähnlich wie beim Knowledgebase-Artikel [2036170](#) auftreten.

Voraussetzungen

Stellen Sie sicher, dass Ihr System die Hardware- und Softwareanforderungen erfüllt. Siehe [Anforderungen für vCenter Server für Windows](#) und [Anforderungen für die vCenter Server Appliance](#)

Wenn Sie Lösungen oder Plug-Ins haben, prüfen Sie die VMware-Produkt-Interoperabilitätmatrix. Siehe http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Verfahren

- 1 Der Installationspfad der vorherigen Version von vCenter Server muss zu den Installationsanforderungen für Microsoft Active Directory Application Mode (ADAM/AD LDS) kompatibel sein.

Der Installationspfad darf keines der folgenden Zeichen enthalten: Nicht-ASCII-Zeichen, Kommas (,), Punkte (.), Ausrufezeichen (!), Nummernzeichen (#), At-Zeichen (@) bzw. Prozentzeichen (%).

Wenn Ihre vorherige vCenter Server-Version dieser Anforderung nicht genügt, müssen Sie eine Neuinstallation von vCenter Server durchführen.

- 2 Stellen Sie sicher, dass das vCenter Server-System kein Active Directory-Domänencontroller ist, weder primär noch als Sicherung.
- 3 Aktualisieren Sie alle ESX/ESXi 4.1-Hosts auf Version 5.x.
- 4 ESX 4.x-Hosts, die Sie nicht aktualisieren möchten, müssen Sie aus der vCenter Server-Bestandsliste entfernen.
- 5 Wenn die von Ihnen aktualisierte vCenter Server 4.x-Umgebung Guided Consolidation 4.x enthält, müssen Sie vor dem Upgrade auf vCenter Server 6.0 Guided Consolidation deinstallieren.

Vorbereiten der vCenter Server-Datenbanken

vCenter Server benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten. Sie können entweder die mitgelieferte PostgreSQL-Datenbank verwenden, die bei der Bereitstellung installiert und konfiguriert werden kann, oder Sie können eine externe Datenbank einrichten.

vCenter Server für Windows unterstützt Oracle- und Microsoft SQL-Datenbanken, während die vCenter Server Appliance nur eine Oracle-Datenbank als externe Datenbank unterstützt.

Die Datenbank wird zwar automatisch vom Installationsprogramm konfiguriert, aber Sie können eine externe Datenbank manuell oder mithilfe eines Skripts konfigurieren. Darüber hinaus benötigt der DSN-Benutzer bestimmte Berechtigungen.

Die Datenbankkennwörter werden auf der virtuellen Windows-Maschine oder dem physischen Host, auf der/dem Sie vCenter Server installieren, und in der vCenter Server Appliance als lesbarer Text gespeichert. Die Dateien mit den Kennwörtern sind durch das Betriebssystem geschützt, d. h., nur ein lokaler Windows-Administrator oder ein Linux-Root-Benutzer kann auf diese Dateien zugreifen und sie lesen.

vCenter Server-Instanzen können nicht dasselbe Datenbankschema verwenden. Mehrere vCenter Server-Datenbanken können sich auf demselben Datenbankserver befinden oder auf mehrere Datenbankserver aufgeteilt werden. Für Oracle-Datenbanken, die das Schemaobjektkonzept verwenden, können Sie mehrere vCenter Server-Instanzen auf einem einzelnen Datenbankserver ausführen, wenn für jede vCenter Server-Instanz ein anderer Schemabesitzer vorhanden ist. Darüber hinaus können Sie für jede vCenter Server-Instanz einen dedizierten Oracle-Datenbankserver verwenden.

Vorbereiten der Oracle-Datenbank vor dem Upgrade auf vCenter Server 6.0

Stellen Sie sicher, dass Ihre Oracle-Datenbank die entsprechenden Voraussetzungen erfüllt, dass Sie die erforderlichen Anmeldedaten haben und dass Sie jede erforderliche Bereinigung und andere Vorbereitungen vor dem Upgrade von vCenter Server ausführen.

Voraussetzungen

Sie müssen die grundlegende Upgrade-Interoperabilität bestätigen, bevor Sie Ihre Oracle-Datenbank für das Upgrade von vCenter Server vorbereiten. Siehe [Datenbankanforderungen für vCenter Server für Windows](#) und [Datenbankanforderungen für die vCenter Server Appliance](#).

Vergewissern Sie sich, dass Sie Ihre Datenbank gesichert haben. Informationen zum Erstellen einer Sicherungskopie der vCenter Server-Datenbank finden Sie in der Oracle-Dokumentation.

Informationen zum korrekten Festlegen von Datenbankberechtigungen finden Sie unter [Datenbankberechtigungsanforderungen für vCenter Server](#).

Verfahren

- 1 Überprüfen Sie, ob Ihre Datenbank die Upgrade-Anforderungen erfüllt. Aktualisieren Sie bei Bedarf die Datenbank auf eine unterstützte Version.
- 2 Wenn Ihr Datenbankserver nicht vom vCenter Server unterstützt wird, führen Sie ein Datenbankupgrade auf eine unterstützte Version durch oder importieren Sie Ihre Datenbank in eine unterstützte Version.
- 3 Wenn Ihre vorhandene Datenbank eine Oracle-Datenbank ist und Sie auf eine neu unterstützte Oracle-Datenbank wie Oracle 11g aktualisieren möchten, aktualisieren Sie Ihre Oracle-Datenbank vor dem Upgrade von vCenter Server.

Sie müssen keine Neuinstallation von vCenter Server durchführen, wenn Ihre vorhandene Datenbank eine Oracle-Datenbank ist.

Sie können z. B. Ihre vorhandene Oracle 9i-Datenbank zunächst auf Oracle 11g oder Oracle 12c aktualisieren und dann vCenter Server 5.x auf vCenter Server 6.0 aktualisieren.

- 4 Überprüfen Sie, dass die Kennwörter aktuell sind und nicht in Kürze ablaufen.
- 5 Sie müssen über Anmeldedaten, den Datenbanknamen und den Namen des Datenbankservers, der von der vCenter Server-Datenbank verwendet werden soll, verfügen.

Suchen Sie im ODBC-System den Verbindungsnamen der Datenbankquelle für die vCenter Server-Datenbank.
- 6 Verwenden Sie den Oracle SERVICE_NAME anstelle der SID, um sicherzustellen, dass Ihre Oracle-Datenbankinstanz verfügbar ist.

- Melden Sie sich beim Datenbankserver an, um das Warnungsprotokoll zu lesen: `$ORACLE_BASE/diag//rdbms/$instance_name/$INSTANCE_NAME/trace/alert_$ INSTANCE_NAME.log`.

- Melden Sie sich beim Datenbankserver an, um die Oracle Listener-Statusausgabe zu lesen.
 - Wenn Sie den SQL*Plus-Client installiert haben, können Sie `tnsping` für die vCenter-Datenbankinstanz verwenden. Wenn der Befehl `tnsping` beim ersten Mal nicht ausgeführt wird, versuchen Sie es nach ein paar Minuten erneut. Sollte dies auch nicht funktionieren, starten Sie die vCenter-Datenbankinstanz auf dem Oracle-Server neu und führen Sie `tnsping` erneut aus, um sicherzustellen, dass die Instanz verfügbar ist.
- 7 Prüfen Sie, ob die JDBC-Treiberdatei in der CLASSPATH-Variablen enthalten ist.
 - 8 Prüfen Sie, ob die Berechtigungen korrekt festgelegt sind.
 - 9 Weisen Sie dem Benutzer die DBA-Rolle zu oder gewähren Sie ihm die erforderlichen Berechtigungen.
 - 10 Suchen Sie das Skript „cleanup_orphaned_data_Oracle.sql“ im ISO-Image und kopieren Sie es auf den Oracle-Server.
 - 11 Melden Sie sich mit dem Konto der vCenter Server-Datenbank bei einer SQL*Plus-Sitzung an.
 - 12 Führen Sie das Bereinigungsskript aus.


```
@pathcleanup_orphaned_data_Oracle.sql
```

Bei der Bereinigung werden überflüssige Daten und Daten ohne übergeordnetes Element, die von keiner vCenter Server-Komponente verwendet werden, entfernt.
 - 13 Sichern Sie die vCenter Server- und die vCenter Inventory Service-Datenbanken vollständig.

Ergebnisse

Ihre Datenbank ist auf das vCenter Server-Upgrade vorbereitet.

Nächste Schritte

Nach dem Abschluss des Upgrades können Sie die folgenden Berechtigungen aus dem Benutzerprofil entfernen: **create any sequence** und **create any table**.

Standardmäßig werden der **RESOURCE** Rolle die Berechtigungen **CREATE PROCEDURE**, **CREATE TABLE** und **CREATE SEQUENCE** zugewiesen. Falls diese Berechtigungen der Rolle **RESOURCE** nicht zugewiesen wurden, gewähren Sie sie dem vCenter Server-Datenbankbenutzer.

Vorbereiten der Microsoft SQL Server-Datenbank vor dem Upgrade auf vCenter Server 6.0

Stellen Sie sicher, dass Ihre Microsoft SQL Server-Datenbank die entsprechenden Voraussetzungen erfüllt, dass Sie die erforderlichen Anmeldedaten haben und dass Sie jede erforderliche Bereinigung und andere Vorbereitungen vor dem Upgrade von vCenter Server ausführen.

Informationen zum Entfernen der DBO-Rolle und zum Migrieren aller Objekte im DBO-Schema auf ein benutzerdefiniertes Schema finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1036331>.

Microsoft SQL Server Express wird von vCenter Server 6.0 nicht mehr unterstützt. Die eingebettete Microsoft SQL Server-Express-Datenbank von vCenter Server 5.x wird beim Upgrade auf vCenter Server 6.0 durch eine eingebettete PostgreSQL-Datenbank ersetzt. Informationen zum Upgrade ohne Migration zur PostgreSQL-Datenbank finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2109321>.

Informationen zum Migrieren der vCenter Server-Datenbank von Microsoft SQL Express zu Microsoft SQL Server finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1028601>.

Wichtig Die integrierte Windows-Authentifizierungsmethode können Sie nicht verwenden, wenn der vCenter Server-Dienst unter dem integrierten Systemkonto von Microsoft Windows ausgeführt wird.

Voraussetzungen

Sie müssen die grundlegende Upgrade-Interoperabilität bestätigen, bevor Sie Ihre Microsoft SQL Server-Datenbank für das Upgrade von vCenter Server vorbereiten. Siehe [Datenbankanforderungen für vCenter Server für Windows](#) und [Datenbankanforderungen für die vCenter Server Appliance](#).

Vergewissern Sie sich, dass Sie Ihre Datenbank gesichert haben. Informationen zum Erstellen einer Sicherungskopie der vCenter Server-Datenbank finden Sie in der Dokumentation zu Microsoft SQL Server.

Informationen zum korrekten Festlegen von Datenbankberechtigungen finden Sie unter [Datenbankberechtigungsanforderungen für vCenter Server](#) und [Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen](#).

Verfahren

- 1 Überprüfen Sie, ob Ihre Datenbank die Upgrade-Anforderungen erfüllt. Aktualisieren Sie bei Bedarf die Datenbank auf eine unterstützte Version.
- 2 Wenn Ihr Datenbankserver nicht vom vCenter Server unterstützt wird, führen Sie ein Datenbankupgrade auf eine unterstützte Version durch oder importieren Sie Ihre Datenbank in eine unterstützte Version.
- 3 Wenn Ihre vorhandene Datenbank eine Microsoft SQL Server-Datenbank ist und Sie auf eine neu unterstützte Microsoft SQL Server-Datenbank wie Microsoft SQL Server 2012 aktualisieren möchten, aktualisieren Sie Ihre Microsoft SQL Server-Datenbank vor dem Upgrade von vCenter Server.

Sie müssen keine Neuinstallation von vCenter Server durchzuführen, wenn Ihre vorhandene Datenbank eine Microsoft SQL Server-Datenbank ist.

Sie können z. B. ein Upgrade einer Microsoft SQL Server 2005-Datenbank auf eine Microsoft SQL Server 2008 R2-SP2-, 2012- oder 2014-Datenbank und dann ein Upgrade von vCenter Server 5.0 oder höher auf vCenter Server 6.0 durchführen.

Wenn Sie die Datenbank von Microsoft SQL Server 2005 auf Microsoft SQL Server 2008 R2-SP2 oder höher migrieren, legen Sie die Kompatibilitätsstufe der Datenbank auf 100 fest.

- 4 Prüfen Sie, ob die Berechtigungen korrekt festgelegt sind.
- 5 Überprüfen Sie, dass die Kennwörter aktuell sind und nicht in Kürze ablaufen.
- 6 Prüfen Sie, ob JDK 1.6 oder höher auf dem vCenter Server-System installiert ist.
- 7 Stellen Sie sicher, dass auf der Maschine, auf der vCenter Server aktualisiert werden soll, die Datei `sqljdbc4.jar` zu der Variablen `CLASSPATH` hinzugefügt wird.

Wenn die Datei `sqljdbc4.jar` noch nicht auf Ihrem System installiert ist, erfolgt die Installation über das vCenter Server-Installationsprogramm.

- 8 Prüfen Sie, ob der Quellname Ihrer Systemdatenbank den Treiber von Microsoft SQL Server Native Client 10 oder 11 verwendet.
- 9 Wenn Sie die DBO-Rolle entfernen und alle Objekte im DBO-Schema auf ein benutzerdefiniertes Schema migrieren möchten, müssen Sie die erforderlichen Berechtigungen gewähren.
 - a Gewähren Sie dem vCenter Server-Benutzer in der vCenter Server-Datenbank die erforderlichen Berechtigungen.
 - b Gewähren Sie dem Benutzer in der MSDB-Datenbank die erforderlichen Berechtigungen.
- 10 Suchen Sie das Skript `cleanup_orphaned_data_MSSQL.sql` im ISO-Image und kopieren Sie es auf den Microsoft SQL-Server.
- 11 Melden Sie sich bei Ihrer Datenbank an.
 - a Öffnen Sie bei Microsoft SQL Server Express ein Befehlsfenster.
 - b Melden Sie sich bei Microsoft SQL Server bei einer Sitzung von Microsoft SQL Server Management Studio als vCenter Server-Datenbankbenutzer an.

- 12 Führen Sie bei Microsoft SQL Server Express das Bereinigungsskript aus.

```
sqlcmd -E -S localhost\VIM_SQLEXP -d VIM_VCDB -i
pathcleanup_orphaned_data_MSSQL.sql
```

- 13 Führen Sie bei Microsoft SQL Server den Inhalt von „`cleanup_orphaned_data_MSSQL.sql`“ aus.

Stellen Sie sicher, dass Sie mit der von vCenter Server verwendeten Datenbank verbunden sind.

Mit dem Bereinigungsskript werden alle überflüssigen Daten in Ihrer vCenter Server-Datenbank bereinigt.

- 14 Sichern Sie die vCenter Server- und die Inventory Service-Datenbanken vollständig.

Ergebnisse

Ihre Datenbank ist auf das vCenter Server-Upgrade vorbereitet.

Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen

Bei dieser Methode der Konfiguration der SQL-Datenbank können Sie das benutzerdefinierte VMW-Schema anstelle des vorhandenen dbo-Schemas verwenden. Darüber hinaus müssen Sie Datenbanküberwachung für einen Benutzer aktivieren, bevor Sie vCenter Server mit einem eingebetteten oder externen Platform Services Controller installieren.

Bei dieser Methode müssen Sie neue Datenbankrollen erstellen und diese dem *Benutzer* der Datenbank zuweisen.

Voraussetzungen

Um vor dem Upgrade von vCenter Server sicherzustellen, dass Sie die richtigen Rollen und Berechtigungen besitzen, aktualisieren Sie die SQL Server-Datenbank und -Benutzer für vCenter Server.

Verfahren

- 1 Melden Sie sich bei einer Microsoft SQL Server Management Studio-Sitzung als Sysadmin oder mit einem Benutzerkonto mit Sysadmin-Rechten an.
- 2 Führen Sie das folgende Skript aus, um die Rollen anzulegen und die Berechtigungen anzuwenden.

Das Skript im vCenter Server-Installationspaket befindet sich in der Datei `/Installationsverzeichnis/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
CREATE SCHEMA [VMW]
go
ALTER USER [vpxuser] WITH DEFAULT_SCHEMA =[VMW]

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
GRANT SELECT ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA :: [VMW] to VC_USER_ROLE
```

```

go
GRANT EXECUTE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , [vpxuser]
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use master
go
grant VIEW SERVER STATE to [vpxuser]
go
GRANT VIEW ANY DEFINITION TO [vpxuser]
go

```

Vorbereiten der PostgreSQL-Datenbank vor dem Upgrade auf vCenter Server 6.0

Vergewissern Sie sich, dass die PostgreSQL-Datenbank die Anforderungen erfüllt, dass Sie über die erforderlichen Anmeldeinformationen verfügen und dass Sie jede Bereinigung oder sonstige Vorbereitung vor dem Upgrade von vCenter Server abgeschlossen haben.

Informationen zum Sichern der vCenter Server-Datenbank finden Sie in der PostgreSQL-Dokumentation.

Voraussetzungen

Sie müssen die grundlegende Upgrade-Interoperabilität bestätigen, bevor Sie Ihre PostgreSQL-Datenbank für das Upgrade von vCenter Server vorbereiten.

Verfahren

- 1 Überprüfen Sie, dass die Kennwörter aktuell sind und nicht in Kürze ablaufen.
- 2 Suchen Sie das Skript `cleanup_orphaned_data_PostgreSQL.sql` im ISO-Image und kopieren Sie es auf Ihren PostgreSQL-Server.
- 3 Melden Sie sich bei der vCenter Server Appliance als Root-Benutzer an.
- 4 Führen Sie das Bereinigungsskript aus.

```
/opt/vmware/PostgreSQL/1.0/bin/psql -U postgres -d VCDB -f
pathcleanup_orphaned_data_Postgres.sql
```

Das Bereinigungsskript löscht und bereinigt alle unnötigen oder verwaisten Daten in der vCenter Server-Datenbank, die von keiner vCenter Server-Komponente verwendet werden.

- 5 Sichern Sie die vCenter Server- und die vCenter Inventory Service-Datenbanken vollständig.

Ergebnisse

Ihre Datenbank ist auf das vCenter Server-Upgrade vorbereitet.

Datenbankberechtigungsanforderungen für vCenter Server

Für vCenter Server ist eine Datenbank erforderlich. Wenn Sie beim Erstellen der Datenbank eine externe Oracle- oder Microsoft SQL Server-Datenbank verwenden möchten, müssen Sie dem Datenbankbenutzer bestimmte Berechtigungen zuweisen.

Beim Upgrade einer Microsoft SQL-Datenbank müssen die Berechtigungen korrekt festgelegt sein.

Tabelle 3-1. Microsoft SQL-Datenbankberechtigungen für vCenter Server

Berechtigung	Beschreibung
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT CREATE TABLE TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer Tabelle.
GRANT CREATE VIEW TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer Ansicht.
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer gespeicherten Prozedur.
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	Berechtigungen zum Ausführen von Auswahl-, Einfüg-, Lösch- und Aktualisierungsfunktionen (SELECT, INSERT,

Tabelle 3-1. Microsoft SQL-Datenbankberechtigungen für vCenter Server (Fortsetzung)

Berechtigung	Beschreibung
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	DELETE, UPDATE) bei Tabellen, die Teil des VMW-Schemas sind.
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Notwendig zum Ausführen einer gespeicherten Prozedur im Datenbankschema.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Notwendig zum Bereitstellen von SQL Server-Aufträgen. Diese Berechtigungen sind nur bei der Installation und beim Upgrade, aber nicht mehr nach der Bereitstellung erforderlich.
GRANT SELECT ON msdb.dbo.sysjobsteps TO VC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	
GRANT VIEW SERVER STATE TO [vpxuser]	
GRANT VIEW ANY DEFINITION TO [vpxuser]	Erforderlich, um dem Benutzer die Berechtigungen zum Anzeigen von Metadaten für SQL Server-Objekte zuzuweisen.

Beim Upgrade einer Oracle-Datenbank müssen die Berechtigungen korrekt festgelegt sein.

Tabelle 3-2. Oracle-Datenbankberechtigungen für vCenter Server

Berechtigung	Beschreibung
GRANT CONNECT TO VPXADMIN	Erforderlich für eine Verbindung mit der Oracle-Datenbank.
GRANT RESOURCE TO VPXADMIN	Notwendig zum Erstellen eines Auslösers, einer Sequenz, eines Typs, einer Prozedur usw. Standardmäßig werden der Rolle RESOURCE die Rechte CREATE PROCEDURE, CREATE TABLE und CREATE SEQUENCE zugewiesen. Falls diese Rechte der Rolle RESOURCE nicht zugewiesen wurden, gewähren Sie sie dem vCenter Server-Datenbankbenutzer.
GRANT CREATE VIEW TO VPXADMIN	Notwendig zum Erstellen einer Ansicht.
GRANT CREATE SEQUENCE TO VPXADMIN	Notwendig zum Erstellen einer Sequenz.
GRANT CREATE TABLE TO VPXADMIN	Notwendig zum Erstellen einer Tabelle.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Notwendig zum Erstellen einer materialisierten Ansicht.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Notwendig zur Sicherstellung, dass die vCenter Server-Datenbank von einer einzelnen vCenter Server-Instanz verwendet wird.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Notwendig bei Installation und Upgrade zum Planen und Verwalten der SQL-Aufträge. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_lock TO VPXADMIN	Notwendig zum Ermitteln vorhandener Sperren auf der vCenter Server-Datenbank.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Notwendig beim Upgrade zum Ermitteln des erforderlichen Festplattenspeicherplatzes. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Notwendig beim Upgrade zum Ermitteln des erforderlichen Festplattenspeicherplatzes. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_data_files TO VPXADMIN	Notwendig zum Überwachen des freien Speicherplatzes, während vCenter Server arbeitet.
GRANT SELECT ON v_\$session TO VPXADMIN	Verwendete Ansicht zum Ermitteln vorhandener Sperren auf der vCenter Server-Datenbank.
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Notwendig, um dem Benutzer der vCenter Server-Datenbank unbegrenzte Tablespace-Berechtigungen zuzuweisen.
GRANT SELECT ON v_\$system_event TO VPXADMIN	Notwendig zum Prüfen der Protokolldateiwechsel.
GRANT SELECT ON v_\$sysmetric_history TO VPXADMIN	Notwendig zum Prüfen der CPU-Nutzung.
GRANT SELECT ON v_\$sysstat TO VPXADMIN	Notwendig zum Ermitteln der Puffercache-Zugriffsrate.

Tabelle 3-2. Oracle-Datenbankberechtigungen für vCenter Server (Fortsetzung)

Berechtigung	Beschreibung
GRANT SELECT ON dba_data_files TO VPXADMIN	Notwendig zum Ermitteln der Tablespace-Nutzung.
GRANT SELECT ON v_\$loghist TO VPXADMIN	Notwendig zum Prüfen der Prüfpunkt-Häufigkeit.

Mit den Berechtigungen zur Master-Datenbank können Sie die vCenter Server-Datenbank überwachen, sodass zum Beispiel beim Erreichen eines bestimmten Grenzwerts eine Warnung angezeigt wird.

Überprüfen, dass vCenter Server mit der lokalen Datenbank kommunizieren kann

Wenn sich Ihre Datenbank auf der gleichen Maschine befindet, auf der vCenter Server installiert werden soll und Sie den Namen dieser Maschine geändert haben, überprüfen Sie die Konfiguration. Stellen Sie sicher, dass der vCenter Server-DSN für die Kommunikation mit dem neuen Namen der Maschine konfiguriert ist.

Das Ändern des vCenter Server-Computernamens wirkt sich auf die Datenbankkommunikation aus, wenn sich der Datenbankserver auf demselben Computer wie der vCenter Server befindet. Falls Sie den Namen des Computers geändert haben, können Sie sicherstellen, dass die Kommunikation intakt bleibt.

Im Fall einer Remotedatenbank können Sie dieses Verfahren überspringen. Die Namensänderung wirkt sich nicht auf die Kommunikation mit Remotedatenbanken aus.

Überprüfen Sie nach dem Umbenennen des Servers zusammen mit dem Datenbankadministrator oder dem Datenbankanbieter, ob alle Komponenten der Datenbank funktionieren.

Voraussetzungen

- Stellen Sie sicher, dass der Datenbankserver läuft.
- Stellen Sie sicher, dass im DNS der vCenter Server-Computernamen aktualisiert wurde.

Verfahren

- 1 Aktualisieren Sie ggf. die Datenquelleninformationen.
- 2 Pingen Sie den Namen des Computers an, um diese Verbindung zu testen.

Lautet der Computernamen beispielsweise `host-1.company.com`, führen Sie den folgenden Befehl an der Windows-Befehlszeile aus:

```
ping host-1.company.com
```

Ist der Ping-Test mit dem Computernamen erfolgreich, wurde der Name im DNS aktualisiert.

Ergebnisse

Die vCenter Server-Kommunikation ist bestätigt. Sie können mit der Vorbereitung anderer Komponenten in der Umgebung fortfahren.

Überprüfen der Netzwerkvoraussetzungen vor dem Upgrade

Stellen Sie sicher, dass Ihr Netzwerk ordnungsgemäß eingerichtet ist und die Konnektivitätsvoraussetzungen für das Upgrade von vCenter Server erfüllt.

Informationen zum Erstellen eines PTR-Eintrags finden Sie in der Dokumentation Ihres vCenter Server-Hostbetriebssystems.

Informationen zum Konfigurieren von Active Directory finden Sie auf der Microsoft-Website.

Domänenbenutzer, die zu einer Windows-Administratorengruppe mit vCenter Server-Administratorberechtigung gehören, können vCenter Server nicht während des Upgrades authentifizieren und verfügen nach dem Upgrade nicht über die vCenter Server-Berechtigung.

Verfahren

- 1 Stellen Sie sicher, dass der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) auf dem System aufgelöst wird, auf dem Sie ein Upgrade von vCenter Server durchführen. Geben Sie **nslookup -nosearch -nodefname *Ihr_vCenter_Server_FQDN*** an der Befehlszeile ein, um zu prüfen, ob der FQDN aufgelöst wird.

Wenn der FQDN aufgelöst werden kann, gibt der Befehl **nslookup** die IP und den Namen des Domänencontrollers zurück.

- 2 Stellen Sie sicher, dass das DNS-Reverse-Lookup einen vollständig qualifizierten Domännennamen zurückgibt, wenn dieser mit der IP-Adresse von vCenter Server abgefragt wird.

Beim Upgrade von vCenter Server schlägt die Installation der Webserverkomponente, die den vSphere Web Client unterstützt, fehl, wenn das Installationsprogramm den vollqualifizierten Domännennamen von vCenter Server nicht über die IP-Adresse abrufen kann.

Das Reverse-Lookup wird unter Verwendung von PTR-Einträgen implementiert.

- 3 Wenn Sie DHCP anstelle einer manuell zugewiesenen (statischen) IP-Adresse für vCenter Server verwenden, stellen Sie sicher, dass der vCenter Server-Computernamen im DNS (Domain Name Service) aktualisiert wird. Testen Sie dies, indem Sie den Computernamen pingen.

Lautet der Computernamen beispielsweise `host-1.company.com`, führen Sie den folgenden Befehl an der Windows-Befehlszeile aus:

```
ping host-1.company.com
```

Ist der Ping-Test mit dem Computernamen erfolgreich, wurde der Name im DNS aktualisiert.

- 4 Stellen Sie sicher, dass die Verwaltungsschnittstelle des ESXi-Hosts von der vCenter Server-Instanz und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat. Stellen Sie sicher, dass der vCenter Server von allen ESXi-Hosts und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat.
- 5 Falls Sie Active Directory als Identitätsquelle verwenden möchten, stellen Sie sicher, dass Active Directory ordnungsgemäß eingerichtet ist. Die DNS-Konfiguration der vCenter Single Sign On-Server-Hostmaschine muss Lookup- und Reverse-Lookup-Einträge für den Domänencontroller des Active Directory enthalten.

Wenn Sie zum Beispiel *meinefirma.com* pingen, muss der Domänencontroller die IP-Adresse für *meinefirma* zurückgeben. Entsprechend muss der Befehl `ping -a` für diese IP-Adresse den Hostnamen des Domänencontrollers zurückgeben.

Vermeiden Sie es, Probleme bei der Namensauflösung durch Bearbeitung der Host-Datei zu korrigieren. Achten Sie stattdessen darauf, dass der DNS-Server ordnungsgemäß eingerichtet ist.

- 6 Wählen Sie vor dem Upgrade den gewünschten Domänenbenutzer für das Upgrade von vCenter Server aus. Erteilen Sie diesem Domänenbenutzer die exklusive Administratorberechtigung für vCenter Server, und nicht als Teil einer Windows-Administratorengruppe.

Ergebnisse

Ihr Netzwerk ist für das Upgrade von vCenter Server bereit.

Nächste Schritte

Bereiten Sie andere Komponenten Ihrer Umgebung vor.

Überprüfen des Lastausgleichsdiensts vor dem Upgrade von vCenter Server

Wenn Sie einen Lastausgleichsdienst für High Availability für vCenter Single Sign-On verwenden, müssen Sie überprüfen, ob dieser unterstützt wird und ordnungsgemäß konfiguriert ist, bevor Sie ein Upgrade auf vCenter Server 6.0 durchführen.

In Umgebungen mit weniger als vier vCenter Server-Systemen empfiehlt VMware in der Regel eine einzige Platform Services Controller-Instanz und den zugehörigen vCenter Single Sign-On-Dienst. In größeren Umgebungen können Sie mehrere durch einen Netzwerk-Lastausgleichsdienst geschützte Platform Services Controller-Instanzen verwenden. Im Whitepaper *vCenter Server 6.0-Bereitstellungshandbuch* auf der VMware-Website wird diese Konfiguration behandelt. Aktuelle Informationen zu Höchstwerten finden Sie unter *Maximalwerte für die Konfiguration*.

Eine Kompatibilitätstabelle zur High Availability für vCenter Single Sign-On und Platform Services Controller finden Sie im VMware Knowledgebase-Artikel <http://kb.vmware.com/kb/2112736>.

Voraussetzungen

Verfahren

- 1 Informationen zum Lastausgleich finden Sie im *vCenter Server 6.0-Bereitstellungshandbuch*.
- 2 Wenn Ihr Lastausgleichsdienst nicht unterstützt wird, ersetzen Sie ihn durch einen unterstützten Lastausgleichsdienst.
- 3 Stellen Sie sicher, dass der Lastausgleichsdienst gemäß den Empfehlungen im *vCenter Server 6.0-Bereitstellungshandbuch* ordnungsgemäß konfiguriert ist.

Vorbereiten der ESXi-Hosts für das Upgrade von vCenter Server

Vor dem Upgrade auf vCenter Server 6.0 müssen Sie Ihre ESXi-Hosts vorbereiten.

Voraussetzungen

- Für das Upgrade von vCenter Server müssen die ESXi-Hosts Version 5.x aufweisen. Wenn auf Ihren ESXi-Hosts eine ältere Version als 5.0 vorhanden ist, führen Sie ein Upgrade auf 5.x durch. Lesen und befolgen Sie sämtliche Best Practices, wenn Sie ein Upgrade Ihrer Hosts auf ESXi 5.x durchführen.
- Für das Upgrade von vCenter Server Appliance auf Version 6.0 muss auf Ihrem Zielhost ESXi 5.1 oder höher ausgeführt werden.
- Für das Upgrade von vCenter Server Appliance auf Version 6.0 müssen sich die ESXi-Quellhosts und -Zielhosts im Sperr- oder Wartungsmodus befinden.

Verfahren

- 1 Sichern Sie die auf dem vCenter Server-System gespeicherten SSL-Zertifikate vor dem Upgrade auf vCenter Server 6.0. So bleiben Ihre SSL-Zertifikate erhalten.

Der Standardspeicherort der SSL-Zertifikate ist %allusersprofile%\Application Data\VMware\VMware VirtualCenter.
- 2 Falls Sie benutzerdefinierte Zertifikate oder Fingerabdruckzertifikate verwenden, lesen Sie den Abschnitt [Host-Upgrades und Zertifikate](#), um Ihre vorbereitenden Schritte festzulegen.
- 3 Wenn Sie vSphere HA-Cluster verwenden, muss die SSL-Zertifikatprüfung aktiviert sein.

Ist die Zertifikatsprüfung während des Upgrades nicht aktiviert, schlägt die Konfiguration von vSphere HA auf den Hosts fehl.
 - a Wählen Sie die vCenter Server-Instanz im Bestandslistenfenster aus.
 - b Wählen Sie die Registerkarte **Verwalten** und dann die Unterregisterkarte **Allgemein** aus.
 - c Stellen Sie sicher, dass für das Feld **SSL-Einstellungen** die Option **vCenter Server benötigt verifizierte Host-SSL-Zertifikate** ausgewählt ist.

Ergebnisse

Ihre ESXi-Hosts sind für das Upgrade von vCenter Server bereit.

Host-Upgrades und Zertifikate

Wenn Sie ein Upgrade eines ESXi-Hosts auf ESXi 6.0 oder höher durchführen, werden beim Upgrade-Prozess selbstsignierte Zertifikate durch VMCA-signierte Zertifikate ersetzt. Der Prozess behält benutzerdefinierte Zertifikate bei, selbst wenn diese Zertifikate abgelaufen oder ungültig sind.

Der empfohlene Upgrade-Workflow hängt von den aktuellen Zertifikaten ab.

Host mit bereitgestellten Fingerabdruckzertifikaten

Wenn der Host derzeit Fingerabdruckzertifikate verwendet, werden ihm im Rahmen des Upgrade-Prozesses automatisch VMCA-Zertifikate zugewiesen.

Hinweis Sie können keine VMCA-Zertifikate auf Legacy-Hosts bereitstellen. Es ist ein Upgrade auf ESXi 6.0 oder höher erforderlich.

Host mit bereitgestellten benutzerdefinierten Zertifikaten

Wenn auf dem Host benutzerdefinierte Zertifikate bereitgestellt wurden, in der Regel von einer Zertifizierungsstelle signierte Zertifikate eines Drittanbieters, dann werden diese Zertifikate beibehalten. Wechseln Sie den Zertifikatsmodus in den benutzerdefinierten Modus, um sicherzustellen, dass die Zertifikate nicht versehentlich ersetzt werden.

Hinweis Wenn sich Ihre Umgebung im VMCA-Modus befindet und Sie die Zertifikate über den vSphere Web Client aktualisieren, werden alle vorhandenen Zertifikate durch von VMCA signierte Zertifikate ersetzt.

Von diesem Zeitpunkt an überwacht vCenter Server die Zertifikate und zeigt Informationen, z. B. über ablaufende Zertifikate, im vSphere Web Client an.

Wenn Sie sich dafür entscheiden, kein Upgrade für die Hosts auf vSphere 6.0 oder höher durchzuführen, behält der Host die derzeit verwendeten Zertifikate bei, selbst wenn der Host von einem vCenter Server-System verwaltet wird, das VMCA-Zertifikate verwendet.

Mit Auto Deploy verwalteten Hosts werden immer neue Zertifikate zugewiesen, wenn sie zum ersten Mal mit der ESXi 6.0-Software gestartet werden. Wenn Sie ein Upgrade für einen Host mit Bereitstellung durch Auto Deploy durchführen, generiert der Auto Deploy-Server eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den Host und sendet diese an VMCA. VMCA speichert das signierte Zertifikat für den Host. Wenn der Auto Deploy-Server Bereitstellungen für den Host durchführt, ruft er das Zertifikat von VMCA ab und schließt es als Bestandteil des Bereitstellungsprozesses ein.

Sie können Auto Deploy mit benutzerdefinierten Zertifikaten verwenden.

Ändern des Zertifikatmodus

In den meisten Fällen ist VMCA die beste Lösung zur Bereitstellung der ESXi-Hosts in Ihrer Umgebung. Wenn Ihre Unternehmensrichtlinie vorsieht, dass Sie benutzerdefinierte Zertifikate mit einer anderen Stammzertifizierungsstelle verwenden, können Sie in den erweiterten Optionen von vCenter Server festlegen, dass den Hosts bei der Zertifikataktualisierung nicht automatisch VMCA-Zertifikate bereitgestellt werden. In diesem Fall übernehmen Sie die Verantwortung für die Zertifikatsverwaltung in Ihrer Umgebung.

In den erweiterten Einstellungen von vCenter Server können Sie in den Fingerabdruckmodus oder den benutzerdefinierten Zertifizierungsstellenmodus wechseln. Der Fingerabdruckmodus sollte lediglich im Notfall eingesetzt werden.

Verfahren

- 1 Wählen Sie den vCenter Server aus, von dem die Hosts verwaltet werden, und klicken Sie auf **Einstellungen**.
- 2 Klicken Sie auf **Erweiterte Einstellungen** und auf **Bearbeiten**.
- 3 Geben Sie im Feld „Filter“ den Ausdruck **certmgmt** ein, um nur die Zertifikatsverwaltungsschlüssel anzuzeigen.
- 4 Ändern Sie „vpxd.certmgmt.mode“ zu **custom** (benutzerdefiniert), wenn Sie Ihre eigenen Zertifikate verwalten möchten, oder zu **thumbprint** (Fingerabdruck), wenn Sie vorübergehend in den Fingerabdruckmodus wechseln möchten. Klicken Sie anschließend auf **OK**.
- 5 Starten Sie den vCenter Server-Dienst neu.

Überprüfen der Vorbereitungen für das Upgrade von vCenter Server

Stellen Sie sicher, dass alle Komponenten Ihrer Umgebung für das Upgrade von vCenter Server bereit sind.

Die Konfiguration der vCenter Server-Dienste vor dem Upgrade wirkt sich auf die Bereitstellung der vCenter Server-Dienste nach dem Upgrade aus.

- Wenn Sie vCenter Server 5.0 verwenden, können Sie während des Upgrades eine eingebettete oder eine externe Platform Services Controller-Instanz konfigurieren. Weitere Informationen hierzu finden Sie unter [Upgrade von vCenter Server 5.0](#).
- Wenn Sie vCenter Server 5.1 oder 5.5 haben, sind während des Upgrades keine Bereitstellungsoptionen verfügbar. Siehe [Upgrade von vCenter Server 5.1 für Windows](#) oder [Upgrade von vCenter Server 5.5 für Windows](#).
- Wenn die vCenter Server 5.1- oder 5.5-Dienste auf derselben virtuellen Maschine bzw. demselben physischen Server bereitgestellt sind, werden sie vom Installationsprogramm auf vCenter Server 6.0 mit einer eingebetteten Platform Services Controller-Instanz aktualisiert.

- Wenn der vCenter Single Sign-On 5.1- oder 5.5-Dienst auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als vCenter Server bereitgestellt ist, wird die Bereitstellung vom Installationsprogramm auf vCenter Server 6.0 mit einer externen Platform Services Controller-Instanz aktualisiert. Informationen zur Konsolidierung verteilter Dienste während des Upgrades finden Sie unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#) und [Beispiele von Upgrade-Pfaden für vCenter Server](#).

Hinweis Die Bereitstellung von vCenter Server-Diensten kann nach dem Upgrade nicht geändert werden.

Informationen zum Upgrade von Diensten finden Sie unter [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#). Informationen zum Upgrade eines extern bereitgestellten vCenter Single Sign-On-Servers finden Sie unter [Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung](#).

Informationen zum Synchronisieren von Systemuhren finden Sie unter [Synchronisieren der Systemuhren im vSphere-Netzwerk](#).

Informationen zum Herunterladen des Installationsprogramms finden Sie unter [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).

Voraussetzungen

Nachdem Sie die grundlegende Kompatibilität und Upgradebereitschaft für Datenbank, Netzwerk, lokale Datenbankkommunikation und ESXi-Hosts sichergestellt haben, können Sie die abschließenden Aufgaben zum Sicherstellen der Upgradebereitschaft Ihrer Umgebung durchführen.

Verfahren

- 1 Melden Sie sich auf der Hostmaschine als Mitglied der Gruppe „Administratoren“ an und verwenden Sie dabei einen Benutzernamen, der ausschließlich ASCII-Zeichen enthält.
- 2 Stellen Sie sicher, dass Ihre Konfiguration vor dem Upgrade für die gewünschte Bereitstellung nach dem Upgrade geeignet ist.
 - Wenn Sie bei vCenter Server 5.1 oder 5.5 auf die Bereitstellung eines eingebetteten Platform Services Controller aktualisieren möchten, stellen Sie sicher, dass die vCenter Server- und vCenter Single Sign-On-Instanzen auf einer einzelnen virtuellen Maschine bzw. einem einzelnen physischen Host bereitgestellt sind.
 - Wenn Sie bei vCenter Server 5.1 oder 5.5 auf die Bereitstellung eines externen Platform Services Controller aktualisieren möchten, stellen Sie sicher, dass vCenter Single Sign-On auf einer anderen virtuellen Maschine bzw. einem anderen physischen Host als der zugehörige vCenter Server bereitgestellt ist.
 - Wenn Sie bei vCenter Server 5.0 auf die Bereitstellung eines eingebetteten Platform Services Controller aktualisieren möchten, sind keine Arbeitsschritte vor dem Upgrade erforderlich.

- Wenn Sie bei vCenter Server 5.0 auf die Bereitstellung eines externen Platform Services Controllers aktualisieren möchten, müssen Sie vor dem Upgrade von vCenter Server eine externe Platform Services Controller-Instanz konfigurieren. Die Informationen zum Platform Services Controller werden während des Upgrades zum Registrieren des externen Platform Services Controller bei vCenter Server verwendet.
- 3 Stellen Sie sicher, dass die erforderlichen Dienste gestartet wurden.
 - Die vCenter Single Sign-On-Instanz, bei der Sie vCenter Server registrieren
 - VMware Certificate Authority
 - VMware Directory Service
 - VMware Identity Manager Service
 - VMware KDC Service
 - tcruntime-C-ProgramData-VMware-cis-runtime-VMwareSTSService
 - 4 Bevor Sie ein vSphere-Produkt installieren oder aktualisieren, synchronisieren Sie die Systemuhren aller Maschinen im vSphere-Netzwerk.
 - 5 Wenn Sie vCenter Server 6.0 nicht im Testmodus verwenden möchten, stellen Sie sicher, dass Sie über gültige Lizenzschlüssel für die erworbene Funktionalität verfügen. Lizenzschlüssel von früheren vSphere-Versionen werden von den Vorgängerversionen weiterhin unterstützt. Von vCenter Server 6.0 werden sie jedoch nicht unterstützt.

Wenn Sie aktuell keinen Lizenzschlüssel haben, können Sie im Testmodus installieren und den vSphere Web Client verwenden, um den Lizenzschlüssel später einzugeben.
 - 6 Schließen Sie alle vSphere Web Client-Instanzen.
 - 7 Stellen Sie sicher, dass keine Konflikte bei Prozessen bestehen.
 - 8 Laden Sie das Installationsprogramm herunter.

Ergebnisse

Ihre Umgebung ist für das Upgrade von vCenter Server bereit.

Synchronisieren der Systemuhren im vSphere-Netzwerk

Stellen Sie sicher, dass auf allen Komponenten im vSphere-Netzwerk die Systemuhren synchronisiert sind. Wenn die Systemuhren der Maschinen im vSphere-Netzwerk nicht synchronisiert sind, werden SSL-Zertifikate, die zeitabhängig sind, bei der Kommunikation zwischen Netzwerkmaschinen möglicherweise nicht als gültig erkannt.

Nicht synchronisierte Systemuhren können Authentifizierungsprobleme verursachen, was zu einem Fehlschlag beim Installieren der vCenter Server Appliance führen bzw. verhindern kann, dass der vpxd-Dienst der vCenter Server Appliance gestartet wird.

Stellen Sie sicher, dass jede Windows-Hostmaschine, auf der eine vCenter-Komponente ausgeführt wird, mit dem NTP-Server synchronisiert wird. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel <http://kb.vmware.com/kb/1318>.

Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

Bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen, sollten Sie sicherstellen, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind.

Diese Aufgabe erläutert, wie Sie NTP über den vSphere Client einrichten. Sie können stattdessen den vCLI-Befehl `vicfg-ntp` verwenden. Weitere Informationen finden Sie in der *vSphere Command-Line Interface-Referenz*.

Verfahren

- 1 Starten Sie den vSphere Client und stellen Sie eine Verbindung mit dem ESXi-Host her.
- 2 Klicken Sie auf der Registerkarte **Konfiguration** auf **Uhrzeitkonfiguration**.
- 3 Klicken Sie auf **Eigenschaften** und anschließend auf **Optionen**.
- 4 Wählen Sie **NTP-Einstellungen**.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Geben Sie im Dialogfeld „NTP-Server hinzufügen“ die IP-Adresse oder den vollqualifizierten Domännennamen des NTP-Servers ein, mit dem synchronisiert werden soll.
- 7 Klicken Sie auf **OK**.

Die Hostuhrzeit wird mit dem NTP-Server synchronisiert.

Ausfallzeiten während des vCenter Server-Upgrades

Beim Upgrade von vCenter Server sind Ausfallzeiten für vCenter Server einzuplanen.

Für vCenter Server sind die folgenden Ausfallzeiten zu erwarten:

- Für das Upgrade muss vCenter Server mindestens 40 bis 50 Minuten lang aus der Produktion genommen werden. Je nach Größe der Datenbank kann dies auch wesentlich länger dauern. 10 bis 15 Minuten dieses Zeitraums werden für das Upgrade des Datenbankschemas benötigt. Diese Schätzung beinhaltet nicht die Zeit zum Wiederverbinden mit dem Host nach dem Upgrade.
- Bei vCenter Server-Implementierungen mit eingebetteter Datenbank kann es etwas länger dauern, die Daten aus der alten vCenter Server-Datenbank in die neue Datenbankinstanz zu migrieren.
- Wenn Microsoft .NET Framework auf dem Rechner nicht installiert ist, ist vor dem Starten der vCenter Server-Installation ein Neustart erforderlich.
- vSphere Distributed Resource Scheduler (DRS) funktioniert während des Upgrades nicht, vSphere HA hingegen schon.

Für die ESXi-Hosts, die von vCenter Server verwaltet werden, oder die virtuellen Maschinen, die auf dem Host ausgeführt werden, sind keine Ausfallzeiten erforderlich.

Verwenden eines Benutzerkontos zur Ausführung von vCenter Server

Sie können das in Microsoft Windows integrierte Systemkonto oder ein Benutzerkonto zum Ausführen von vCenter Server verwenden. Mit einem Benutzerkonto können Sie die Windows-Authentifizierung für SQL Server aktivieren und für mehr Sicherheit sorgen.

Das Benutzerkonto muss ein Konto mit Administratorrechten für die lokale Maschine sein. Im Installationsassistenten wird der Kontoname in der Form *Domänenname\Benutzername* angegeben. Sie müssen die SQL Server-Datenbank konfigurieren, damit das Domänenkonto auf SQL Server zugreifen kann.

Das in Microsoft Windows integrierte Systemkonto verfügt über mehr Berechtigungen und Rechte auf dem Server als für das vCenter Server-System erforderlich ist, was zu Sicherheitsproblemen führen kann.

Wichtig Wenn der vCenter Server-Dienst unter dem integrierten Systemkonto von Microsoft Windows ausgeführt wird, unterstützt vCenter Server 6.0 bei Verwendung von Microsoft SQL Server nur DSNs mit SQL Server-Authentifizierung.

Mit der Windows-Authentifizierung konfigurierte SQL Server-DSNs verwenden Sie dasselbe Benutzerkonto für den VMware VirtualCenter Management Webservices-Dienst und den DSN-Benutzer.

Selbst wenn Sie die Microsoft Windows-Authentifizierung nicht für SQL Server verwenden möchten oder Sie eine Oracle-Datenbank verwenden, sollten Sie ein lokales Benutzerkonto für das vCenter Server-System einrichten. Die einzige Anforderung besteht darin, dass das Benutzerkonto ein Konto mit Administratorrechten auf der lokalen Maschine ist und über die Berechtigung **Anmelden als Dienst** verfügt.

Erforderliche Informationen für das Upgrade von vCenter Server für Windows

Der Upgrade-Assistent für vCenter Server fordert Sie zur Eingabe der Upgrade-Informationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für künftige Upgrades von vCenter Server für Windows benötigen.

Die Standardwerte werden in der Tabelle unten nur dargestellt, wenn Sie bei der Installation der Quellinstanz von vCenter Server keine Änderungen an diesen Werten vorgenommen haben.

Tabelle 3-3. Erforderliche Informationen für das Upgrade von vCenter Server für Windows

Erforderliche Informationen		Standardwert	Ihr Eintrag
Benutzername des vCenter Single Sign-On-Administrators		administrator@vsphere.local	Während der Durchführung des Upgrades können Sie den Standardbenutzernamen nicht ändern.
Administratorkennwort für vCenter Single Sign-On			
Dieselben Anmeldedaten für vCenter Server verwenden aktivieren oder deaktivieren		Standardmäßig aktiviert	
vCenter Server-Benutzername		administrator@vsphere.local	
vCenter Server-Kennwort			
Syslog-Dienst-Port		514	
TLS-Port für den Syslog-Dienst		1514	
Auto Deploy-Management-Port		6502	
Auto Deploy-Dienst-Port		6501	
ESXi Dump Collector-Port		6500	
Zielverzeichnis Die Ordnerpfade dürfen die folgenden Zeichen nicht enthalten: Nicht-ASCII-Zeichen, Kommas (,), Punkte (.), Ausrufezeichen (!), Nummernzeichen (#), At-Zeichen (@) und Prozentzeichen (%).	Verzeichnis zur Installation von vCenter Server	C:\Programme\VMware	
	Verzeichnis zur Speicherung von Daten für vCenter Server	C:\ProgramData\VMware	
	Verzeichnis zum Import Ihrer 5.x-Daten	C:\ProgramData\VMware\VMware\vCenterServer\export	
Dem Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) von VMware beitreten oder nicht daran teilnehmen		Am CEIP teilnehmen	
Informationen über das CEIP finden Sie im Abschnitt Programm zur Verbesserung der Benutzerfreundlichkeit in <i>vCenter Server und Hostverwaltung</i> .			

Erforderliche Informationen für das Upgrade der vCenter Server Appliance

Der Upgrade-Assistent für vCenter Server Appliance fordert Sie zur Eingabe der Bereitstellungsinformationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Wichtig Upgrades von vCenter Server Appliance 5.1 Update 3 und höher auf vCenter Server Appliance 6.0 werden unterstützt. Für das Upgrade von vCenter Server Appliance 5.0 müssen Sie zuerst die vCenter Server Appliance auf Version 5.1 Update 3 oder 5.5 Update 2 aktualisieren und dann ein Upgrade auf vCenter Server Appliance 6.0 vornehmen. Informationen zum Aktualisieren der vCenter Server Appliance 5.0 auf Version 5.1 Update 3 finden Sie in der *Dokumentation zu VMware vSphere 5.1*. Informationen zum Aktualisieren von vCenter Server Appliance 5.0 auf Version 5.5 Update 2 finden Sie in der *Dokumentation zu VMware vSphere 5.5*.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für das Upgrade von vCenter Server Appliance, Version 5.1 Update 3 oder 5.5.x, benötigen.

Tabelle 3-4. Erforderliche Informationen für das Upgrade von vCenter Server Appliance 5.1.x oder 5.5.x

Erforderliche Informationen		Standardwert	Ihr Eintrag
IP-Adresse oder FQDN des ESXi-Zielhosts, auf dem Sie ein Upgrade der vCenter Server Appliance durchführen			
Anmeldedaten eines Benutzers mit Administratorrechten für den ESXi-Zielhost	Benutzername des ESXi-Zielhosts		
	Kennwort des ESXi-Zielhosts		
Name für vCenter Server Appliance 6.0			
Version der vCenter Server Appliance, für die ein Upgrade auf vCenter Server Appliance 6.0 durchgeführt werden soll			
Daten zur vCenter Server Appliance, für die ein Upgrade durchgeführt werden soll	IP-Adresse oder FQDN der vCenter Server Appliance		
	Benutzername des vCenter Single Sign-On-Administrators	Bei einem Upgrade von vCenter Server Appliance 5.5.x ist dies „administrator@vsphere.local“	
	Kennwort des vCenter Single Sign-On-Administrators		
	HTTPS-Portnummer für vCenter Server		
	Kennwort des Root-Benutzers		

Tabelle 3-4. Erforderliche Informationen für das Upgrade von vCenter Server Appliance 5.1.x oder 5.5.x (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
	Pfad für temporäre Upgrade-Dateien	/tmp/vmware/cis-export-folder	
	Leistungsdaten und sonstige Verlaufsdaten migrieren	Standardmäßig deaktiviert	
IP-Adresse oder FQDN des ESXi-Quellhosts, auf dem sich die vCenter Server Appliance befindet, für die Sie ein Upgrade durchführen möchten			
Anmeldedaten eines Benutzers mit Administratorrechten für den ESXi-Quellhost	Benutzername des ESXi-Quellhosts		
	Kennwort des ESXi-Quellhosts		
vCenter Single Sign-On-Einstellungen	Kennwort für vCenter Single Sign-On		
Nur erforderlich bei einem Upgrade von vCenter Server Appliance, Version 5.1.x	Domänenname für vCenter Single Sign-On		
	Site-Name für vCenter Single Sign-On		
Größe der vCenter Server Appliance. Die Optionen hängen von der Größe Ihrer vSphere-Umgebung ab.		Sehr klein (bis zu 20 Hosts, 400 virtuelle Maschinen)	
<ul style="list-style-type: none"> ■ Sehr klein (bis zu 20 Hosts, 400 virtuelle Maschinen) ■ Klein (bis zu 150 Hosts, 3,000 virtuelle Maschinen) ■ Mittel (bis zu 300 Hosts, 6,000 virtuelle Maschinen) ■ Groß (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen) 			
Name des Datenspeichers, in dem die neue Version der vCenter Server Appliance bereitgestellt wird			
Thin-Festplattenmodus aktivieren oder deaktivieren		Standardmäßig deaktiviert	
Temporäres Netzwerk für die Kommunikation zwischen der vCenter Server Appliance, für die ein Upgrade durchgeführt werden soll, und der neuen vCenter Server Appliance			
Version der IP-Adresse		IPv4	
Methode für Zuweisung der IP-Adresse		DHCP	
Einstellungen für statische Zuweisung	Netzwerkadresse		
	Subnetzmaske		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		

Tabelle 3-4. Erforderliche Informationen für das Upgrade von vCenter Server Appliance 5.1.x oder 5.5.x (Fortsetzung)

Erforderliche Informationen	Standardwert	Ihr Eintrag
Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
<p>Dem Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) von VMware beitreten oder nicht daran teilnehmen</p> <p>Informationen über das CEIP finden Sie im Abschnitt Programm zur Verbesserung der Benutzerfreundlichkeit in <i>vCenter Server und Hostverwaltung</i>.</p> <p>Nur erforderlich bei einem Upgrade von vCenter Server Appliance mit eingebettetem vCenter Single Sign-On</p>	Am CEIP teilnehmen	

Upgrade und Update von vCenter Server für Windows

4

Das Upgrade von vCenter Server beinhaltet ein Upgrade des Datenbankschemas, die Migration von vCenter Single Sign-On zum Platform Services Controller sowie das Upgrade der vCenter Server-Software.

Dieses Kapitel enthält die folgenden Themen:

- Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows
- Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0
- Herunterladen des Installationsprogramms für vCenter Server für Windows Installer
- Upgrade von vCenter Single Sign-On 5.1 für die externe Bereitstellung
- Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung
- Upgrade von vCenter Server 5.0
- Upgrade von vCenter Server 5.1 für Windows
- Upgrade von vCenter Server 5.5 für Windows
- Aktualisieren von Java-Komponenten und vCenter Server tc Server mit VIMPatch

Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows

Die Upgrade-Optionen für vCenter Server unter Windows hängen von Ihrer aktuellen Bereitstellung und Version ab.

Der Upgrade-Vorgang von vCenter Server für Windows beinhaltet Folgendes:

- 1 Export der vCenter Server 5.x-Konfiguration
- 2 Deinstallation der vCenter Server 5.x-Konfiguration
- 3 Installation von vCenter Server 6.0
- 4 Migration und Konfiguration der vCenter Server 5.x-Dienste und -Daten für die Bereitstellung von vCenter Server 6.0

Das Ergebnis des Upgrades hängt von Ihrer aktuellen Bereitstellung ab:

- Bei dem Upgrade einer Bereitstellung von vCenter Server 5.0 können Sie während des Upgrades eine eingebettete oder eine externe Instanz von Platform Services Controller konfigurieren.
- Bei dem Upgrade einer Bereitstellung von vCenter Server der Version 5.1 oder 5.5 mit Diensten, die auf einer einzelnen virtuellen Maschine (VM) bzw. einem einzelnen physischen Server bereitgestellt sind, wird für die Bereitstellung ein Upgrade auf vCenter Server mit eingebettetem Platform Services Controller durchgeführt.
- Bei dem Upgrade einer Bereitstellung von vCenter Server der Version 5.1 oder 5.5 mit vCenter Single Sign-On, die auf einer anderen VM bzw. physischen Server bereitgestellt sind als vCenter Server, wird für die Bereitstellung ein Upgrade auf vCenter Server mit externem Platform Services Controller durchgeführt.
- Bei dem Upgrade mehrerer Instanzen von vCenter Server müssen Sie die Upgrades nacheinander unter Einhaltung der vorgegebenen Reihenfolge vornehmen. Siehe [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).

Abbildung 4-1. Upgrade-Workflow für vCenter Server 5.0 für Windows

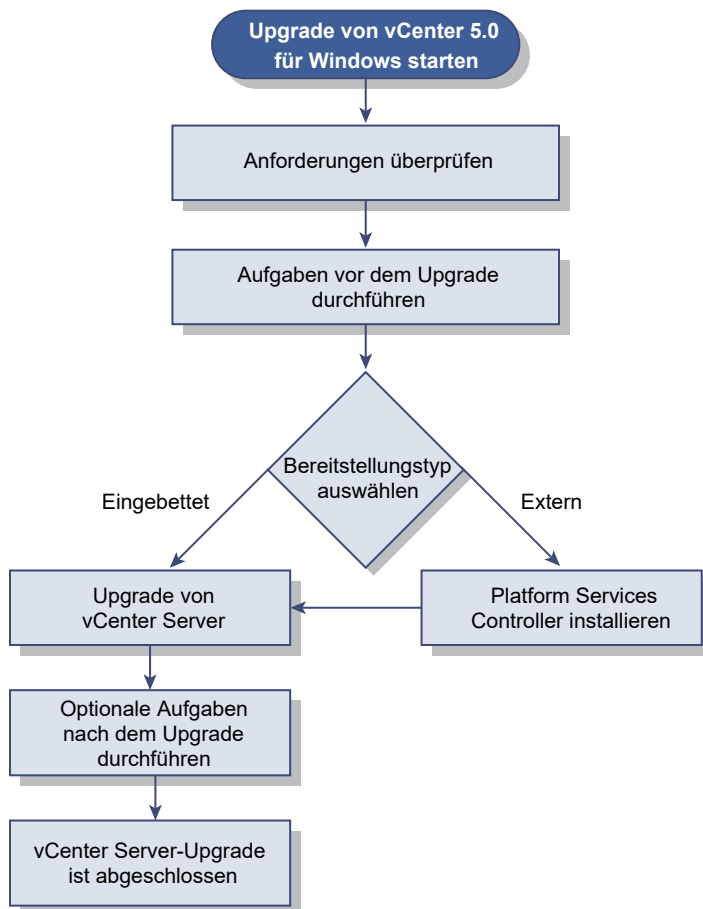
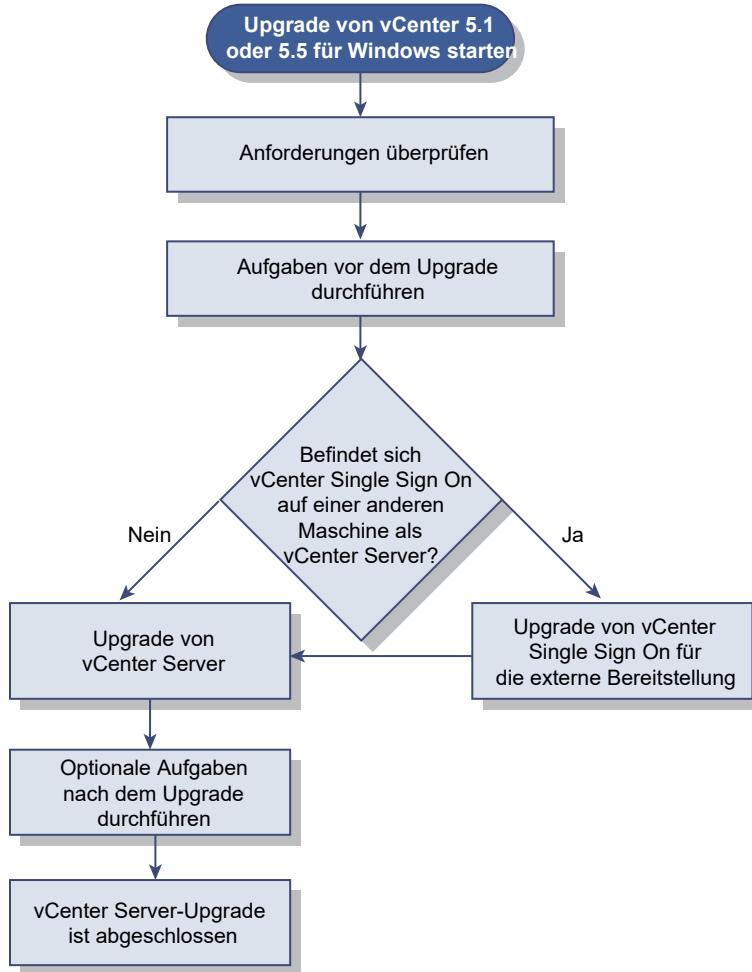


Abbildung 4-2. Upgrade-Workflow für vCenter Server 5.1 oder 5.5 für Windows



Während des Upgrade-Prozesses können Sie keine Dienste deinstallieren oder neu installieren. Beispielsweise kann Inventory Service nicht mehr separat bereitgestellt werden. Dieser Dienst ist Teil der vCenter Server-Gruppe von Diensten für vCenter Server 6.0.

Hinweis Das Bereitstellungsmodell von vCenter Server kann während eines Upgrades nicht geändert werden. Beispielsweise können Sie nicht von vCenter Server mit einer eingebetteten Platform Services Controller-Instanz auf vCenter Server mit einer externen Platform Services Controller-Instanz umstellen (oder umgekehrt).

Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0

Während des Upgrade-Prozesses werden benutzerdefinierte Installationen von vCenter Server 5.1 oder 5.5 für Windows mit Diensten auf mehreren Maschinen (falls erforderlich) auf das vCenter Server-System aktualisiert und migriert.

Wenn alle vCenter Server 5.x-Dienste im gleichen System bereitgestellt sind, werden sie an Ort und Stelle aktualisiert und brauchen nach dem Upgrade nicht konfiguriert zu werden. Wenn jedoch ein oder mehrere Dienste remote bereitgestellt wurden, werden die Dienste von der Software während des Upgrades zur virtuellen Maschine bzw. zum physischen Server von vCenter Server migriert. Für manche Dienste sind nach dem Upgrade eine Neukonfiguration oder andere Aktionen erforderlich. Die folgenden vCenter Server 5.x für Windows-Dienste werden während des Upgrade-Vorgangs migriert, um Bestandteil der Dienstgruppe von vCenter Server zu werden:

- Verzeichnisdienste
- vSphere Web Client
- vSphere Auto Deploy
- vSphere Syslog Collector
- vSphere ESXi Dump Collector

vCenter Server und vCenter Single Sign On sind die einzigen Dienste, die nicht migriert werden. vCenter Single Sign On-Instanzen werden an Ort und Stelle aktualisiert und werden Bestandteil eines externen Platform Services Controller, wenn sie auf einem anderen System als dem System mit vCenter Server bereitgestellt werden.

Abbildung 4-3. Zur Dienstgruppe von vCenter Server migrierte Komponentendienste

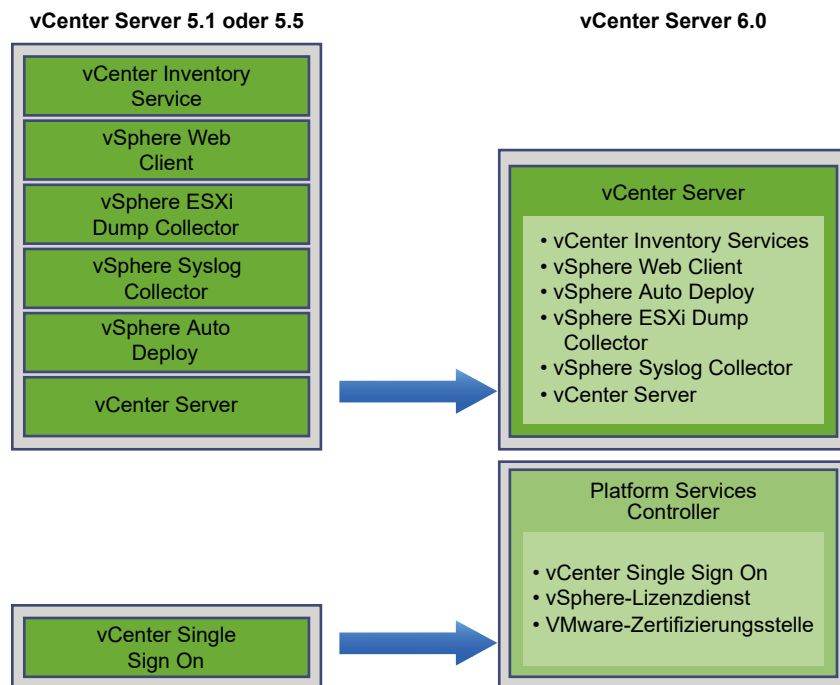


Tabelle 4-1. Migration von verteilten vCenter Server 5.x-Diensten während des Upgrade

Dienstname	Dienstspeicherort vor dem Upgrade	Dienstspeicherort nach dem Upgrade	Aktionen nach dem Upgrade
vCenter Inventory Service	Nicht auf dem vCenter Server-System installiert	Auf dem vCenter Server-System installiert	<p>Daten von vCenter Inventory Service 5.x werden in die Inventory Service 6.0-Instanz kopiert, die zusammen mit vCenter Server 6.0 installiert wird. Sie müssen die Daten nicht manuell kopieren.</p> <p>vCenter Inventory Service 5.x wird noch ausgeführt, aber nicht mehr verwendet. Er muss manuell angehalten und entfernt werden.</p>
vSphere Web Client	Nicht auf dem vCenter Server-System installiert	Auf dem vCenter Server-System installiert	<p>Daten von vCenter Server 5.x werden in die vSphere Web Client 6.0-Instanz kopiert, die zusammen mit vCenter Server 6.0 installiert wird.</p> <p>vSphere Web Client 5.x wird noch ausgeführt, aber nicht mehr verwendet. Er muss manuell angehalten und entfernt werden.</p>
vSphere Auto Deploy	Nicht auf dem vCenter Server-System installiert	Zum vCenter Server-System migriert	<p>Daten von vSphere Auto Deploy werden in die Auto Deploy 6.0-Instanz kopiert, die zusammen mit vCenter Server 6.0 installiert wird.</p> <p>Verweisen Sie die DHCP-Einstellungen von vCenter Server erneut auf den migrierten vSphere Auto Deploy-Dienst. vCenter Server</p> <p>vSphere Auto Deploy 5.x wird weiterhin ausgeführt, aber nicht mehr verwendet. Er muss manuell angehalten und entfernt werden.</p>
vSphere Syslog Collector	Nicht auf dem vCenter Server-System installiert	<p>Auf dem vCenter Server-System installiert</p> <p>Daten werden nicht migriert.</p> <p>Konfigurationen für Ports, Protokolle und die Rotationsprotokollgröße werden beibehalten.</p>	<ul style="list-style-type: none"> ■ Die ESXi-Systeminformationen können auf einem alten System gespeichert bleiben, bis Sie ihnen einen neuen Speicherort zuweisen. ■ Für ESXi-Hosts kann eine Neukonfiguration erforderlich sein, damit sie auf den neuen vSphere Syslog Collector-Server verweisen.
vSphere ESXi Dump Collector	Nicht auf dem vCenter Server-System installiert	<p>Auf dem vCenter Server-System installiert</p> <p>Daten werden nicht migriert.</p>	<ul style="list-style-type: none"> ■ ESXi-Core-Dump-Daten können auf einem älteren System gespeichert bleiben, bis Sie sie migrieren. ■ Für ESXi-Hosts kann eine Neukonfiguration erforderlich sein, damit sie auf den neuen vSphere ESXi Dump-Server verweisen.

Weitere Informationen zu Upgrade-Szenarien finden Sie unter [Beispiele von Upgrade-Pfaden für vCenter Server](#). Informationen zu den nach einem Upgrade erforderlichen Dienstneukonfigurationen finden Sie unter [Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade](#).

Herunterladen des Installationsprogramms für vCenter Server für Windows Installer

Laden Sie das Installationsprogramm (ISO-Datei) für vCenter Server für Windows sowie die zugehörigen vCenter Server-Komponenten und Support-Tools herunter.

Voraussetzungen

Erstellen Sie ein Customer Connect-Konto unter <https://my.vmware.com/web/vmware/>.

Verfahren

- 1 Laden Sie das Installationsprogramm für vCenter Server von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.

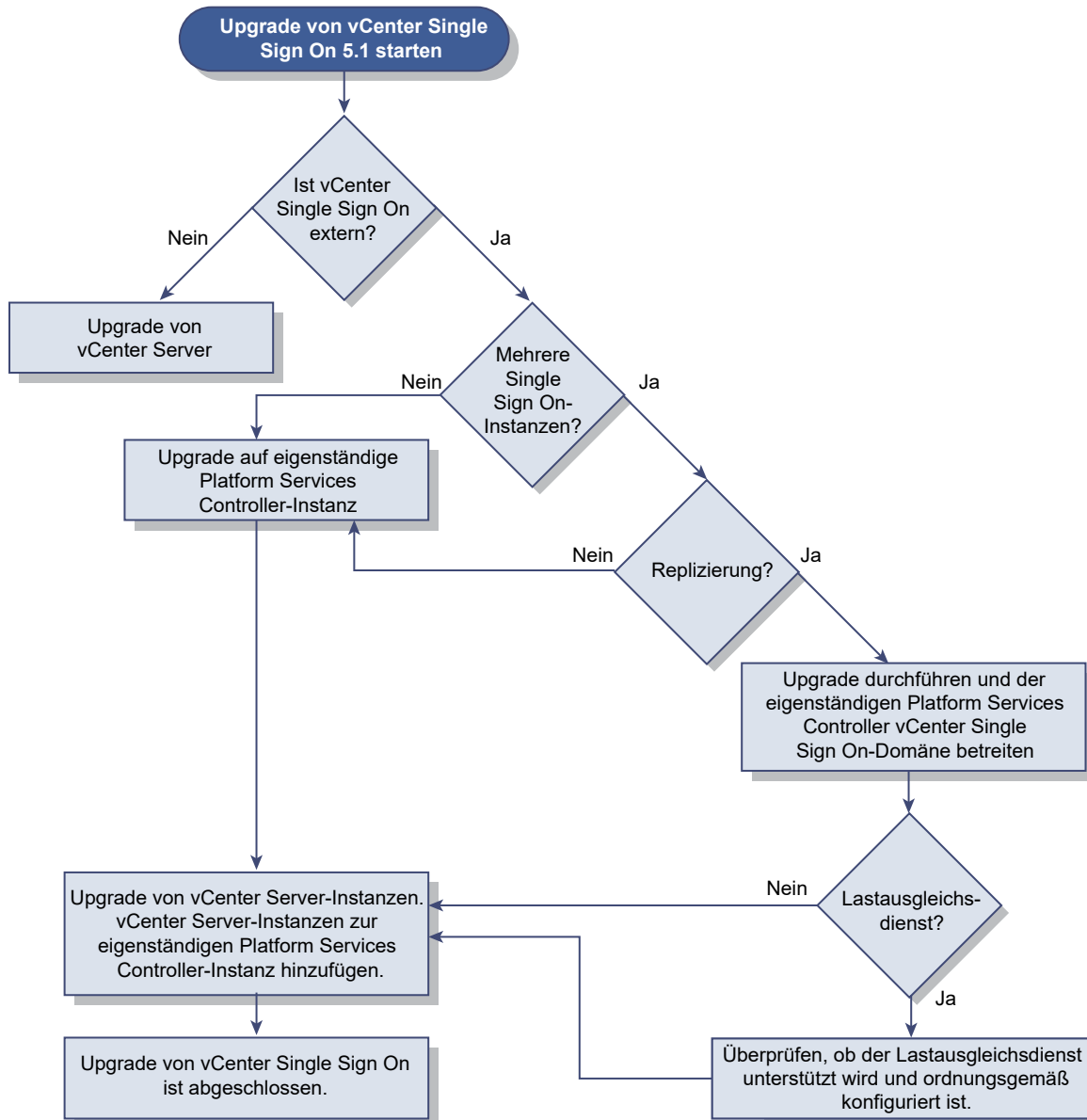
vCenter Server ist eine Komponente von VMware vCloud Suite und VMware vSphere und unter „Datencenter- und Cloud-Infrastruktur“ aufgeführt.
- 2 Bestätigen Sie, dass „md5sum“ korrekt ist.

Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Using MD5 Checksums“ (Verwenden von MD5-Prüfsummen) unter <http://www.vmware.com/download/md5.html>.
- 3 Mounten Sie das ISO-Image auf der virtuellen Windows-Maschine oder dem physischen Server, auf der/dem vCenter Server für Windows installiert werden soll.

Upgrade von vCenter Single Sign-On 5.1 für die externe Bereitstellung

Sie können ein Upgrade Ihrer extern bereitgestellten Instanz von vCenter Single Sign-On 5.1 auf eine extern bereitgestellte Platform Services Controller-Instanz mit dem Installationsprogramm von vCenter Server für Windows durchführen.

Abbildung 4-4. Upgrade-Workflow für vCenter Single Sign-On 5.1 für Windows



Wenn Sie eine extern bereitgestellte Instanz von vCenter Single Sign-On 5.1 auf eine extern bereitgestellte Platform Services Controller-Instanz in einer gemischten Versionsumgebung aktualisieren, funktionieren alle vCenter Server 5.1-Instanzen ohne jegliche Probleme oder erforderliche Aktionen weiter mit dem aktualisierten Platform Services Controller, genauso wie bei der vCenter Single Sign-On-Instanz.

- Weitere Informationen dazu, wie vCenter Single Sign-On sich auf Ihr Upgrade auswirkt, finden Sie unter [Auswirkungen von vCenter Single Sign On auf Upgrades](#).
- Informationen zum Verhalten von vCenter Server in gemischten Versionsumgebungen finden Sie unter [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Updates](#).

- Informationen zu Bereitstellungsoptionen finden Sie unter [Bereitstellungsmodelle für vCenter Server](#).

Voraussetzungen

- Ihre aktuelle vCenter Single Sign-On-Instanz muss auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als die vCenter Server-Instanz installiert worden sein.
- Überprüfen Sie, ob Ihre Konfiguration die Upgrade-Anforderungen erfüllt. Weitere Informationen hierzu finden Sie unter [Anforderungen für vCenter Server für Windows](#).
- Führen Sie die vorbereitenden Aufgaben für das Upgrade aus. Weitere Informationen hierzu finden Sie unter [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Erstellen Sie unbedingt eine Sicherungskopie Ihrer vCenter Server-Konfiguration und -Datenbank.
- Laden Sie das Installationsprogramm für vCenter Server herunter. Weitere Informationen hierzu finden Sie unter [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).

Hinweis Eine Instanz von vCenter Single Sign-On 5.1, die auf derselben virtuellen Maschine bzw. demselben physischen Server wie vCenter Server 5.1 bereitgestellt wurde, wird automatisch auf eine eingebettete Platform Services Controller-Instanz aktualisiert, wenn Sie ein Upgrade auf vCenter Server 6.0 durchführen.

Verfahren

- 1 Laden Sie die vCenter Server für Windows-ISO-Datei herunter. Extrahieren Sie die ISO-Datei lokal oder mounten Sie die ISO-Datei als Laufwerk.
- 2 Doppelklicken Sie im Software-Installationsprogramm auf die Datei **autorun.exe**, um das Installationsprogramm zu starten.
- 3 Wählen Sie vCenter Server für Windows aus und klicken Sie auf Installieren.

Das Installationsprogramm führt im Hintergrund Prüfvorgänge vor dem Upgrade aus, um Ihre vorhandenen Einstellungen für vCenter Single Sign-On zu ermitteln und Sie über etwaige Probleme zu benachrichtigen, die sich negativ auf den Upgrade-Vorgang auswirken könnten. Die Seite „Willkommen“ des Installationsprogramms für vCenter Server wird geöffnet.

- 4 Überprüfen Sie die ermittelten Informationen und den Upgrade-Pfad.

Wenn ein Dialogfeld mit Hinweisen zu fehlenden Anforderungen anstelle eines Begrüßungsbildschirms angezeigt wird, befolgen Sie die im Dialogfeld aufgeführten Anweisungen.

- 5 Lesen Sie die Informationen auf der Begrüßungsseite und akzeptieren Sie die Lizenzvereinbarung.

Das Installationsprogramm führt im Hintergrund Prüfungsvorgänge vor dem Upgrade aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. Möglicherweise erhalten Sie eine Warnung, wenn die alten Zertifikate aktuelle VMware-Sicherheitsstandards nicht erfüllen.

- 6 Führen Sie ein Upgrade der vCenter Single Sign-On-Instanzen durch.

Sie können eine Platform Services Controller-Site erstellen oder hinzufügen.

- Wenn dies die erste oder primäre vCenter Single Sign-On-Instanz ist, führen Sie ein Upgrade auf eine neue eigenständige Platform Services Controller-Instanz durch, indem Sie einen neuen Domännennamen und Site-Namen für vCenter Single Sign-On konfigurieren.
- Wenn mindestens zwei vCenter Single Sign-On-Instanzen vorhanden sind und dies die zweite oder eine weitere vCenter Single Sign-On-Instanz ist, fügen Sie sie zur vCenter Single Sign-On-Site der primären Platform Services Controller-Instanz hinzu, um die Replizierung zu aktivieren.

Replizierungsinformationen werden während des Upgrades beibehalten.

Die vCenter Single Sign-On 5.1-Domäne „System-Domain“ wird zu der von Ihnen ausgewählten neuen Domäne migriert.

- 7 Konfigurieren Sie die Ports und klicken Sie auf Weiter.

Das Installationsprogramm prüft, ob die ausgewählten Ports verfügbar sind, und zeigt eine Fehlermeldung an, wenn ein ausgewählter Port nicht verwendet werden kann.

- 8 Konfigurieren Sie die Verzeichnisse „Installieren“, „Daten“ und „Exportieren“ und klicken Sie auf Weiter.

Das Installationsprogramm prüft den Festplattenspeicherplatz und die Berechtigungen für die ausgewählten Verzeichnisse und zeigt eine Fehlermeldung an, wenn die ausgewählten Verzeichnisse die Voraussetzungen nicht erfüllen.

- 9 Lesen Sie die Seite mit dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware und entscheiden Sie, ob Sie dem Programm beitreten möchten.

Informationen über das CEIP finden Sie im Abschnitt „Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit“ in *vCenter Server und Hostverwaltung*.

- 10 Überprüfen Sie, ob die Einstellungen auf der Seite „Übersicht“ stimmen. Vergewissern Sie sich, dass Sie eine Sicherungskopie Ihres Systems erstellt haben, und klicken Sie auf Upgrade.

Ein Fortschrittsbalken wird angezeigt, wenn das Installationsprogramm den Upgrade-Vorgang startet. Nach Abschluss des Vorgangs überprüft das Installationsprogramm das Upgrade.

- 11 Bevor Sie auf Fertig stellen klicken, sollten Sie die Schritte nach dem Upgrade durchlesen.

- 12 Klicken Sie auf Fertig stellen, um das Upgrade abzuschließen.

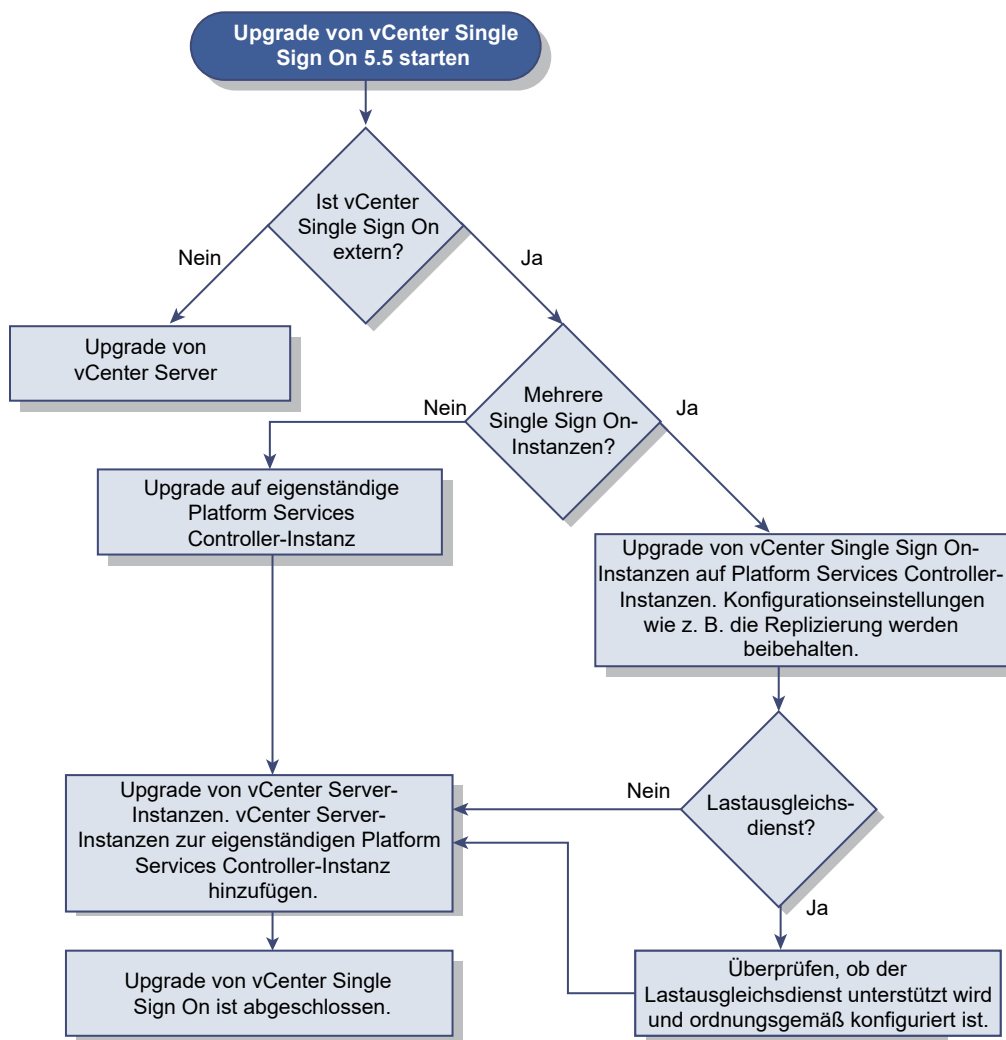
Nächste Schritte

Nach der Konfiguration einer externen Platform Services Controller-Instanz können Sie für vCenter Server ein Upgrade auf eine externe Bereitstellung durchführen.

Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung

Sie können ein Upgrade Ihrer extern bereitgestellten Instanz von vCenter Single Sign-On 5.5 auf eine extern bereitgestellte Platform Services Controller-Instanz mit dem Installationsprogramm von vCenter Server für Windows durchführen.

Abbildung 4-5. Upgrade-Workflow für vCenter Single Sign-On 5.5 für Windows



Wenn Sie eine extern bereitgestellte Instanz von vCenter Single Sign-On 5.5 auf einen extern bereitgestellten Platform Services Controller in einer gemischten Versionsumgebung aktualisieren, funktionieren alle vCenter Server 5.5-Instanzen ohne jegliche Probleme oder erforderliche Aktionen weiter mit dem aktualisierten Platform Services Controller, genauso wie bei der vCenter Single Sign-On-Instanz.

Hinweis Eine Instanz von vCenter Single Sign-On 5.5, die auf derselben virtuellen Maschine bzw. demselben physischen Server wie vCenter Server 5.5 bereitgestellt wurde, wird automatisch auf einen eingebetteten Platform Services Controller aktualisiert, wenn Sie ein Upgrade auf vCenter Server 6.0 durchführen.

- Weitere Informationen dazu, wie vCenter Single Sign-On sich auf Ihr Upgrade auswirkt, finden Sie unter [Auswirkungen von vCenter Single Sign On auf Upgrades](#).
- Informationen zum Verhalten von vCenter Server in gemischten Versionsumgebungen finden Sie unter [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).
- Informationen zu Bereitstellungsoptionen finden Sie unter [Bereitstellungsmodelle für vCenter Server](#).

Voraussetzungen

- Ihre aktuelle vCenter Single Sign-On-Instanz muss auf einer anderen virtuellen Maschine (VM) bzw. einem anderen physischen Server als die vCenter Server-Instanz installiert worden sein.
- Überprüfen Sie, ob Ihre Konfiguration die Upgrade-Anforderungen erfüllt. Weitere Informationen finden Sie unter [Anforderungen für vCenter Server für Windows](#).
- Führen Sie die vorbereitenden Aufgaben für das Upgrade aus. Siehe [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Erstellen Sie unbedingt eine Sicherungskopie Ihrer vCenter Server-Konfiguration und -Datenbank.
- Um sicherzustellen, dass sich der VMware Directory Service (vmdir) in einem stabilen Status befindet und beendet werden kann, starten Sie ihn manuell neu. Der VMware Directory Service muss beendet werden, damit die Upgradesoftware für vCenter Server während des Upgrade-Vorgangs vCenter Single Sign-On deinstallieren kann.
- Laden Sie das Installationsprogramm für vCenter Server herunter. Siehe [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).

Verfahren

- 1 Laden Sie die vCenter Server für Windows-ISO-Datei herunter. Extrahieren Sie die ISO-Datei lokal oder mounten Sie die ISO-Datei als Laufwerk.
- 2 Doppelklicken Sie im Software-Installationsprogramm auf die Datei **autorun.exe**, um das Installationsprogramm zu starten.

- 3 Wählen Sie vCenter Server für Windows aus und klicken Sie auf Installieren.

Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um Ihre vorhandenen Einstellungen für vCenter Single Sign-On zu ermitteln und Sie über etwaige Probleme zu benachrichtigen, die sich negativ auf den Upgrade-Vorgang auswirken könnten.

Die Seite „Willkommen“ des Installationsprogramms für vCenter Server wird geöffnet.

- 4 Überprüfen Sie die ermittelten Informationen und den Upgrade-Pfad.

Wenn ein Dialogfeld mit Hinweisen zu fehlenden Anforderungen anstelle eines Begrüßungsbildschirms angezeigt wird, befolgen Sie die im Dialogfeld aufgeführten Anweisungen.

- 5 Lesen Sie die Informationen auf der Begrüßungsseite und akzeptieren Sie die Lizenzvereinbarung.

- 6 Geben Sie die Anmeldedaten für **administrator@vsphere.local** ein.

Das Installationsprogramm führt im Hintergrund Prüfvorgänge vor dem Upgrade aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. Möglicherweise erhalten Sie eine Warnung, wenn die alten Zertifikate aktuelle VMware-Sicherheitsstandards nicht erfüllen.

- 7 Folgen Sie den Anweisungen, um das Upgrade der vCenter Single Sign-On-Instanz auf eine Platform Services Controller-Instanz durchzuführen.

Sie können eine Platform Services Controller-Instanz erstellen oder hinzufügen.

- Wenn dies die erste oder primäre vCenter Single Sign-On-Instanz ist, führen Sie ein Upgrade auf eine neue eigenständige Platform Services Controller-Instanz durch, indem Sie einen neuen Domänennamen und Site-Namen für vCenter Single Sign-On konfigurieren.
- Wenn mindestens zwei vCenter Single Sign-On-Instanzen vorhanden sind und dies die zweite oder eine weitere vCenter Single Sign-On-Instanz ist, fügen Sie sie zur vCenter Single Sign-On-Site der primären Platform Services Controller-Instanz hinzu, um die Replizierung zu aktivieren.

Replizierungsinformationen werden während des Upgrades beibehalten.

Die vCenter Single Sign-On 5.5-Domäne *System-Domain* wird zu der von Ihnen ausgewählten neuen Domäne migriert.

- 8 Konfigurieren Sie die Ports und klicken Sie auf Weiter.

Stellen Sie sicher, dass die Ports 80 und 443 frei und verfügbar sind, damit vCenter Single Sign-On diese Ports verwenden kann. Andernfalls verwenden Sie während der Installation benutzerdefinierte Ports.

Das Installationsprogramm prüft, ob die ausgewählten Ports verfügbar sind, und zeigt eine Fehlermeldung an, wenn ein ausgewählter Port nicht verwendet werden kann.

- 9 Konfigurieren Sie die Verzeichnisse „Installieren“, „Daten“ und „Exportieren“ und klicken Sie auf Weiter.

Das Installationsprogramm prüft den Festplattenspeicherplatz und die Berechtigungen für die ausgewählten Verzeichnisse und zeigt eine Fehlermeldung an, wenn die ausgewählten Verzeichnisse die Voraussetzungen nicht erfüllen.

- 10 Lesen Sie die Seite mit dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware und entscheiden Sie, ob Sie dem Programm beitreten möchten.

Informationen über das CEIP finden Sie im Abschnitt „Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit“ in *vCenter Server und Hostverwaltung*.

- 11 Überprüfen Sie, ob die Einstellungen auf der Seite „Übersicht“ stimmen. Vergewissern Sie sich, dass Sie eine Sicherungskopie Ihres Systems erstellt haben, und klicken Sie auf Upgrade.

Ein Fortschrittsbalken wird angezeigt, wenn das Installationsprogramm den Upgrade-Vorgang startet. Nach Abschluss des Vorgangs überprüft das Installationsprogramm das Upgrade.

- 12 Bevor Sie auf Fertig stellen klicken, sollten Sie die Schritte nach dem Upgrade durchlesen.

- 13 Klicken Sie auf Fertig stellen, um das Upgrade abzuschließen.

Nächste Schritte

Nach der Konfiguration einer externen Platform Services Controller-Instanz können Sie für vCenter Server ein Upgrade auf eine externe Bereitstellung durchführen.

Upgrade von vCenter Server 5.0

Sie können ein Upgrade Ihrer vorhandenen vCenter Server 5.0-Bereitstellung mit dem Installationsprogramm von vCenter Server für Windows durchführen.

Bei einem Upgrade von vCenter Server 5.0 können Sie während des Upgrades einen eingebetteten oder einen externen Platform Services Controller konfigurieren.

- Die von vCenter Server verwendeten Ports werden beibehalten. Die Ports können nicht während des Upgrades geändert werden. Informationen zu erforderlichen Ports finden Sie unter [Erforderliche Ports für vCenter Server und Platform Services Controller](#).
- Das Installationsprogramm migriert die Datenbank automatisch von Microsoft SQL Server Express zur PostgreSQL (vPostgres)-Datenbank, die Bestandteil von vCenter Server ist. Informationen zum Migrieren von Microsoft SQL Server Express zu Microsoft SQL Server und zum anschließenden Upgrade auf vCenter 6.0 finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1028601> und in der Microsoft-Dokumentation. Informationen zum Upgrade ohne Migration zur PostgreSQL-Datenbank finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2109321>.
- Informationen zu Bereitstellungsoptionen finden Sie unter [Bereitstellungsmodelle für vCenter Server](#) und [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#).

- Informationen zu den Schritten nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Voraussetzungen

- Überprüfen Sie, ob Ihre Konfiguration die Upgrade-Anforderungen erfüllt. Weitere Informationen hierzu finden Sie unter [Anforderungen für vCenter Server für Windows](#).
- Führen Sie die vorbereitenden Aufgaben für das Upgrade aus. Siehe [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Erstellen Sie unbedingt eine Sicherungskopie Ihrer vCenter Server-Konfiguration und -Datenbank.
- Laden Sie das Installationsprogramm für vCenter Server herunter. Siehe [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).

Verfahren

- 1 Laden Sie die vCenter Server für Windows-ISO-Datei herunter. Extrahieren Sie die ISO-Datei lokal oder mounten Sie die ISO-Datei als Laufwerk.

- 2 Doppelklicken Sie im Software-Installationsprogramm auf die Datei **autorun.exe**, um das Installationsprogramm zu starten.

- 3 Wählen Sie vCenter Server für Windows aus und klicken Sie auf Installieren.

Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um Ihre vorhandenen Einstellungen zu ermitteln und Sie über etwaige Probleme zu benachrichtigen, die sich negativ auf den Upgrade-Vorgang auswirken könnten.

Die Seite „Willkommen“ des Installationsprogramms für vCenter Server wird geöffnet.

- 4 Wenn das Installationsprogramm die ermittelten Information und den Upgrade-Pfad anzeigt, überprüfen Sie die Korrektheit dieser Informationen.

Wenn ein Dialogfeld mit Hinweisen zu fehlenden Anforderungen anstelle eines Begrüßungsbildschirms angezeigt wird, befolgen Sie die im Dialogfeld aufgeführten Anweisungen.

- 5 Schließen Sie die Schritte im Installationsassistenten ab und akzeptieren Sie die Lizenzvereinbarungen.

- 6 Geben Sie Ihre Administratoranmeldedaten für vCenter Server ein.

Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. Möglicherweise erhalten Sie eine Warnung, wenn die alten Zertifikate aktuelle VMware-Sicherheitsstandards nicht erfüllen.

7 Wählen Sie das Bereitstellungsmodell für vCenter Server aus.

- Wenn Sie vCenter Server mit einem eingebetteten Platform Services Controller auswählen, müssen Sie eine vCenter Single Sign-On-Domäne und -Site auswählen oder hinzufügen und dann auf Weiter klicken.

Wichtig Sie können zwar einer vCenter Single Sign-On-Domäne beitreten, aber Sie sollten vCenter Server mit eingebettetem Platform Services Controller als eigenständige Installation in Betracht ziehen und nicht für die Replizierung von Infrastrukturdaten verwenden.

- Wenn Sie vCenter Server mit einem externen Platform Services Controller auswählen, geben Sie die Informationen für den externen Platform Services Controller ein und klicken dann auf Weiter.

Für eine eingebettete Platform Services Controller-Instanz migriert das Installationsprogramm die vCenter Single Sign-On-Domäne *System-Domain* zur neuen Domäne, die für den Platform Services Controller ausgewählt ist. Für einen externen Platform Services Controller überprüft das Installationsprogramm die eingegebenen Informationen, indem mithilfe der eingegebenen Anmeldedaten eine Verbindung zur Platform Services Controller-Instanz hergestellt wird.

8 Konfigurieren Sie die Ports und klicken Sie auf Weiter.

Das Installationsprogramm prüft, ob die ausgewählten Ports verfügbar sind, und zeigt eine Fehlermeldung an, wenn ein ausgewählter Port nicht verwendet werden kann.

9 Konfigurieren Sie die Verzeichnisse „Installieren“, „Daten“ und „Daten exportieren“ und klicken Sie auf Weiter.

Das Installationsprogramm prüft den Festplattenspeicherplatz und die Berechtigungen für die ausgewählten Verzeichnisse und zeigt eine Fehlermeldung an, wenn die ausgewählten Verzeichnisse die Voraussetzungen nicht erfüllen.

10 Wenn Sie sich für die eingebettete Bereitstellung entscheiden, lesen Sie die Seite Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) von VMware durch und geben Sie an, ob Sie an dem Programm teilnehmen möchten.

Informationen über das CEIP finden Sie im Abschnitt „Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit“ in *vCenter Server und Hostverwaltung*.

11 Überprüfen Sie die Seite „Übersicht“, um sicherzustellen, dass die Einstellungen korrekt sind. Erstellen Sie unbedingt eine Sicherungskopie der vCenter Server-Maschine und der vCenter Server-Datenbank und klicken Sie auf Upgrade.

Ein Fortschrittsbalken wird angezeigt, wenn das Installationsprogramm den Upgrade-Vorgang startet. Nach Abschluss des Vorgangs überprüft das Installationsprogramm das Upgrade.

12 Bevor Sie auf Fertig stellen klicken, sollten Sie die Schritte nach dem Upgrade durchlesen.

13 Klicken Sie auf Fertig stellen, um das Upgrade abzuschließen.

Ergebnisse

Das Upgrade von vCenter Server für Windows ist abgeschlossen. Informationen zu den Aufgaben nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Upgrade von vCenter Server 5.1 für Windows

Sie können ein Upgrade Ihrer vorhandenen vCenter Server 5.1-Bereitstellung mit dem Installationsprogramm von vCenter Server für Windows durchführen.

Die Konfiguration der vCenter Server 5.1-Dienste bestimmt die Bereitstellung der Komponenten und Dienste nach dem Upgrade.

- Wenn sich vCenter Single Sign On 5.1 auf derselben virtuellen Maschine bzw. demselben physischen Server wie vCenter Server befindet, wird die Konfiguration vom Installationsprogramm auf vCenter Server mit einer eingebetteten Platform Services Controller-Bereitstellung aktualisiert.
- Wenn sich vCenter Single Sign On 5.1 auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als vCenter Server befindet, wird die Konfiguration vom Installationsprogramm auf vCenter Server mit einer externen Platform Services Controller-Bereitstellung aktualisiert.
- vCenter Server 5.1-Ports, die von vCenter Server und vCenter Single Sign On verwendet werden, werden beibehalten. Die Ports können nicht während des Upgrades geändert werden. Informationen zu erforderlichen Ports finden Sie unter [Erforderliche Ports für vCenter Server und Platform Services Controller](#).
- vCenter Server-Dienste werden nicht mehr separat von vCenter Server bereitgestellt. Für separat bereitgestellte Dienste der Version 5.1 erfolgt während des Upgrade-Vorgangs das Upgrade und die Migration zur vCenter Server-VM bzw. zum physischen Server. Weitere Informationen zur Migration von Diensten finden Sie unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#) und [Beispiele von Upgrade-Pfaden für vCenter Server](#).

- Das Installationsprogramm migriert die Datenbank automatisch von Microsoft SQL Server Express zur PostgreSQL-Datenbank, die Bestandteil von vCenter Server ist. Informationen zum Migrieren von Microsoft SQL Server Express zu Microsoft SQL Server und zum anschließenden Upgrade auf vCenter 6.0 finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1028601> und in der Microsoft-Dokumentation. Informationen zum Upgrade ohne Migration zur PostgreSQL-Datenbank finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2109321>.

Hinweis Wenn Sie eine externe vCenter Single Sign On-Instanz verwenden, müssen Sie dafür zunächst ein Upgrade auf Platform Services Controller 6.0 durchführen, bevor Sie für Ihre vCenter Server 5.5-Instanzen ein Upgrade auf Version 6.0 durchführen. Siehe [Upgrade von vCenter Single Sign-On 5.1 für die externe Bereitstellung](#).

- Informationen zu Bereitstellungsoptionen finden Sie unter [Bereitstellungsmodelle für vCenter Server](#) und [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#).
- Informationen zum Verhalten von vCenter Server in gemischten Versionsumgebungen finden Sie unter [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).
- Informationen zum Upgrade von vCenter Single Sign On 5.1 finden Sie unter [Upgrade von vCenter Single Sign-On 5.1 für die externe Bereitstellung](#).
- Informationen zu den Schritten nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Voraussetzungen

- Überprüfen Sie, ob Ihre Konfiguration die Upgrade-Anforderungen erfüllt. Siehe [Anforderungen für vCenter Server für Windows](#).
- Führen Sie die vorbereitenden Aufgaben für das Upgrade aus. Siehe [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Erstellen Sie unbedingt eine Sicherungskopie Ihrer vCenter Server-Konfiguration und -Datenbank.
- Laden Sie das Installationsprogramm für vCenter Server herunter. Siehe [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).

Verfahren

- 1 Laden Sie die vCenter Server für Windows-ISO-Datei herunter. Extrahieren Sie die ISO-Datei lokal oder mounten Sie die ISO-Datei als Laufwerk.
- 2 Doppelklicken Sie im Software-Installationsprogramm auf die Datei **autorun.exe**, um das Installationsprogramm zu starten.

- 3 Wählen Sie vCenter Server für Windows aus und klicken Sie auf Installieren.

Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um Ihre vorhandenen Einstellungen für vCenter Single Sign On zu ermitteln und Sie über etwaige Probleme zu benachrichtigen, die sich negativ auf den Upgrade-Vorgang auswirken könnten.

Die Seite „Willkommen“ des Installationsprogramms für vCenter Server wird geöffnet.

- 4 Wenn das Installationsprogramm die ermittelten Information und den Upgrade-Pfad anzeigt, überprüfen Sie die Korrektheit dieser Informationen.

Wenn ein Dialogfeld mit Hinweisen zu fehlenden Anforderungen anstelle eines Begrüßungsbildschirms angezeigt wird, befolgen Sie die im Dialogfeld aufgeführten Anweisungen.

- 5 Schließen Sie die Schritte im Installationsassistenten ab und akzeptieren Sie die Lizenzvereinbarungen.

Das Installationsprogramm führt im Hintergrund Prüfvorgänge vor dem Upgrade aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. Möglicherweise erhalten Sie eine Warnung, wenn die alten Zertifikate aktuelle VMware-Sicherheitsstandards nicht erfüllen.

- 6 Konfigurieren Sie die Platform Services Controller-Instanz.

- Wenn vCenter Server und vCenter Single Sign On auf derselben Maschine installiert sind, konfigurieren Sie Platform Services Controller und klicken Sie dann auf Weiter.
- Wenn sich vCenter Server und vCenter Single Sign On nicht auf derselben Maschine befinden, geben Sie die angeforderten Informationen für den externen Platform Services Controller ein und klicken Sie dann auf Weiter.

Für eine eingebettete Platform Services Controller-Instanz migriert das Installationsprogramm die vCenter Single Sign On-Domäne *System-Domain* zur neuen Domäne, die für den Platform Services Controller ausgewählt ist. Für einen externen Platform Services Controller überprüft das Installationsprogramm die eingegebenen Informationen, indem mithilfe der eingegebenen Anmeldedaten eine Verbindung zur Platform Services Controller-Instanz hergestellt wird.

- 7 Konfigurieren Sie die Ports und klicken Sie auf Weiter.

Das Installationsprogramm prüft, ob die ausgewählten Ports verfügbar sind, und zeigt eine Fehlermeldung an, wenn ein ausgewählter Port nicht verwendet werden kann.

- 8 Konfigurieren Sie die Verzeichnisse „Installieren“, „Daten“ und „Daten exportieren“ und klicken Sie auf Weiter.

Das Installationsprogramm prüft den Festplattenspeicherplatz und die Berechtigungen für die ausgewählten Verzeichnisse und zeigt eine Fehlermeldung an, wenn die ausgewählten Verzeichnisse die Voraussetzungen nicht erfüllen.

- 9 Überprüfen Sie die Seite „Übersicht“, um sicherzustellen, dass die Einstellungen korrekt sind. Erstellen Sie unbedingt eine Sicherungskopie der vCenter Server-Maschine und der vCenter Server-Datenbank und klicken Sie auf Upgrade.

Ein Fortschrittsbalken wird angezeigt, wenn das Installationsprogramm den Upgrade-Vorgang startet. Nach Abschluss des Vorgangs überprüft das Installationsprogramm das Upgrade.

- 10 Bevor Sie auf Fertig stellen klicken, sollten Sie die Schritte nach dem Upgrade durchlesen.
- 11 Klicken Sie auf Fertig stellen, um das Upgrade abzuschließen.

Ergebnisse

Das Upgrade von vCenter Server für Windows ist abgeschlossen. Informationen zu den Aufgaben nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Upgrade von vCenter Server 5.5 für Windows

Sie können ein Upgrade Ihrer vorhandenen vCenter Server 5.5-Bereitstellung mit dem Installationsprogramm von vCenter Server für Windows durchführen.

Die Konfiguration der vCenter Server 5.5-Dienste bestimmt die Bereitstellung der Komponenten und Dienste nach dem Upgrade.

- Wenn sich vCenter Single Sign-On 5.5 auf derselben virtuellen Maschine bzw. demselben physischen Server wie vCenter Server befindet, wird die Konfiguration vom Installationsprogramm auf vCenter Server mit einer eingebetteten Platform Services Controller-Bereitstellung aktualisiert.
- Wenn sich vCenter Single Sign-On 5.5 auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als dem vCenter Server befindet, wird die Konfiguration vom Installationsprogramm auf dem vCenter Server mit einer externen Platform Services Controller-Bereitstellung aktualisiert.
- vCenter Server 5.5-Ports, die von vCenter Server und vCenter Single Sign-On verwendet werden, werden beibehalten. Die Ports können nicht während des Upgrades geändert werden. Informationen zu erforderlichen Ports finden Sie unter [Erforderliche Ports für vCenter Server und Platform Services Controller](#).
- vCenter Server-Dienste werden nicht mehr separat von vCenter Server bereitgestellt. Für separat bereitgestellte Dienste der Version 5.5 erfolgt während des Upgrade-Vorgangs das Upgrade und die Migration zur vCenter Server-VM bzw. zum physischen Server. Weitere Informationen zur Migration von Diensten finden Sie unter [Migration von verteilten vCenter Server für Windows-Diensten während des Upgrades auf vCenter Server 6.0](#) und [Beispiele von Upgrade-Pfaden für vCenter Server](#).

- Das Installationsprogramm migriert die Datenbank automatisch von Microsoft SQL Server Express zur PostgreSQL-Datenbank, die Bestandteil von vCenter Server ist. Informationen zum Migrieren von Microsoft SQL Server Express zu Microsoft SQL Server und zum anschließenden Upgrade auf vCenter 6.0 finden Sie im VMware-Knowledgebase-Artikel unter <http://kb.vmware.com/kb/1028601> und in der Microsoft-Dokumentation. Informationen zum Upgrade ohne Migration zur PostgreSQL-Datenbank finden Sie im VMware-Knowledgebase-Artikel <http://kb.vmware.com/kb/2109321>.

Hinweis Wenn Sie eine externe vCenter Single Sign-On-Instanz verwenden, müssen Sie dafür zunächst ein Upgrade auf Platform Services Controller 6.0 durchführen, bevor Sie für Ihre vCenter Server 5.5-Instanzen ein Upgrade auf Version 6.0 durchführen. Siehe [Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung](#).

- Informationen zu Bereitstellungsoptionen finden Sie unter [Bereitstellungsmodelle für vCenter Server](#) und [Informationen zum Upgrade-Vorgang von vCenter Server 6.0 für Windows](#).
- Informationen zum Verhalten von vCenter Server in gemischten Versionsumgebungen finden Sie unter [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).
- Informationen zum Upgrade von vCenter Single Sign-On 5.5 finden Sie unter [Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung](#).
- Informationen zu den Schritten nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Voraussetzungen

- Überprüfen Sie, ob Ihre Konfiguration die Upgrade-Anforderungen erfüllt. Weitere Informationen hierzu finden Sie unter [Anforderungen für vCenter Server für Windows](#).
- Führen Sie die vorbereitenden Aufgaben für das Upgrade aus. Siehe [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Erstellen Sie unbedingt eine Sicherungskopie Ihrer vCenter Server-Konfiguration und -Datenbank.
- Um sicherzustellen, dass sich der VMware Directory Service (vmdir) in einem stabilen Status befindet und beendet werden kann, starten Sie ihn manuell neu. Der VMware Directory Service muss beendet werden, damit die Upgradesoftware für vCenter Server während des Upgrade-Vorgangs vCenter Single Sign-On deinstallieren kann.
- Laden Sie das Installationsprogramm für vCenter Server herunter. Weitere Informationen hierzu finden Sie unter [Herunterladen des Installationsprogramms für vCenter Server für Windows Installer](#).
- Wenn sich vCenter Single Sign-On 5.5 auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server als der vCenter Server befindet, führen Sie zunächst ein Upgrade von vCenter Single Sign-On 5.5 durch, bevor Sie das Upgrade von vCenter Server 5.5 vornehmen. Siehe [Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung](#).

Verfahren

- 1 Laden Sie die vCenter Server für Windows-ISO-Datei herunter. Extrahieren Sie die ISO-Datei lokal oder mounten Sie die ISO-Datei als Laufwerk.

- 2 Doppelklicken Sie im Software-Installationsprogramm auf die Datei **autorun.exe**, um das Installationsprogramm zu starten.

- 3 Wählen Sie vCenter Server für Windows aus und klicken Sie auf Installieren.

Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um Ihre vorhandenen Einstellungen für vCenter Single Sign-On zu ermitteln und Sie über etwaige Probleme zu benachrichtigen, die sich negativ auf den Upgrade-Vorgang auswirken könnten.

Die Seite „Willkommen“ des Installationsprogramms für vCenter Server wird geöffnet.

- 4 Klicken Sie auf **Weiter** und akzeptieren Sie die Lizenzvereinbarung.

- 5 Geben Sie Ihre Anmeldedaten für vCenter Server und vCenter Single Sign-On ein.

Option	Aktion
Wenn vCenter Single Sign-On auf derselben virtuellen Maschine oder demselben physischen Server installiert ist	<ol style="list-style-type: none"> 1 Geben Sie vCenter Single Sign-On-Anmeldedaten ein. 2 (Optional) Heben Sie die Auswahl des Kontrollkästchens Dieselben Anmeldedaten für vCenter Server verwenden auf, um abweichende Anmeldedaten für den vCenter Server-Benutzer zu verwenden, und geben Sie die gewünschten Anmeldedaten ein. 3 Klicken Sie auf Weiter. <p>Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. Möglicherweise erhalten Sie eine Warnung, wenn die alten Zertifikate aktuelle VMware-Sicherheitsstandards nicht erfüllen.</p>
Wenn vCenter Single Sign-On auf einer anderen virtuellen Maschine oder einem anderen physischen Server installiert ist	<ol style="list-style-type: none"> 1 Geben Sie Ihre Anmeldedaten für vCenter Server ein und klicken Sie auf Weiter. Das Installationsprogramm führt Prüfvorgänge im Hintergrund aus, um etwaige Probleme zu erkennen, die zum Fehlschlagen des Upgrade-Vorgangs führen könnten. 2 Registrieren Sie den vCenter Server bei einer vCenter Single Sign-On-Instanz in einem bestehenden Platform Services Controller 6.0. <ol style="list-style-type: none"> a (Optional) Ändern Sie den standardmäßigen vCenter Single Sign-On-HTTPS-Port. b Geben Sie Ihr Administratorkennwort für vCenter Single Sign-On ein und klicken Sie auf Weiter. 3 Überprüfen Sie das von dem Remoteserver bereitgestellte Zertifikat.

- 6 Konfigurieren Sie die Ports und klicken Sie auf Weiter.

Stellen Sie sicher, dass die Ports 80 und 443 frei und verfügbar sind, damit vCenter Single Sign-On diese Ports verwenden kann. Andernfalls verwenden Sie während der Installation benutzerdefinierte Ports.

Das Installationsprogramm prüft, ob die ausgewählten Ports verfügbar sind, und zeigt eine Fehlermeldung an, wenn ein ausgewählter Port nicht verwendet werden kann.

- 7 Konfigurieren Sie die Verzeichnisse „Installieren“, „Daten“ und „Daten exportieren“ und klicken Sie auf Weiter.

Das Installationsprogramm prüft den Festplattenspeicherplatz und die Berechtigungen für die ausgewählten Verzeichnisse und zeigt eine Fehlermeldung an, wenn die ausgewählten Verzeichnisse die Voraussetzungen nicht erfüllen.

- 8 Lesen Sie die Seite mit dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware und entscheiden Sie, ob Sie dem Programm beitreten möchten.

Informationen über das CEIP finden Sie im Abschnitt „Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit“ in *vCenter Server und Hostverwaltung*.

- 9 Überprüfen Sie die Seite „Übersicht“, um sicherzustellen, dass die Einstellungen korrekt sind. Aktivieren Sie das Kontrollkästchen, um sicherzustellen, dass Sie eine Sicherungskopie der vCenter Server-Maschine und der vCenter Server-Datenbank erstellt haben, und klicken Sie auf Upgrade.

Das Installationsprogramm startet den Upgrade-Vorgang und zeigt einen Fortschrittsbalken an. Nach Abschluss des Vorgangs überprüft das Installationsprogramm das Upgrade.

- 10 Bevor Sie auf Fertig stellen klicken, sollten Sie die Schritte nach dem Upgrade durchlesen.
- 11 Klicken Sie auf Fertig stellen, um das Upgrade abzuschließen.

Ergebnisse

Das Upgrade von vCenter Server für Windows ist abgeschlossen. Informationen zu den Aufgaben nach dem Upgrade finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Aktualisieren von Java-Komponenten und vCenter Server tc Server mit VIMPatch

Sie können die Java-Version aller vCenter Server-Komponenten je nach JRE-Server getrennt aktualisieren, indem Sie die ISO-Datei VIMPatch verwenden.

Sie können den Patch anwenden, ohne die vCenter Server-Komponenten neu zu installieren. Der Patch stellt Aktualisierungen für JRE bereit.

Voraussetzungen

- Laden Sie den Patch für Java-Komponenten von der VMware-Download-Seite unter <https://my.vmware.com/group/vmware/patch> herunter. Das Namensformat lautet `VMware-VIMPatch-6.0.0-build_number-YYYYMMDD.iso`.
- Stoppen Sie alle vCenter Server-Komponentenvorgänge, da beim Anwenden des Patches alle laufenden Dienste gestoppt werden.

Verfahren

- 1 Mounten Sie `VMware-VIMPatch-6.0.0-build_number-YYYYMMDD.iso` in dem System, in dem die vCenter Server-Komponente installiert ist.

- 2 Doppelklicken Sie auf *ISO_mount_directory/autorun.exe*.

Ein vCenter Server-Assistent zum Aktualisieren der Java-Komponenten wird geöffnet.

- 3 Klicken Sie auf **Patch auf alle anwenden**.

Mit dem Patch wird geprüft, ob die Java-Komponenten aktualisiert sind, und bei Bedarf werden sie im Hintergrund aktualisiert.

Aktualisieren und Patchen der vCenter Server Appliance und Platform Services Controller- Appliance

5

Sie können das Upgrade von vCenter Server Appliance mithilfe des Client-Integrations-Plug-Ins durchführen. Sie können die vCenter Server Appliance und Platform Services Controller-Appliance mit den Patches über die Verwaltungsschnittstelle der Appliance oder mit dem in der Appliance-Shell verfügbaren Dienstprogramm `software-packages` aktualisieren.

Wichtig Upgrades von vCenter Server Appliance 5.1 Update 3 und höher auf vCenter Server Appliance 6.0 werden unterstützt. Für das Upgrade von vCenter Server Appliance 5.0 müssen Sie zuerst die vCenter Server Appliance auf Version 5.1, Update 3 oder 5.5 Update 2 aktualisieren und dann ein Upgrade auf vCenter Server Appliance 6.0 durchführen. Informationen zum Aktualisieren der vCenter Server Appliance 5.0 auf Version 5.1 Update 3 finden Sie in der *Dokumentation zu VMware vSphere 5.1*. Informationen zum Aktualisieren von vCenter Server Appliance 5.0 auf Version 5.5 Update 2 finden Sie in der *Dokumentation zu VMware vSphere 5.5*.

Version 6.0 der vCenter Server Appliance verwendet die eingebettete PostgreSQL-Datenbank, die für Umgebungen mit bis zu 1.000 Hosts und bis zu 10.000 virtuellen Maschinen geeignet ist.

Version 6.0 der vCenter Server Appliance wird mit der virtuellen Hardwareversion 8 bereitgestellt, die 32 virtuelle CPUs pro virtueller Maschine in ESXi unterstützt. In Abhängigkeit von den Hosts, die Sie mit der vCenter Server Appliance verwalten werden, sollten Sie möglicherweise ein Upgrade der ESXi -Hosts durchführen und die Hardwareversion der vCenter Server Appliance aktualisieren, um mehr virtuelle CPUs zu unterstützen:

- ESXi 5,5.x bietet Unterstützung bis zur virtuellen Hardwareversion 10 mit bis zu 64 virtuellen CPUs pro virtueller Maschine.
- ESXi 6.0 bietet Unterstützung bis zur virtuellen Hardwareversion 11 mit bis zu 128 virtuellen CPUs pro virtueller Maschine.

Informationen zur Bereitstellung der vCenter Server Appliance finden Sie unter *Installations- und Einrichtungshandbuch für vSphere*.

Informationen zu Bestandslisten- und sonstigen Konfigurationsgrenzwerten in der vCenter Server Appliance finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*.

Informationen zum Konfigurieren der vCenter Server Appliance finden Sie unter *vCenter Server Appliance-Konfiguration*.

Dieses Kapitel enthält die folgenden Themen:

- [Upgrade der vCenter Server Appliance](#)
- [Patches der vCenter Server Appliance und Platform Services Controller-Appliance](#)

Upgrade der vCenter Server Appliance

Für ein Upgrade auf die neueste Version der vCenter Server Appliance müssen Sie das Client-Integrations-Plug-In verwenden. Alle für das vCenter Server Appliance-Upgrade erforderlichen Installationsdateien sind in einer ISO-Datei enthalten, die Sie von der VMware-Website herunterladen können.

Vor dem Upgrade der vCenter Server Appliance müssen Sie die ISO-Datei herunterladen und auf der Windows-Hostmaschine mounten, auf der Sie das Upgrade durchführen möchten. Installieren Sie das Client-Integrations-Plug-In und starten Sie dann den Upgrade-Assistenten.

Informationen zu den Anforderungen für das Upgrade der vCenter Server Appliance finden Sie unter [Anforderungen für die vCenter Server Appliance](#).

Informationen zu den während des Upgrades der vCenter Server Appliance erforderlichen Eingaben finden Sie unter [Erforderliche Informationen für das Upgrade der vCenter Server Appliance](#).

Beim Upgrade der vCenter Server Appliance handelt es sich um eine Migration der alten Version auf die neueste Version, wodurch die neue Version vCenter Server Appliance 6.0 auf einem ESXi-Host der Version 5.0 oder höher bereitgestellt wird. Die Konfigurationseinstellungen der vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen, werden migriert und auf die neu bereitgestellte vCenter Server Appliance angewendet. Der neuen Appliance wird eine temporäre IP-Adresse zugewiesen, um das Upgrade von der alten Appliance zu vereinfachen. Die IP-Adresse und der Hostname der vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen, werden im Rahmen des Upgrade-Vorgangs auf vCenter Server Appliance 6.0 angewendet. Am Ende des Upgrades wird die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchgeführt haben, ausgeschaltet.

Wichtig Wenn die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen, in einer gemischten IPv4- und IPv6-Umgebung konfiguriert ist, bleiben nur die IPv4-Einstellungen erhalten.

Wenn die vCenter Server Appliance, für die Sie ein Upgrade durchführen, eine nicht-flüchtige verteilte virtuelle Portgruppe verwendet, bleibt die Portgruppe nicht erhalten. Nach dem Upgrade können Sie die neue Appliance manuell mit der ursprünglichen nicht-flüchtigen verteilten virtuellen Portgruppe der alten Appliance verbinden.

In einer DHCP-Umgebung schlägt das Upgrade der vCenter Server Appliance fehl, wenn die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchzuführen versuchen, und vCenter Server Appliance 6.0 auf Hosts in unterschiedlichen Netzwerken ausgeführt werden.

Informationen zum Upgrade-Vorgang von vCenter Server Appliance

Sie können ein Upgrade von vCenter Server Appliance 5.1 Update 3 und 5.5.x auf Version 6.0 durchführen.

Der Upgrade-Vorgang beinhaltet Folgendes:

- 1 Exportieren der Konfiguration von vCenter Server Appliance 5.1 Update 3 oder 5.5.x.
- 2 Bereitstellen von vCenter Server Appliance 6.0.
- 3 Migrieren der Dienste und Konfigurationsdaten von vCenter Server Appliance 5.1 Update 3 oder 5.5.x zur neuen vCenter Server Appliance 6.0-Bereitstellung.

Nicht-flüchtige verteilte virtuelle Portgruppen werden nicht migriert. Nach dem Upgrade können Sie die neue Appliance manuell mit einer nicht-flüchtigen verteilten virtuellen Portgruppe verbinden.

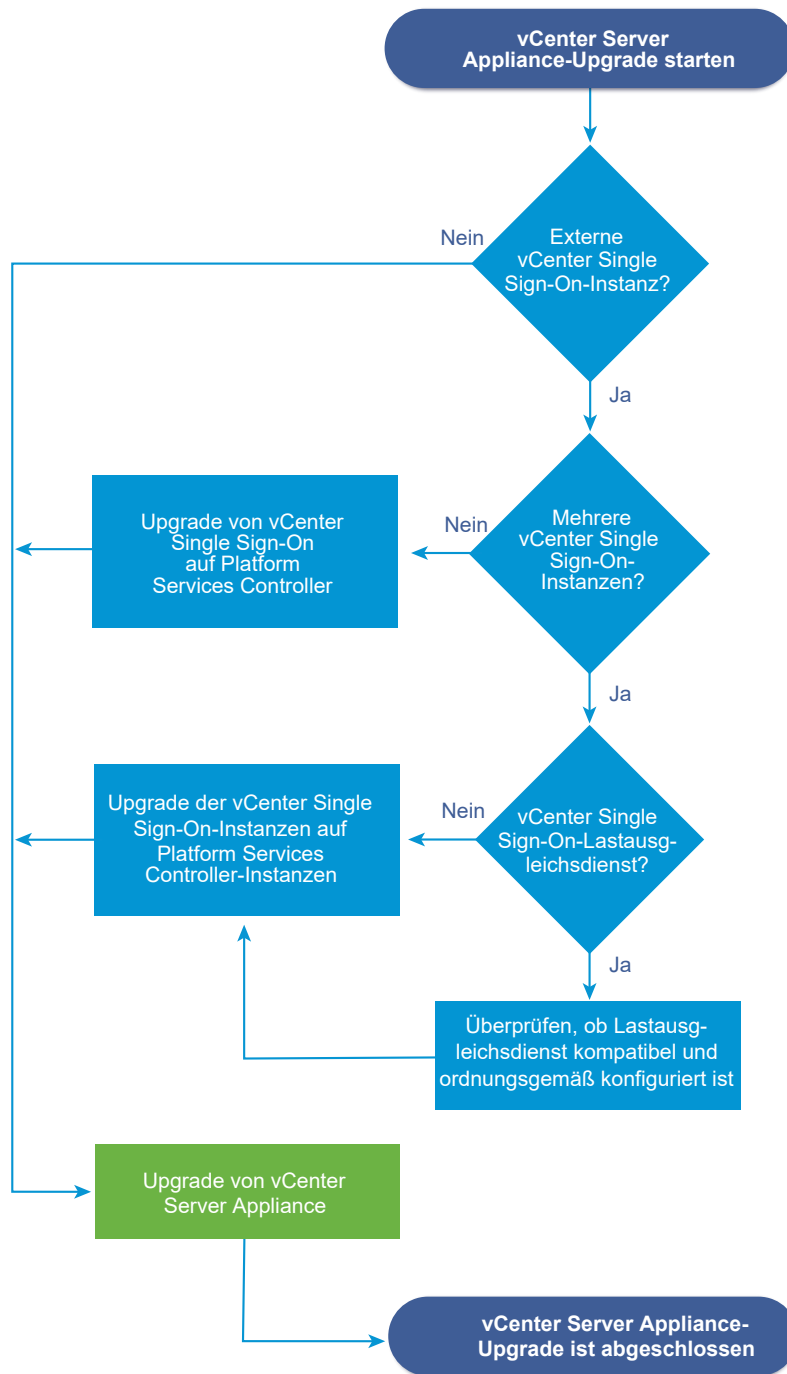
- 4 Ausschalten der Maschine mit vCenter Server Appliance 5.1 Update 3 oder 5.5.x, für die Sie ein Upgrade durchführen möchten.

Hinweis Das Upgrade der vCenter Server Appliance-Instanz, die bei einem externen vCenter Single Sign-On-Server registriert ist, wird nur für vCenter Server Appliance 5.5.x unterstützt.

Wenn Ihre aktuelle vCenter Server Appliance-Version älter als Version 5.1 Update 3 ist, müssen Sie vor dem Upgrade auf vCenter Server Appliance 6.0 zuerst ein Upgrade auf Version 5.1 Update 3 oder höher durchführen.

Wenn mehrere Instanzen von vCenter Server Appliance vorhanden sind, werden gleichzeitige Upgrades nicht unterstützt. Für die Instanzen müssen Sie nacheinander ein Upgrade durchführen.

Abbildung 5-1. Upgrade-Workflow für vCenter Server Appliance



- Informationen zur Kompatibilität von vCenter Single Sign-On und Platform Services Controller im Hinblick auf die Verwendung von qualifizierten Lastausgleichsdiensten und die damit verbundenen Anforderungen finden Sie unter [Kompatibilitätstabelle zur High Availability für vCenter Single Sign-On und Platform Services Controller](#).
- Informationen zu den Anforderungen für vCenter Server Appliance finden Sie unter [Anforderungen für die vCenter Server Appliance](#).

- Informationen zur Upgrade-Vorbereitung für vCenter Server Appliance finden Sie unter [Kapitel 3 Vor dem Upgrade von vCenter Server](#).
- Informationen zu den Upgrade-Vorgängen für vCenter Server Appliance finden Sie unter [Kapitel 5 Aktualisieren und Patchen der vCenter Server Appliance und Platform Services Controller-Appliance](#).
- Informationen zu den Vorgängen nach dem Upgrade für vCenter Server Appliance finden Sie unter [Kapitel 6 Nach dem Upgrade auf vCenter Server](#).

Herunterladen des Installationsprogramms der vCenter Server Appliance

Laden Sie das ISO-Installationsprogramm der vCenter Server Appliance und das Client-Integrations-Plug-in herunter.

Voraussetzungen

Erstellen Sie ein Customer Connect-Konto unter <https://my.vmware.com/web/vmware/>.

Verfahren

- 1 Laden Sie das Installationsprogramm für vCenter Server Appliance von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.

- 2 Bestätigen Sie, dass „md5sum“ korrekt ist.

Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Using MD5 Checksums“ (Verwenden von MD5-Prüfsummen) unter <http://www.vmware.com/download/md5.html>.

- 3 Mounten Sie das ISO-Image auf der virtuellen Windows-Maschine oder dem physischen Server, auf der bzw. dem das Client-Integrations-Plug-In zur Bereitstellung oder Aktualisierung der vCenter Server Appliance installiert werden soll.

Wenn Sie eine virtuelle Windows-Maschine verwenden, können Sie das ISO-Image als Datenspeicher-ISO-Datei für das CD-/DVD-Laufwerk der virtuellen Maschine konfigurieren, indem Sie den vSphere Web Client verwenden. Weitere Informationen finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Installieren des Client-Integrations-Plug-Ins

Sie müssen das Client-Integrations-Plug-In installieren, bevor Sie die vCenter Server Appliance bereitstellen oder aktualisieren können.

Voraussetzungen

[Herunterladen des Installationsprogramms der vCenter Server Appliance](#).

Verfahren

- 1 Wechseln Sie im Installationsprogramm für vCenter Server Appliance zum Verzeichnis `vc` und doppelklicken Sie auf `VMware-ClientIntegrationPlugin-6.0.0.exe`.
Der Assistent **Client-Integrations-Plug-In-Installation** wird eingeblendet.
- 2 Klicken Sie auf der Begrüßungsseite auf **Weiter**.
- 3 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 4 (Optional) Ändern Sie den Standardpfad zum Installationsordner des Client-Integrations-Plug-Ins und klicken Sie auf **Weiter**.
- 5 Prüfen Sie auf der Seite „Bereit zum Installieren des Plug-Ins“ des Assistenten die Informationen und klicken Sie auf **Installieren**.
- 6 Klicken Sie nach Abschluss der Installation auf **Beenden**.

Upgrade von vCenter Server Appliance mit eingebetteter vCenter Single Sign-On-Instanz

Mit dem Client-Integrations-Plug-In können Sie für vCenter Server Appliance 5.1 Update 3 und 5.5.x mit eingebetteter vCenter Single Sign-On-Instanz ein Upgrade auf vCenter Server Appliance 6.0 mit eingebettetem Platform Services Controller durchführen.

Sie können Version 6.0 von vCenter Server Appliance nur auf Hosts bereitstellen, auf denen ESXi 5.0 oder höher ausgeführt wird. Wenn Sie deshalb die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, auf einem Host mit einer älteren Version als ESXi 5.0 ausgeführt wird, müssen Sie zunächst ESXi 5.0 oder höher installieren, damit der Upgrade-Assistent vCenter Server Appliance 6.0 zu diesem Host migrieren kann.

Um sicherzustellen, dass eine vCenter Server Appliance-Instanz Zertifikate mit dem ordnungsgemäßen FQDN aufweist, müssen Sie sie mithilfe einer der folgenden Methoden bereitstellen:

- Starten Sie vCenter Server Appliance mithilfe von DHCP. DHCP weist einen vollqualifizierten Hostnamen zu.
- Stellen Sie vCenter Server Appliance auf einer vorhandenen vCenter Server-Instanz bereit. Die OVF-Eigenschaften für den Hostnamen werden während der Bereitstellung festgelegt.

Wenn Sie vCenter Server Appliance nicht mit den ordnungsgemäßen FQDNs bereitstellen, müssen Sie die Zertifikate neu generieren. Weitere Informationen hierzu finden Sie unter [Fehler bei VMware Component Manager während des Starts nach dem Upgrade von vCenter Server Appliance](#).

Voraussetzungen

- Überprüfen Sie, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind. Weitere Informationen hierzu finden Sie unter [Synchronisieren der Systemuhren im vSphere-Netzwerk](#).

- Stellen Sie sicher, dass sich der ESXi-Zielhost, auf dem Sie die vCenter Server Appliance bereitstellen, nicht im Sperr- oder im Wartungsmodus befindet.
- Stellen Sie sicher, dass für die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, genügend freier Speicherplatz für die Daten des Upgrades vorhanden ist.
- Vergewissern Sie sich, dass Port 22 für die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, geöffnet ist. Beim Upgrade-Prozess wird eine eingehende SSH-Verbindung eingerichtet, um die exportierten Daten von der vorhandenen Appliance herunterzuladen.
- Vergewissern Sie sich, dass Port 443 auf dem ESXi-Quellhost geöffnet ist, auf dem sich die vCenter Server Appliance-Instanz befindet, für die Sie ein Upgrade durchführen möchten. Beim Upgrade-Prozess wird eine HTTPS-Verbindung zum ESXi-Quellhost eingerichtet, um sicherzustellen, dass die vCenter Server Appliance-Instanz für das Upgrade bereit ist, und um eine SSH-Verbindung zwischen der neuen und der vorhandenen Appliance einzurichten.
- Stellen Sie sicher, dass das vCenter Server SSL-Zertifikat für Ihre vorhandene vCenter Server Appliance ordnungsgemäß konfiguriert ist. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel [2057223](#).
- Wenn Sie eine externe Datenbank verwenden, sollten Sie die vCenter Server Appliance-Datenbank sichern.
- Erstellen Sie einen Snapshot der vCenter Server Appliance, die Sie aktualisieren möchten.
- Installieren Sie die neue Version des Client-Integrations-Plug-Ins. Weitere Informationen hierzu finden Sie unter [Installieren des Client-Integrations-Plug-Ins](#).

Verfahren

- 1 Doppelklicken Sie im Verzeichnis des Softwareinstallationsprogramms auf **vcsa-setup.html**.
- 2 Warten Sie bis zu drei Sekunden, bis der Browser das Client-Integrations-Plug-In erkennt, und lassen Sie bei Aufforderung zu, dass das Plug-In im Browser ausgeführt wird.
- 3 Klicken Sie auf der Homepage auf **Upgrade**.
- 4 Klicken Sie in der Warnmeldung zur Unterstützung des Upgrades auf **OK**, um den Upgrade-Assistenten für vCenter Server Appliance zu starten.
- 5 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 6 Stellen Sie eine Verbindung zu dem Zielsystem her, auf dem Sie die vCenter Server Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.
 - a Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des ESXi-Hosts ein.
 - b Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den ESXi-Host ein, z. B. den Root-Benutzer.
- 7 (Optional) Akzeptieren Sie die Zertifikatwarnung, falls vorhanden, indem Sie auf **Ja** klicken.

- 8 Geben Sie einen Namen für vCenter Server Appliance 6.0 ein.
- 9 (Optional) Aktivieren Sie das Kontrollkästchen **SSH aktivieren**, um die SSH-Verbindung mit der vCenter Server Appliance zu ermöglichen.
- 10 Geben Sie auf der Seite „Verbindung herstellen mit Quell-Appliance“ die Details der Appliance ein, für die Sie ein Upgrade durchführen möchten.
 - a Wählen Sie im Dropdown-Menü **Version der vorhandenen Appliance** die vCenter Server Appliance-Version aus, für die Sie ein Upgrade auf vCenter Server Appliance 6.0 durchführen möchten.

Option	Beschreibung
vCSA 5.1 U3	Ermöglicht das Upgrade von vCenter Server Appliance 5.1 Update 3.
vCSA 5.5	Ermöglicht das Upgrade von vCenter Server Appliance 5.5.x.

- b Wählen Sie im Dropdown-Menü **Typ der vorhandenen Appliance** die Option **Eingebetteter Platform Services Controller** aus.

- c Geben Sie unter „vCenter Server Appliance“ die erforderlichen Daten der vCenter Server Appliance-Instanz ein, für die Sie ein Upgrade durchführen möchten.

Option	Aktion
IP-Adresse/FQDN von vCenter Server	Geben Sie die IP-Adresse oder den FQDN der vCenter Server Appliance-Instanz ein, für die Sie ein Upgrade durchführen möchten.
Benutzername des vCenter-Administrators	Geben Sie den Benutzernamen des vCenter Single Sign-On-Administrators ein. Bei einem Upgrade von vCenter Server Appliance 5.5.x ist dies „administrator@vsphere.local“.
Kennwort des vCenter-Administrators	Geben Sie das Kennwort des vCenter Single Sign-On-Administrators ein.
vCenter-HTTPS-Port	Ändern Sie optional die standardmäßige vCenter-HTTPS-Portnummer. Der Standardwert ist 443.
Root-Kennwort der Appliance (Betriebssystem)	Geben Sie das Kennwort für den Root-Benutzer ein.
Pfad für temporäre Upgrade-Dateien	Ändern Sie optional den Standardpfad zu dem Ordner, in dem die Konfigurationsdaten gespeichert werden. Standardmäßig werden alle Daten und Informationen zu den Einstellungen der vCenter Server Appliance, für die Sie ein Upgrade durchführen möchten, nach <code>/tmp/vmware/cis-export-folder</code> exportiert. Die Daten werden später zu vCenter Server Appliance 6.0 migriert.
Leistungsdaten und sonstige Verlaufsdaten migrieren	Wählen Sie optional aus, ob Sie die Migration optionaler Leistungs- und Verlaufsdaten, die in der Datenbank gespeichert sind, aktivieren möchten. Hierzu zählen Informationen zu Alarmen, Ereignissen, Statistiken usw. Wenn die Informationen sehr umfangreich sind, kann das Upgrade durch die Migration verlangsamt werden.

- d Geben Sie unter „ESXi-Quellhost“ die Informationen zu dem Host ein, auf dem sich die vCenter Server Appliance befindet, für die Sie ein Upgrade durchführen möchten.

Option	Beschreibung
IP-Adresse/FQDN des ESXi-Hosts	IP-Adresse oder FQDN des ESXi-Hosts, auf dem sich die vCenter Server Appliance befindet, für die Sie ein Upgrade durchführen möchten.
Benutzername des ESXi-Hosts	Der Benutzername des Benutzers mit Administratorrechten für den primären Host.
Kennwort des ESXi-Hosts	Das Kennwort des Administrators.

- 11 (Optional) Akzeptieren Sie ggf. die Warnmeldung, indem Sie auf **Ja** klicken.

- 12 Richten Sie die vCenter Single Sign-On-Einstellungen für die neu bereitgestellte Appliance ein und klicken Sie auf **Weiter**.

Wichtig Dieser Schritt ist nur dann obligatorisch, wenn Sie ein Upgrade von vCenter Server Appliance 5.1 Update 3 durchführen. Für Upgrades von vCenter Server Appliance 5.5.x werden die vCenter Single Sign-On-Daten automatisch zu vCenter Server Appliance 6.0 migriert.

Option	Beschreibung
vCenter SSO-Kennwort	Geben Sie das Kennwort für vCenter Single Sign-On ein. Das Kennwort muss zwischen acht und 20 Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen wie z. B. ein Dollarzeichen (\$), ein Ausrufezeichen (!), Klammern (()) oder ein At-Zeichen (@) enthalten.
Kennwort bestätigen	Bestätigen Sie das Kennwort für vCenter Single Sign-On.
SSO-Domänenname:	Geben Sie den Domänennamen für vCenter Single Sign-On ein. Der Domänenname muss den Standard RFC 1035 erfüllen.
SSO-Site-Name:	Geben Sie den Site-Namen für vCenter Single Sign-On ein.

- 13 Wählen Sie auf der Seite „Appliance-Größe auswählen“ des Assistenten die vCenter Server Appliance-Größe für die vSphere-Bestandslistengröße aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Sehr klein (bis zu 10 Hosts, 100 VMs)	Stellt eine Appliance mit 2 CPUs und 8 GB Arbeitsspeicher bereit.
Klein (bis zu 100 Hosts, 1.000 VMs)	Stellt eine Appliance mit 4 CPUs und 16 GB Arbeitsspeicher bereit.
Mittel (bis zu 400 Hosts, 4.000 VMs)	Stellt eine Appliance mit 8 CPUs und 24 GB Arbeitsspeicher bereit.
Groß (bis zu 1.000 Hosts, 10.000 VMs)	Stellt eine Appliance mit 16 CPUs und 32 GB Arbeitsspeicher bereit.

- 14 Wählen Sie aus der Liste mit den verfügbaren Datenspeichern den Speicherort für alle Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus. Aktivieren Sie optional Thin Provisioning, indem Sie **Thin-Festplattenmodus aktivieren** auswählen.

- 15 Wählen Sie das temporäre Netzwerk für die Kommunikation zwischen der vCenter Server Appliance, für die Sie ein Upgrade durchführen möchten, und der neu bereitgestellten vCenter Server Appliance aus. Wählen Sie die Methode für die Zuweisung der IP-Adresse für vCenter Server Appliance aus und klicken Sie auf **Weiter**.

Die im Dropdown-Menü **Temporäres Netzwerk auswählen** angezeigten Netzwerke hängen von den ESXi-Netzwerkeinstellungen ab. Nicht-flüchtige verteilte virtuelle Portgruppen werden nicht unterstützt und deshalb nicht im Dropdown-Menü angezeigt.

Option	Beschreibung
DHCP	Zum Zuteilen der IP-Adresse wird ein DHCP-Server verwendet.
Statisch	<p>Sie werden aufgefordert, die IP-Adresse und die Netzwerkeinstellungen einzugeben.</p> <ul style="list-style-type: none"> a Geben Sie eine temporäre IP-Adresse für die neue vCenter Server Appliance ein. b Geben Sie die Subnetzmaske ein. c Geben Sie das Netzwerk-Gateway ein. d Geben Sie FQDNs oder IP-Adressen der Netzwerk-DNS-Server ein. <p>Die Namen müssen durch Kommas getrennt werden.</p>

- 16 Lesen Sie die Seite mit dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware und entscheiden Sie, ob Sie dem Programm beitreten möchten.

Informationen über das CEIP finden Sie im Abschnitt „Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit“ in *vCenter Server und Hostverwaltung*.

- 17 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Einstellungen für das Upgrade von vCenter Server Appliance und klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.

- 18 (Optional) Klicken Sie nach Abschluss der Bereitstellung auf den Link **https://vCenter_Server_Appliance-IP-Adresse/vsphere-client**, um den vSphere Web Client zu starten, und melden Sie sich bei der vCenter Server-Instanz in der vCenter Server Appliance an.

- 19 Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Ergebnisse

Das Upgrade der vCenter Server Appliance wird durchgeführt. Die alte vCenter Server Appliance-Instanz wird deaktiviert und die neue Appliance wird gestartet.

Nächste Schritte

Wenn die alte vCenter Server Appliance-Instanz eine nicht-flüchtige verteilte virtuelle Portgruppe verwendet, können Sie die neue Appliance mit der ursprünglichen nicht-flüchtigen verteilten virtuellen Portgruppe verbinden, um die Portgruppeneinstellung zu erhalten. Weitere Informationen zum Konfigurieren des Netzwerks für virtuelle Maschinen auf einem vSphere Distributed Switch finden Sie unter *vSphere-Netzwerk*.

Upgrade von vCenter Server Appliance mit externer vCenter Single Sign-On-Instanz

Für das Upgrade von vCenter Server Appliance 5.5.x mit einer registrierten externen vCenter Single Sign-On-Instanz auf vCenter Server Appliance 6.0 mit externem Platform Services Controller können Sie das Client-Integrations-Plug-In verwenden.

Sie können Version 6.0 von vCenter Server Appliance nur auf Hosts bereitstellen, auf denen ESXi 5.0 oder höher ausgeführt wird. Wenn Sie deshalb die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, auf einem Host mit einer älteren Version als ESXi 5.0 ausgeführt wird, müssen Sie zunächst ESXi 5.0 oder höher installieren, damit der Upgrade-Assistent vCenter Server Appliance 6.0 zu diesem Host migrieren kann.

Umgebungen mit gemischten Versionen werden für Produktionsumgebungen nicht unterstützt und führen möglicherweise zu einem eingeschränkten Funktionsspektrum der Umgebung. Sie werden nur für den Zeitraum des Übergangs zwischen vCenter Server Appliance-Versionen empfohlen. Nachdem Sie für alle vCenter Server Appliance-Instanzen ein Upgrade durchgeführt und sie zum Platform Services Controller hinzugefügt haben, wird die Funktion „Verknüpfter Modus“ durch die Funktion „Erweiterter verknüpfter Modus“ ersetzt.

Um sicherzustellen, dass eine vCenter Server Appliance-Instanz Zertifikate mit dem ordnungsgemäßen FQDN aufweist, müssen Sie sie mithilfe einer der folgenden Methoden bereitstellen:

- Starten Sie vCenter Server Appliance mithilfe von DHCP. DHCP weist einen vollqualifizierten Hostnamen zu.
- Stellen Sie vCenter Server Appliance auf einer vorhandenen vCenter Server-Instanz bereit. Die OVF-Eigenschaften für den Hostnamen werden während der Bereitstellung festgelegt.

Wenn Sie vCenter Server Appliance nicht mit den ordnungsgemäßen FQDNs bereitstellen, müssen Sie die Zertifikate neu generieren. Weitere Informationen hierzu finden Sie unter [Fehler bei VMware Component Manager während des Starts nach dem Upgrade von vCenter Server Appliance](#).

Voraussetzungen

- Überprüfen Sie, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind. Weitere Informationen hierzu finden Sie unter [Synchronisieren der Systemuhren im vSphere-Netzwerk](#).
- Stellen Sie sicher, dass sich der ESXi-Zielhost, auf dem Sie die vCenter Server Appliance bereitstellen, nicht im Sperr- oder im Wartungsmodus befindet.
- Stellen Sie sicher, dass für die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, genügend freier Speicherplatz für die Daten des Upgrades vorhanden ist.

- Vergewissern Sie sich, dass Port 22 für die vCenter Server Appliance-Instanz, für die Sie ein Upgrade durchführen möchten, geöffnet ist. Beim Upgrade-Prozess wird eine eingehende SSH-Verbindung eingerichtet, um die exportierten Daten von der vorhandenen Appliance herunterzuladen.
- Vergewissern Sie sich, dass Port 443 auf dem ESXi-Quellhost geöffnet ist, auf dem sich die vCenter Server Appliance-Instanz befindet, für die Sie ein Upgrade durchführen möchten. Beim Upgrade-Prozess wird eine HTTPS-Verbindung zum ESXi-Quellhost eingerichtet, um sicherzustellen, dass die vCenter Server Appliance-Instanz für das Upgrade bereit ist, und um eine SSH-Verbindung zwischen der neuen und der vorhandenen Appliance einzurichten.
- Stellen Sie sicher, dass das vCenter Server SSL-Zertifikat für Ihre vorhandene vCenter Server Appliance ordnungsgemäß konfiguriert ist. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel [2057223](#).
- Wenn Sie eine externe Datenbank verwenden, sollten Sie die vCenter Server Appliance-Datenbank sichern.
- Führen Sie ein Upgrade der extern bereitgestellten vCenter Single Sign-On 5.5-Instanz auf einen extern bereitgestellten Platform Services Controller durch. Informationen zum Upgrade von vCenter Single Sign-On 5.5 finden Sie unter [Upgrade von vCenter Single Sign-On 5.5 für die externe Bereitstellung](#).
- Erstellen Sie einen Snapshot der vCenter Server Appliance, die Sie aktualisieren möchten.
- Installieren Sie die neue Version des Client-Integrations-Plug-Ins. Weitere Informationen hierzu finden Sie unter [Installieren des Client-Integrations-Plug-Ins](#).

Verfahren

- 1 Doppelklicken Sie im Verzeichnis des Softwareinstallationsprogramms auf **vcsa-setup.html**.
- 2 Warten Sie bis zu drei Sekunden, bis der Browser das Client-Integrations-Plug-In erkennt, und lassen Sie bei Aufforderung zu, dass das Plug-In im Browser ausgeführt wird.
- 3 Klicken Sie auf der Homepage auf **Upgrade**.
- 4 Klicken Sie in der Warnmeldung zur Unterstützung des Upgrades auf **OK**, um den Upgrade-Assistenten für vCenter Server Appliance zu starten.
- 5 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 6 Stellen Sie eine Verbindung zu dem Zielserver her, auf dem Sie die vCenter Server Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.
 - a Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des ESXi-Hosts ein.
 - b Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den ESXi-Host ein, z. B. den Root-Benutzer.
- 7 (Optional) Akzeptieren Sie die Zertifikatwarnung, falls vorhanden, indem Sie auf **Ja** klicken.
- 8 Geben Sie einen Namen für vCenter Server Appliance 6.0 ein.

- 9 (Optional) Aktivieren Sie das Kontrollkästchen **SSH aktivieren**, um die SSH-Verbindung mit der vCenter Server Appliance zu ermöglichen.
- 10 Geben Sie auf der Seite „Verbindung herstellen mit Quell-Appliance“ die Details der Appliance ein, für die Sie ein Upgrade durchführen möchten.
 - a Wählen Sie im Dropdown-Menü **Version der vorhandenen Appliance** die vCenter Server Appliance-Version aus, für die Sie ein Upgrade auf vCenter Server Appliance 6.0 durchführen möchten.

Option	Beschreibung
vCSA 5.1 U3	Ermöglicht das Upgrade von vCenter Server Appliance 5.1 Update 3.
vCSA 5.5	Ermöglicht das Upgrade von vCenter Server Appliance 5.5.x.

- b Wählen Sie im Dropdown-Menü **Typ der vorhandenen Appliance** die Option **vCenter Server** aus.

- c Geben Sie unter „vCenter Server Appliance“ die erforderlichen Daten der vCenter Server Appliance-Instanz ein, für die Sie ein Upgrade durchführen möchten.

Option	Aktion
IP-Adresse/FQDN von vCenter Server	Geben Sie die IP-Adresse oder den FQDN der vCenter Server Appliance-Instanz ein, für die Sie ein Upgrade durchführen möchten.
Benutzername des vCenter-Administrators	Geben Sie den Benutzernamen des vCenter Single Sign-On-Administrators ein. Bei einem Upgrade von vCenter Server Appliance 5.5.x ist dies „administrator@vsphere.local“.
Kennwort des vCenter-Administrators	Geben Sie das Kennwort des vCenter Single Sign-On-Administrators ein.
vCenter-HTTPS-Port	Ändern Sie optional die standardmäßige vCenter-HTTPS-Portnummer. Der Standardwert ist 443.
Root-Kennwort der Appliance (Betriebssystem)	Geben Sie das Kennwort für den Root-Benutzer ein.
Pfad für temporäre Upgrade-Dateien	Ändern Sie optional den Standardpfad zu dem Ordner, in dem die Konfigurationsdaten gespeichert werden. Standardmäßig werden alle Daten und Informationen zu den Einstellungen der vCenter Server Appliance, für die Sie ein Upgrade durchführen möchten, nach <code>/tmp/vmware/cis-export-folder</code> exportiert. Die Daten werden später zu vCenter Server Appliance 6.0 migriert.
Leistungsdaten und sonstige Verlaufsdaten migrieren	Wählen Sie optional aus, ob Sie die Migration optionaler Leistungs- und Verlaufsdaten, die in der Datenbank gespeichert sind, aktivieren möchten. Hierzu zählen Informationen zu Alarmen, Ereignissen, Statistiken usw. Wenn die Informationen sehr umfangreich sind, kann das Upgrade durch die Migration verlangsamt werden.

- d Geben Sie unter „ESXi-Quellhost“ die Informationen zu dem Host ein, auf dem sich die vCenter Server Appliance befindet, für die Sie ein Upgrade durchführen möchten.

Option	Beschreibung
IP-Adresse/FQDN des ESXi-Hosts	IP-Adresse oder FQDN des ESXi-Hosts, auf dem sich die vCenter Server Appliance befindet, für die Sie ein Upgrade durchführen möchten.
Benutzername des ESXi-Hosts	Der Benutzername des Benutzers mit Administratorrechten für den primären Host.
Kennwort des ESXi-Hosts	Das Kennwort des Administrators.

- 11 (Optional) Akzeptieren Sie ggf. die Warnmeldung, indem Sie auf **Ja** klicken.

- 12 Wählen Sie auf der Seite „Appliance-Größe auswählen“ des Assistenten die vCenter Server Appliance-Größe für die vSphere-Bestandslistengröße aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Sehr klein (bis zu 10 Hosts, 100 VMs)	Stellt eine Appliance mit 2 CPUs und 8 GB Arbeitsspeicher bereit.
Klein (bis zu 100 Hosts, 1.000 VMs)	Stellt eine Appliance mit 4 CPUs und 16 GB Arbeitsspeicher bereit.
Mittel (bis zu 400 Hosts, 4.000 VMs)	Stellt eine Appliance mit 8 CPUs und 24 GB Arbeitsspeicher bereit.
Groß (bis zu 1.000 Hosts, 10.000 VMs)	Stellt eine Appliance mit 16 CPUs und 32 GB Arbeitsspeicher bereit.

- 13 Wählen Sie aus der Liste mit den verfügbaren Datenspeichern den Speicherort für alle Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus. Aktivieren Sie optional Thin Provisioning, indem Sie **Thin-Festplattenmodus aktivieren** auswählen.
- 14 Wählen Sie das temporäre Netzwerk für die Kommunikation zwischen der vCenter Server Appliance, für die Sie ein Upgrade durchführen möchten, und der neu bereitgestellten vCenter Server Appliance aus. Wählen Sie die Methode für die Zuweisung der IP-Adresse für vCenter Server Appliance aus und klicken Sie auf **Weiter**.

Die im Dropdown-Menü **Temporäres Netzwerk auswählen** angezeigten Netzwerke hängen von den ESXi-Netzwerkeinstellungen ab. Nicht-flüchtige verteilte virtuelle Portgruppen werden nicht unterstützt und deshalb nicht im Dropdown-Menü angezeigt.

Option	Beschreibung
DHCP	Zum Zuteilen der IP-Adresse wird ein DHCP-Server verwendet.
Statisch	<p>Sie werden aufgefordert, die IP-Adresse und die Netzwerkeinstellungen einzugeben.</p> <ul style="list-style-type: none"> a Geben Sie eine temporäre IP-Adresse für die neue vCenter Server Appliance ein. b Geben Sie die Subnetzmaske ein. c Geben Sie das Netzwerk-Gateway ein. d Geben Sie FQDNs oder IP-Adressen der Netzwerk-DNS-Server ein. <p>Die Namen müssen durch Kommas getrennt werden.</p>

- 15 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Einstellungen für das Upgrade von vCenter Server Appliance und klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen.
- 16 (Optional) Klicken Sie nach Abschluss der Bereitstellung auf den Link **https://vCenter_Server_Appliance-IP-Adresse/vsphere-client**, um den vSphere Web Client zu starten, und melden Sie sich bei der vCenter Server-Instanz in der vCenter Server Appliance an.
- 17 Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Ergebnisse

Das Upgrade der vCenter Server Appliance wird durchgeführt. Die alte vCenter Server Appliance-Instanz wird deaktiviert und die neue Appliance wird gestartet.

Nächste Schritte

Wenn die alte vCenter Server Appliance-Instanz eine nicht-flüchtige verteilte virtuelle Portgruppe verwendet, können Sie die neue Appliance mit der ursprünglichen nicht-flüchtigen verteilten virtuellen Portgruppe verbinden, um die Portgruppeneinstellung zu erhalten. Weitere Informationen zum Konfigurieren des Netzwerks für virtuelle Maschinen auf einem vSphere Distributed Switch finden Sie unter *vSphere-Netzwerk*.

Patchen der vCenter Server Appliance und Platform Services Controller-Appliance

VMware veröffentlicht in regelmäßigen Abständen Patches für die vCenter Server Appliance, die möglicherweise mit Produkten von Drittanbietern auf der Plattform, der Kernproduktfunktion oder beidem in Verbindung steht. Mithilfe der Appliance-Verwaltungsschnittstelle oder der Appliance-Shell können Sie Patches auf eine vCenter Server Appliance-Instanz anwenden, die einen vCenter Server mit eingebettetem Platform Services Controller, einen vCenter Server mit externem Platform Services Controller oder einen Platform Services Controller enthält.

VMware verteilt die verfügbaren Patches auf zweierlei Art und Weise, eine für ISO-basiertes und eine andere für URL-basierte Patching-Modelle.

- Sie können die Patch-ISO-Images von <https://my.vmware.com/group/vmware/patch> herunterladen.

VMware veröffentlicht zwei Typen von ISO-Images, die Patches enthalten.

Download-Dateiname	Beschreibung
VMware-vCenter-Server-Appliance- produktversion-build-nummer-patch-TP.iso	Drittanbieter-Patch für die vCenter Server Appliance und Platform Services Controller-Appliance, der nur Fixes für Sicherheit und Drittanbieterprodukte enthält (z. B. JRE, tcServer und Komponenten von SUSE Linux Enterprise Server).
VMware-vCenter-Server-Appliance- produktversion-build-nummer-patch-FP.iso	Vollständiger Produkt-Patch für die vCenter Server Appliance und Platform Services Controller-Appliance, der die VMware-Software-Patches und Fixes für Sicherheit und Drittanbieterprodukte enthält (z. B. JRE, tcServer und Komponenten von SUSE Linux Enterprise Server).

- Sie können die vCenter Server Appliance und Platform Services Controller-Appliance konfigurieren, um eine Repository-URL als Quelle verfügbarer Patches zu verwenden. Die Appliance ist mit einer VMware-Standard-Repository-URL voreingestellt.

Sie können die Patches im ZIP-Format von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunterladen und ein benutzerdefiniertes Repository auf einem lokalen Webserver erstellen. Der Download-Dateiname lautet `VMware-vCenter-Server-Appliance-produktversion-build-nummer-updaterepo.zip`.

Wenn Patches verfügbar sind, können Sie auswählen, ob nur die Drittanbieter-Patches für Sicherheit und Drittanbieterprodukte (z. B. JRE, tcServer und Komponenten von SUSE Linux Enterprise Server) angewendet werden sollen oder alle VMware-Software-Patches zusammen mit den Drittanbieter-Patches angewendet werden sollen.

Wichtig Patches von Drittanbietern gehören gewöhnlich zur Sicherheitskategorie. Sie müssen immer mindestens die Sicherheits-Patches anwenden.

Vor der Aktualisierung einer vCenter Server Appliance-Instanz mit einem externen Platform Services Controller müssen Sie die Patches auf den Platform Services Controller und dessen Replizierungspartner (soweit in der vCenter Single Sign-On-Domäne vorhanden) anwenden. Weitere Informationen hierzu finden Sie unter [Aktualisierungssequenz für vSphere 6.0 und dessen kompatible VMware-Produkte](#).

Patchen der vCenter Server Appliance mit der Appliance-Verwaltungsschnittstelle

Sie können sich bei der Verwaltungsschnittstelle der Appliance einer vCenter Server Appliance anmelden, die einen vCenter Server mit eingebettetem Platform Services Controller, einen vCenter Server mit externem Platform Services Controller oder einen Platform Services Controller enthält, um die installierten Patches anzuzeigen, auf neue Patches zu prüfen und diese zu installieren sowie automatische Prüfungen auf verfügbare Patches zu konfigurieren.

Zur Durchführung von ISO-basiertem Patching laden Sie ein ISO-Image herunter, hängen das ISO-Image an das CD/DVD-Laufwerk der Appliance an, prüfen auf verfügbare Patches im ISO-Image und installieren die Patches.

Zur Durchführung von URL-basiertem Patching prüfen Sie auf verfügbare Patches in einer Repository-URL und installieren die Patches. Die vCenter Server Appliance ist mit einer VMware-Standard-Repository-URL für das Build-Profil der Appliance voreingestellt. Sie können die Appliance konfigurieren, um die VMware-Standard-Repository-URL oder eine benutzerdefinierte Repository-URL zu verwenden, z. B. eine Repository-URL, die Sie zuvor auf einem innerhalb Ihres Datacenters ausgeführten lokalen Webserver erstellt haben.

Anmelden bei der vCenter Server Appliance-Verwaltungsschnittstelle

Melden Sie sich bei der vCenter Server Appliance-Verwaltungsschnittstelle an, um auf die vCenter Server Appliance-Konfigurationseinstellungen zuzugreifen.

Hinweis Die Anmeldesitzung läuft ab, wenn Sie die vCenter Server Appliance-Verwaltungsschnittstelle 10 Minuten lang im Leerlauf lassen.

Voraussetzungen

Stellen Sie sicher, dass die vCenter Server Appliance erfolgreich bereitgestellt wurde und ausgeführt wird.

Verfahren

- 1 Navigieren Sie in einem Webbrowser zur vCenter Server Appliance-Verwaltungsschnittstelle, <https://Appliance-IP-Adresse-oder-FQDN:5480>.
- 2 Melden Sie sich als Root an.

Das standardmäßige Root-Kennwort ist das Kennwort, das Sie während der Bereitstellung der vCenter Server Appliance festlegen.

Konfigurieren des Repository für URL-basiertes Patching

Für URL-basiertes Patching wird die vCenter Server Appliance standardmäßig konfiguriert, um die VMware-Standard-Repository-URL, die für das Build-Profil der Appliance voreingestellt ist, zu verwenden. Sie können eine benutzerdefinierte Repository-URL als die aktuelle Quelle für Patches entsprechend den Anforderungen Ihrer Umgebung konfigurieren.

Das aktuelle Repository für URL-basiertes Patching ist standardmäßig die VMware-Standard-Repository-URL.

Hinweis Sie können den Befehl `proxy.set` verwenden, um einen Proxy-Server für die Verbindung zwischen der vCenter Server Appliance und der Repository-URL zu konfigurieren. Weitere Informationen zu den API-Befehlen in der Appliance-Shell finden Sie unter *vCenter Server Appliance-Konfiguration*.

Wenn die vCenter Server Appliance nicht mit dem Internet verbunden ist oder sofern dies von Ihren Sicherheitsrichtlinien vorgesehen ist, können Sie ein benutzerdefiniertes Repository erstellen und konfigurieren, das auf einem lokalen Webserver innerhalb Ihres Datacenters ausgeführt wird und die Daten von der VMware-Standard-Repository-URL repliziert. Wahlweise können Sie eine Authentifizierungsrichtlinie für den Zugriff auf den Webserver einrichten, auf dem sich das benutzerdefinierte Patch-Repository befindet.

Voraussetzungen

Melden Sie sich bei der vCenter Server Appliance-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Wenn Sie eine benutzerdefinierte Repository-URL konfigurieren möchten, erstellen Sie das Repository auf Ihrem lokalen Webserver.
 - a Laden Sie die ZIP-Datei mit dem vCenter Server Appliance-Patch von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.
 - b Erstellen Sie auf Ihrem Webserver ein Repository-Verzeichnis unter dem Stammverzeichnis.
Erstellen Sie z. B. das Verzeichnis **vc_update_repo**.
 - c Extrahieren Sie die ZIP-Datei in das Repository-Verzeichnis.
Die extrahierten Dateien befinden sich in den Unterverzeichnissen **manifest** und **package-pool**.
- 2 Klicken Sie in der vCenter Server Appliance-Verwaltungsschnittstelle auf **Aktualisieren**.
- 3 Klicken Sie auf **Einstellungen**.
- 4 Wählen Sie die Repository-Einstellungen aus.

Option	Beschreibung
Standard-Repository verwenden	Verwendet die VMware-Standard-Repository-URL, die für das Build-Profil der Appliance voreingestellt ist.
Angegebenes Repository verwenden	<p>Verwendet ein benutzerdefiniertes Repository. Sie müssen die Repository-URL, z. B. <code>http://web_server_name.your_company.com/vc_update_repo</code>, eingeben.</p> <p>Wenn die Repository-Richtlinie eine Authentifizierung erfordert, geben Sie einen Benutzernamen und ein Kennwort ein.</p>

- 5 Klicken Sie auf **OK**.

Nächste Schritte

[Prüfen auf und Installieren von vCenter Server Appliance-Patches](#)

Prüfen auf und Installieren von vCenter Server Appliance-Patches

Sie können entweder von einem ISO-Image oder direkt von einer Repository-URL auf Patches prüfen und diese installieren.

Wichtig Die in der Appliance ausgeführten Dienste sind während der Installation der Patches nicht verfügbar. Sie müssen diese Vorgehensweise während eines Wartungszeitraums durchführen. Als Vorsichtsmaßnahme für den Fall einer Fehlfunktion können Sie die vCenter Server Appliance sichern. Informationen zum Sichern und Wiederherstellen von vCenter Server finden Sie unter *Installations- und Einrichtungshandbuch für vSphere*.

Voraussetzungen

- Melden Sie sich bei der vCenter Server Appliance-Verwaltungsschnittstelle als Root-Benutzer an.
- Falls Sie die Appliance mithilfe eines ISO-Images patchen, das Sie vorher von <https://my.vmware.com/group/vmware/patch> heruntergeladen haben, müssen Sie das ISO-Image an das CD/DVD-Laufwerk der vCenter Server Appliance anhängen. Sie können das ISO-Image als Datenspeicher-ISO-Datei für das CD/DVD-Laufwerk der Appliance konfigurieren, indem Sie den vSphere Web Client verwenden. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Wenn Sie die Appliance von einer Repository-URL patchen, stellen Sie sicher, dass Sie die Repository-Einstellungen konfiguriert haben, und dass auf die aktuelle Repository-URL zugegriffen werden kann. Siehe [Konfigurieren des Repository für URL-basiertes Patching](#).
- Stellen Sie beim Patchen einer vCenter Server Appliance mit externem Platform Services Controller sicher, dass Sie die Patches auf den Platform Services Controller und dessen Replizierungspartner (soweit in der vCenter Single Sign-On-Domäne vorhanden) angewendet haben.

Verfahren

- 1 Klicken Sie in der vCenter Server Appliance-Verwaltungsschnittstelle auf **Aktualisieren**.

Im Bereich „Aktuelle Versionsdetails“ können Sie die Version und die Build-Nummer von vCenter Server Appliance anzeigen. Sie können auch den Verlauf von installierten Patches anzeigen, sofern vorhanden.

- 2 Klicken Sie auf **Updates überprüfen** und wählen Sie eine Quelle aus.

Option	Beschreibung
URL prüfen	Prüft die konfigurierte Repository-URL auf verfügbare Patches
CD-ROM prüfen	Prüft das ISO-Image, das Sie an das CD/DVD-Laufwerk der Appliance angehängt haben, auf verfügbare Patches

Im Bereich „Verfügbare Updates“ können Sie die Details zu den in der ausgewählten Quelle verfügbaren Patches anzeigen.

Wichtig Bei einigen Updates müssen Sie möglicherweise einen Neustart des Systems durchführen. Informationen zu diesen Updates finden Sie im Bereich „Verfügbare Updates“.

- 3 Klicken Sie auf **Updates installieren** und wählen Sie den anzuwendenden Bereich von Patches aus.

Option	Beschreibung
Alle Updates installieren	Wendet alle verfügbaren VMware- und Drittanbieter-Patches an
Drittanbieter-Updates installieren	Wendet nur die Drittanbieter-Patches an

- 4 Lesen Sie die Endbenutzer-Lizenzvereinbarung und akzeptieren Sie sie.
- 5 Klicken Sie nach Abschluss der Installation auf **OK**.
- 6 Wenn für die Patch-Installation die Appliance neu gestartet werden muss, klicken Sie auf **Übersicht** und anschließend auf **Neu starten**, um die Appliance zurückzusetzen.

Ergebnisse

Im Bereich „Verfügbare Updates“ können Sie den geänderten Aktualisierungsstatus der Appliance anzeigen.

Aktivieren der automatischen Suche nach vCenter Server Appliance-Patches

Sie können die vCenter Server Appliance konfigurieren, sodass in regelmäßigen Abständen in der konfigurierten Repository-URL automatisch nach verfügbaren Patches gesucht wird.

Voraussetzungen

- Melden Sie sich bei der vCenter Server Appliance-Verwaltungsschnittstelle als Root-Benutzer an.
- Prüfen Sie, ob Sie die Repository-Einstellungen konfiguriert haben und die aktuelle Repository-URL verfügbar ist. Siehe [Konfigurieren des Repository für URL-basiertes Patching](#).

Verfahren

- 1 Klicken Sie in der vCenter Server Appliance-Verwaltungsschnittstelle auf **Aktualisieren**.
- 2 Klicken Sie auf **Einstellungen**.
- 3 Wählen Sie **Automatisch auf Aktualisierungen prüfen** und wählen Sie den Zeitpunkt im UTC-Format, zu dem automatisch nach verfügbaren Patches gesucht werden soll.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Die Appliance führt in der konfigurierten Repository-URL regelmäßig eine Suche nach verfügbaren Patches durch. Im Fensterbereich „Verfügbare Updates“ können Sie Informationen zu den verfügbaren Patches sehen. Sie können sich auch den Systemzustand der vCenter Server Appliance mit Benachrichtigungen zu verfügbaren Patches anzeigen lassen. Siehe *vCenter Server Appliance-Konfiguration*.

Patchen der vCenter Server Appliance mit der Appliance-Shell

Mithilfe des `software-packages`-Dienstprogramms in der Appliance-Shell einer vCenter Server Appliance, die einen vCenter Server mit eingebettetem Platform Services Controller, einen vCenter Server mit externem Platform Services Controller oder einen Platform Services Controller enthält, können Sie die installierten Patches anzeigen sowie die neuen Patches bereitstellen und installieren.

Zur Durchführung des ISO-basierten Patchings laden Sie ein ISO-Image herunter, hängen das ISO-Image an das CD/DVD-Laufwerk der Appliance an, stellen wahlweise die verfügbaren Patches des ISO-Images auf der Appliance bereit und installieren die Patches.

Zur Durchführung von URL-basiertem Patching stellen Sie wahlweise die verfügbaren Patches einer Repository-URL auf der Appliance bereit und installieren die Patches. Die vCenter Server Appliance ist mit einer VMware-Standard-Repository-URL für das Build-Profil der Appliance voreingestellt. Sie können zur Konfiguration der Appliance den Befehl `update.set` verwenden, um die VMware-Standard-Repository-URL oder eine benutzerdefinierte Repository-URL zu verwenden, z. B. eine Repository-URL, die Sie zuvor auf einem innerhalb Ihres Datacenters ausgeführten lokalen Webserver erstellt haben. Sie können auch den Befehl `proxy.set` verwenden, um einen Proxy-Server für die Verbindung zwischen der vCenter Server Appliance und der Repository-URL zu konfigurieren.

Anzeigen einer Liste aller installierten Patches in der vCenter Server Appliance

Sie können mit dem `Software-Paket-Dienstprogramm` eine Liste der Patches anzeigen, die derzeit auf die vCenter Server Appliance angewendet sind. Sie können außerdem die Liste der installierten Patches in chronologischer Reihenfolge und Details zu einem speziellen Patch anzeigen.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Führen Sie zum Anzeigen der vollständigen Liste der Patches und Softwarepakete, die in der vCenter Server Appliance installiert sind, folgenden Befehl aus:

```
software-packages list
```

- 3 Führen Sie zum Anzeigen aller auf die vCenter Server Appliance angewendeten Patches in chronologischer Reihenfolge den folgenden Befehl aus:

```
software-packages list --history
```

Die Liste wird in chronologischer Reihenfolge angezeigt. Ein einzelner Patch in dieser Liste kann ein Update unterschiedlicher Pakete sein.

- 4 Führen Sie zum Anzeigen von Details zu einem speziellen Patch folgenden Befehl aus:

```
software-packages list --patch patch_name
```

Wenn Sie zum Beispiel die Details zum Patch `VMware-vCenter-Server-Appliance-Patch1` anzeigen möchten, führen Sie den folgenden Befehl aus:

```
software-packages list --patch VMware-vCenter-Server-Appliance-Patch1
```

Sie können die vollständige Liste der Details zum Patch wie Anbieter, Beschreibung und Installationsdatum anzeigen.

Konfigurieren von URL-basiertem Patching

Für URL-basiertes Patching ist die vCenter Server Appliance mit einer standardmäßigen VMware-Repository-URL für das Build-Profil der Appliance voreingestellt. Sie können den Befehl `update.set` zur Konfiguration der Appliance verwenden, sodass die standardmäßige oder eine benutzerdefinierte Repository-URL als aktuelle Quelle für Patches verwendet wird und automatische Suchen nach Patches ermöglicht werden.

Das aktuelle Repository für URL-basiertes Patching ist standardmäßig die VMware-Standard-Repository-URL.

Hinweis Sie können den Befehl `proxy.set` verwenden, um einen Proxy-Server für die Verbindung zwischen der vCenter Server Appliance und der Repository-URL zu konfigurieren. Weitere Informationen zu den API-Befehlen in der Appliance-Shell finden Sie unter *vCenter Server Appliance-Konfiguration*.

Wenn die vCenter Server Appliance nicht mit dem Internet verbunden ist oder sofern dies von Ihren Sicherheitsrichtlinien vorgesehen ist, können Sie ein benutzerdefiniertes Repository erstellen und konfigurieren, das auf einem lokalen Webserver innerhalb Ihres Datacenters ausgeführt wird und die Daten von der VMware-Standard-Repository-URL repliziert. Wahlweise können Sie eine Authentifizierungsrichtlinie für den Zugriff auf den Webserver einrichten, auf dem sich das benutzerdefinierte Patch-Repository befindet.

Verfahren

- 1 Wenn Sie eine benutzerdefinierte Repository-URL konfigurieren möchten, erstellen Sie das Repository auf Ihrem lokalen Webserver.
 - a Laden Sie die ZIP-Datei mit dem vCenter Server Appliance-Patch von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.
 - b Erstellen Sie auf Ihrem Webserver ein Repository-Verzeichnis unter dem Stammverzeichnis.
Erstellen Sie z. B. das Verzeichnis **vc_update_repo**.
 - c Extrahieren Sie die ZIP-Datei in das Repository-Verzeichnis.
Die extrahierten Dateien befinden sich in den Unterverzeichnissen `manifest` und `package-pool`.
- 2 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.
Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 3 Um Informationen zu den aktuellen URL-basierten Patch-Einstellungen anzuzeigen, führen Sie den Befehl `update.get` aus.

Sie können sich Informationen zur aktuellen Repository-URL, zur standardmäßigen Repository-URL, zur Zeit, zu der die Appliance zuletzt nach Patches gesucht hat, zur Zeit, zu der die Appliance zuletzt Patches installiert hat, und zur aktuellen Konfiguration der automatischen Suchen nach Patches anzeigen lassen.

- 4 Konfigurieren Sie das aktuelle Repository für URL-basiertes Patching.

- Um die Appliance für die Verwendung der standardmäßigen VMware-Repository-URL zu konfigurieren, führen Sie folgenden Befehl aus:

```
update.set --currentURL default
```

- Um die Appliance für die Verwendung einer benutzerdefinierten VMware-Repository-URL zu konfigurieren, führen Sie folgenden Befehl aus:

```
update.set --currentURL http://web_server_name.your_company.com/vc_update_repo [--username Benutzername] [--password Kennwort]
```

wobei die rechteckigen Klammern die Befehlsoptionen einschließen.

Wenn das benutzerdefinierte Repository eine Authentifizierung erfordert, verwenden Sie die Optionen `--username Benutzername` und `--password Kennwort`.

- 5 Um in regelmäßigen Abständen automatische Suchvorgänge nach vCenter Server Appliance-Patches in der aktuellen Repository-URL durchzuführen, führen Sie folgenden Befehl aus:

```
update.set --CheckUpdates enabled [--day Tag] [--time HH:MM:SS]
```

wobei die rechteckigen Klammern die Befehlsoptionen einschließen.

Verwenden Sie die Option `--day Tag`, um den Tag für die Durchführung der regelmäßigen Prüfungen für Patches festzulegen. Sie können einen bestimmten Wochentag festlegen, z. B. `Monday` oder `Everyday`. Der Standardwert ist `Everyday`.

Verwenden Sie die Option `--time HH:MM:SS`, um die Zeit in UTC zum Durchführen der regelmäßigen Prüfungen für Patches festzulegen. Der Standardwert ist `00:00:00`.

Die Appliance führt in der aktuellen Repository-URL regelmäßig eine Suche nach verfügbaren Patches durch.

- 6 Um automatische Prüfungen auf vCenter Server Appliance-Patches zu deaktivieren, führen Sie folgenden Befehl durch:

```
update.set --CheckUpdates disabled
```

Nächste Schritte

Falls Sie die Appliance so konfiguriert haben, dass automatische Prüfungen auf verfügbare Patches durchgeführt werden, können Sie in regelmäßigen Abständen den Systemzustand der vCenter Server Appliance nach Benachrichtigungen zu verfügbaren Patches durchsuchen. Siehe *vCenter Server Appliance-Konfiguration*.

Bereitstellen von Patches an die vCenter Server Appliance

Bevor Sie verfügbare Patches installieren, können Sie die Patches für die Appliance bereitstellen. Sie können das `software-packages`-Dienstprogramm verwenden, um Patches bereitzustellen, entweder von einem lokalen Repository durch Anhängen des ISO-Images an die Appliance oder direkt von einem Remote-Repository unter Verwendung einer Repository-URL.

Voraussetzungen

- Falls Sie Patches über ein ISO-Image bereitstellen, das Sie vorher von <https://my.vmware.com/group/vmware/patch> heruntergeladen haben, müssen Sie das ISO-Image an das CD/DVD-Laufwerk der vCenter Server Appliance anhängen. Sie können das ISO-Image als Datenspeicher-ISO-Datei für das CD/DVD-Laufwerk der Appliance konfigurieren, indem Sie den vSphere Web Client verwenden. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Wenn Sie Patches von einem Remote-Repository bereitstellen, stellen Sie sicher, dass Sie die Repository-Einstellungen konfiguriert haben, und dass auf die aktuelle Repository-URL zugegriffen werden kann. Siehe [Konfigurieren von URL-basiertem Patching](#).

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Stellen Sie die Patches bereit.

- Um die im angehängten ISO-Image enthaltenen Patches bereitzustellen, führen Sie den folgenden Befehl aus:

```
software-packages stage --iso
```

- Um die in der aktuellen Repository-URL enthaltenen Patches bereitzustellen, führen Sie den folgenden Befehl aus:

```
software-packages stage --url
```

Standardmäßig ist die aktuelle Repository-URL die Standard-Repository-URL von VMware.

Wenn Sie nur die Drittanbieter-Patches bereitstellen möchten, verwenden Sie die Option `--thirdParty`.

- Um die Patches bereitzustellen, die in einer aktuell nicht in der Appliance konfigurierten Repository-URL enthalten sind, führen Sie den folgenden Befehl aus:

```
software-packages stage --url URL_of_the_repository
```

Wenn Sie nur die Drittanbieter-Patches bereitstellen möchten, verwenden Sie die Option `--thirdParty`.

Falls Sie die Endbenutzer-Lizenzvereinbarung direkt akzeptieren, verwenden Sie die Option `--acceptEulas`.

Um z. B. nur Drittanbieter-Patches von der aktuellen Repository-URL bereitzustellen und die Endbenutzer-Lizenzvereinbarung (EULA) direkt zu akzeptieren, führen Sie den folgenden Befehl aus:

```
software-packages stage --url --thirdParty --acceptEulas
```

Während des Bereitstellungsvorgangs verifiziert der Befehl, dass es sich bei einem Patch um einen VMware-Patch handelt, dass im Bereitstellungsbereich genügend Speicherplatz vorhanden ist und dass die Patches nicht verändert wurden. Nur vollkommen neue Patches oder Patches für bestehende Pakete, die aktualisiert werden können, werden bereitgestellt.

- 3 (Optional) Um Informationen zu den bereitgestellten Patches anzuzeigen, führen Sie den folgenden Befehl aus:

```
software-packages list --staged
```

Jeder Patch enthält eine Metadatei mit Informationen wie Patchversion, Produktname, verpflichtender Systemneustart usw.

- 4 (Optional) Um eine Liste der bereitgestellten Patches anzuzeigen, führen Sie den folgenden Befehl aus:

```
software-packages list --staged --verbose
```

- 5 (Optional) Um die Bereitstellung der bereitgestellten Patches aufzuheben, führen Sie den folgenden Befehl aus:

```
software-packages unstage
```

Alle durch den Bereitstellungsvorgang generierten Verzeichnisse und Dateien werden entfernt.

Nächste Schritte

Installieren Sie die bereitgestellten Patches. Siehe [Installieren von vCenter Server Appliance-Patches](#).

Wichtig Wenn Sie Patches über ein ISO-Image bereitgestellt haben, sollte das ISO-Image weiterhin an das CD/DVD-Laufwerk der Appliance angehängt bleiben. Das ISO-Image muss während der Bereitstellung und Installation an das CD/DVD-Laufwerk der Appliance angehängt sein.

Installieren von vCenter Server Appliance-Patches

Sie können das Dienstprogramm `software-packages` verwenden, um die bereitgestellten Patches zu installieren. Sie können das Dienstprogramm `software-packages` auch verwenden, um Patches direkt von einem angehängten ISO-Image oder einer Repository-URL ohne Bereitstellung der Patch-Nutzlast zu installieren.

Wichtig Die in der Appliance ausgeführten Dienste sind während der Installation der Patches nicht verfügbar. Sie müssen diese Vorgehensweise während eines Wartungszeitraums durchführen. Als Vorsichtsmaßnahme für den Fall einer Fehlfunktion können Sie die vCenter Server Appliance sichern. Informationen zum Sichern und Wiederherstellen von vCenter Server finden Sie unter *Installations- und Einrichtungshandbuch für vSphere*.

Voraussetzungen

- Falls Sie bereitgestellte Patches installieren, überprüfen Sie, ob Sie die richtige Patch-Nutzlast bereitgestellt haben. Weitere Informationen hierzu finden Sie unter [Bereitstellen von Patches an die vCenter Server Appliance](#).
- Wenn Sie Patches installieren, die Sie zuvor über ein ISO-Image bereitgestellt haben, sollten Sie überprüfen, ob das ISO-Image an das CD/DVD-Laufwerk von vCenter Server Appliance angehängt ist. Weitere Informationen hierzu finden Sie unter [Bereitstellen von Patches an die vCenter Server Appliance](#).
- Falls Sie Patches direkt von einem ISO-Image installieren, das Sie vorher von <https://my.vmware.com/group/vmware/patch> heruntergeladen haben, müssen Sie das ISO-Image an das CD/DVD-Laufwerk der vCenter Server Appliance anhängen. Sie können das ISO-Image als Datenspeicher-ISO-Datei für das CD/DVD-Laufwerk der Appliance konfigurieren, indem Sie den vSphere Web Client verwenden. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.
- Falls Sie Patches direkt von einem Repository installieren, stellen Sie sicher, dass Sie die Repository-Einstellungen konfiguriert haben, und dass auf die aktuelle Repository-URL zugegriffen werden kann. Weitere Informationen hierzu finden Sie unter [Konfigurieren von URL-basiertem Patching](#).

- Stellen Sie beim Patchen einer vCenter Server Appliance mit externem Platform Services Controller sicher, dass Sie die Patches auf den Platform Services Controller und dessen Replizierungspartner (soweit in der vCenter Single Sign-On-Domäne vorhanden) angewendet haben.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Installieren Sie die Patches.

- Um bereitgestellte Patches zu installieren, führen Sie folgenden Befehl aus:

```
software-packages install --staged
```

- Um Patches direkt von einem angehängten ISO-Image zu installieren, führen Sie folgenden Befehl aus:

```
software-packages install --iso
```

- Um Patches direkt von der aktuellen Repository-URL zu installieren, führen Sie folgenden Befehl aus:

```
software-packages install --url
```

Standardmäßig ist die aktuelle Repository-URL die Standard-Repository-URL von VMware.

Falls Sie nur die Patches von Drittanbietern installieren möchten, verwenden Sie die Option `--thirdParty`.

- Um Patches direkt von einer Repository-URL zu installieren, die aktuell nicht konfiguriert ist, führen Sie folgenden Befehl aus:

```
software-packages install --url URL_of_the_repository
```

Falls Sie nur die Patches von Drittanbietern installieren möchten, verwenden Sie die Option `--thirdParty`.

Falls Sie die Endbenutzer-Lizenzvereinbarung direkt akzeptieren, verwenden Sie die Option `--acceptEulas`.

Um beispielsweise nur Patches von Drittanbietern auf der aktuellen Repository-URL zu installieren, ohne die Patches mit einer direkten Annahme der Endbenutzer-Lizenzvereinbarung bereitzustellen, führen Sie folgenden Befehl aus:

```
software-packages install --url --thirdParty --acceptEulas
```

- 3 Falls die Installation von Patches einen Neustart der Appliance erfordert, führen Sie folgenden Befehl aus, um die Appliance zurückzusetzen:

```
shutdown reboot -r "patch reboot"
```

Nach dem Upgrade auf vCenter Server

6

Beachten Sie nach dem Upgrade auf vCenter Server die folgenden Post-Upgrade-Optionen und -Anforderungen.

- Sie können die Upgradeprotokolle der Datenbank überprüfen. Siehe [Erfassen der Upgradeprotokolle für die Datenbank](#).
- Schließen Sie Komponentenneukonfigurationen ab, die für Änderungen während des Upgrades erforderlich sind.
- Stellen Sie sicher, dass Sie den Authentifizierungsvorgang verstehen, und identifizieren Sie Ihre Identitätsquellen.
- Aktualisieren Sie alle zusätzlichen Module, die mit dieser Instanz von vCenter Server verknüpft sind, wie z. B. vSphere Update Manager.
- Optional können Sie ein Upgrade oder eine Migration der ESXi-Hosts in der vCenter Server-Bestandsliste auf dieselbe Version der vCenter Server-Instanz durchführen.

Dieses Kapitel enthält die folgenden Themen:

- [Abschließen der Komponentenkonfiguration nach dem Upgrade für vCenter Server](#)
- [Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade](#)
- [Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy](#)
- [Aktualisieren des vSphere-Clients](#)
- [Konfigurieren von VMware vCenter Server - tc Server-Einstellungen im vCenter Server](#)
- [Einrichten des vCenter Server-Administratorbenutzers](#)
- [Authentifizieren für die vCenter Server-Umgebung](#)
- [Identitätsquellen für vCenter Server mit vCenter Single Sign On](#)
- [Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien](#)
- [Neuverweisen von vCenter Server auf einen anderen externen Platform Services Controller](#)
- [Neukonfigurieren einer eigenständigen vCenter Server-Instanz mit einem eingebetteten Platform Services Controller auf eine vCenter Server-Instanz mit einem externen Platform Services Controller](#)

- [Neukonfigurieren mehrerer beigetretener Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller auf vCenter Server mit einem externen Platform Services Controller](#)

Abschließen der Komponentenkonfiguration nach dem Upgrade für vCenter Server

Schließen Sie die Post-Upgrade-Optionen ab und erfüllen Sie die Post-Upgrade-Anforderungen Ihrer Konfiguration.

Wenn vor dem Upgrade ein lokaler Auto Deploy-Dienst bei vCenter Server registriert war, wird dieser ohne Änderung des Speicherorts automatisch aktualisiert. Auto Deploy-Remotedienste, die vor dem Upgrade bei vCenter Server registriert waren, werden auf die Maschine migriert, auf der sich vCenter Server zum Zeitpunkt des Upgrades befindet.

Wenn vor dem Upgrade ein vSphere Web Client-Dienst bei vCenter Server registriert war, wird dieser ohne Änderung des Speicherorts automatisch aktualisiert. Eine vSphere Web Client-Remote-Instanz, die vor dem Upgrade bei vCenter Server registriert war, wird auf die Maschine migriert, auf der sich vCenter Server zum Zeitpunkt des Upgrades befindet.

Informationen zum Neuverweisen von zuvor verteilten Komponentendiensten, die während des Upgrades auf den physischen Server oder die virtuelle Maschine von vCenter Server migriert werden, finden Sie unter [Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade](#).

Die SSL-Zertifizierungsprüfung ist erforderlich, um vSphere HA auf den Hosts zu konfigurieren.

Verfahren

- 1 Melden Sie sich auf der VMware-Website bei Ihrer Kontoseite an, um auf das Lizenzportal zuzugreifen. Führen Sie über das Lizenzportal ein Upgrade Ihrer vCenter Server-Lizenz durch. Weisen Sie mithilfe des vSphere Web Client dem vCenter Server-Host den aktualisierten Lizenzschlüssel zu.
- 2 Kopieren Sie für Oracle-Datenbanken den Oracle JDBC-Treiber (`ojdbc14.jar` oder `ojdbc5.jar`) in den Ordner `[VMware vCenter Server]\tomcat\lib`.
- 3 Wenn Sie für Microsoft SQL Server-Datenbanken die Massenprotokollierung für das Upgrade aktivieren, deaktivieren Sie diese Funktion nach Abschluss des Upgrades.
- 4 Wenn Sie vSphere HA-Cluster verwenden, muss die SSL-Zertifikatprüfung aktiviert sein.
Ist die Zertifikatsprüfung während des Upgrades nicht aktiviert, schlägt die Konfiguration von vSphere HA auf den Hosts fehl.
 - a Wählen Sie die vCenter Server-Instanz im Bestandslistenfenster aus.
 - b Wählen Sie die Registerkarte **Verwalten** und dann die Unterregisterkarte **Allgemein** aus.
 - c Stellen Sie sicher, dass für das Feld **SSL-Einstellungen** die Option **vCenter Server benötigt verifizierte Host-SSL-Zertifikate** ausgewählt ist.

Neukonfigurieren migrierter vCenter Server-Dienste nach dem Upgrade

vCenter Server 5.x-Dienste, die zuvor separat von vCenter Server bereitgestellt wurden, erfordern möglicherweise ein Neukonfiguration, nachdem sie während des Upgrade-Vorgangs zum vCenter Server-System migriert wurden.

vCenter Server-Komponenten können nicht mehr separat bereitgestellt werden. Wenn Komponenten von vCenter Server 5.x zuvor auf anderen Systemen als dem vCenter Server-System bereitgestellt wurden, werden sie von der Upgrade-Software zum vCenter Server-System migriert. Es kann vorkommen, dass erneut auf die migrierten Dienste verwiesen werden muss oder sonstige Schritte erforderlich sind.

Für vCenter Server Appliance 5.5-Instanzen mit Remote-Relay der Protokolle an externe Empfänger wie etwa LogInsight oder Splunk, migriert die Upgrade-Software die Relay-Konfiguration zum VMware Syslog-Dienst, der Bestandteil von vCenter Server Appliance 6.0 ist.

Bei einem Upgrade in einer gemischten Versionsumgebung sind vCenter Server 5.x-Instanzen, die die vCenter Single Sign On-Instanz verwendeten, nicht davon betroffen. Diese Instanzen verwenden ohne Probleme oder erforderliche Updates weiter die aktualisierte Platform Services Controller-Instanz wie vor dem Upgrade. vCenter Server 5.5-Instanzen sind weiter sichtbar für vSphere Web Client 5.5-Instanzen, nicht aber für vSphere Web Client 6.0-Instanzen. Siehe [Im Übergang befindliche gemischte Versionsumgebungen während vCenter Server-Upgrades](#).

Verfahren

- 1 Wenn Ihr vSphere Auto Deploy-Dienst zuvor auf einer anderen Maschine als vCenter Server installiert wurde und während des Upgrade-Vorgangs verlagert wurde, aktualisieren Sie Ihre DHCP- und TFTP-Einstellungen, sodass auf den verlagerten vSphere Auto Deploy-Dienst verwiesen wird.
 - a Laden Sie die Datei `deploy-tftp.zip` herunter und ersetzen Sie den tftp-Root-Ordner. Ihre Konfiguration hängt vom jeweiligen TFTP-Client ab.
 - b Konfigurieren Sie die `.conf-DHCP`-Datei, um den aktualisierten vSphere Auto Deploy-Dienst und die zugehörige `.tramp`-Datei zu verwenden. Ihre Konfiguration hängt vom jeweiligen DHCP-Setup ab.
- 2 Wenn Ihr vSphere Web Client zuvor auf einer anderen Maschine als vCenter Server installiert wurde und während des Upgrade-Vorgangs verlagert wurde, aktualisieren Sie den FQDN und die IP-Adresse, sodass auf den neuen Speicherort verwiesen wird.
- 3 Wenn VMware vSphere Syslog Collector zuvor auf einer anderen Maschine als vCenter Server installiert wurde, verweisen Sie die ESXi-Hosts auf den neuen Speicherort des vSphere Syslog Collector-Servers, wobei es sich um die aktualisierte vCenter Server 6.0-Instanz für Windows handelt.

- 4 Wenn Ihr vSphere ESXi Dump Collector-Server zuvor auf einer anderen Maschine als vCenter Server installiert wurde, verweisen Sie die ESXi-Hosts auf den neuen Speicherort des vSphere ESXi Dump Collector-Servers.
- 5 Um die Konfigurationsänderungen für das Remote-Relay der Protokolle an den vSphere Syslog-Dienst in einer aktualisierten vCenter Server Appliance anzuwenden, starten Sie den Dienst unmittelbar nach Abschluss des Upgrades auf Version 6.0 neu.
- 6 Um vCenter Server 5.5-Instanzen anzuzeigen, für die in einer im Übergang befindlichen gemischten Umgebung mit Version 5.5 und 6.0 noch kein Upgrade durchgeführt wurde, starten Sie die vSphere Web Client-Legacy-Instanz neu.
- 7 Wenn vCenter Server 5.x-Dienste weiterhin auf separaten virtuellen Maschinen oder physischen Servern ausgeführt werden, können Sie diese herunterfahren und entfernen. Sie werden von vCenter Server 6.0 nicht verwendet.

Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy

Installieren Sie vSphere Authentication Proxy, um ESXi-Hosts den Beitritt zu einer Domäne zu ermöglichen, ohne Active Directory-Anmeldeinformationen zu verwenden. vSphere Authentication Proxy verbessert die Sicherheit für von PXE gestartete Hosts sowie von Hosts, die unter Verwendung von Auto Deploy bereitgestellt werden, weil Active Directory-Anmeldeinformationen nicht in der Hostkonfiguration gespeichert werden müssen.

Wenn auf Ihrem System eine frühere Version von vSphere Authentication Proxy installiert ist, sorgt dieser Vorgang dafür, dass ein Upgrade von vSphere Authentication Proxy auf die aktuelle Version durchgeführt wird.

Sie können vSphere Authentication Proxy auf derselben Maschine wie den verknüpften vCenter Server oder auf einer anderen Maschine installieren, die über eine Netzwerkverbindung mit vCenter Server verfügt. vSphere Authentication Proxy wird ab vCenter Server-Version 5.0 unterstützt.

Der vSphere Authentication Proxy-Dienst bindet an eine IPv4-Adresse für die Kommunikation mit vCenter Server und bietet keine Unterstützung für IPv6. Die vCenter Server-Instanz kann sich auf einer Hostmaschine in einer Netzwerkumgebung befinden, in der nur IPv4, IPv4 und IPv6 oder nur IPv6 eingesetzt wird. Allerdings muss die Maschine, die eine Verbindung zu vCenter Server über den vSphere Web Client herstellt, über eine IPv4-Adresse verfügen, damit der vSphere Authentication Proxy-Dienst funktionieren kann.

Voraussetzungen

- Installieren Sie Microsoft .NET Framework 3.5 auf dem System, auf dem Sie vSphere Authentication Proxy installieren möchten.
- Stellen Sie sicher, dass Sie über Administratorberechtigungen verfügen.

- Stellen Sie sicher, dass die Hostmaschine über einen unterstützten Prozessor und ein unterstütztes Betriebssystem verfügt.
- Achten Sie darauf, dass die Hostmaschine über eine gültige IPv4-Adresse verfügt. Sie können vSphere Authentication Proxy auf einer Maschine in einer Netzwerkumgebung installieren, in der nur IPv4 oder sowohl IPv4 als auch IPv6 eingesetzt werden. Sie können vSphere Authentication Proxy jedoch nicht in einer Netzwerkumgebung installieren, in der nur IPv6 eingesetzt wird.
- Wenn Sie vSphere Authentication Proxy auf einer Windows Server 2008 R2-Hostmaschine installieren, laden Sie den im Windows-KB-Artikel 981506 auf der Website support.microsoft.com beschriebenen Windows-Hotfix herunter und installieren Sie ihn. Wenn dieser Hotfix nicht installiert ist, kann der vSphere Authentication Proxy-Adapter nicht initialisiert werden. Zu diesem Problem werden Fehlermeldungen in der Datei `camadapter.log` protokolliert, die den Meldungen `CAM-Website konnte nicht mit CTL gebunden werden` und `CAMAdapter konnte nicht initialisiert werden` ähneln.
- Laden Sie das vCenter Server-Installationsprogramm herunter.

Sammeln Sie die folgenden Informationen, um die Installation bzw. das Upgrade abzuschließen:

- Der Installationsspeicherort von vSphere Authentication Proxy, wenn Sie den Standardspeicherort nicht verwenden.
- Die Adresse und Anmeldeinformationen von vCenter Server, mit dem vSphere Authentication Proxy eine Verbindung herstellt: IP-Adresse oder Name, HTTP-Port, Benutzername und Kennwort.
- Der Hostname oder die IP-Adresse, die zum Identifizieren von vSphere Authentication Proxy im Netzwerk verwendet wird.

Verfahren

- 1 Fügen Sie die Hostmaschine dort hinzu, wo Sie den Authentication Proxy-Dienst für die Domäne installieren.
- 2 Verwenden Sie das Domänenadministratorkonto, um sich bei der Hostmaschine anzumelden.
- 3 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.
- 4 Wählen Sie **VMware vSphere Authentication Proxy** aus und klicken Sie auf **Installieren**.
- 5 Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation bzw. das Upgrade abzuschließen.

Während der Installation registriert sich der Authentifizierungsdienst mit der vCenter Server-Instanz, auf der Auto Deploy registriert ist.

Ergebnisse

Wenn Sie den vSphere Authentication Proxy-Dienst installieren, erstellt das Installationsprogramm ein Domänenkonto mit den entsprechenden Berechtigungen zum Ausführen des Authentication Proxy-Diensts. Der Name des Kontos beginnt mit dem Präfix `CAM-` und ihm wird ein 32-stelliges, nach dem Zufallsprinzip generiertes Kennwort zugeordnet. Das Kennwort ist so konfiguriert, dass es nie abläuft. Ändern Sie die Kontoeinstellungen nicht.

Nächste Schritte

Konfigurieren Sie ESXi für die Verwendung von vSphere Authentication Proxy zum Beitritt in eine Domäne. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Aktualisieren des vSphere-Clients

Benutzer virtueller Maschinen und vCenter Server-Administratoren müssen den vSphere-Client 6.0 verwenden, um eine Verbindung mit vCenter Server 6.0 oder eine direkte Verbindung mit ESXi 6.0-Hosts herzustellen.

Sie können den VI Client 2.5, den vSphere Client 4.x, den vSphere Client 5.x und den vSphere Client 6.0 auf derselben Maschine installieren. Aktualisieren Sie nach dem Upgrade von vCenter Server vSphere Client auf die gleiche Version, um Kompatibilitätsprobleme zu vermeiden, die den Betrieb des vSphere Client beeinträchtigen können.

Der Upgrade-Vorgang von vSphere-Client erfordert keine Ausfallzeit. Die virtuelle Maschinen oder Clients brauchen nicht ausgeschaltet zu werden.

Voraussetzungen

- Stellen Sie sicher, dass Ihnen das Installationsprogramm für vCenter Server oder für den vSphere-Client zur Verfügung steht.
- Stellen Sie sicher, dass Sie Mitglied der Administratorgruppe auf diesem System sind.
- Stellen Sie sicher, dass das System über einen Internetzugang verfügt.

Verfahren

- 1 (Optional) Verwenden Sie die Option **Software** in der Windows-Systemsteuerung, um alle vorherigen Versionen von vCenter Server zu entfernen.

Sie müssen ältere Versionen von vCenter Server-Clients nicht entfernen. Diese Versionen sind zum Herstellen einer Verbindung mit Legacy-Hosts hilfreich.

- 2 Führen Sie das vSphere-Client-Installationsprogramm aus.
 - Starten Sie das vCenter Server-Installationsprogramm. Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe` und wählen Sie **vSphere-Client**.
 - Doppelklicken Sie nach dem Herunterladen des vSphere-Clients auf die Datei `VMware-viclient-Build-Nummer.exe`.

Ergebnisse

Nachdem Sie den vSphere Client 6.0 installiert haben, können Sie eine Verbindung zu einem ESXi-Host herstellen, indem Sie den Domännennamen oder eine IP-Adresse des Hosts und den Benutzernamen und das Kennwort eines Benutzers auf dieser Maschine verwenden.

Nächste Schritte

Verwenden Sie den vSphere Client, um eine direkte Verbindung mit einem ESXi-Host herzustellen. Verwenden Sie dazu Ihren Benutzernamen und Ihr Kennwort.

Wenn der vSphere Client Sicherheitswarnungen und Ausnahmen anzeigt, wenn Sie sich anmelden oder manche Vorgänge ausführen, wie z. B. Leistungsdiagramme öffnen oder die Registerkarte **Übersicht** anzeigen, kann dies daran liegen, dass die Sicherheitseinstellungen von Internet Explorer (IE) auf „Hoch“ gesetzt sind. Wenn Ihre IE-Sicherheitseinstellungen auf „Hoch“ gesetzt sind, aktivieren Sie die IE-Einstellung **Skripting des Internet Explorer-Browsersteuerelements zulassen**.

Konfigurieren von VMware vCenter Server - tc Server-Einstellungen im vCenter Server

Ab vCenter Server 5.1 können VMware Tomcat Server-Einstellungen nicht mehr über die Windows-Benutzeroberfläche konfiguriert werden. Die Versionen 5.1 und höher von vCenter Server verwenden VMware vCenter Server - tc Server, eine Unternehmensversion von Apache Tomcat 7. Tomcat-Version 7 stellt keine Systemsteuerung auf der Windows-Benutzeroberfläche bereit. Stattdessen konfigurieren Sie Tomcat, indem Sie die Konfigurationsdateien manuell bearbeiten.

Einstellungen für Java-Optionen werden in den folgenden Dateien gespeichert.

- vCenter Server.
`installation_directory\VMware\Infrastructure\tomcat\conf\wrapper.conf`
- vCenter Inventory Service.
`installation_directory\VMware\Infrastructure\Inventory Service\conf\wrapper.conf`
- Profile-Driven Storage Service.
`installation_directory\VMware\Infrastructure\Profile-Driven Storage\conf\wrapper.conf`
- vSphere Web Client.
`installation_directory\VMware\vSphereWebClient\server\bin\service\conf\wrapper.conf`

Tabelle 6-1. Die Einstellung für die maximale Java-Heap-Größe der JVM für Inventory Service und den profilgesteuerten Speicherdienst in den `wrapper.conf`-Dateien

Java-Option	Einstellung und Standardwert
<p><code>maxmemorysize</code></p> <p>Die maximale JVM-Heap-Größe in Megabyte. Diese Einstellung steuert die maximale Größe für den Java-Heap. Durch die Optimierung dieses Parameters kann der Overhead für die Speicherbereinigung gesenkt werden, wodurch Antwortzeit und Durchsatz des Servers verbessert werden. Für einige Anwendungen ist die Standardeinstellung für diese Option zu niedrig, was zu einer höheren Anzahl an kleineren Speicherbereinigungen führt.</p>	<p>Inventory Service: <code>wrapper.java.maxmemory=2048</code></p> <p>Profile-Driven Storage Service: <code>wrapper.java.maxmemory=1024</code></p> <p>Der vSphere Web Client: Für große Bereitstellungen müssen Sie diese Option möglicherweise auf <code>wrapper.java.maxmemory=2048</code> setzen.</p>
<p><code>ping.timeoutduration</code></p>	<p>Der vSphere Web Client: Für große Bereitstellungen müssen Sie diese Option möglicherweise auf <code>wrapper.ping.timeout=120</code> setzen.</p>

vCenter Server Die Sicherheits- und Porteinstellungen werden in den folgenden Dateien gespeichert:

- `Installationsverzeichnis\VMware\Infrastructure\tomcat\conf\server.xml`
- `installation_directory\VMware\Infrastructure\tomcat\conf\catalina.properties`

Tabelle 6-2. Port- und Sicherheitseinstellungen für vCenter Server in den Dateien `server.xml` und `catalina.properties`

Port- bzw. Sicherheitseinstellung für vCenter Server	Einstellung und Standardwert
Basisport zum Herunterfahren	<code>base.shutdown.port=8003</code>
<p>Basis-JMX-Port. Der durch die Klasse <code>com.springsource.tcserver.serviceability.rmi.JmxSocketListener</code> implementierte Listener ist für tc Server spezifisch. Dieser Listener ermöglicht die JMX-Management von tc Server und ist die JMX-Konfiguration, die von der AMS-Verwaltungskonsole zum Verwalten von tc Server-Instanzen verwendet wird. Das Port-Attribut gibt den Port des JMX-Servers für die Verbindung mit Verwaltungsprodukten wie AMS an. Die Variable <code>\$jmx.port</code> ist in der Standarddatei <code>catalina.properties</code> auf „6969“ eingestellt. Das Bindungsattribut gibt den Host des JMX-Servers an. Standardmäßig ist dieses Attribut auf „localhost“ (127.0.0.1) eingestellt.</p> <p>Mit der Standardeinstellung „-1“ wird der Port deaktiviert.</p>	<code>base.jmx.port=-1</code>
Web Services HTTPS	<code>bio-vmsl.http.port=8080</code>
Web Services HTTPS	<code>bio-vmsl.https.port=8443</code>

Tabelle 6-2. Port- und Sicherheitseinstellungen für vCenter Server in den Dateien `server.xml` und `catalina.properties` (Fortsetzung)

Port- bzw. Sicherheitseinstellung für vCenter Server	Einstellung und Standardwert
SSL-Zertifikat	bio- vmssl.keyFile.name=C:\ProgramData\VMware\VMware VirtualCenter\SSL\rui.pfx
Kennwort für SSL-Zertifikat	bio-vmssl.SSL.password=testpassword

Siehe *Getting Started with vFabric tc Server* und *vFabric tc Server Administration* unter <https://www.vmware.com/support/pubs/vfabric-tcserver.html>.

Sie können die Windows-Dienste für vCenter Server über die Systemsteuerung „Verwaltung“ unter „Dienste“ verwalten. Der Windows-Dienst für vCenter Server ist als „VMware VirtualCenter Management Webservices“ aufgeführt.

Festlegen der maximalen Anzahl von Datenbankverbindungen nach einem vCenter Server-Upgrade

Standardmäßig erstellt ein vCenter Server gleichzeitig maximal 50 Datenbankverbindungen. Wenn Sie für diese Option in der Vorgängerversion von vCenter Server einen Wert unter 50 konfigurieren und anschließend das Upgrade auf vCenter Server 5.x durchführen, stellt das Upgrade die Standardeinstellung 50 wieder her. Wenn Sie für diese Option in der Vorgängerversion von vCenter Server einen Wert über 50 konfigurieren, behält das System nach dem Upgrade auf vCenter Server 5.x den vorherigen Wert bei. Sie können die vom Standard abweichende Einstellung neu konfigurieren.

Eine Erhöhung der Anzahl der Datenbankverbindungen bietet sich dann an, wenn vCenter Server häufig zahlreiche Vorgänge ausführt und die Leistung entscheidend ist. Eine Verringerung der Anzahl ist dann angebracht, wenn es sich um eine freigegebene Datenbank handelt und die Verbindungen zur Datenbank kostenintensiv sind. Ändern Sie diesen Wert nur dann, wenn bei Ihrem System eines der folgenden Probleme vorliegt.

Führen Sie diese Aufgabe aus, bevor Sie die Authentifizierung für Ihre Datenbank konfigurieren. Weitere Informationen zur Konfiguration der Authentifizierung finden Sie in der Dokumentation zu Ihrer Datenbank.

Verfahren

- 1 Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.
- 2 Wählen Sie vCenter Server in der Bestandsliste aus.
- 3 Klicken Sie auf die Registerkarte **Verwalten**.
- 4 Wählen Sie **Einstellungen**.
- 5 Wählen Sie **Allgemein** aus.
- 6 Klicken Sie auf **Bearbeiten**.

- 7 Wählen Sie **Datenbank**.
- 8 Ändern Sie den Wert für **Maximale Verbindungen** entsprechend.
- 9 Klicken Sie auf **OK**.
- 10 Starten Sie den vCenter Server neu.

Ergebnisse

Die neue Datenbankeinstellung tritt in Kraft.

Einrichten des vCenter Server-Administratorbenutzers

Die Art und Weise, wie der vCenter Server-Administratorbenutzer eingerichtet wird, hängt von der vCenter Single Sign On-Bereitstellung ab.

In vSphere-Versionen vor vSphere 5.1 sind vCenter Server-Administratoren diejenigen Benutzer, die zur lokalen Administratorgruppe des Betriebssystems gehören.

Wenn Sie in vSphere 5.1.x, 5.5 und 6.0 vCenter Server installieren, müssen Sie den standardmäßigen (anfänglichen) vCenter Server-Administratorbenutzer bzw. die standardmäßige Administratorgruppe angeben. Für Bereitstellungen, bei denen sich vCenter Server und vCenter Single Sign On auf der gleichen virtuellen Maschine bzw. dem gleichen physischen Server befinden, können Sie die lokale Betriebssystemgruppe „Administratoren“ als administrative vCenter Server-Benutzer festlegen. Diese Option ist der Standard. Dieses Verhalten hat sich seit vCenter Server 5.0 nicht geändert.

Für größere Installationen, bei denen vCenter Single Sign On im Rahmen des Platform Services Controller und vCenter Server auf unterschiedlichen virtuellen Maschinen oder physischen Servern bereitgestellt werden, können Sie nicht so vorgehen wie in vCenter Server 5.0. Stattdessen müssen Sie die vCenter Server-Administratorrolle einem Benutzer oder einer Gruppe von einer Identitätsquelle zuweisen, die beim vCenter Single Sign On-Server registriert ist: Active Directory, OpenLDAP oder die Systemidentitätsquelle.

Authentifizieren für die vCenter Server-Umgebung

In vCenter Server 5.1 und höher authentifizieren sich Benutzer über vCenter Single Sign On.

Wenn in vCenter Server-Versionen vor vCenter Server 5.1 ein Benutzer eine Verbindung zu vCenter Server herstellt, authentifiziert vCenter Server den Benutzer, indem dieser anhand einer Active Directory-Domäne bzw. der Liste der lokalen Benutzer des Betriebssystems validiert wird.

Der Benutzer „administrator@*ihr_domänenname*“ hat standardmäßig vCenter Single Sign-On-Administratorberechtigungen. Bei Anmeldung beim vCenter Single Sign-On-Server über vSphere Web Client kann der Benutzer „administrator@*ihr_domänenname*“ anderen Benutzern vCenter Single Sign-On-Administratorrechte zuweisen. Diese Benutzer können sich von den Benutzern unterscheiden, die vCenter Server verwalten.

Die Benutzer können sich bei vCenter Server mit dem vSphere Web Client anmelden. Die Benutzer authentifizieren sich bei vCenter Single Sign-On. Benutzer können alle vCenter Server-Instanzen anzeigen, für die der Benutzer über Berechtigungen verfügt. Nachdem die Benutzer eine Verbindung zu vCenter Server hergestellt haben, ist keine weitere Authentifizierung erforderlich. Welche Aktionen Benutzer für Objekte durchführen können, hängt von den vCenter Server-Berechtigungen des Benutzers für diese Objekte ab.

Weitere Informationen über vCenter Single Sign On finden Sie unter *vSphere-Sicherheit*.

Identitätsquellen für vCenter Server mit vCenter Single Sign On

Sie können Identitätsquellen verwenden, um vCenter Single Sign On eine oder mehrere Domänen hinzuzufügen. Bei einer Domäne handelt es sich um ein Repository für Benutzer und Gruppen, das der vCenter Single Sign On-Server für die Benutzerauthentifizierung verwenden kann.

Eine Identitätsquelle ist eine Sammlung von Benutzer- und Gruppendaten. Die Benutzer- und Gruppendaten werden in Active Directory, OpenLDAP oder lokal im Betriebssystem der Maschine, auf der vCenter Single Sign On installiert ist, gespeichert.

Nach der Installation hat jede Instanz von vCenter Single Sign On die Identitätsquelle *Ihr_Domänenname*, z. B. „vsphere.local“. Diese Identitätsquelle ist für vCenter Single Sign On intern. Ein vCenter Single Sign On-Administrator kann Identitätsquellen hinzufügen, die Standardidentitätsquelle festlegen und Benutzer und Gruppen in der Identitätsquelle „vsphere.local“ erstellen.

Typen von Identitätsquellen

vCenter Server-Versionen vor Version 5.1 haben Active Directory und Benutzer des lokalen Betriebssystems als Benutzer-Repositories unterstützt. Deshalb konnten lokale Betriebssystembenutzer sich immer beim vCenter Server-System authentifizieren. vCenter Server 5.1 und 5.5 verwenden vCenter Single Sign On für die Authentifizierung. Eine Aufstellung der für vSphere 5.1 unterstützten Identitätsquellen finden Sie in der Dokumentation zu vCenter Single Sign On 5.1. vCenter Single Sign On 5.5 unterstützt die folgenden Typen von Benutzer-Repositories als Identitätsquellen, unterstützt aber nur eine einzige standardmäßige Identitätsquelle.

- Active Directory-Versionen 2003 und später. Wird als **Active Directory (integrierte Windows-Authentifizierung)** im vSphere Web Client angezeigt. Mit vCenter Single Sign On können Sie eine einzelne Active Directory-Domäne als Identitätsquelle angeben. Die Domäne kann untergeordnete Domänen haben, oder es kann sich dabei um eine Gesamtstruktur-Stammdomäne handeln. Im VMware-KB-Artikel [2064250](#) werden Microsoft Active Directory-Vertrauensstellungen behandelt, die von vCenter Single Sign On unterstützt werden.

- Active Directory über LDAP. vCenter Single Sign On unterstützt mehrere Active Directory- über LDAP-Identitätsquellen. Dieser Identitätsquellentyp wird zur Gewährleistung der Kompatibilität mit dem in vSphere 5.1 enthaltenen vCenter Single Sign On-Dienst bereitgestellt. Er wird als **Active Directory als ein LDAP-Server** im vSphere Web Client angezeigt.
- OpenLDAP Version 2.4 und höher. vCenter Single Sign On unterstützt mehrere OpenLDAP- Identitätsquellen. Wird als **OpenLDAP** auf dem vSphere Web Client angezeigt.
- Benutzer des lokalen Betriebssystems. Benutzer des lokalen Betriebssystems sind lokale Benutzer in dem Betriebssystem, unter dem der vCenter Single Sign On-Server läuft. Die Identitätsquelle des lokalen Betriebssystems existiert nur in einfachen vCenter Single Sign On- Serverbereitstellungen. In Bereitstellungen mit mehreren vCenter Single Sign On-Instanzen steht sie nicht zur Verfügung. Nur eine Identitätsquelle des lokalen Betriebssystems ist gestattet. Wird als **localos** auf dem vSphere Web Client angezeigt.

Hinweis Verwenden Sie keine lokalen Betriebssystembenutzer, wenn sich der Platform Services Controller auf einer anderen Maschine als das vCenter Server-System befindet. Die Verwendung lokaler Betriebssystembenutzer kann bei einer eingebetteten Bereitstellung sinnvoll sein, wird jedoch nicht empfohlen.

- vCenter Single Sign On-Systembenutzer. Genau eine Systemidentitätsquelle, nämlich „vsphere.local“, wird bei der Installation von vCenter Single Sign On erstellt. Wird als **vsphere.local** auf dem vSphere Web Client angezeigt.

Hinweis Es ist jeweils immer nur eine Standarddomäne vorhanden. Wenn sich ein Benutzer aus einer Nicht-Standarddomäne anmeldet, muss dieser Benutzer den Domänennamen (*DOMAI\user*) hinzufügen, um erfolgreich authentifiziert zu werden.

Die vCenter Single Sign On-Identitätsquellen werden von vCenter Single Sign On- Administratorbenutzern verwaltet.

Sie können einer vCenter Single Sign On-Serverinstanz Identitätsquellen hinzufügen. Remoteidentitätsquellen sind auf Active Directory- und OpenLDAP-Server-Implementierungen beschränkt.

Weitere Informationen über vCenter Single Sign On finden Sie unter *vSphere-Sicherheit*.

Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien

Wenn Sie ein Zertifikat auf einem ESXi-Host mithilfe der vSphere Web Services SDK ersetzen, werden das vorherige Zertifikat und der Schlüssel einer *BAK*-Datei hinzugefügt. Sie können vorherige Zertifikate durch Verschieben der Daten in der *BAK*-Datei in das aktuelle Zertifikat und die Schlüsseldateien wiederherstellen.

Das Hostzertifikat und der Schlüssel befinden sich am Speicherort `/etc/vmware/ssl/rui.crt` bzw. `/etc/vmware/ssl/rui.key`. Wenn Sie ein Hostzertifikat und einen Schlüssel mithilfe des verwalteten Objekts `vim.CertificateManager` der vSphere Web Services SDK ersetzen, werden der vorherige Schlüssel und das Zertifikat der Datei `/etc/vmware/ssl/rui.bak` hinzugefügt.

Hinweis Wenn Sie das Zertifikat mithilfe von HTTP PUT, `vifs` oder über die ESXi Shell ersetzen, werden die vorhandenen Zertifikate nicht der BAK-Datei hinzugefügt.

Verfahren

- 1 Suchen Sie auf dem ESXi-Host die Datei `/etc/vmware/ssl/rui.bak`.

Die Datei weist das folgende Format auf.

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 Kopieren Sie den Text von `-----BEGIN PRIVATE KEY-----` bis `-----END PRIVATE KEY-----` in die Datei `/etc/vmware/ssl/rui.key`.

`-----BEGIN PRIVATE KEY-----` und `-----END PRIVATE KEY-----` müssen im Text enthalten sein.

- 3 Kopieren Sie den Text von `-----BEGIN CERTIFICATE-----` bis `-----END CERTIFICATE-----` in die Datei `/etc/vmware/ssl/rui.crt`.

`-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----` müssen im Text enthalten sein.

- 4 Starten Sie den Host neu oder senden Sie `ssl_reset`-Ereignisse zu allen Diensten, die die Schlüssel verwenden.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

Neuverweisen von vCenter Server auf einen anderen externen Platform Services Controller

Durch Verbinden externer Platform Services Controller-Instanzen in derselben vCenter Single Sign-On-Domäne wird die Hochverfügbarkeit Ihres Systems sichergestellt.

Wenn ein externer Platform Services Controller nicht mehr reagiert oder wenn Sie die Last eines externen Platform Services Controller verteilen möchten, können Sie die vCenter Server-Instanzen an einen anderen Platform Services Controller in derselben Domäne oder Site verweisen.

- Sie können die vCenter Server-Instanz auf eine vorhandene funktionsfähige Platform Services Controller-Instanz mit freier Auslastungskapazität in derselben Domäne oder Site verweisen.
- Sie können eine neue Platform Services Controller-Instanz in derselben Domäne und Site installieren bzw. bereitstellen, auf die die vCenter Server-Instanz verwiesen werden soll.

Voraussetzungen

- Wenn die alte Platform Services Controller-Instanz nicht mehr reagiert, entfernen Sie den Knoten und bereinigen Sie die veralteten vmdir-Daten durch Ausführen des Befehls `cmsso-util unregister`. Informationen zum Stilllegen einer Platform Services Controller-Instanz finden Sie unter <https://kb.vmware.com/kb/2106736>.
- Stellen Sie sicher, dass sich die alten und die neuen Platform Services Controller-Instanzen in derselben vCenter Single Sign-On-Domäne oder -Site befinden, indem Sie den Befehl `vdcrepadmin -f showservers` ausführen. Informationen zur Verwendung des Befehls finden Sie unter <https://kb.vmware.com/kb/2127057>.

Verfahren

- 1 Melden Sie sich bei der vCenter Server-Instanz an.
 - Melden Sie sich bei Verwendung einer vCenter Server Appliance bei der vCenter Server Appliance-Shell als der Root-Benutzer an.
 - Melden Sie sich bei Verwendung einer vCenter Server-Instanz unter Windows als ein Administrator bei der virtuellen Maschine oder dem physischen Server von vCenter Server an.
- 2 Wenn die vCenter Server-Instanz unter Windows ausgeführt wird, navigieren Sie in der Windows-Eingabeaufforderung zu `C:\Programme\VMware\vCenter Server\bin`.
- 3 Führen Sie den Befehl `cmsso-util repoint` aus.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

wobei die rechteckigen Klammern die Befehlsoptionen einschließen.

Dabei ist `psc_fqdn_or_static_ip` der Systemname, mit dem der Platform Services Controller identifiziert wird. Dieser Systemname muss ein FQDN oder eine statische IP-Adresse sein.

Hinweis Der FQDN-Wert unterliegt der Groß-/Kleinschreibung.

Verwenden Sie die Option `--dc-port port_number`, falls der Platform Services Controller auf einem benutzerdefinierten HTTPS-Port ausgeführt wird. Der Standardwert für den HTTPS-Port ist 443.

- 4 Melden Sie sich mit dem vSphere Web Client bei der vCenter Server-Instanz an und prüfen Sie, ob der vCenter Server ausgeführt wird und verwaltet werden kann.

Ergebnisse

Die vCenter Server-Instanz wird mit dem neuen Platform Services Controller registriert.

Neukonfigurieren einer eigenständigen vCenter Server-Instanz mit einem eingebetteten Platform Services Controller auf eine vCenter Server-Instanz mit einem externen Platform Services Controller

Wenn Sie eine eigenständige vCenter Server-Instanz mit einem eingebetteten Platform Services Controller bereitgestellt und installiert haben und Sie die vCenter Single Sign-On-Domäne mit weiteren vCenter Server-Instanzen erweitern möchten, können Sie die vorhandenen vCenter Server-Instanzen neu konfigurieren und sie an einen externen Platform Services Controller neu verweisen.

Abbildung 6-1. Neukonfigurieren einer eigenständigen vCenter Server-Instanz mit einem eingebetteten Platform Services Controller und Neuverweisen der Instanz auf einen externen Platform Services Controller

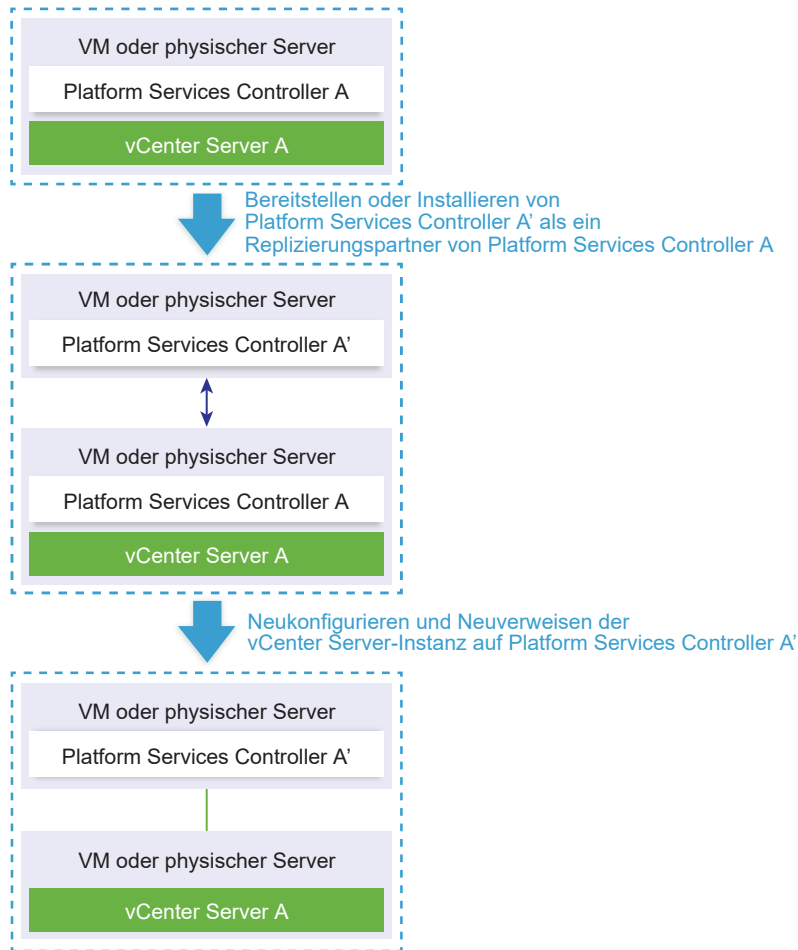



Tabelle 6-3. Legende

Pfeil oder Zeile	Beschreibung
	Replizierungsvereinbarung zwischen zwei Platform Services Controller-Instanzen
	vCenter Server-Registrierung bei einem externen Platform Services Controller
	Übergangsschritt

Hinweis Die Neukonfiguration einer vCenter Server-Instanz mit einem eingebetteten Platform Services Controller und das Neuzeuweisen der Instanz zu einer externen Platform Services Controller-Instanz ist ein unumkehrbarer Vorgang, nach dessen Ausführung Sie nicht zur vCenter Server-Instanz mit einem eingebetteten Platform Services Controller zurückwechseln können.

Voraussetzungen

- Stellen Sie die externe Platform Services Controller-Instanz als einen Replizierungspartner der vorhandenen eingebetteten Platform Services Controller-Instanz in derselben vCenter Single Sign-On-Site bereit oder installieren Sie sie.

Hinweis Sie können die aktuelle vCenter Single Sign-On-Site unter Verwendung des `vmfad-cli`-Befehls ermitteln.

- Bei Verwendung einer vCenter Server Appliance mit einem eingebetteten Platform Services Controller melden Sie sich bei der Appliance-Shell als Root-Benutzer an und führen Sie den Befehl aus.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- Bei Verwendung einer Windows-Installation einer vCenter Server-Instanz mit einem eingebetteten Platform Services Controller melden Sie sich bei der Windows-Maschine als ein Administrator an, öffnen Sie die Windows-Eingabeaufforderung und führen Sie den Befehl aus.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- Erstellen Sie Snapshots der vCenter Server-Instanzen mit einem eingebetteten Platform Services Controller und den externen Platform Services Controller-Instanzen, damit Sie die Snapshots wiederherstellen können, falls die Neukonfiguration fehlschlägt.

Verfahren

- 1 Melden Sie sich bei der vCenter Server-Instanz mit einem eingebetteten Platform Services Controller an.

Option	Schritte
Für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller	<p>Melden Sie sich bei der Appliance-Shell als Root-Benutzer an.</p> <ul style="list-style-type: none"> ■ Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie Alt+F1. ■ Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten.
Für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller	Melden Sie sich als Administrator an der Windows-Maschine an.

- 2 Stellen Sie sicher, dass alle Platform Services Controller-Dienste ausgeführt werden.

Option	Schritte
Für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller	Führen Sie den Befehl <code>service-control --status --all</code> aus.
Für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller	Wählen Sie Start > Systemsteuerung > Verwaltung > Dienste aus.

Die folgenden Platform Services Controller-Dienste müssen ausgeführt werden: VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service und VMware Directory Service.

- 3 Wenn vCenter Server mit einer eingebetteten Platform Services Controller-Instanz unter Windows ausgeführt wird, öffnen Sie die Windows-Eingabeaufforderung und navigieren Sie zu `C:\Programme\VMware\vCenter Server\bin`.
- 4 Führen Sie den Befehl `cmsso-util reconfigure` aus.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username Benutzername
--domain-name domain_name --passwd Kennwort [--dc-port port_number]
```

wobei die eckigen Klammern [] optionale Elemente einschließen.

Dabei ist *psc_fqdn_or_static_ip* der Systemname, mit dem die externe Platform Services Controller-Instanz identifiziert wird. Dieser Systemname muss ein FQDN oder eine statische IP-Adresse sein.

Hinweis Der FQDN-Wert unterliegt der Groß-/Kleinschreibung.

Die Optionen *username* und *password* sind der Benutzername und das Kennwort des Administrators für vCenter Single Sign-On *domain_name*.

Verwenden Sie die Option `--dc-port`, falls der externe Platform Services Controller auf einem benutzerdefinierten HTTPS-Port ausgeführt wird. Der Standardwert für den HTTPS-Port ist 443.

Wenn beispielsweise der externe Platform Services Controller auf dem benutzerdefinierten HTTPS-Port 449 ausgeführt wird, müssen Sie folgenden Befehl ausführen:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username Administrator --
domain-name vsphere.local --passwd Kennwort1! --dc-port 449
```

- 5 Melden Sie sich mit dem vSphere Web Client bei der vCenter Server-Instanz an und prüfen Sie, ob der vCenter Server ausgeführt wird und verwaltet werden kann.

Ergebnisse

Der vCenter Server mit eingebettetem Platform Services Controller wird herabgestuft, und der vCenter Server wird an den externen Platform Services Controller umgeleitet.

Nächste Schritte

Sie können zusätzliche vCenter Server- und Platform Services Controller-Instanzen in der vCenter Single Sign-On-Domäne bereitstellen oder installieren.

Neukonfigurieren mehrerer beigetretener Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller auf vCenter Server mit einem externen Platform Services Controller

Wenn Sie mindestens zwei beigetretene Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller bereitgestellt oder installiert haben, können Sie sie als mehrere vCenter Server-Instanzen neu konfigurieren, die beigetretene externe Platform Services Controller-Instanzen verwenden.

Abbildung 6-2. Beispiel für das Neukonfigurieren von drei beigetretenen Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller zwischen zwei vCenter Single Sign-On-Sites

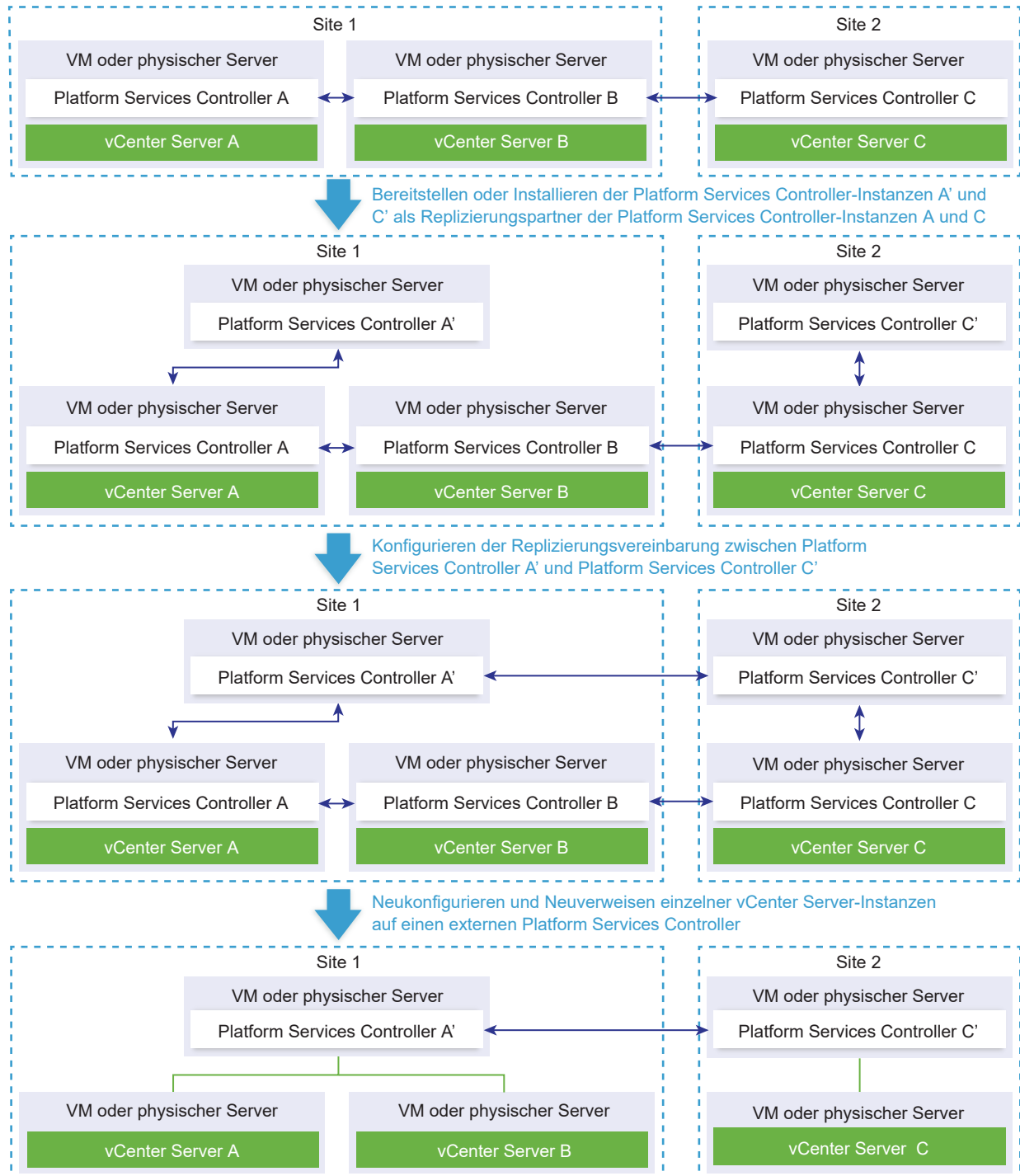





Tabelle 6-4. Legende

Pfeil oder Zeile	Beschreibung
	Replizierungsvereinbarung zwischen zwei Platform Services Controller-Instanzen
	vCenter Server-Registrierung bei einem externen Platform Services Controller
	Übergangsschritt

Hinweis Die Neukonfiguration einer vCenter Server-Instanz mit einem eingebetteten Platform Services Controller und das Neuzeuweisen der Instanz zu einer externen Platform Services Controller-Instanz ist ein unumkehrbarer Vorgang, nach dessen Ausführung Sie nicht zur vCenter Server-Instanz mit einem eingebetteten Platform Services Controller zurückwechseln können.

Voraussetzungen

- Stellen Sie für jede vCenter Single Sign-On-Site eine externe Platform Services Controller-Instanz als einen Replizierungspartner einer vorhandenen eingebetteten Platform Services Controller-Instanz aus dieser Site bereit oder installieren Sie sie.

Hinweis Sie können die aktuellen vCenter Single Sign-On-Sites unter Verwendung des `vmfad-cli`-Befehls ermitteln.

- Bei Verwendung einer vCenter Server Appliance mit einem eingebetteten Platform Services Controller melden Sie sich bei der Appliance-Shell als Root-Benutzer an und führen Sie den Befehl aus.

```
/usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
```

- Bei Verwendung einer Windows-Installation einer vCenter Server-Instanz mit einem eingebetteten Platform Services Controller melden Sie sich bei der Windows-Maschine als ein Administrator an, öffnen Sie die Windows-Eingabeaufforderung und führen Sie den Befehl aus.

```
C:\Program Files\VMware\vCenter Server\vmafdd\vmafd-cli get-site-name --server-name localhost
```

- Erstellen Sie Snapshots der vCenter Server-Instanzen mit einem eingebetteten Platform Services Controller und den externen Platform Services Controller-Instanzen, damit Sie die Snapshots wiederherstellen können, falls die Neukonfiguration fehlschlägt.

Sicherstellen, dass alle Dienste der eingebetteten Platform Services Controller-Instanzen ausgeführt werden

Um ein erfolgreiches Neuverweisen einer vCenter Server-Instanz aus einem eingebetteten auf einen externen Platform Services Controller sicherzustellen, müssen alle Dienste einer vorhandenen eingebetteten Platform Services Controller-Instanz ausgeführt werden.

Verfahren

- 1 Melden Sie sich bei der vCenter Server-Instanz mit einem eingebetteten Platform Services Controller an.

Option	Schritte
Für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller	<p>Melden Sie sich bei der Appliance-Shell als Root-Benutzer an.</p> <ul style="list-style-type: none"> ■ Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie Alt+F1. ■ Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten.
Für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller	Melden Sie sich als Administrator an der Windows-Maschine an.

- 2 Stellen Sie sicher, dass alle Platform Services Controller-Dienste ausgeführt werden.

Option	Schritte
Für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller	Führen Sie den Befehl <code>service-control --status --all</code> aus.
Für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller	Wählen Sie Start > Systemsteuerung > Verwaltung > Dienste aus.

Die folgenden Platform Services Controller-Dienste müssen ausgeführt werden: VMware License Service, VMware Identity Management Service, VMware Security Token Service, VMware Certificate Service und VMware Directory Service.

- 3 Wiederholen Sie diesen Vorgang für jede vCenter Server-Instanz mit einem eingebetteten Platform Services Controller.

Konfigurieren der Replizierungsvereinbarung zwischen allen externen Platform Services Controller-Instanzen

Nach dem Bereitstellen oder Installieren einer externen replizierenden Platform Services Controller-Instanz in jeder vCenter Single Sign-On-Site müssen Sie alle externen Platform Services Controller-Instanzen der Replizierungsvereinbarung hinzufügen.

Abbildung 6-3. Beispiel für die Konfiguration der Replizierungsvereinbarung zwischen zwei externen Platform Services Controller-Instanzen in verschiedenen vCenter Single Sign-On-Sites

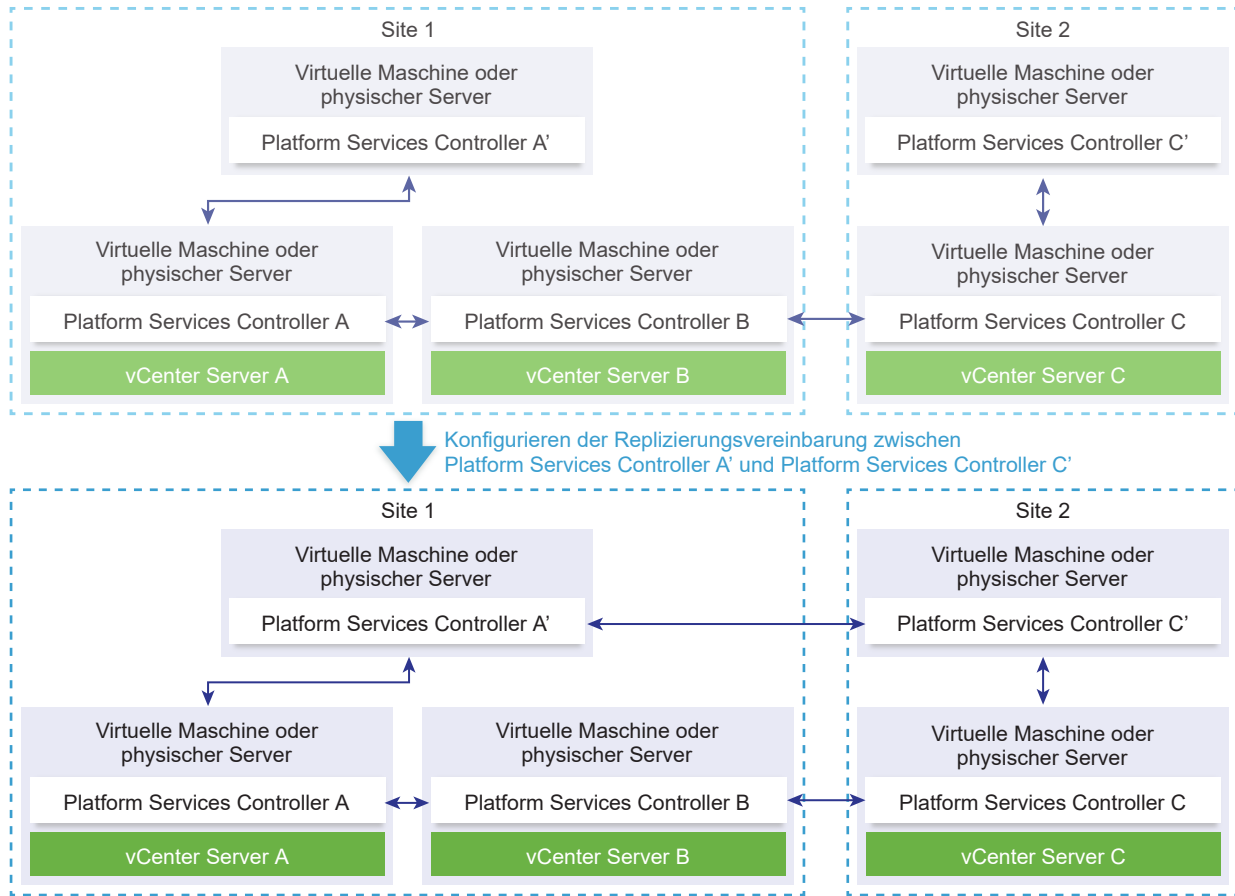


Tabelle 6-5. Legende

Pfeil oder Zeile	Beschreibung
	Replizierungsvereinbarung zwischen zwei Platform Services Controller-Instanzen
	vCenter Server-Registrierung bei einem externen Platform Services Controller
	Übergangsschritt

Für die Konfiguration der Replizierungsvereinbarung zwischen zwei Platform Services Controller-Instanzen können Sie eine Verbindung zu einer der vCenter Server- oder Platform Services Controller-Instanzen aus der vCenter Single Sign-On-Domäne verwenden.

Verfahren

- 1 Stellen Sie eine Verbindung zu einer vCenter Server- oder Platform Services Controller-Instanz aus der vCenter Single Sign-On-Domäne her.

Option	Schritte
Wenn Sie eine Verbindung mit einer vCenter Server Appliance oder Platform Services Controller-Appliance herstellen möchten	<p>Melden Sie sich bei der Appliance-Bash-Shell als Root-Benutzer an.</p> <ol style="list-style-type: none"> 1 Anmelden bei der Appliance-Shell <ul style="list-style-type: none"> ■ Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie Alt+F1. ■ Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten. 2 Die Bash-Shell aktivieren <pre>shell.set --enabled true</pre> 3 Führen Sie den Befehl <code>shell</code> aus.
Wenn Sie eine Verbindung mit einer Windows-Installation von vCenter Server oder Platform Services Controller herstellen möchten	<p>Melden Sie sich bei der Windows-Maschine als ein Administrator an und öffnen Sie die Windows-Eingabeaufforderung.</p>

- 2 Führen Sie den `vdcrepadmin`-Befehl mit dem `showpartners`-Parameter für eine externe Platform Services Controller-Instanz aus.

Sie ermitteln die vorhandenen Partnerschaften der Platform Services Controller-Instanz mit anderen Platform Services Controller-Instanzen in der vCenter Single Sign-On-Domäne.

- Wenn Sie eine Verbindung mit einer vCenter Server Appliance oder Platform Services Controller-Appliance verwenden, führen Sie den folgenden Befehl aus.

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f showpartners -h psc_fqdn_or_static_ip -u administrator
```

- Wenn Sie eine Verbindung zu einer Windows-Installation einer vCenter Server- oder Platform Services Controller-Instanz verwenden, führen Sie den folgenden Befehl aus.

```
C:\Program Files\VMware\vCenter Server\vmware-vmware\bin\vdcrepadmin -f showpartners -h psc_fqdn_or_static_ip -u administrator
```

Geben Sie bei einer entsprechenden Aufforderung das Administratorkennwort für vCenter Single Sign-On ein.

- 3 Wiederholen Sie Schritt 2 für jede externe Platform Services Controller-Instanz.

Sie haben die vorhandenen Partnerschaften zwischen allen Platform Services Controller-Instanzen in der vCenter Single Sign-On-Domäne ermittelt.

- 4 Wenn es eine externe Platform Services Controller-Instanz gibt, die sich nicht mit einer anderen externen Platform Services Controller-Instanz in der Replizierungsvereinbarung befindet, führen Sie den `vdcrepadmin`-Befehl mit dem `createagreement`-Parameter für diese Platform Services Controller-Instanz aus, um sie zu einer anderen externen Platform Services Controller-Instanz hinzuzufügen.

- Wenn Sie eine Verbindung mit einer vCenter Server Appliance oder Platform Services Controller-Appliance verwenden, führen Sie den folgenden Befehl aus.

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f createagreement -2 -h
psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u administrator
```

- Wenn Sie eine Verbindung zu einer Windows-Installation einer vCenter Server- oder Platform Services Controller-Instanz verwenden, führen Sie den folgenden Befehl aus.

```
C:\Program Files\VMware\vCenter Server\vmware-vmware\bin\vdcrepadmin -f
createagreement -2 -h psc_fqdn_or_static_ip -H partner_psc_fqdn_or_static_ip -u
administrator
```

Geben Sie bei einer entsprechenden Aufforderung das Administratorkennwort für vCenter Single Sign-On ein.

Sie haben eine Partnerschaft zwischen den zwei Platform Services Controller-Instanzen erstellt.

- 5 Wiederholen Sie Schritt 4 für jede externe Platform Services Controller-Instanz, die sich nicht mit einer anderen externen Platform Services Controller-Instanz in einer Replizierungsvereinbarung befindet.
- 6 Wiederholen Sie Schritt 2 und Schritt 3, um zu überprüfen, ob Sie eine Partnerschafts-Ringtopologie der externen Platform Services Controller-Instanzen erstellt haben.

Neukonfigurieren aller vCenter Server-Instanzen und Neuverweisen von einer eingebetteten auf eine externe Platform Services Controller-Instanz

Mit der Neukonfiguration stufen Sie jeden eingebetteten Platform Services Controller herab und verweisen die vCenter Server-Instanz neu, sodass eine externe Platform Services Controller-Instanz verwendet wird.

Abbildung 6-4. Beispiel für das Neukonfigurieren von drei beigetretenen Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller und das Neuverweisen dieser auf die externen Platform Services Controller-Instanzen

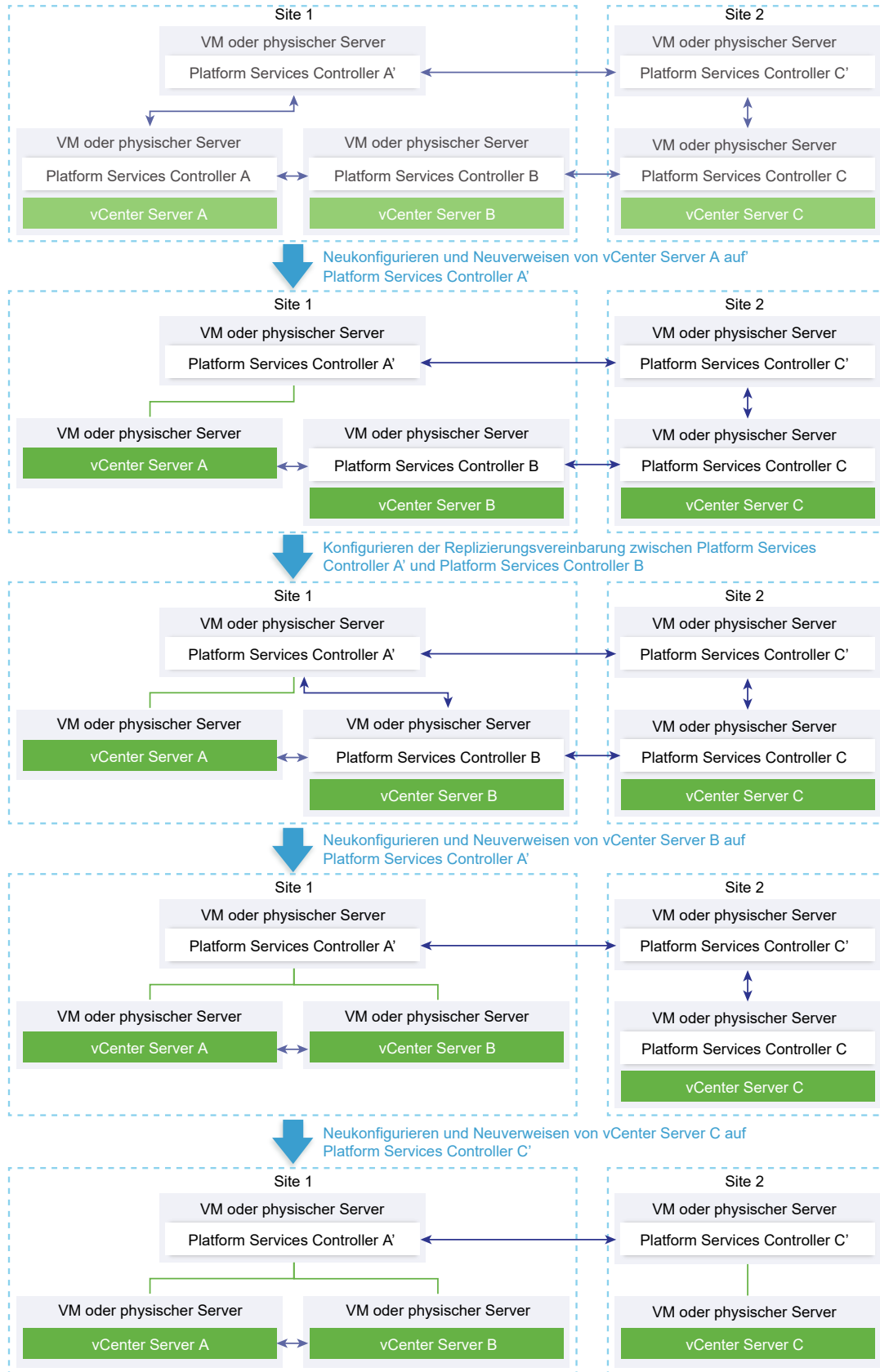





Tabelle 6-6. Legende

Pfeil oder Zeile	Beschreibung
	Replizierungsvereinbarung zwischen zwei Platform Services Controller-Instanzen
	vCenter Server-Registrierung bei einem externen Platform Services Controller
	Übergangsschritt

Verfahren

- 1 Melden Sie sich bei der vCenter Server-Instanz mit einem eingebetteten Platform Services Controller an.

Option	Schritte
Für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller	<p>Melden Sie sich bei der Appliance-Shell als Root-Benutzer an.</p> <ul style="list-style-type: none"> ■ Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie Alt+F1. ■ Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten.
Für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller	Melden Sie sich als Administrator an der Windows-Maschine an.

- 2 Wenn der vCenter Server mit einer eingebetteten Platform Services Controller-Instanz und der externen Platform Services Controller-Instanz keine direkten Replizierungspartner sind, erstellen Sie eine solche Replizierungsvereinbarung.

- Führen Sie für eine vCenter Server Appliance mit einem eingebetteten Platform Services Controller über die Appliance-Bash-Shell den folgenden Befehl aus.

```
/usr/lib/vmware-vmware/bin/vdcrepadmin -f createagreement -h localhost -H
psc_fqdn_or_static_ip -u administrator
```

- Führen Sie für eine Windows-Installation von vCenter Server mit einem eingebetteten Platform Services Controller über die Windows-Eingabeaufforderung den folgenden Befehl aus.

```
C:\Program Files\VMware\vCenter Server\vmware-vmware\bin\vdcrepadmin -f
createagreement -h localhost -H psc_fqdn_or_static_ip -u administrator
```

Geben Sie bei einer entsprechenden Aufforderung das Administratorkennwort für vCenter Single Sign-On ein.

- 3 Wenn vCenter Server mit einer eingebetteten Platform Services Controller-Instanz unter Windows ausgeführt wird, navigieren Sie in der Windows-Eingabeaufforderung zu C:\Programme\VMware\vCenter Server\bin.

4 Führen Sie den Befehl `cmsso-util reconfigure` aus.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username Benutzername
--domain-name domain_name --passwd Kennwort [--dc-port port_number]
```

wobei die eckigen Klammern [] optionale Elemente einschließen.

Dabei ist *psc_fqdn_or_static_ip* der Systemname, mit dem die externe Platform Services Controller-Instanz identifiziert wird. Dieser Systemname muss ein FQDN oder eine statische IP-Adresse sein.

Hinweis Der FQDN-Wert unterliegt der Groß-/Kleinschreibung.

Die Optionen *username* und *password* sind der Benutzername und das Kennwort des Administrators für vCenter Single Sign-On *domain_name*.

Verwenden Sie die Option `--dc-port`, falls der externe Platform Services Controller auf einem benutzerdefinierten HTTPS-Port ausgeführt wird. Der Standardwert für den HTTPS-Port ist 443.

Wenn beispielsweise der externe Platform Services Controller auf dem benutzerdefinierten HTTPS-Port 449 ausgeführt wird, müssen Sie folgenden Befehl ausführen:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username Administrator --
domain-name vsphere.local --passwd Kennwort1! --dc-port 449
```

Wichtig Wenn Sie die vCenter Server-Instanz zur Verwendung einer externen Platform Services Controller-Instanz, die sich in einer anderen vCenter Single Sign-On-Site befindet, neu verwiesen haben, müssen Sie die vCenter Server-Instanz in diese vCenter Single Sign-On-Site verschieben. Informationen zum Verschieben von vCenter Server zwischen verschiedenen vCenter Single Sign-On-Sites finden Sie im VMware-Knowledgebase-Artikel [Repointing the VMware vCenter Server 6.0 between sites in a vSphere Domain](#).

- 5 Melden Sie sich mit dem vSphere Web Client bei der vCenter Server-Instanz an und prüfen Sie, ob der vCenter Server ausgeführt wird und verwaltet werden kann.
- 6 Wiederholen Sie diesen Vorgang für jede vCenter Server-Instanz mit einem eingebetteten Platform Services Controller.

Ergebnisse

Die vCenter Server-Instanzen mit einem eingebetteten Platform Services Controller werden herabgestuft, und die vCenter Server-Instanzen werden zu den externen Platform Services Controller-Instanzen umgeleitet.

Upgrade von Update Manager

7

Das Upgrade auf Update Manager 6.0 ist nur von Update Manager 5.x möglich, sofern diese Version unter einem 64-Bit-Betriebssystem installiert ist.

Wenn Sie eine frühere Version von Update Manager als Version 5.x oder aber Update Manager auf einer 32-Bit-Plattform ausführen, können Sie kein direktes Upgrade auf Update Manager 6.0 durchführen. Sie müssen das Datenmigrationstool verwenden, das mit dem Update Manager 5.0-Installationsmedium mitgeliefert wird, um Ihr Update Manager-System auf Update Manager 5.0 unter einem 64-Bit-Betriebssystem zu migrieren, und dann ein direktes Upgrade von Version 5.0 auf Version 6.0 durchführen. Detaillierte Informationen zur Verwendung des Datenmigrationstools finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager* für Update Manager 5.0.

Wenn Sie Update Manager aktualisieren, können Sie den Installationspfad und den Speicherort für Patch-Downloads nicht ändern. Um diese Parameter zu ändern, müssen Sie eine neue Version von Update Manager installieren, anstatt ihn zu aktualisieren.

Vorherige Versionen von Update Manager verwenden einen 512-Bit-Schlüssel und ein selbstsigniertes Zertifikat, wobei keines von beiden während des Upgrades ersetzt wird. Wenn Sie einen sichereren 2048-Bit-Schlüssel benötigen, können Sie entweder eine Neuinstallation von Update Manager 6.0 durchführen oder das Update Manager-Dienstprogramm zum Ersetzen des vorhandenen Zertifikats verwenden.

Geplante Aufgaben zum Prüfen auf Patches und für Standardisierungen von virtuellen Maschinen werden während des Upgrades nicht entfernt. Nach dem Upgrade können Sie geplante Prüfaufgaben, die aus vorherigen Versionen vorhanden sind, bearbeiten und entfernen. Sie können vorhandene geplante Standardisierungsaufgaben entfernen, jedoch nicht bearbeiten.

VM-Patch-Baselines werden während des Upgrades entfernt. Vorhandene geplante Aufgaben, die diese enthalten, werden normal ausgeführt und ignorieren nur die Prüf- und Standardisierungsvorgänge, die VM-Patch-Baselines verwenden.

Sie müssen die Update Manager-Datenbank während des Update Manager-Upgrades aktualisieren. Sie können auswählen, ob Sie die vorhandenen Daten in der Datenbank beibehalten oder während des Upgrades ersetzen möchten.

Wenn Sie Update Manager installieren bzw. ein Upgrade für Update Manager durchführen, werden die erforderlichen Java-Komponenten (JRE) automatisch installiert bzw. es wird ein automatisches Upgrade auf dem System durchgeführt. Ab Update Manager 5.5 Update 1 können Sie die Java-Komponenten getrennt von einem Update Manager-Upgrade-Vorgang auf eine Version aktualisieren, die nicht gemeinsam mit Update Manager-Versionen veröffentlicht wird.

Dieses Kapitel enthält die folgenden Themen:

- [Upgrade von Update Manager-Server](#)

Upgrade von Update Manager-Server

Zum Upgrade einer Instanz von Update Manager, die auf einer 64-Bit-Maschine installiert ist, müssen Sie zuerst ein Upgrade von vCenter Server auf eine kompatible Version durchführen.

Die Version Update Manager 6.0 ermöglicht Upgrades nur von Update Manager 5.x.

Voraussetzungen

- Stellen Sie sicher, dass der Datenbankbenutzer über die erforderlichen Berechtigungen verfügt. Siehe Kapitel *Vorbereiten der Update Manager-Datenbank* in *Installieren und Verwalten von VMware vSphere Update Manager*.
- Halten Sie den Update Manager-Dienst an und sichern Sie die Update Manager-Datenbank. Das Installationsprogramm aktualisiert das Datenbankschema, wodurch die Datenbank unwiderruflich inkompatibel zu vorherigen Update Manager-Versionen wird.

Verfahren

- 1 Aktualisieren Sie vCenter Server auf eine kompatible Version.

Hinweis Der vCenter Server-Installationsassistent gibt eine Warnmeldung aus, dass Update Manager nicht kompatibel ist, wenn vCenter Server aktualisiert wird.

Wenn Sie dazu aufgefordert werden, müssen Sie die Maschine, auf der vCenter Server ausgeführt wird, neu starten. Anderenfalls ist es möglich, dass Sie kein Upgrade von Update Manager durchführen können.

- 2 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe` und wählen Sie **vSphere Update Manager > Server**.

Wenn Sie die Datei `autorun.exe` nicht ausführen können, navigieren Sie zum Ordner `UpdateManager` und führen Sie `VMware-UpdateManager.exe` aus.

- 3 Wählen Sie eine Sprache für das Installationsprogramm aus und klicken Sie auf **OK**.
- 4 Klicken Sie in der Aktualisierungswarnmeldung auf **OK**.
- 5 Überprüfen Sie die Begrüßungsseite und klicken Sie auf **Weiter**.
- 6 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

- 7 Überprüfen Sie die Support-Informationen, wählen Sie, ob Sie alte Upgrade-Dateien löschen möchten, ob Sie Updates sofort nach der Installation von den Standard-Download-Quellen herunterladen möchten, und klicken Sie auf **Weiter**.

Wenn Sie die Option **Alte Host-Upgrade-Dateien aus dem Repository löschen** deaktivieren, werden Dateien aufbewahrt, die Sie nicht mit Update Manager 6.0 verwenden können.

Wenn Sie die Option **Updates von Standardquellen sofort nach der Installation herunterladen** deaktivieren, lädt Update Manager Updates einmal täglich entsprechend dem Standard-Download-Zeitplan oder sofort herunter, wenn Sie auf der Seite „Download-Einstellungen“ auf **Jetzt herunterladen** klicken. Sie können den Standard-Download-Zeitplan ändern, nachdem die Installation abgeschlossen ist.

- 8 Geben Sie die vCenter Server-Systemanmeldedaten ein und klicken Sie auf **Weiter**.

Damit die Update Manager-Registrierung weiterhin mit dem ursprünglichen vCenter Server-System gültig bleibt, behalten Sie die IP-Adresse des vCenter Server-Systems bei und geben Sie die Anmeldedaten der Originalinstallation ein.

- 9 Geben Sie das Datenbankkennwort für die Update Manager-Datenbank ein und klicken Sie auf **Weiter**.

Das Datenbankkennwort ist nur erforderlich, wenn DSN keine Windows NT-Authentifizierung verwendet.

- 10 Wählen Sie auf der Seite für das Datenbank-Upgrade **Ja, ich möchte meine Update Manager-Datenbank aktualisieren** und **Ich habe eine Sicherungskopie der vorhandenen Update Manager-Datenbank erstellt** und klicken Sie auf **Weiter**.

- 11 (Optional) Wählen Sie auf der Seite mit der Warnung über die erneute Initialisierung der Datenbank aus, dass die vorhandene Datenbank beibehalten werden soll, wenn sie bereits auf das neueste Schema aktualisiert wurde.

Wenn Sie Ihre vorhandene Datenbank mit einer leeren ersetzen, gehen alle vorhandenen Daten verloren.

- 12 Geben Sie die Porteinstellungen für den Update Manager an, wählen Sie aus, ob Sie die Proxyeinstellungen konfigurieren möchten, und klicken Sie auf **Weiter**.

Konfigurieren Sie die Proxy-Einstellungen, wenn der Computer, auf dem Update Manager installiert ist, auf das Internet zugreifen kann.

- 13 (Optional) Geben Sie die Informationen zum Proxyserver und Port ein, geben Sie an, ob der Proxy authentifiziert werden soll, und klicken Sie auf **Weiter**.

- 14 Klicken Sie auf **Installieren**, um mit dem Upgrade zu beginnen.

- 15 Klicken Sie auf **Beenden**.

Ergebnisse

Sie haben den Update Manager-Server aktualisiert.

Nächste Schritte

Führen Sie ein Upgrade auf das Update Manager-Client-Plug-In durch.

Vor dem Upgrade von Hosts

8

Damit das Upgrade Ihres Hosts erfolgreich verläuft, machen Sie sich mit den einhergehenden Änderungen vertraut und bereiten Sie sich auf diese vor.

Dieses Kapitel enthält die folgenden Themen:

- [Empfohlene Vorgehensweisen für Upgrades von ESXi](#)
- [Upgrade-Optionen für ESXi 6.0](#)
- [Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern](#)
- [Verwenden von manuell zugewiesenen IP-Adressen für Upgrades, die mit vSphere Update Manager durchgeführt werden](#)
- [Medienoptionen für das Starten des ESXi-Installationsprogramms](#)
- [Verwenden von Anwendungen für die Remoteverwaltung](#)
- [Herunterladen des ESXi-Installationsprogramms](#)

Empfohlene Vorgehensweisen für Upgrades von ESXi

Halten Sie sich beim Upgrade von Hosts an die empfohlenen Vorgehensweisen, um ein erfolgreiches Upgrade zu gewährleisten.

Beachten Sie die folgenden empfohlenen Vorgehensweisen beim ESXi-Upgrade:

- 1 Informieren Sie sich zunächst ausreichend über den Vorgang beim ESXi-Upgrade, die Auswirkungen dieses Prozesses auf Ihre bestehende Bereitstellung und die erforderliche Vorbereitung für das Upgrade.
 - Wenn Ihr vSphere-System VMware-Lösungen oder Plug-Ins enthält, stellen Sie sicher, dass sie mit der Version von vCenter Server, auf die Sie ein Upgrade durchführen, kompatibel sind. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
 - Lesen Sie [Upgrade-Optionen für ESXi 6.0](#), um sich mit den unterstützten Upgradeszenarien und den Optionen und Werkzeugen, die für das Upgrade zur Verfügung stehen, vertraut zu machen.
 - Informationen über bekannte Probleme bei der Installation finden Sie in den Versionshinweisen für VMware vSphere.

- 2 Bereiten Sie das System auf das Upgrade vor.
 - Stellen Sie sicher, dass ein Upgrade Ihrer aktuellen Version von ESXi möglich ist. Siehe [Upgrade-Optionen für ESXi 6.0](#).
 - Stellen Sie sicher, dass die Systemhardware die Anforderungen für ESXi erfüllt. Weitere Informationen finden Sie unter [Kapitel 2 Upgrade-Anforderungen](#) und im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php>. Überprüfen Sie die Systemkompatibilität, die E/A-Kompatibilität mit Netzwerk- und Host Bus Adapter-Karten (HBA), die Speicherkompatibilität und die Kompatibilität der Backup-Software.
 - Stellen Sie sicher, dass auf dem Host ausreichend Speicherplatz für das Upgrade vorhanden ist.
 - Wenn ein SAN mit dem Host verbunden ist, trennen Sie das FibreChannel-System ab, bevor Sie mit dem Upgrade fortfahren. Deaktivieren Sie keine HBA-Karten im BIOS.
- 3 Sichern Sie den Host, bevor Sie ein Upgrade durchführen. Dann können Sie den Host wiederherstellen, sollte das Upgrade fehlschlagen.
- 4 Je nach verwendeter Upgrade-Methode müssen Sie möglicherweise alle virtuellen Maschinen auf dem Host migrieren oder ausschalten. Lesen Sie dazu in der Anleitung zur gewählten Upgrade-Methode nach.
- 5 Testen Sie das System nach dem Upgrade, um sicherzustellen, dass das Upgrade erfolgreich abgeschlossen wurde.
- 6 Wenden Sie die Lizenzen des Hosts an. Siehe [Anwenden von Lizenzen nach einem Upgrade auf ESXi 6.0](#).
- 7 Ziehen Sie es in Erwägung, einen Syslog-Server für die Remoteprotokollierung einzurichten, um ausreichend Speicherplatz für Protokolldateien zu gewährleisten. Die Einrichtung der Protokollierung auf einem Remotehost ist besonders wichtig für Hosts, die über begrenzten lokalen Speicher verfügen. vSphere Syslog Collector ist ein Dienst von vCenter Server 6.0 und kann zum Erfassen von Protokollen auf allen Hosts verwendet werden. Siehe [Erforderlicher freier Speicherplatz für die Systemprotokollierung](#). Informationen zum Einrichten und Konfigurieren von Syslog und dem Syslog-Server, zur Einrichtung von Syslog über die Hostprofil-Schnittstelle und zur Installation von vSphere Syslog Collector finden Sie in der Dokumentation zu *Installations- und Einrichtungshandbuch für vSphere*.
- 8 Wenn das Upgrade fehlgeschlagen ist und Sie den Host gesichert haben, können Sie den Host wiederherstellen.

Upgrade-Optionen für ESXi 6.0

VMware bietet mehrere Möglichkeiten zum Durchführen eines Upgrades von ESXi 5.x-Hosts auf ESXi 6.0-Hosts.

Die Details und die Ebene der Unterstützung für ein Upgrade auf ESXi 6.0 hängen vom zu aktualisierenden Host und von der verwendeten Upgrade-Methode ab. Stellen Sie sicher, dass der Upgrade-Pfad von Ihrer aktuellen Version von ESXi auf die Version, auf die Sie ein Upgrade durchführen möchten, unterstützt wird. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Sie können ein Upgrade eines ESXi 5.x-Hosts, eines asynchron freigegebenen Treibers oder anderer Drittanbieteranpassungen durchführen, ein interaktives Upgrade von CD oder DVD, ein Upgrade im Skriptmodus oder ein Upgrade mit vSphere Update Manager. Wenn Sie ein Upgrade eines ESXi 5.x-Hosts, der benutzerdefinierte VIBs aufweist, auf Version 6.0 vornehmen, werden die benutzerdefinierten VIBs migriert. Weitere Informationen hierzu finden Sie unter [Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern](#).

Unterstützte Methoden für ein direktes Upgrade auf ESXi 6.0:

- vSphere Update Manager.
- Interaktives Upgrade von CD, DVD oder USB-Laufwerk.
- Skript-Upgrade.
- vSphere Auto Deploy. Wenn der ESXi 5.x-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host mit einem ESXi 6.0-Image erneut bereitzustellen.
- `esxcli`-Befehl.

vSphere Update Manager

vSphere Update Manager ist Software zum Durchführen von Upgrades, Migrationen und Updates von Cluster-Hosts, virtuellen Maschinen und Gastbetriebssystemen sowie zum Anwenden von Patches auf diese. vSphere Update Manager koordiniert Upgrades von Hosts und virtuellen Maschinen. Wenn Ihre Site vCenter Server verwendet, empfiehlt VMware die Verwendung von vSphere Update Manager. Eine Anleitung zum Durchführen eines koordinierten Host-Upgrades finden Sie unter [Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades](#). Eine Anleitung zum Durchführen eines koordinierten Upgrades einer virtuellen Maschine finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*.

Durchführen eines interaktiven Upgrades mithilfe eines ISO-Images des ESXi-Installationsprogramms auf CD/DVD oder einem USB-Flash-Laufwerk

Sie können das ESXi 6.0-Installationsprogramm von einer CD/DVD oder einem USB-Flash-Laufwerk aus starten, um ein interaktives Upgrade durchzuführen. Diese Methode eignet sich für Bereitstellungen mit einer kleinen Anzahl von Hosts. Das Installationsprogramm funktioniert genauso wie bei einer Neuinstallation. Wenn Sie jedoch eine Zielfestplatte auswählen, die bereits eine ESXi 5.0.x-, ESXi 5.1.x- oder ESXi 5.5.x-Installation enthält, wird der Host auf Version 6.0 aktualisiert. Sie erhalten außerdem die Möglichkeit, einige der vorhandenen Hosteinstellungen und Konfigurationsdateien zu migrieren und den

bestehenden VMFS-Datenspeicher beizubehalten. Weitere Informationen hierzu finden Sie unter [Interaktives Upgrade von Hosts](#).

Skriptgesteuerte Upgrades durchführen

Sie können für Hosts ein Upgrade von ESXi 5.0.x, ESXi 5.1.x und ESXi 5.5.x auf ESXi 6.0 durchführen, indem Sie ein Update-Skript ausführen, was ein effizientes, unbeaufsichtigtes Upgrade ermöglicht. Skriptgesteuerte Upgrades bieten eine effiziente Möglichkeit zum Bereitstellen mehrerer Hosts. Sie können von einem CD-, DVD- oder einem USB-Flash-Laufwerk aus ein Skript zum Durchführen eines Upgrades von ESXi verwenden oder eine PXE (Preboot Execution Environment) für das Installationsprogramm angeben. Zudem können Sie ein Skript von einer interaktiven Installation aus aufrufen. Weitere Informationen hierzu finden Sie unter [Installieren oder Upgraden von Hosts mithilfe eines Skripts](#).

vSphere Auto Deploy

Nachdem ein ESXi 5.x-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host erneut bereitzustellen und mit einem neuen Image-Profil neu zu starten. Dieses Profil enthält ein ESXi-Upgrade oder einen Patch, ein Hostkonfigurationsprofil und optional Drittanbietertreiber oder Management-Agenten von VMware-Partnern. Sie können benutzerdefinierte Images mithilfe von vSphere ESXi Image Builder CLI erstellen. Weitere Informationen hierzu finden Sie unter [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

esxcli

Sie können das `esxcli`-Befehlszeilendienstprogramm für ESXi verwenden, um ein Upgrade von ESXi 5.0.x-Hosts, ESXi 5.1.x-Hosts oder ESXi 5.5.x-Hosts auf ESXi 6.0-Hosts durchzuführen.

Die Dienstprogramme `esxupdate` und `vihostupdate` werden für ESXi 6.0-Upgrades nicht unterstützt. Weitere Informationen hierzu finden Sie unter [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#).

Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern

Auf einem Host können benutzerdefinierte vSphere-Installationspakete (vSphere Installation Bundles, VIBs) installiert sein, zum Beispiel für Treiber von Drittanbietern oder für Management-Agenten. Beim Upgrade eines ESXi 5.x-Hosts auf ESXi 6.0 werden alle unterstützten benutzerdefinierten VIBs migriert. Dabei spielt es keine Rolle, ob die VIBs im ISO-Image des Installationsprogramms enthalten sind.

Falls der Host oder das ISO-Image des Installationsprogramms ein VIB enthält, das einen Konflikt verursacht und das Upgrade verhindert, wird in einer Fehlermeldung das VIB angegeben, das den Konflikt verursacht hat. Führen Sie eine der folgenden Aktionen aus, um ein Upgrade für den Host durchzuführen:

- Entfernen Sie das VIB, das den Konflikt verursacht hat, vom Host und führen Sie das Upgrade erneut durch. Wenn Sie vSphere Update Manager verwenden, wählen Sie während der Standardisierung die Option zum Löschen von Drittanbieter-Softwaremodulen aus. Weitere Informationen finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*. Sie können auch das VIB, das den Konflikt verursacht hat, mithilfe von `esxcli`-Befehlen vom Host entfernen. Weitere Informationen finden Sie unter [Entfernen von VIBs von einem Host](#).
- Verwenden Sie die vSphere ESXi Image Builder CLI, um ein benutzerdefiniertes ISO-Image des Installationsprogramms zu erstellen, mit dem der Konflikt behoben wird. Weitere Informationen zur Installation und Verwendung der vSphere ESXi Image Builder CLI finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

Verwenden von manuell zugewiesenen IP-Adressen für Upgrades, die mit vSphere Update Manager durchgeführt werden

Wenn Sie vSphere Update Manager für das Upgrade eines Hosts von ESXi 5.x auf ESXi 6.0 verwenden, müssen Sie für die Hosts manuell zugewiesene IP-Adressen verwenden. Manuell zugewiesene IP-Adressen werden auch als statische IP-Adressen bezeichnet.

IP-Adressen, die mithilfe von DHCP (Dynamic Host Configuration Protocol) angefordert werden, können bei mit vSphere Update Manager durchgeführten Host-Upgrades Probleme verursachen. Wenn ein Host seine DHCP-IP-Adresse während eines Upgrades verliert, da der auf dem DHCP-Server konfigurierte Lease-Zeitraum abgelaufen ist, geht die Verbindung von vSphere Update Manager zum Host verloren. Selbst wenn das Host-Upgrade oder die Hostmigration erfolgreich verläuft, meldet vSphere Update Manager in diesem Fall einen Upgrade- oder Migrationsfehler, da er keine Verbindung zum Host herstellen kann. Verwenden Sie zum Verhindern dieses Szenarios manuell zugewiesene IP-Adressen für die Hosts.

Medienoptionen für das Starten des ESXi-Installationsprogramms

Das ESXi-Installationsprogramm muss für das System erreichbar sein, auf dem Sie ESXi installieren.

Für das ESXi-Installationsprogramm werden die folgenden Startmedien unterstützt:

- Starten von CD/DVD. Weitere Informationen hierzu finden Sie unter [Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD](#).

- Starten von einem USB-Flash-Laufwerk. Weitere Informationen hierzu finden Sie unter [Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades](#).
- Starten vom Netzwerk per PXE-Startvorgang. [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#)
- Starten von einem Remotespeicherort aus mit einer Remoteverwaltungsanwendung. Siehe [Verwenden von Anwendungen für die Remoteverwaltung](#).

Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD

Wenn Sie über keine ESXi-Installations-CD/DVD verfügen, können Sie eine erstellen.

Sie können auch ein Installer-ISO-Image erstellen, das ein benutzerdefiniertes Installationsskript enthält. Weitere Informationen hierzu finden Sie unter [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#).

Verfahren

- 1 Laden Sie das ESXi-Installationsprogramm von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.
ESXi ist unter „Datencenter- und Cloud-Infrastruktur“ aufgeführt
- 2 Bestätigen Sie, dass „md5sum“ korrekt ist.
Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Verwenden von MD5-Prüfsummen“ unter <http://www.vmware.com/download/md5.html>.
- 3 Brennen Sie das ISO-Image auf eine CD oder eine DVD.

Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades

Sie können ein USB-Flash-Laufwerk für das Starten der ESXi-Installation oder des Upgrades formatieren.

Die Anweisungen in diesem Verfahren setzen voraus, dass das USB-Flash-Laufwerk als „/dev/sdb“ erkannt wird.

Hinweis Die Datei `ks.cfg` mit dem Installationsskript darf sich nicht in dem USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird.

Voraussetzungen

- Linux-Maschine mit Superuser-Zugriff darauf
- USB-Flash-Laufwerk, das von der Linux-Maschine erkannt werden kann
- Das ESXi-ISO-Image `VMware-VMvisor-Installer-version_number-build_number.x86_64.iso`, das die Datei `isolinux.cfg` enthält

■ Syslinux-Paket

Verfahren

- 1 Wenn Ihr USB-Flash-Laufwerk nicht als „/dev/sdb“ erkannt wird oder Sie nicht genau wissen, wie Ihr USB-Flash-Laufwerk erkannt wird, legen Sie dies fest.

- a Führen Sie dazu in der Befehlszeile den Befehl zum Anzeigen der aktuellen Protokollmeldungen aus.

```
tail -f /var/log/messages
```

- b Schließen Sie Ihr USB-Flash-Laufwerk an.

Es werden mehrere Meldungen angezeigt, die sich auf das USB-Flash-Laufwerk beziehen, und zwar in folgendem oder ähnlichem Format.

```
Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable disk
```

In diesem Beispiel gibt *sdb* das USB-Gerät an. Falls Ihr Gerät anderweitig identifiziert wird, verwenden Sie anstelle von *sdb* die betreffende Identifizierung.

- 2 Erstellen Sie eine Partitionstabelle auf dem USB-Flash-Gerät.

```
/sbin/fdisk /dev/sdb
```

- a Geben Sie *d* ein, um Partitionen zu löschen, bis alle Partitionen gelöscht sind.
 - b Geben Sie *n* ein, um die primäre Partition 1 zu erstellen, die sich über die gesamte Festplatte erstreckt.
 - c Geben Sie *t* ein, um für den Typ eine passende Einstellung für das Dateisystem FAT32 festzulegen, z. B. *c*.
 - d Geben Sie *a* ein, um das aktive Flag auf Partition 1 zu setzen.
 - e Geben Sie *p* ein, um die Partitionstabelle auszugeben.

Das Ergebnis sollte der folgenden Meldung ähneln.

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes 255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes Device Boot Start End Blocks Id
System /dev/sdb1 1 243 1951866 c W95 FAT32 (LBA)
```

- f Geben Sie *w* ein, um die Partitionstabelle zu schreiben und das Programm zu verlassen.

- 3 Formatieren Sie das USB-Flash-Laufwerk mit dem Dateisystem Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

- 4 Installieren Sie den Syslinux-Bootloader auf dem USB-Flash-Laufwerk.

Die Speicherorte der ausführbaren Syslinux-Datei und der Datei `mbr.bin` unterscheiden sich möglicherweise bei den unterschiedlichen Syslinux-Versionen. Wenn Sie beispielsweise Syslinux 6.02 heruntergeladen haben, führen Sie die folgenden Befehle aus.

```
/usr/bin/syslinux /dev/sdb1
cat /usr/lib/syslinux/mbr/mbr.bin > /dev/sdb
```

- 5 Erstellen Sie ein Zielverzeichnis und mounten Sie das USB-Flash-Laufwerk darauf.

```
mkdir /usbdisk
mount /dev/sdb1 /usbdisk
```

- 6 Erstellen Sie ein Zielverzeichnis und mounten Sie das ESXi-Installer-ISO-Image darauf.

```
mkdir /esxi_cdrom
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

- 7 Kopieren Sie die Inhalte des ISO-Image auf das USB-Flash-Laufwerk.

```
cp -r /esxi_cdrom/* /usbdisk
```

- 8 Benennen Sie die Datei `isolinux.cfg` in `syslinux.cfg` um.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

- 9 Bearbeiten Sie in der Datei `/usbdisk/syslinux.cfg` die Zeile `APPEND -c boot.cfg` in `APPEND -c boot.cfg -p 1`.

- 10 Unmounten Sie das USB-Flash-Laufwerk.

```
umount /usbdisk
```

- 11 Unmounten Sie das ESXi-Installer-ISO-Image.

```
umount /esxi_cdrom
```

Ergebnisse

Das USB-Flash-Laufwerk kann das ESXi-Installationsprogramm starten.

Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts

Sie können ein USB-Flash-Laufwerk zum Speichern des ESXi-Installations- oder -Upgrade-Skripts verwenden, das während der Skriptinstallation bzw. des Skript-Upgrades von ESXi verwendet wird.

Wenn auf der Installationsmaschine mehrere USB-Flash-Laufwerke vorhanden sind, durchsucht die Installationssoftware alle angeschlossenen USB-Flash-Laufwerke nach dem Installations- oder Upgrade-Skript.

Die Anweisungen in diesem Verfahren setzen voraus, dass das USB-Flash-Laufwerk als `/dev/sdb` erkannt wird.

Hinweis Die Datei `ks`, die das Installations- oder Upgrade-Skript enthält, darf sich nicht auf dem selben USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird.

Voraussetzungen

- Linux-Maschine
- Installations- oder Upgrade-Skript für ESXi, die Kickstart-Datei `ks.cfg`
- USB-Flash-Laufwerk

Verfahren

- 1 Schließen Sie das USB-Flash-Laufwerk an eine Linux-Maschine an, die auf das Installations- bzw. Upgrade-Skript zugreifen kann.

- 2 Erstellen Sie eine Partitionstabelle.

```
/sbin/fdisk /dev/sdb
```

- a Geben Sie `d` ein, um Partitionen zu löschen, bis alle Partitionen gelöscht sind.
- b Geben Sie `n` ein, um die primäre Partition 1 zu erstellen, die sich über die gesamte Festplatte erstreckt.
- c Geben Sie `t` ein, um für den Typ eine passende Einstellung für das Dateisystem FAT32 festzulegen, z. B. `c`.
- d Geben Sie `p` ein, um die Partitionstabelle auszugeben.

Das Ergebnis sollte dem folgenden Text ähneln:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1           1         243       1951866    c   W95 FAT32 (LBA)
```

- e Geben Sie `w` ein, um die Partitionstabelle zu schreiben und den Vorgang zu beenden.
- 3 Formatieren Sie das USB-Flash-Laufwerk mit dem Dateisystem Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

- 4 Mounten Sie das USB-Flash-Laufwerk.

```
mount /dev/sdb1 /usbdisk
```

- 5 Kopieren Sie das ESXi-Installationsskript auf das USB-Flash-Laufwerk.

```
cp ks.cfg /usbdisk
```

- 6 Unmounten Sie das USB-Flash-Laufwerk.

Ergebnisse

Das USB-Flash-Laufwerk enthält das Installations- oder das Upgrade-Skript für ESXi.

Nächste Schritte

Wenn Sie das ESXi-Installationsprogramm starten, verweisen Sie für das Installations- oder Upgrade-Skript auf den Speicherort des USB-Flash-Laufwerks. Siehe [Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts](#) und [Grundlegendes zu PXE-Konfigurationsdateien](#).

Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript

Sie können das standardmäßige ESXi-Installer-ISO-Image mit einem eigenen Installations- oder Upgrade-Skript anpassen. Diese Anpassung ermöglicht Ihnen die Durchführung einer skriptbasierten, unbeaufsichtigten Installation bzw. eines skriptbasierten, unbeaufsichtigten Upgrades, wenn Sie das resultierende Installer-ISO-Image starten.

Siehe auch [Grundlegendes zu Installations- und Upgrade-Skripts](#) und [Grundlegende Informationen zur Datei „boot.cfg“](#).

Voraussetzungen

- Linux-Maschine
- Das ESXi-ISO-Image `VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso`, wobei `6.x.x` die Version von ESXi ist, die Sie installieren, und `XXXXXX` die Buildnummer des ISO-Images des Installationsprogramms
- Ihr benutzerdefiniertes Installations- oder Upgrade-Skript, die Kickstart-Datei `ks_cust.cfg`.

Verfahren

- 1 Laden Sie das ESXi-ISO-Image von der VMware-Website herunter.

- 2 Mounten Sie das ISO-Image in einen Ordner:

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /  
esxi_cdrom_mount
```

`XXXXXX` ist die ESXi-Build-Nummer für die Version, die Sie installieren bzw. auf die Sie ein Upgrade ausführen.

- 3 Kopieren Sie den Inhalt von `cdrom` in einen anderen Ordner:

```
cp -r /esxi_cdrom_mount /esxi_cdrom
```

- 4 Kopieren Sie die Kickstart-Datei nach `/esxi_cdrom`

```
cp ks_cust.cfg /esxi_cdrom
```

- 5 (Optional) Ändern Sie die Datei `boot.cfg` mithilfe der Option `kernelopt` dahingehend, dass sie den Speicherort des Installations- oder Upgrade-Skripts angibt.

Sie müssen den Skriptpfad in Großbuchstaben eingeben, zum Beispiel

```
kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
```

Die Installation bzw. das Upgrade wird vollkommen automatisch, da das Angeben der Kickstart-Datei während der Installation oder des Upgrades entfällt.

- 6 Neuerstellung des ISO-Images:

```
mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c  
boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table /esxi_cdrom
```

Ergebnisse

Das ISO-Image enthält Ihr benutzerdefiniertes Installations- bzw. Upgrade-Skript.

Nächste Schritte

Installieren Sie ESXi aus dem ISO-Image.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang

Sie verwenden PXE (Preboot Execution Environment) für den Startvorgang eines Hosts und um das ESXi-Installationsprogramm von einer Netzwerkschnittstelle zu starten.

ESXi 6.0 wird in einem ISO-Format verteilt, das für die Installation auf Flash-Arbeitsspeicher oder auf eine lokale Festplatte entwickelt wurde. Mithilfe von PXE können Sie die Dateien extrahieren und starten.

PXE verwendet Dynamic Host Configuration Protocol (DHCP) und Trivial File Transfer Protocol (TFTP), um ein Betriebssystem über ein Netzwerk zu starten.

Das Starten mit PXE setzt eine gewisse Netzwerkinfrastruktur und eine Maschine mit einem PXE-fähigen Netzwerkadapter voraus. Die meisten Maschinen, die ESXi ausführen können, verfügen über Netzwerkadapter, die PXE-Startvorgänge ermöglichen.

Hinweis Stellen Sie sicher, dass der vSphere Auto Deploy-Server über eine IPv4-Adresse verfügt. Das Starten per PXE-Startvorgang wird nur mit IPv4 unterstützt.

Grundlegendes zu TFTP-Server, PXELINUX und gPXE

Trivial File Transfer Protocol (TFTP) ähnelt dem FTP-Dienst und wird normalerweise nur für Netzwerkstartsysteme oder zum Laden der Firmware auf Netzwerkgeräten (z. B. Routern) verwendet.

Die meisten Linux-Distributionen enthalten eine Kopie des tftp-hpa-Servers. Wenn Sie eine unterstützte Lösung benötigen, erwerben Sie einen unterstützten TFTP-Server von einem Anbieter Ihrer Wahl.

Wenn Ihr TFTP-Server auf einem Microsoft Windows-Host ausgeführt werden soll, müssen Sie tftpd32 Version 2.11 oder höher verwenden. Weitere Informationen hierzu finden Sie unter <http://tftpd32.jounin.net/>. Frühere Versionen von tftpd32 sind nicht kompatibel mit PXELINUX und gPXE.

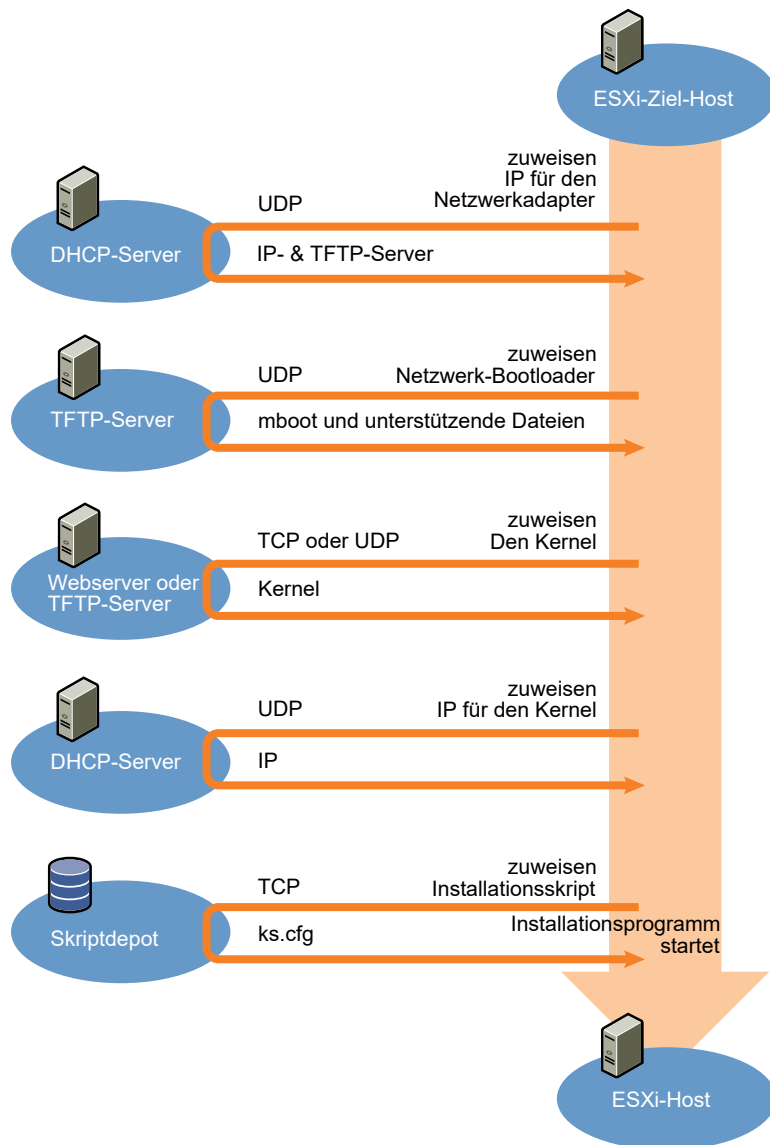
Sie können sich einen TFTP-Server auch von einem der verpackten Appliances auf dem VMware Marketplace beschaffen.

Die PXELINUX- und gPXE-Umgebungen ermöglichen das Starten des ESXi-Installationsprogramms durch die Zielformatierung. PXELINUX ist Teil des SYSLINUX-Pakets, das sich unter <http://www.kernel.org/pub/linux/utils/boot/syslinux/> befindet. Viele Linux-Distributionen enthalten das Paket bereits. Viele Versionen von PXELINUX enthalten zudem gPXE. Einige Distributionen, wie z. B. Red Hat Enterprise Linux Version 5.3, enthalten frühere Versionen von PXELINUX, die gPXE nicht enthalten.

Wenn Sie gPXE nicht verwenden, können Probleme beim Starten des ESXi-Installationsprogramms auf einem stark ausgelasteten Netzwerk auftreten. TFTP ist manchmal unzuverlässig beim Übertragen großer Datenmengen. Wenn Sie PXELINUX ohne gPXE verwenden, werden die Binärdatei `pxelinux.0`, die Konfigurationsdatei, der Kernel und andere Dateien über TFTP übertragen. Wenn Sie gPXE verwenden, werden nur die Binärdatei `gpxelinux.0` und die Konfigurationsdatei über TFTP übertragen. Mit gPXE können Sie einen Webserver zum Übertragen des Kernels und anderer zum Starten des ESXi-Installationsprogramms erforderlichen Dateien verwenden.

Hinweis VMware testet den PXE-Startvorgang mit PXELINUX Version 3.86. Dies deutet jedoch nicht auf eine eingeschränkte Unterstützung hin. Wenden Sie sich an den jeweiligen Anbieter zwecks Unterstützung von Agenten von Drittanbietern, die Sie zum Einrichten Ihrer PXE-Startinfrastruktur verwenden.

Abbildung 8-1. Überblick über den Installationsprozess per PXE-Startvorgang



Beispiel-DHCP-Konfiguration

Der DHCP-Server muss zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang die Adresse des TFTP-Servers sowie einen Zeiger auf das Verzeichnis `pxelinux.0` oder `gpxelinux.0` senden.

Der DHCP-Server wird von der Zielmaschine zum Abrufen einer IP-Adresse verwendet. Der DHCP-Server muss feststellen können, ob die Zielmaschine starten darf, und den Speicherort der PXELINUX-Binärdatei (die sich gewöhnlich auf einem TFTP-Server befindet) kennen. Beim Start der Zielmaschine sendet sie ein Paket über das Netzwerk, das diese Informationen anfordert, damit sie selbst starten kann. Der DHCP-Server antwortet.

Vorsicht Richten Sie keinen neuen DHCP-Server ein, wenn sich bereits einer in Ihrem Netzwerk befindet. Falls mehrere DHCP-Server auf die DHCP-Anforderungen reagieren, können Maschinen falsche oder widersprüchliche IP-Adressen abrufen oder nicht die richtigen Startinformationen erhalten. Sprechen Sie mit einem Netzwerkadministrator, bevor Sie einen DHCP-Server einrichten. Zur Unterstützung bei der Konfiguration von DHCP wenden Sie sich an den Hersteller Ihres DHCP-Servers.

Viele DHCP-Server können Hosts per PXE-Startvorgang starten. Wenn Sie eine Version von DHCP für Microsoft Windows verwenden, lesen Sie die DHCP-Serverdokumentation, um zu erfahren, wie die Argumente `next-server` und `filename` an die Zielmaschine übergeben werden.

gPXE-Beispiel

In diesem Beispiel wird gezeigt, wie ein ISC DHCP-Server der Version 3.0 für das Aktivieren von gPXE konfiguriert wird.

```
allow booting;
allow bootp;
# gPXE options
option space gppe;
option gppe-encap-opts code 175 = encapsulate gppe;
option gppe.bus-id code 177 = string;
class "pxeclients" {
    match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
    next-server TFTP server address;
    if not exists gppe.bus-id {
        filename "/gpxelinux.0";
    }
}
subnet Network address netmask Subnet Mask {
    range Starting IP AddressEnding IP Address;
}
```

Wenn eine Maschine einen Startvorgang per PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `gpxelinux.0` auf dem TFTP-Server zur Verfügung. Die zugeordnete IP-Adresse befindet sich in dem Bereich, der im Subnetzabschnitt der Konfigurationsdatei definiert ist.

PXELINUX (ohne gPXE) Beispiel

In diesem Beispiel wird gezeigt, wie ein ISC DHCP-Server der Version 3.0 für das Aktivieren von PXELINUX konfiguriert wird.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
    match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
    next-server xxx.xxx.xx.xx;
    filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
    range 192.168.48.100 192.168.48.250;
}
```

Wenn eine Maschine einen Startvorgang per PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `pxelinux.0` auf dem TFTP-Server zur Verfügung. Die zugeordnete IP-Adresse befindet sich in dem Bereich, der im Subnetzabschnitt der Konfigurationsdatei definiert ist.

Grundlegendes zu PXE-Konfigurationsdateien

Die PXE-Konfigurationsdatei legt das Menü fest, das dem ESXi-Zielhost angezeigt wird, wenn er startet und den TFTP-Server kontaktiert. Für das Starten des ESXi-Installationsprogramms per PXE-Startvorgang benötigen Sie eine PXE-Konfigurationsdatei.

Der TFTP-Server überwacht ständig PXE-Clients im Netzwerk. Wenn er erkennt, dass ein PXE-Client PXE-Dienste anfordert, sendet er ein Netzwerkpaket, das ein Startmenü enthält, an den Client.

Erforderliche Dateien

Die PXE-Konfigurationsdatei muss die Pfade zu den folgenden Dateien enthalten:

- `mboot.c32` ist der Bootloader.
- `boot.cfg` ist die Bootloader-Konfigurationsdatei.

Siehe [Grundlegende Informationen zur Datei „boot.cfg“](#).

Dateiname der PXE-Konfigurationsdatei

Wählen Sie als Dateinamen der PXE-Konfigurationsdatei eine der folgenden Optionen aus:

- `01-mac-Adresse_von_ESXi-Zielhost`. Beispiel: `01-23-45-67-89-0a-bc`
- Die IP-Adresse des ESXi-Zielhosts in hexadezimaler Schreibweise.
- Standard

Die anfängliche Startdatei `pxelinux.0` oder `gpxelinux.0` versucht, eine PXE-Konfigurationsdatei zu laden. Sie versucht es mit der MAC-Adresse des ESXi-Zielhosts, der der Code des ARP-Typs, der für Ethernet „01“ lautet, vorangestellt ist. Schlägt der Versuch fehl, versucht sie es mit der IP-Adresse des ESXi-Zielsystems in hexadezimaler Schreibweise. Letztendlich wird versucht, eine Datei namens `default` zu laden.

Speicherort der PXE-Konfigurationsdatei

Speichern Sie die Datei auf dem TFTP-Server im Verzeichnis `var/lib/tftpboot/pxelinux.cfg/`.

Sie können die Datei z. B. auf dem TFTP-Server unter `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6` speichern. Die MAC-Adresse des Netzwerkadapters auf dem ESXi-Zielhost ist 00-21-5a-ce-40-f6.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei

Sie können einen TFTP-Server zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und einer PXE-Konfigurationsdatei verwenden.

Siehe auch [Grundlegendes zu Installations- und Upgrade-Skripts](#) und [Grundlegende Informationen zur Datei „boot.cfg“](#).

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- TFTP-Server mit gPXE, der den PXE-Startvorgang unterstützt. Siehe [Grundlegendes zu TFTP-Server, PXELINUX und gPXE](#).
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Siehe [Beispiel-DHCP-Konfiguration](#).
- PXELINUX.
- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php>.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- (Optional) Installationsskript, die Kickstart-Datei. Siehe [Grundlegendes zu Installations- und Upgrade-Skripts](#).
- Netzwerkadapter mit PXE-Unterstützung auf dem Ziel-ESXi-Host
- IPv4-Netzwerk. IPv6 wird für die PXE-Startvorgänge nicht unterstützt.

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Um die VLAN-ID anzugeben, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Verfahren

- 1 Erstellen Sie das Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

- 2 Installieren Sie auf der Linux-Maschine PXELINUX.

PXELINUX ist im Syslinux-Paket enthalten. Extrahieren Sie die Dateien, suchen Sie die Datei `pxelinux.0` und kopieren Sie sie in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

- 3 Konfigurieren Sie den DHCP-Server zum Senden der folgenden Informationen an jeden Clienthost:

- Name oder IP-Adresse Ihres TFTP-Servers
- Name der anfänglichen Startdatei, `pxelinux.0`

- 4 Kopieren Sie den Inhalt des ESXi-Installationsprogramm-Images in das Verzeichnis `/var/lib/tftpboot` des TFTP-Servers.

- 5 (Optional) Fügen Sie für eine Skriptinstallation in der `boot.cfg`-Datei die Option `kernelopt` in die Zeile nach dem Kernelbefehl ein, um den Speicherort des Installationsskripts anzugeben.
Verwenden Sie den folgenden Code als Beispiel, wobei `xxx.xxx.xxx.xxx` die IP-Adresse des Servers ist, auf dem sich das Installationsskript befindet, und `esxi_ksFiles` das Verzeichnis, in dem sich die Datei `ks.cfg` befindet.

```
kernelopt=ks=http://xxx.xxx.xxx.xxx/esxi_ksFiles/ks.cfg
```

- 6 Erstellen Sie eine PXE-Konfigurationsdatei.

Diese Datei legt fest, wie der Host gestartet wird, wenn kein Betriebssystem verfügbar ist. Die PXE-Konfigurationsdatei referenziert die Startdateien. Verwenden Sie den folgenden Code als Beispiel, wobei `xxxxxxx` die Build-Nummer des Images des ESXi-Installationsprogramms ist.

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 Geben Sie die MAC-Adresse (Media Access Control) der Zielhostmaschine als Name der Datei an: `01-mac-Adresse_von_ESXi-Zielhost`.

Beispiel: `01-23-45-67-89-0a-bc`.

- 8 Speichern Sie die PXE-Konfigurationsdatei unter `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

9 Starten Sie die Maschine mit dem Netzwerkadapter.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „islinux.cfg“

Sie können das ESXi-Installationsprogramm per PXE-Startvorgang mithilfe von PXELINUX starten und die Datei „islinux.cfg“ als PXE-Konfigurationsdatei verwenden.

Siehe auch [Grundlegendes zu Installations- und Upgrade-Skripts](#) und [Grundlegende Informationen zur Datei „boot.cfg“](#).

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- TFTP-Server mit PXELINUX, der den PXE-Startvorgang unterstützt. Siehe [Grundlegendes zu TFTP-Server, PXELINUX und gPXE](#).
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Siehe [Beispiel-DHCP-Konfiguration](#).
- PXELINUX.
- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php>.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- (Optional) Installationsskript, die Kickstart-Datei. Siehe [Grundlegendes zu Installations- und Upgrade-Skripts](#).
- Netzwerkadapter mit PXE-Unterstützung auf dem Ziel-ESXi-Host
- IPv4-Netzwerk. IPv6 wird für die PXE-Startvorgänge nicht unterstützt.

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Um die VLAN-ID anzugeben, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Verfahren

1 Erstellen Sie das Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

2 Installieren Sie auf der Linux-Maschine PXELINUX.

PXELINUX ist im Syslinux-Paket enthalten. Extrahieren Sie die Dateien, suchen Sie die Datei `pxelinux.0` und kopieren Sie sie in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

3 Konfigurieren Sie den DHCP-Server.

Der DHCP-Server sendet die folgenden Informationen an Ihre Clienthosts:

- Name oder IP-Adresse Ihres TFTP-Servers

- Name der anfänglichen Startdatei, `pxelinux.0`
- 4 Kopieren Sie den Inhalt des ESXi-Installationsprogramm-Images in das Verzeichnis `/var/lib/tftpboot` des TFTP-Servers.
- 5 (Optional) Fügen Sie für eine Skriptinstallation in der `boot.cfg`-Datei die Option `kernelopt` in die nächste Zeile nach dem `kernel`-Befehl ein, um den Speicherort des Installationsskripts anzugeben.

Im folgenden Beispiel ist `XXX.XXX.XXX.XXX` die IP-Adresse des Servers, auf dem sich das Installationsskript befindet.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

- 6 Kopieren Sie die Datei `isolinux.cfg` vom ISO-Image des ESXi-Installationsprogramms in das Verzeichnis `/tftpboot/pxelinux.cfg`.

Die Datei `isolinux.cfg` enthält den folgenden Code, bei dem `xxxxxxx` die Build-Nummer des ESXi-Installationsprogramm-Images ist:

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
    KERNEL mboot.c32
    APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
    LOCALBOOT 0x80
MENU LABEL ^Boot from local disk
```

- 7 Benennen Sie die Datei `isolinux.cfg` mit der MAC-Adresse der Zielhostmaschine um: `01-mac-Adresse_von_ESXi-Zielhost`. Beispiel: `01-23-45-67-89-0a-bc`
- 8 Starten Sie die Maschine mit dem Netzwerkadapter.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von gPXE

Sie können das ESXi-Installationsprogramm per PXE-Startvorgang mithilfe von gPXE ausführen.

Siehe auch [Grundlegendes zu Installations- und Upgrade-Skripts](#) und [Grundlegende Informationen zur Datei „boot.cfg“](#).

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde

- HTTP-Webserver, auf den Ihre Ziel-ESXi-Hosts zugreifen können
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist: `/etc/dhcpd.conf` wird für Clienthosts mit einem TFTP-Server und der anfänglichen Startdatei `gpxelinux.0/undionly.kpxe` konfiguriert. Weitere Informationen hierzu finden Sie unter [Beispiel-DHCP-Konfiguration](#).
- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im Hardware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php>.
- gPXELINUX
- (Optional) ESXi-Installationsskript. Weitere Informationen hierzu finden Sie unter [Grundlegendes zu Installations- und Upgrade-Skripts](#).

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Wenn Sie die VLAN-ID angeben möchten, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Verfahren

- 1 Kopieren Sie den Inhalt des ISO-Images des ESXi-Installationsprogramms in das Verzeichnis `/var/www/html` des HTTP-Servers.
- 2 Passen Sie die `boot.cfg`-Datei mit den Informationen für den HTTP-Server an.

Verwenden Sie den folgenden Code als Beispiel, wobei `XXX.XXX.XXX.XXX` die IP-Adresse des HTTP-Servers ist. Die Zeile `kernelopt` ist optional. Verwenden Sie diese Option, um den Speicherort des Installationsskripts für eine Skriptinstallation anzugeben.

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz --- http://
XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 --- http://XXX.XXX.XXX.XXX/s.v00
--- http://XXX.XXX.XXX.XXX/weaselin.t00 --- http://XXX.XXX.XXX.XXX/tools.t00 --- http://
XXX.XXX.XXX.XXX/imgdb.tgz --- http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

- 3 Starten Sie den Host per gPXE-Startvorgang und drücken Sie Strg+B, um auf das GPT-Menü zuzugreifen.
- 4 Geben Sie die folgenden Befehle zum Starten mit dem ESXi-Installationsprogramm ein, wobei `XXX.XXX.XXX.XXX` die IP-Adresse des HTTP-Servers ist.

```
dhcp net0 ( if dhcp is not set)
kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

Installieren und Starten von ESXi mit Software FCoE

Sie können ESXi von einer FCoE LUN mit VMware Software-FCoE-Adaptern und Netzwerkadaptern mit FCoE-Auslagerungsfunktionen installieren und starten. Ihr Host benötigt keinen dedizierten FCoE HBA.

In der Dokumentation *vSphere-Speicher* finden Sie Informationen über die Installation und das Starten von ESXi mit Software FCoE.

Verwenden von Anwendungen für die Remoteverwaltung

Remotemanagement-Anwendungen ermöglichen Ihnen die Installation von ESXi auf Servermaschinen an Remotestandorten.

Zu den für die Installation unterstützten Remotemanagement-Anwendungen gehören HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM Management Module (MM), und Remote Supervisor Adapter II (RSA II). Eine Liste der zurzeit unterstützten Servermodelle und Remotemanagement-Firmwareversionen finden Sie unter [Unterstützte Remotemanagement-Servermodelle und Firmware-Versionen](#). Wenn Sie Unterstützung für Remotemanagement-Anwendungen benötigen, wenden Sie sich an Ihren Hersteller.

Sie können Remotemanagement-Anwendungen verwenden, um interaktive Installationen und Skriptinstallationen von ESXi remote durchzuführen.

Wenn Sie Remotemanagement-Anwendungen verwenden, um ESXi zu installieren, können bei ausgelasteten Systemen oder Netzwerken bei Verwendung der virtuellen CD Probleme mit beschädigten Dateien auftreten. Falls eine Remoteinstallation eines ISO-Images fehlschlägt, schließen Sie die Installation unter Verwendung des physischen CD-Mediums ab.

Herunterladen des ESXi-Installationsprogramms

Laden Sie das Installationsprogramm für ESXi herunter.

Voraussetzungen

Erstellen Sie ein Customer Connect-Konto unter <https://my.vmware.com/web/vmware/>.

Verfahren

- 1 Laden Sie das ESXi-Installationsprogramm von der VMware-Website unter <https://my.vmware.com/web/vmware/downloads> herunter.

ESXi ist unter „Datacenter- & Cloud-Infrastruktur“ aufgeführt.

- 2 Bestätigen Sie, dass „md5sum“ korrekt ist.

Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Using MD5 Checksums“ (Verwenden von MD5-Prüfsummen) unter <http://www.vmware.com/download/md5.html>.

Upgrade der Hosts wird durchgeführt

9

Führen Sie nach dem Upgrade von vCenter Server und vSphere Update Manager ein Upgrade von VMware ESXi 5.x-Hosts auf ESXi 6.0 durch. Für ESXi 5.0.x-, ESXi 5.1.x- und ESXi 5.5.x-Hosts können Sie ein direktes Upgrade auf ESXi 6.0 durchführen.

Für das Upgrade von Hosts können Sie die unter [Upgrade-Optionen für ESXi 6.0](#) beschriebenen Tools und Methoden verwenden.

Vorsicht Wenn Sie ein Upgrade von Hosts durchführen, die von vCenter Server verwaltet werden, müssen Sie vor dem Upgrade von ESXi ein Upgrade auf vCenter Server durchführen. Wenn Sie das Upgrade nicht in der richtigen Reihenfolge durchführen, kommt es möglicherweise zu Datenverlust und einer Unterbrechung des Serverzugriffs.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades](#)
- [Installieren oder Upgraden von Hosts mithilfe eines Skripts](#)
- [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#)
- [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#)
- [Interaktives Upgrade von Hosts](#)

Verwenden von vSphere Update Manager zum Durchführen von koordinierten Host-Upgrades

Mit koordinierten Upgrades können Sie ein Upgrade der Objekte in Ihrer vSphere-Bestandsliste in einem zweischrittigen Verfahren durchführen: Host-Upgrades, gefolgt von Upgrades von virtuellen Maschinen. Dieser Prozess kann auf Cluster-Ebene zur Automatisierung weiterer Teile des Vorgangs und auf der Ebene einzelner Hosts oder virtueller Maschinen zur Feinabstimmung konfiguriert werden.

Beispielsweise können Sie eine Host-Upgrade-Baseline zum Upgrade eines ESXi 5.x-Hosts auf ESXi 6.0 oder eine VM-Upgrade-Baseline zum Upgrade von VMware Tools und der Hardware der virtuellen Maschine auf die neueste Version definieren. Verwenden Sie assistentenbasierte Arbeitsabläufe, um zunächst Host-Upgrades für einen ganzen Cluster und anschließend ein VM-Upgrade für alle virtuelle Maschinen zu planen.

Wichtig Nachdem Sie den Host auf ESXi 6.0 aktualisiert haben, ist ein Rollback auf die Version 5.x von ESXi nicht mehr möglich. Sichern Sie Ihren Host, bevor Sie ein Upgrade durchführen, sodass Sie Ihren 5.x-Host wiederherstellen können, falls das Upgrade oder die Migration fehlschlägt.

Die Arbeitsabläufe des Assistenten verhindern fehlerhafte Upgrade-Sequenzen. Beispielsweise verhindert der Assistent, dass Sie die VM-Hardware vor den Hosts in einem Cluster aktualisieren.

Sie können mithilfe des Distributed Resource Schedulers (DRS) Ausfallzeiten virtueller Maschinen während des Upgrade-Prozesses verhindern.

Update Manager überwacht Hosts und virtuelle Maschinen auf Übereinstimmung mit Ihren definierten Upgrade-Baselines. Nichtübereinstimmungen werden in detaillierten Berichten und in der Dashboard-Ansicht aufgeführt. Update Manager unterstützt die Massenwartung.

Die folgenden vSphere-Komponenten werden von Update Manager aktualisiert.

- ESXi-Kernel (vmkernel)
- Hardware der virtuellen Maschine
- VMware Tools
- Virtuelle Appliances

Für Komponenten, die hier nicht aufgelistet sind, können Sie das Upgrade durchführen, indem Sie eine andere Upgrade-Methode verwenden. Für Drittanbieterkomponenten können Sie dazu die entsprechenden Drittanbieter-Tools verwenden.

In den folgenden Themen wird beschrieben, wie mit Update Manager ein koordiniertes Upgrade Ihrer ESXi-Hosts durchgeführt werden kann.

- [Konfigurieren von Host- und Clustereinstellungen](#)
- [Durchführen eines koordinierten Upgrades von Hosts mithilfe von vSphere Update Manager](#)

Informationen dazu, wie Sie mit Update Manager ein koordiniertes Upgrade der virtuellen Maschinen auf den Hosts durchführen, finden Sie unter der *Installieren und Verwalten von VMware vSphere Update Manager*-Dokumentation.

Konfigurieren von Host- und Clustereinstellungen

Wenn Sie vSphere-Objekte in einem Cluster mit aktiviertem vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA) und vSphere Fault Tolerance (FT) aktualisieren, können Sie vSphere Distributed Power Management (DPM), die HA-Zugangssteuerung und FT

für den gesamten Cluster vorübergehend deaktivieren. Wenn das Update abgeschlossen ist, stellt Update Manager diese Funktionen wieder her.

Updates erfordern möglicherweise, dass der Host bei der Wartung in den Wartungsmodus versetzt wird. Virtuelle Maschinen können nicht ausgeführt werden, wenn sich ein Host im Wartungsmodus befindet. Um die Verfügbarkeit sicherzustellen, kann vCenter Server virtuelle Maschinen auf andere ESXi-Hosts in einem Cluster migrieren, bevor der Host in den Wartungsmodus versetzt wird. vCenter Server migriert die virtuellen Maschinen, wenn der Cluster für vSphere vMotion konfiguriert und DRS aktiviert ist.

Wenn ein Host über keine ausgeführten virtuellen Maschinen verfügt, versetzt DPM den Host möglicherweise in den Standby-Modus und unterbricht somit einen Update Manager-Vorgang. Um sicherzustellen, dass die Prüf- und Staging-Vorgänge erfolgreich abgeschlossen werden, deaktiviert Update Manager während dieser Vorgänge DPM. Um die erfolgreiche Wartung sicherzustellen, sollte Update Manager DPM und die HA-Zugangssteuerung vor dem Wartungsvorgang deaktivieren. Nach Abschluss des Vorgangs stellt Update Manager DPM und die HA-Zugangssteuerung wieder her. Update Manager deaktiviert die HA-Zugangssteuerung vor dem Staging und der Wartung, aber nicht vor der Prüfung.

Wenn DPM Hosts bereits in den Standby-Modus versetzt hat, schaltet Update Manager die Hosts vor der Prüfung, dem Staging oder der Wartung ein. Nach Abschluss der Prüfung, des Stagings oder der Wartung schaltet Update Manager DPM und die HA-Zugangssteuerung ein und ermöglicht DPM ggf., die Hosts in den Standby-Modus zu versetzen. Update Manager wartet keine ausgeschalteten Hosts.

Wenn Hosts in den Standby-Modus versetzt werden und DPM aus irgendeinem Grund manuell deaktiviert wird, wartet Update Manager die Hosts nicht bzw. schaltet sie nicht ein.

Deaktivieren Sie die HA-Zugangssteuerung in einem Cluster vorübergehend, damit vSphere vMotion fortfahren kann. Dadurch werden Ausfallzeiten der Maschinen auf den von Ihnen gewarteten Hosts verhindert. Nach Abschluss der Wartung des gesamten Clusters stellt Update Manager die Einstellungen für die HA-Zugangssteuerung wieder her.

Wenn FT für virtuelle Maschinen auf Hosts in einem Cluster aktiviert ist, sollten Sie FT vorübergehend ausschalten, bevor Sie Update Manager-Vorgänge auf dem Cluster vornehmen. Wenn FT für die virtuellen Maschinen auf einem Host aktiviert ist, wartet Update Manager diesen Host nicht. Warten Sie alle Hosts in einem Cluster mit denselben Updates, damit FT nach der Wartung erneut aktiviert werden kann. Eine primäre virtuelle Maschine und eine sekundäre virtuelle Maschine können sich nicht auf Hosts mit unterschiedlicher ESXi-Version und unterschiedlichem Patch-Level befinden.

Beachten Sie bei der Wartung von Hosts, die Teil eines Virtual SAN-Clusters sind, folgendes Verhalten:

- Für den Vorgang der Hostwartung kann erheblicher Zeitaufwand erforderlich sein.
- Bedingt durch den Aufbau kann sich jeweils nur ein Host aus einem Virtual SAN-Cluster im Wartungsmodus befinden.

- Update Manager wartet nacheinander Hosts, die Teil eines Virtual SAN-Clusters sind, auch wenn Sie die Option für die gleichzeitige Wartung der Hosts festlegen.
- Wenn ein Host Mitglied eines Virtual SAN-Clusters ist und eine virtuelle Maschine auf dem Host eine VM-Speicherrichtlinie mit der Einstellung „Anzahl der zulässigen Fehler=0“ verwendet, kann es auf dem Host beim Wechsel in den Wartungsmodus zu ungewöhnlichen Verzögerungen kommen. Die Verzögerungen treten auf, weil das Virtual SAN die virtuelle Maschine im Virtual SAN-Datenspeicher-Cluster von einer Festplatte auf eine andere migrieren muss. Verzögerungen können einige Stunden dauern. Sie können dies vermeiden, indem Sie die Einstellung „Anzahl der zulässigen Fehler=1“ für die VM-Speicherrichtlinie festlegen. Dadurch werden zwei Kopien der Dateien virtueller Maschinen im Virtual SAN-Datenspeicher erstellt.

Durchführen eines koordinierten Upgrades von Hosts mithilfe von vSphere Update Manager

Mit vSphere Update Manager können Sie anhand einer einzelnen Upgrade-Baseline oder einer Baselinegruppe koordinierte Upgrades der ESXi-Hosts in Ihrer vSphere-Bestandsliste durchführen.

In diesem Workflow wird allgemein beschrieben, wie ein koordiniertes Upgrade auf Hosts in Ihrer vSphere-Bestandsliste durchgeführt wird. vSphere Update Manager 6.0 unterstützt Host-Upgrades auf ESXi 6.0 für Hosts, auf denen ESXi 5.x ausgeführt wird.

Koordinierte Upgrades von Hosts können auf der Ordner-, Cluster- oder Datencenterebene durchgeführt werden.

Hinweis Die letzten beiden Schritte in diesem Verfahren stellen Alternativen dar. Wählen Sie eine der beiden Optionen aus.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen für vCenter Server 6.0, ESXi 6.0 und vSphere Update Manager 6.0 erfüllt. Siehe [Upgrade von Update Manager-Server](#).
- Installieren Sie vCenter Server 6.0 oder führen Sie ein Upgrade auf diese Version durch. Siehe [Kapitel 4 Upgrade und Update von vCenter Server für Windows](#).
- Installieren Sie vSphere Update Manager 6.0 oder führen Sie ein Upgrade auf diese Version durch. Siehe [Kapitel 7 Upgrade von Update Manager](#).

Verfahren

1 Konfigurieren der Hosteinstellungen für den Wartungsmodus

ESXi-Host-Updates können möglicherweise erst aufgespielt werden, wenn der Host in den Wartungsmodus versetzt worden ist. Update Manager versetzt die ESXi-Hosts vor dem Anwenden dieser Updates in den Wartungsmodus. Sie können konfigurieren, wie Update Manager reagiert, wenn der Host nicht in den Wartungsmodus versetzt werden kann.

2 Konfigurieren von Clustereinstellungen

Für die ESXi-Hosts in einem Cluster kann der Standardisierungsvorgang entweder in einer Sequenz oder parallel ausgeführt werden. Bestimmte Funktionen können einen Standardisierungsfehler verursachen. Wenn VMware DPM, die HA-Zugangssteuerung oder die Fehlertoleranz aktiviert sind, sollten Sie diese Funktionen vorübergehend deaktivieren, um sicherzustellen, dass die Standardisierung erfolgreich verläuft.

3 Aktivieren der Standardisierung auf von PXE gestarteten ESXi-Hosts

Sie können Update Manager so konfigurieren, dass er eine andere Software die Standardisierung von durch PXE gestarteten ESXi-Hosts initiieren lässt. Die Standardisierung installiert Patches und Software-Module auf den Hosts, in der Regel gehen die Host-Updates jedoch nach einem Neustart verloren.

4 Importieren von Host-Upgrade-Images und Erstellen von Host-Upgrade-Baselines

Sie können Upgrade-Baselines für ESXi-Hosts mit ESXi 6.0-Images erstellen, die Sie in das Update Manager-Repository importieren.

5 Erstellen einer Host-Baselinegruppe

Sie können eine Host-Upgrade-Baseline mit mehreren Patch- oder Erweiterungs-Baselines kombinieren bzw. mehrere Patch- und Erweiterungs-Baselines in einer Baselinegruppe zusammenfassen.

6 Anhängen von Baselines und Baselinegruppen an Objekte

Zum Anzeigen der Übereinstimmungsinformation und Standardisieren von Objekten in der Bestandsliste anhand bestimmter Baselines und Baselinegruppen müssen Sie zunächst vorhandene Baselines und Baselinegruppen an diese Objekte anhängen.

7 Manuelles Initiieren einer Prüfung von ESXi-Hosts

Vor der Standardisierung sollten Sie die vSphere-Objekte anhand der angehängten Baselines und Baselinegruppen prüfen. Um sofort eine Prüfung von Hosts in der vSphere-Bestandsliste auszuführen, initiieren Sie diese manuell.

8 Anzeigen der Übereinstimmungsinformationen für vSphere-Objekte

Sie können die Übereinstimmungsinformationen für die virtuellen Maschinen, virtuellen Appliances und Hosts anhand von Baselines und Baselinegruppen, die Sie anhängen, überprüfen.

9 Standardisieren von Hosts anhand einer Upgrade-Baseline

Sie können ESXi-Hosts gleichzeitig anhand einer einzelnen angehängten Upgrade-Baseline standardisieren. Sie können alle Hosts in Ihrer vSphere-Bestandsliste unter Verwendung einer einzelnen Upgrade-Baseline aktualisieren, die ein ESXi 6.0-Image enthält.

10 Standardisieren von Hosts anhand von Baselinegruppen

Sie können Hosts mithilfe angehängter Gruppen von Upgrade-, Patch- und Erweiterungs-Baselines standardisieren. Baselinegruppen können mehrere Patch- und Erweiterungs-Baselines enthalten oder ein Upgrade-Baseline, das mit mehreren Patch- und Erweiterungs-Baselines kombiniert werden kann.

Konfigurieren der Hosteinstellungen für den Wartungsmodus

ESXi-Host-Updates können möglicherweise erst aufgespielt werden, wenn der Host in den Wartungsmodus versetzt worden ist. Update Manager versetzt die ESXi-Hosts vor dem Anwenden dieser Updates in den Wartungsmodus. Sie können konfigurieren, wie Update Manager reagiert, wenn der Host nicht in den Wartungsmodus versetzt werden kann.

Für Hosts in einem anderen Container als einem Cluster und für einzelne Hosts kann keine Migration der virtuellen Maschinen mit VMotion durchgeführt werden. Wenn vCenter Server die virtuellen Maschinen nicht auf einen anderen Host migrieren kann, können Sie konfigurieren, wie Update Manager reagiert.

Hosts, die Teil eines Virtual SAN-Clusters sind, können nicht gleichzeitig in den Wartungsmodus verschoben werden. Dies ist eine Besonderheit der Virtual SAN-Cluster.

Wenn ein Host Mitglied eines Virtual SAN-Clusters ist und eine virtuelle Maschine auf dem Host eine VM-Speicherrichtlinie mit der Einstellung „Anzahl der zulässigen Fehler=0“ verwendet, kann es auf dem Host beim Wechsel in den Wartungsmodus zu ungewöhnlichen Verzögerungen kommen. Die Verzögerungen treten auf, weil das Virtual SAN die virtuelle Maschine im Virtual SAN-Datenspeicher-Cluster von einer Festplatte auf eine andere migrieren muss. Verzögerungen können einige Stunden dauern. Sie können dies vermeiden, indem Sie die Einstellung „Anzahl der zulässigen Fehler=1“ für die VM-Speicherrichtlinie festlegen. Dadurch werden zwei Kopien der Dateien virtueller Maschinen im Virtual SAN-Datenspeicher erstellt.

Voraussetzungen

Erforderliche Rechte: **VMware vSphere Update Manager.Konfigurieren**

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.
- 2 Je nach Client, den Sie zum Herstellen der Verbindung zu vCenter Server verwenden, führen Sie folgende Schritte aus.

Client	Schritte
vSphere Web Client	1 Klicken Sie auf der Registerkarte Einstellungen unter „Verwalten“ auf Host-/Clustereinstellungen . Klicken Sie auf Bearbeiten .
vSphere Client	1 Klicken Sie auf der Registerkarte Konfiguration unter „Einstellungen“ auf ESXi-Host-/Clustereinstellungen .

- 3 Wählen Sie unter „Einstellungen für den Wartungsmodus“ eine Option aus dem Dropdown-Menü **VM-Betriebszustand** aus, um die Änderung des Betriebszustands der virtuellen Maschinen und Appliances zu ermitteln, die auf dem zu standardisierenden Host ausgeführt werden.

Option	Beschreibung
Virtuelle Maschinen ausschalten	Schalten Sie vor der Standardisierung alle virtuellen Maschinen und virtuellen Appliances aus.
Virtuelle Maschinen anhalten	Halten Sie vor der Standardisierung alle laufenden virtuellen Maschinen und virtuellen Appliances an.
VM-Betriebszustand nicht ändern	Belassen Sie die virtuellen Maschinen und virtuellen Appliances in ihrem aktuellen Betriebszustand. Dies ist die Standardeinstellung.

- 4 (Optional) Wählen Sie **Versuchen Sie im Falle eines Fehlschlags, erneut in den Wartungsmodus zu wechseln** und geben Sie die Verzögerung bis zur Wiederholung an sowie die Anzahl an Wiederholungen.

Falls ein Host vor der Standardisierung nicht in den Wartungsmodus wechseln kann, Update Manager wartet den Zeitraum der Verzögerung bis zur Wiederholung ab und versucht erneut, den Host in den Wartungsmodus zu versetzen. Dieser Vorgang wird so oft wiederholt, wie dies im Feld **Anzahl an Wiederholungen** angegeben ist.

- 5 (Optional) Wählen Sie die Option **Deaktivieren Sie vorübergehend alle Wechselmedien, die möglicherweise verhindern, dass ein Host in den Wartungsmodus versetzt wird**.

Update Manager standardisiert keine Hosts, auf denen sich virtuelle Maschinen befinden, die mit CD-/DVD- oder Diskettenlaufwerken verbunden sind. Mit den virtuellen Maschinen auf einem Host verbundene Wechselmedienlaufwerke verhindern möglicherweise, dass der Host in den Wartungsmodus versetzt wird, und unterbrechen die Standardisierung.

Nach der Standardisierung verbindet Update Manager die Wechselmedien neu, sofern diese noch verfügbar sind.

- 6 Klicken Sie auf **Akzeptieren**.

Ergebnisse

Diese Einstellungen werden zu den Standard-Fehlerantworteneinstellungen. Sie können beim Konfigurieren einzelner Standardisierungsaufgaben andere Einstellungen angeben.

Konfigurieren von Clustereinstellungen

Für die ESXi-Hosts in einem Cluster kann der Standardisierungsvorgang entweder in einer Sequenz oder parallel ausgeführt werden. Bestimmte Funktionen können einen Standardisierungsfehler verursachen. Wenn VMware DPM, die HA-Zugangssteuerung oder die Fehlertoleranz aktiviert

sind, sollten Sie diese Funktionen vorübergehend deaktivieren, um sicherzustellen, dass die Standardisierung erfolgreich verläuft.

Hinweis Das parallele Standardisieren von Hosts kann die Leistung signifikant verbessern, indem es die für die Cluster-Standardisierung benötigte Zeit reduziert. Update Manager standardisiert Hosts parallel, ohne gegen die von DRS festgelegten Einschränkungen für die Clusterressourcen zu verstoßen. Sehen Sie davon ab, Hosts parallel zu standardisieren, sofern die Hosts Teil eines Virtual SAN-Clusters sind. Aufgrund der besonderen Merkmale des Virtual SAN-Clusters kann ein Host nicht in den Wartungsmodus wechseln, solange sich andere Hosts im Cluster bereits im Wartungsmodus befinden.

Voraussetzungen

Erforderliche Rechte: **VMware vSphere Update Manager.Konfigurieren**

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.
- 2 Je nach Client, den Sie zum Herstellen der Verbindung zu vCenter Server verwenden, führen Sie folgende Schritte aus.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Verwalten unter „Einstellungen“ auf Host-/Clustereinstellungen. 2 Klicken Sie auf Bearbeiten.
vSphere Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Konfiguration unter „Einstellungen“ auf ESX-Host-/Clustereinstellungen.

- 3 Wählen Sie die Kontrollkästchen für die Funktionen aus, die Sie deaktivieren oder aktivieren möchten.

Option	Beschreibung
Distributed Power Management (DPM)	<p>VMware DPM überwacht die Ressourcennutzung der im Cluster ausgeführten virtuellen Maschinen. Wenn Überkapazitäten vorhanden sind, empfiehlt VMware DPM das Verschieben virtueller Maschinen auf andere Hosts im Cluster und das Versetzen des ursprünglichen Hosts in den Standby-Modus, um Energie zu sparen. Falls nicht genügend Kapazitäten vorhanden sind, empfiehlt VMware DPM möglicherweise die Reaktivierung von Hosts, die sich im Standby-Modus befinden.</p> <p>Wenn Sie DPM nicht deaktivieren, überspringt Update Manager das Cluster mit aktiviertem VMware DPM. Wenn Sie VMware DPM vorübergehend deaktivieren, deaktiviert Update Manager DPM auf dem Cluster, standardisiert die Hosts im Cluster und reaktiviert VMware DPM nach Abschluss der Standardisierung.</p>
HA-Zugangssteuerung	<p>Die Zugangssteuerung ist eine von VMware HA verwendete Richtlinie, um die Failover-Kapazität in einem Cluster zu gewährleisten. Wenn die HA-Zugangssteuerung während der Standardisierung aktiviert ist, werden die virtuellen Maschinen in einem Cluster möglicherweise nicht mit vMotion migriert.</p> <p>Wenn Sie die HA-Zugangssteuerung nicht deaktivieren, überspringt Update Manager das Cluster mit aktivierter HA-Zugangssteuerung. Wenn Sie die HA-Zugangssteuerung vorübergehend deaktivieren, deaktiviert Update Manager die HA-Zugangssteuerung, standardisiert das Cluster und reaktiviert die HA-Zugangssteuerung nach Abschluss der Standardisierung.</p>
Fault Tolerance (FT)	<p>Die VMware-Fehlertoleranz bietet eine unterbrechungsfreie Verfügbarkeit für virtuelle Maschinen durch die automatische Erstellung und Verwaltung einer sekundären virtuellen Maschine, die mit der primären virtuellen Maschine identisch ist. Wenn Sie FT für die virtuellen Maschinen auf einem Host nicht ausschalten möchten, standardisiert Update Manager diesen Host nicht.</p>
Parallele Standardisierung für Hosts im Cluster aktivieren	<p>Update Manager kann Hosts in Clustern parallel standardisieren. Update Manager berechnet kontinuierlich die maximale Anzahl an Hosts, die parallel standardisiert werden können, ohne gegen die DRS-Einstellungen zu verstoßen. Falls Sie die Einstellung nicht auswählen, standardisiert Update Manager die Hosts in einem Cluster sequenziell.</p> <p>Bedingt durch den Aufbau kann sich jeweils nur ein Host aus einem Virtual SAN-Cluster im Wartungsmodus befinden. Update Manager standardisiert nacheinander Hosts, die Teil eines Virtual SAN-Clusters sind, auch wenn Sie die Option auswählen, um sie gleichzeitig zu standardisieren.</p>
Migrieren Sie ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster, wenn ein Host in den Wartungsmodus wechseln muss	<p>Update Manager migriert die angehaltenen und ausgeschalteten virtuelle Maschinen von Hosts, die in den Wartungsmodus wechseln müssen, auf andere Hosts im Cluster. Sie können virtuelle Maschinen im Bereich „Einstellungen für den Wartungsmodus“ vor der Standardisierung ausschalten oder anhalten.</p>

- 4 Klicken Sie auf **Akzeptieren**.

Ergebnisse

Diese Einstellungen werden zu den Standard-Fehlerantworteseinstellungen. Sie können beim Konfigurieren einzelner Standardisierungsaufgaben andere Einstellungen angeben.

Aktiveren der Standardisierung auf von PXE gestarteten ESXi-Hosts

Sie können Update Manager so konfigurieren, dass er eine andere Software die Standardisierung von durch PXE gestarteten ESXi-Hosts initiieren lässt. Die Standardisierung installiert Patches und Software-Module auf den Hosts, in der Regel gehen die Host-Updates jedoch nach einem Neustart verloren.

Die globale Einstellung auf der Update Manager-Registerkarte **Konfiguration** ermöglicht, dass Lösungen wie z. B. ESX Agent Manager oder Cisco Nexus 1000V die Standardisierung von durch PXE gestarteten ESXi-Hosts initiieren. Dagegen ermöglicht die Einstellung **Patch-Standardisierung eingeschalteter, von PXE gestarteter ESXi-Hosts aktivieren** im **Standardisierungsassistenten** dem Update Manager das Patchen von durch PXE gestarteten Hosts.

Verwenden Sie zum Beibehalten von Updates auf statusfreien Hosts nach einem Neustart ein PXE-Start-Image, das die Updates enthält. Sie können das PXE-Start-Image vor dem Anwenden der Updates mit dem Update Manager aktualisieren, sodass die Updates nicht wegen eines Neustarts verloren gehen. Update Manager führt seinerseits keinen Neustart der Hosts aus, da er auf von PXE gestarteten ESXi-Hosts keine Updates installiert, die einen Neustart erfordern.

Voraussetzungen

Erforderliche Rechte: **VMware vSphere Update Manager.Konfigurieren**

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.
- 2 Je nach Client, den Sie zum Herstellen der Verbindung zu vCenter Server verwenden, führen Sie folgende Schritte aus.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Verwalten unter „Einstellungen“ auf Host-/Clustereinstellungen. 2 Klicken Sie auf Bearbeiten.
vSphere Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Konfiguration unter „Einstellungen“ auf ESX-Host-/Clustereinstellungen.

- 3 Wenn Sie die Installation von Software für Lösungen auf von PXE gestarteten ESXi-Hosts zulassen möchten, wählen Sie **Installation zusätzlicher Software auf von PXE gestarteten ESXi-Hosts zulassen**.
- 4 Klicken Sie auf **Akzeptieren**.

Importieren von Host-Upgrade-Images und Erstellen von Host-Upgrade-Baselines

Sie können Upgrade-Baselines für ESXi-Hosts mit ESXi 6.0-Images erstellen, die Sie in das Update Manager-Repository importieren.

Sie können ESXi .iso-Images verwenden, um ein Upgrade von ESXi 5.x-Hosts auf ESXi 6.0 durchzuführen.

Verwenden Sie für das Upgrade von Hosts das von VMware verteilte ESXi-Installer-Image mit dem Namensformat `VMware-VMvisor-Installer-6.0.0-Buildnummer.x86_64.iso` oder ein benutzerdefiniertes Image, das mithilfe von vSphere ESXi Image Builder erstellt wurde.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Berechtigung **Datei hochladen** verfügen. Weitere Informationen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter *vCenter Server und Hostverwaltung*.

Verbinden Sie den vSphere Client mit einem vCenter Server-System, bei dem der Update Manager registriert ist, und klicken Sie auf der Startseite im Symbol „Lösungen und Anwendungen“ auf **Update Manager**.

Verfahren

- 1 Klicken Sie auf der Registerkarte **ESXi-Images** oben rechts auf **ESXi-Image importieren**.
- 2 Wechseln Sie auf der Seite „ESXi-Image auswählen“ des Assistenten **ESXi-Image importieren** zu dem ESXi-Image, das Sie hochladen möchten, und wählen Sie es aus.
- 3 Klicken Sie auf **Weiter**.

Vorsicht Schließen Sie den Import-Assistenten nicht. Durch das Schließen des Import-Assistenten wird der Hochladevorgang nämlich gestoppt.

- 4 (Optional) Wählen Sie im Fenster **Sicherheitswarnung** eine Option zum Behandeln der Zertifikatswarnung aus.

Die Zertifikate, die während der Installation für vCenter Server und ESXi-Hosts erzeugt werden, sind nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert. Aus diesem Grund wird bei jeder SSL-Verbindung mit einem dieser Systeme auf dem Client eine Warnmeldung angezeigt.

Option	Aktion
Ignorieren	Klicken Sie auf Ignorieren , um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren und den Upload-Vorgang zu starten.
Abbrechen	Klicken Sie auf Abbrechen , um das Fenster zu schließen und den Upload-Vorgang zu stoppen.
Dieses Zertifikat installieren und keine Sicherheitswarnungen anzeigen	Wählen Sie dieses Kontrollkästchen und klicken Sie auf Ignorieren , um das Zertifikat zu installieren und um den Empfang von Sicherheitswarnungen zu beenden.

- 5 Klicken Sie nach dem Hochladen der Datei auf **Weiter**.
- 6 (Optional) Erstellen Sie eine Host-Upgrade-Baseline.
 - a Lassen Sie die Option **Erstellen einer Baseline mit dem ESXi-Image** ausgewählt.
 - b Geben Sie einen Namen und optional eine Beschreibung für die Host-Upgrade-Baseline ein.
- 7 Klicken Sie auf **Beenden**.

Ergebnisse

Das ESXi-Image, das Sie hochgeladen haben, wird im Bereich „Importierte ESXi-Images“ angezeigt. Im Bereich „Softwarepakete“ finden Sie weitere Informationen zu den Softwarepaketen, die im ESXi-Image enthalten sind.

Wenn Sie auch eine Host-Upgrade-Baseline erstellt haben, wird die neue Baseline im Bereich „Baselines“ der Registerkarte **Baselines und Gruppen** angezeigt.

Nächste Schritte

Zum Aktualisieren der Hosts in Ihrer Umgebung müssen Sie eine Host-Upgrade-Baseline erstellen, sofern Sie dies noch nicht getan haben.

Erstellen einer Host-Baselinegruppe

Sie können eine Host-Upgrade-Baseline mit mehreren Patch- oder Erweiterungs-Baselines kombinieren bzw. mehrere Patch- und Erweiterungs-Baselines in einer Baselinegruppe zusammenfassen.

Hinweis Sie können jederzeit auf **Beenden** im **Assistent „Neue Baselinegruppe“** klicken, um Ihre Baselinegruppe zu speichern. Sie können ihr dann zu einem späteren Zeitpunkt weitere Baselines hinzufügen.

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.
- 2 Klicken Sie auf der Registerkarte **Baselines und Gruppen** auf **Erstellen** (über dem Fenster „Baselinegruppen“).

- 3 Je nach Client, den Sie zum Herstellen der Verbindung zu vCenter Server verwenden, führen Sie folgende Schritte aus.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Host-Baselines unter Verwalten über dem Bereich „Baselinegruppen“ auf Erstellen. 2 Geben Sie einen eindeutigen Namen für die Baselinegruppe ein und klicken Sie auf Weiter.
vSphere Client	<ol style="list-style-type: none"> 1 Klicken Sie auf der Registerkarte Baselines und Gruppen über dem Bereich „Baselinegruppen“ auf Erstellen. 2 Geben Sie einen eindeutigen Namen für die Baselinegruppe ein. 3 Wählen Sie unter „Typ der Baselinegruppe“ die Option Host-Baselinegruppe und klicken Sie auf Weiter.

- 4 Wählen Sie eine Host-Upgrade-Baseline aus, um sie in die Baselinegruppe aufzunehmen.
- 5 (Optional) Falls Sie den vSphere Client verwenden, erstellen Sie eine neue Host-Upgrade-Baseline, indem Sie im unteren Teil der Seite „Upgrades“ auf **Neue Host-Upgrade-Baseline erstellen** klicken und die Schritte des Assistenten **Neue Baseline** ausführen.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie die Patch-Baselines aus, die Sie in die Baselinegruppe aufnehmen möchten.
- 8 (Optional) Falls Sie den vSphere Client verwenden, erstellen Sie eine neue Patch-Baseline, indem Sie im unteren Teil der Seite „Patches“ auf **Neue Host-Patch-Baseline erstellen** klicken und den Assistenten **Neue Baseline** abschließen.
- 9 Klicken Sie auf **Weiter**.
- 10 Wählen Sie die Erweiterungs-Baselines aus, die Sie in die Baselinegruppe aufnehmen möchten.
- 11 (Optional) Falls Sie den vSphere Client verwenden, erstellen Sie eine neue Erweiterungs-Baseline, indem Sie im unteren Teil der Seite „Patches“ auf **Eine neue Erweiterungs-Baseline erstellen** klicken und den Assistenten **Neue Baseline** abschließen.
- 12 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Ergebnisse

Die Host-Baselinegruppe wird in der Liste der Baselinegruppen angezeigt.

Anhängen von Baselines und Baselinegruppen an Objekte

Zum Anzeigen der Übereinstimmungsinformation und Standardisieren von Objekten in der Bestandsliste anhand bestimmter Baselines und Baselinegruppen müssen Sie zunächst vorhandene Baselines und Baselinegruppen an diese Objekte anhängen.

Sie können Baselines und Baselinegruppen über die Ansicht „Übereinstimmung“ des Update Manager-Clients an Objekte anhängen.

Sie können Baselines und Baselinegruppen an einzelne Objekte anhängen, effizienter ist es jedoch, sie an Containerobjekte wie Ordner, vApps, Cluster und Datacenter anzuhängen. Einzelne vSphere-Objekte übernehmen Baselines, die an das übergeordnete Containerobjekt angehängt sind. Beim Entfernen eines Objekts aus einem Container werden auch die übernommenen Baselines vom Objekt entfernt.

Wenn Ihr vCenter Server-System über eine gemeinsame vCenter Single Sign On-Domäne mit anderen vCenter Server-Systemen verbunden ist, können Sie Baselines und Baselinegruppen an Objekte anhängen, die von dem vCenter Server-System verwaltet werden, bei dem Update Manager registriert ist. Die Baselines und Baselinegruppen, die Sie anhängen, gelten für die Update Manager-Instanz, die bei dem vCenter Server-System registriert ist.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Berechtigung **Baseline anhängen** verfügen.

Verfahren

- 1 Verbinden Sie den vSphere Client mit einem vCenter Server-System, bei dem der Update Manager registriert ist, und wählen Sie **Home > Bestandsliste**.

- 2 Wählen Sie den Objekttyp aus, an den Sie die Baseline anhängen möchten.

Beispiele hierfür sind: **Hosts und Cluster** oder **VMs und Vorlagen**.

- 3 Wählen Sie das Objekt in der Bestandsliste aus und klicken Sie auf die Registerkarte **Update Manager**.

Wenn Ihr vCenter Server-System über eine gemeinsame vCenter Single Sign On-Domäne mit anderen vCenter Server-Systemen verbunden ist, wird die Registerkarte **Update Manager** nur für das vCenter Server-System angezeigt, bei dem eine Instanz von Update Manager registriert ist.

- 4 Klicken Sie in der oberen rechten Ecke auf **Anhängen**.

- 5 Wählen Sie im Fenster **Baseline oder Gruppe anhängen** eine oder mehrere Baselines oder Baselinegruppen aus, die an das Objekt angehängt werden sollen.

Wenn Sie eine oder mehrere Baselinegruppen auswählen, werden alle Baselines in den Gruppen ausgewählt. Sie können die Auswahl einzelner Baselines in einer Gruppe nicht aufheben.

- 6 (Optional) Klicken Sie auf den Link **Baselinegruppe erstellen** oder **Baseline erstellen**, um eine Baselinegruppe bzw. eine Baseline zu erstellen, und führen Sie die verbleibenden Schritte des entsprechenden Assistenten aus.

- 7 Klicken Sie auf **Anhängen**.

Ergebnisse

Die Baselines und Baselinegruppen, die Sie zum Anhängen ausgewählt haben, werden in den Fenstern „Angehängte Baselinegruppen“ und „Angehängte Baselines“ der Registerkarte **Update Manager** angezeigt.

Manuelles Initiieren einer Prüfung von ESXi-Hosts

Vor der Standardisierung sollten Sie die vSphere-Objekte anhand der angehängten Baselines und Baselinegruppen prüfen. Um sofort eine Prüfung von Hosts in der vSphere-Bestandsliste auszuführen, initiieren Sie diese manuell.

Verfahren

- 1 Verbinden Sie den vSphere-Client mit einem vCenter Server-System, bei dem der Update Manager registriert ist, und wählen Sie in der Navigationsleiste **Home > Bestandsliste > Hosts und Cluster**.
- 2 Klicken Sie mit der rechten Maustaste auf ein Host-, ein Datacenter- oder beliebiges Containerobjekt und wählen Sie **Auf Updates prüfen**.
- 3 Wählen Sie die Update-Typen aus, die geprüft werden sollen.
Sie können entweder auf **Patches und Erweiterungen** oder auf **Upgrades** prüfen.
- 4 Klicken Sie auf **Prüfen**.

Ergebnisse

Das ausgewählte Bestandslistenobjekt und alle seine untergeordneten Objekte werden anhand aller Patches, Erweiterungen und Upgrades in den angehängten Baselines geprüft. Je umfangreicher die virtuelle Infrastruktur ist und je weiter oben in der Objekthierarchie Sie die Prüfung initiieren, desto länger dauert der Vorgang.

Anzeigen der Übereinstimmungsinformationen für vSphere-Objekte

Sie können die Übereinstimmungsinformationen für die virtuellen Maschinen, virtuellen Appliances und Hosts anhand von Baselines und Baselinegruppen, die Sie anhängen, überprüfen.

Wenn Sie ein Containerobjekt auswählen, sehen Sie den Gesamtübereinstimmungsstatus der angehängten Baselines sowie alle einzelnen Übereinstimmungsstatus. Wenn Sie eine einzelne Baseline auswählen, die dem Containerobjekt angehängt ist, sehen Sie den Übereinstimmungsstatus der Baseline.

Wenn Sie eine einzelne virtuelle Maschine, eine einzelne Appliance oder einen einzelnen Host auswählen, sehen Sie den Gesamtübereinstimmungsstatus des ausgewählten Objekts anhand aller angehängten Baselines sowie die Anzahl der Updates. Wenn Sie dann eine einzelne Baseline auswählen, die diesem Objekt angehängt ist, sehen Sie die Anzahl der Updates gruppiert nach Übereinstimmungsstatus für diese Baseline.

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.
- 2 Wählen Sie den Objekttyp aus, dessen Übereinstimmungsinformationen Sie anzeigen möchten.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Abhängig von den Übereinstimmungsinformationen, die Sie angezeigt haben möchten, führen Sie folgende Schritte durch: <ol style="list-style-type: none"> a Um die Übereinstimmungsinformationen anzuzeigen, wählen Sie Start > Hosts und Cluster und wählen einen Host, einen Cluster, ein Datacenter oder eine vCenter Server-Instanz. b Um Übereinstimmungsinformationen zu virtuellen Maschinen anzuzeigen, wählen Sie Start > VMs und Vorlagen und wählen eine virtuelle Maschine, einen Ordner oder eine virtuelle Appliance. 2 Wählen Sie die Registerkarte Verwalten und dann die Registerkarte Update Manager.
vSphere Client	<ol style="list-style-type: none"> 1 Abhängig von den Übereinstimmungsinformationen, die Sie angezeigt haben möchten, führen Sie folgende Schritte durch: <ol style="list-style-type: none"> a Um die Übereinstimmungsinformationen anzuzeigen, wählen Sie Start > Bestandsliste > Hosts und Cluster und wählen einen Host, einen Cluster, ein Datacenter oder eine vCenter Server-Instanz. b Um Übereinstimmungsinformationen zu virtuellen Maschinen anzuzeigen, wählen Sie Start > Bestandsliste > VMs und Vorlagen und wählen eine virtuelle Maschine, einen Ordner oder eine virtuelle Appliance. 2 Wählen Sie die Registerkarte Update Manager aus.

- 3 Wählen Sie eine der angehängten Baselines, um die Übereinstimmungsinformationen für das Objekt zu dieser Baseline anzuzeigen.

Standardisieren von Hosts anhand einer Upgrade-Baseline

Sie können ESXi-Hosts gleichzeitig anhand einer einzelnen angehängten Upgrade-Baseline standardisieren. Sie können alle Hosts in Ihrer vSphere-Bestandsliste unter Verwendung einer einzelnen Upgrade-Baseline aktualisieren, die ein ESXi 6.0-Image enthält.

Hinweis Alternativ können Sie auch Hosts unter Verwendung einer Baselinegruppe aktualisieren. Weitere Informationen hierzu finden Sie unter [Standardisieren von Hosts anhand von Baselinegruppen](#).

Update Manager 6.0 unterstützt das Upgrade von ESXi 5.x auf ESXi 6.0. Host-Upgrades auf ESXi 5.0, ESXi 5.1 oder ESXi 5.5 werden nicht unterstützt.

Verwenden Sie für das Upgrade von Hosts das von VMware verteilte ESXi-Installer-Image mit dem Namensformat `VMware-VMvisor-Installer-6.0.0-Buildnummer.x86_64.iso` oder ein benutzerdefiniertes Image, das mithilfe von vSphere ESXi Image Builder erstellt wurde.

Softwaremodule von Drittanbietern auf einem ESXi 5.x-Host bleiben nach einem Upgrade auf ESXi 6.0 intakt.

Hinweis Bei einem nicht erfolgreichen Upgrade von ESXi 5.x auf ESXi 6.0 können Sie kein Rollback auf Ihre vorherige ESXi 5.x-Instanz durchführen.

Voraussetzungen

Um einen Host anhand einer Upgrade-Baseline zu standardisieren, hängen Sie die Baseline an den Host an.

Überprüfen Sie alle Prüfungsmeldungen im Fenster **Upgrade-Details** auf potenzielle Probleme mit Hardware, Drittanbieter-Software und auf Konfigurationsprobleme, die möglicherweise ein erfolgreiches Upgrade auf ESXi 6.0 verhindern.

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Wählen Sie Start > Hosts und Cluster aus. 2 Klicken Sie im Bestandslistenobjektnavigator mit der rechten Maustaste auf ein Datencenter, ein Cluster oder einen Host und wählen Sie Update Manager > Standardisieren. <p>Wenn Sie ein Containerobjekt auswählen, werden alle Hosts unter dem ausgewählten Objekt standardisiert.</p>
vSphere Client	<ol style="list-style-type: none"> 1 Wählen Sie in der Navigationsleiste Start > Bestandsliste > Hosts und Cluster. 2 Klicken Sie aus dem Objektnavigator mit der rechten Maustaste auf ein Datencenter, ein Cluster oder einen Host und wählen Sie Standardisieren. <p>Wenn Sie ein Containerobjekt auswählen, werden alle Hosts unter dem ausgewählten Objekt standardisiert.</p>

Der Standardisierungsassistent wird geöffnet.

- 2 Wählen Sie **Upgrade-Baselines**.
- 3 Wählen Sie auf der Seite „Standardisierungsauswahl“ des Standardisierungsassistenten die Upgrade-Baseline aus, die übernommen werden soll.
- 4 (Optional) Wählen Sie die Hosts aus, die Sie standardisieren möchten, und klicken Sie auf **Weiter**.
Wenn Sie einen einzelnen Host und kein Containerobjekt standardisieren möchten, wird der Host standardmäßig ausgewählt.
- 5 Akzeptieren Sie auf der Seite mit der Endbenutzer-Lizenzvereinbarung die Bedingungen und klicken Sie auf **Weiter**.

- 6 (Optional) Wählen Sie auf der Seite für das ESXi 6.0-Upgrade die Option zum Ignorieren von Warnungen über nicht unterstützte Geräte auf dem Host oder nicht mehr unterstützten VMFS-Datenspeicher aus, um mit der Standardisierung fortzufahren.

- 7 Klicken Sie auf **Weiter**.

- 8 Geben Sie auf der Seite „Zeitplan“ einen eindeutigen Namen für die Aufgabe und eine optionale Beschreibung an.

Die Zeit, die Sie für die geplante Aufgabe festlegen, ist die Zeit der vCenter Server-Instanz, mit der Update Manager verbunden ist.

- 9 Wählen Sie **Sofort**, um den Vorgang sofort nach Abschluss des Assistenten zu starten, oder geben Sie eine Uhrzeit zum Starten des Standardisierungsvorgangs an, und klicken Sie auf **Weiter**.

- 10 Auf der Seite „Standardisierungsoptionen für den Host“ können Sie im Dropdown-Menü **Betriebszustand** die Änderung des Betriebszustands der virtuellen Maschinen und virtuellen Appliances angeben, die auf den zu standardisierenden Hosts ausgeführt werden.

Option	Beschreibung
Virtuelle Maschinen ausschalten	Schalten Sie vor der Standardisierung alle virtuellen Maschinen und virtuellen Appliances aus.
Virtuelle Maschinen anhalten	Halten Sie vor der Standardisierung alle laufenden virtuellen Maschinen und virtuellen Appliances an.
VM-Betriebszustand nicht ändern	<p>Belassen Sie die virtuellen Maschinen und virtuellen Appliances in ihrem aktuellen Betriebszustand.</p> <p>Ein Host kann erst dann in den Wartungsmodus wechseln, wenn die virtuellen Maschinen auf dem Host ausgeschaltet, angehalten oder mit vMotion auf andere Hosts in einem DRS-Cluster migriert wurden.</p>

Für einige Updates ist es erforderlich, dass der Host vor der Standardisierung in den Wartungsmodus versetzt wird. Virtuelle Maschinen und Appliances können nicht ausgeführt werden, wenn sich ein Host im Wartungsmodus befindet.

Um die Ausfallzeit während der Hoststandardisierung, die auf Kosten der Verfügbarkeit der virtuellen Maschine geht, zu vermindern, können Sie angeben, dass die virtuellen Maschinen und virtuellen Appliances vor der Standardisierung heruntergefahren oder angehalten werden. Wenn Sie in einem DRS-Cluster die virtuellen Maschinen nicht ausschalten, dauert die Standardisierung länger, aber die virtuellen Maschinen stehen während des gesamten Standardisierungsvorgangs zur Verfügung, weil sie mit vMotion auf andere Hosts migriert werden.

- 11 (Optional) Wählen Sie die Option **Versuchen Sie im Falle eines Fehlschlags, erneut in den Wartungsmodus zu wechseln**, und geben Sie die Anzahl an Wiederholungen sowie die Wartezeit zwischen den wiederholten Versuchen an.

Update Manager wartet den Zeitraum der Verzögerung bis zur Wiederholung ab und versucht erneut, den Host in den Wartungsmodus zu versetzen. Dieser Vorgang wird so oft wiederholt, wie dies im Feld **Anzahl an Wiederholungen** angegeben ist.

- 12 (Optional) Wählen Sie **Alle mit den virtuellen Maschinen auf dem Host verbundenen Wechselmedien trennen**.

Update Manager standardisiert keine Hosts, auf denen sich virtuelle Maschinen befinden, die mit CD-, DVD- oder Diskettenlaufwerken verbunden sind. In einer Clusterumgebung verhindern verbundene Mediengeräte möglicherweise die Ausführung von vMotion, wenn der Zielhost nicht über ein identisches Gerät oder ein gemountetes ISO-Image verfügt, was wiederum den Quellhost daran hindert, in den Wartungsmodus zu wechseln.

Nach der Standardisierung verbindet Update Manager die Wechselmedien neu, sofern diese noch verfügbar sind.

- 13 Klicken Sie auf **Weiter**.

- 14 Bearbeiten Sie die Cluster-Standardisierungsoptionen.

Die Seite „Cluster-Standardisierungsoptionen“ ist nur dann verfügbar, wenn Sie Hosts in einem Cluster standardisieren.

Option	Details
Deaktivieren Sie das Distributed Power Management (DPM), falls es für einen der ausgewählten Cluster aktiviert ist.	Update Manager standardisiert keine Cluster mit aktivem DPM. DPM überwacht die Ressourcennutzung der im Cluster ausgeführten virtuellen Maschinen. Wenn Überkapazitäten vorhanden sind, empfiehlt DPM das Verschieben virtueller Maschinen auf andere Hosts im Cluster und versetzt den ursprünglichen Host in den Standby-Modus, um Energie zu sparen. Das Versetzen von Hosts in den Standby-Modus unterbricht möglicherweise die Standardisierung.
Deaktivieren Sie die High Availability Admission Control, falls sie für einen der ausgewählten Cluster aktiviert ist.	Update Manager standardisiert keine Cluster mit aktiver HA-Zugangssteuerung. Die Zugangssteuerung ist eine von VMware HA verwendete Richtlinie, um die Failover-Kapazität in einem Cluster zu gewährleisten. Wenn die HA-Zugangssteuerung während der Standardisierung aktiviert ist, werden die virtuellen Maschinen in einem Cluster möglicherweise nicht mit vMotion migriert.
Deaktivieren Sie Fault Tolerance (FT), wenn sie für die VMs auf den ausgewählten Hosts aktiviert ist.	Wenn FT für die virtuellen Maschinen auf einem Host aktiviert ist, standardisiert Update Manager diesen Host nicht. Für die Aktivierung von Fault Tolerance müssen die Hosts, auf denen die primären und sekundären virtuellen Maschinen ausgeführt werden, über dieselbe Version verfügen und auf ihnen müssen dieselben Patches installiert sein. Falls Sie unterschiedliche Patches auf diese Hosts anwenden, kann Fault Tolerance (FT) nicht reaktiviert werden.

Option	Details
Aktivieren Sie die parallele Standardisierung für die Hosts in den ausgewählten Clustern.	<p>Standardisieren Sie Hosts in Clustern auf parallele Art und Weise. Falls die Einstellung nicht ausgewählt ist, standardisiert Update Manager die Hosts in einem Cluster sequenziell.</p> <p>Bedingt durch den Aufbau kann sich jeweils nur ein Host aus einem Virtual SAN-Cluster im Wartungsmodus befinden. Update Manager standardisiert nacheinander Hosts, die Teil eines Virtual SAN-Clusters sind, auch wenn Sie die Option auswählen, um sie gleichzeitig zu standardisieren.</p> <p>Standardmäßig berechnet Update Manager kontinuierlich die maximale Anzahl an Hosts, die gleichzeitig standardisiert werden können, ohne gegen die DRS-Einstellungen zu verstoßen. Sie können die Anzahl an gleichzeitig standardisierten Hosts auf eine bestimmte Anzahl beschränken.</p> <hr/> <p>Hinweis Update Manager standardisiert nur die Hosts gleichzeitig, auf denen virtuelle Maschinen ausgeschaltet oder angehalten sind. Sie können virtuelle Maschinen über das Menü Betriebszustand im Bereich „Einstellungen für den Wartungsmodus“ auf der Seite „Standardisierungsoptionen für den Host“ ausschalten oder anhalten.</p>
Migrieren Sie ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster, wenn ein Host in den Wartungsmodus wechseln muss.	<p>Update Manager migriert die angehaltenen und ausgeschalteten virtuellen Maschinen von Hosts, die in den Wartungsmodus wechseln müssen, auf andere Hosts im Cluster. Sie können virtuelle Maschinen im Bereich „Einstellungen für den Wartungsmodus“ vor der Standardisierung ausschalten oder anhalten.</p>

15 (Optional) Generieren Sie einen Bericht zu den Cluster-Standardisierungsoptionen, indem Sie auf der Seite „Cluster-Standardisierungsoptionen“ auf **Bericht generieren** und anschließend auf **Weiter** klicken.

16 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Beispiel

Hinweis Im Bereich „Aktuelle Aufgaben“ wird die Standardisierungsaufgabe angezeigt und verbleibt beim größten Teil der Aufgabe bei etwa 22 Prozent. Der Vorgang wird weiterhin ausgeführt und benötigt etwa 15 Minuten, bis er abgeschlossen ist.

Standardisieren von Hosts anhand von Baselinegruppen

Sie können Hosts mithilfe angehängter Gruppen von Upgrade-, Patch- und Erweiterungs-Baselines standardisieren. Baselinegruppen können mehrere Patch- und Erweiterungs-Baselines enthalten oder ein Upgrade-Baseline, das mit mehreren Patch- und Erweiterungs-Baselines kombiniert werden kann.

Sie können ein koordiniertes Upgrade unter Verwendung einer Host-Baselinegruppe durchführen. Die Upgrade-Baseline in der Baselinegruppe wird zuerst und anschließend werden die Patch- und Erweiterungs-Baselines ausgeführt.

Hinweis Alternativ können Sie auch Hosts unter Verwendung einer einzelnen Upgrade-Baseline aktualisieren. Weitere Informationen hierzu finden Sie unter [Standardisieren von Hosts anhand einer Upgrade-Baseline](#).

Voraussetzungen

Stellen Sie sicher, dass mindestens eine Baselinegruppe an den Host angehängt ist.

Überprüfen Sie alle Prüfungsmeldungen im Fenster **Upgrade-Details** auf potenzielle Probleme mit Hardware, Drittanbieter-Software und auf Konfigurationsprobleme, die möglicherweise ein erfolgreiches Upgrade auf ESXi 6.0 verhindern.

Verfahren

- 1 Verwenden Sie den vSphere Client oder den vSphere Web Client, um sich mit einem vCenter Server-System zu verbinden, bei dem Update Manager registriert ist.

Client	Schritte
vSphere Web Client	<ol style="list-style-type: none"> 1 Wählen Sie Start > Hosts und Cluster aus. 2 Klicken Sie im Bestandslistenobjektnavigator mit der rechten Maustaste auf ein Datencenter, ein Cluster oder einen Host und wählen Sie Update Manager > Standardisieren. <p>Wenn Sie ein Containerobjekt auswählen, werden alle Hosts unter dem ausgewählten Objekt standardisiert.</p>
vSphere Client	<ol style="list-style-type: none"> 1 Wählen Sie in der Navigationsleiste Start > Bestandsliste > Hosts und Cluster. 2 Klicken Sie aus dem Objektnavigator mit der rechten Maustaste auf ein Datencenter, ein Cluster oder einen Host und wählen Sie Standardisieren. <p>Wenn Sie ein Containerobjekt auswählen, werden alle Hosts unter dem ausgewählten Objekt standardisiert.</p> <p>Wenn Sie ein Containerobjekt auswählen, werden alle Hosts unter dem ausgewählten Objekt standardisiert.</p>

Der Standardisierungsassistent wird geöffnet.

- 2 Wählen Sie auf der Seite „Standardisierungsauswahl“ des **Standardisierungsassistenten** die Baselinegruppe und Baselines aus, die übernommen werden sollen.

- 3 (Optional) Wählen Sie die Hosts aus, die Sie standardisieren möchten, und klicken Sie auf **Weiter**.

Wenn Sie einen einzelnen Host und kein Containerobjekt standardisieren möchten, wird der Host standardmäßig ausgewählt.

- 4 Akzeptieren Sie auf der Seite mit der Endbenutzer-Lizenzvereinbarung die Bedingungen und klicken Sie auf **Weiter**.

- 5 (Optional) Wählen Sie auf der Seite für das ESXi 6.0-Upgrade die Option zum Ignorieren von Warnungen über nicht unterstützte Geräte auf dem Host oder nicht mehr unterstützten VMFS-Datenspeicher aus, um mit der Standardisierung fortzufahren.

- 6 Klicken Sie auf **Weiter**.

- 7 (Optional) Deaktivieren Sie auf der Seite „Patches und Erweiterungen“ bestimmte Patches oder Erweiterungen, die Sie vom Standardisierungsprozess ausschließen möchten, und klicken Sie auf **Weiter**.

- 8 (Optional) Überprüfen Sie auf der Seite „Dynamische Patches und Erweiterungen, die ausgeschlossen werden sollen“ die Liste der auszuschließenden Patches oder Erweiterungen und klicken Sie auf **Weiter**.

- 9 Geben Sie auf der Seite „Zeitplan“ einen eindeutigen Namen für die Aufgabe und eine optionale Beschreibung an.

Die Zeit, die Sie für die geplante Aufgabe festlegen, ist die Zeit der vCenter Server-Instanz, mit der Update Manager verbunden ist.

- 10 Wählen Sie **Sofort**, um den Vorgang sofort nach Abschluss des Assistenten zu starten, oder geben Sie eine Uhrzeit zum Starten des Standardisierungsvorgangs an, und klicken Sie auf **Weiter**.

- 11 Auf der Seite „Standardisierungsoptionen für den Host“ können Sie im Dropdown-Menü **Betriebszustand** die Änderung des Betriebszustands der virtuellen Maschinen und virtuellen Appliances angeben, die auf den zu standardisierenden Hosts ausgeführt werden.

Option	Beschreibung
Virtuelle Maschinen ausschalten	Schalten Sie vor der Standardisierung alle virtuellen Maschinen und virtuellen Appliances aus.
Virtuelle Maschinen anhalten	Halten Sie vor der Standardisierung alle laufenden virtuellen Maschinen und virtuellen Appliances an.
VM-Betriebszustand nicht ändern	Belassen Sie die virtuellen Maschinen und virtuellen Appliances in ihrem aktuellen Betriebszustand. Ein Host kann erst dann in den Wartungsmodus wechseln, wenn die virtuellen Maschinen auf dem Host ausgeschaltet, angehalten oder mit vMotion auf andere Hosts in einem DRS-Cluster migriert wurden.

Für einige Updates ist es erforderlich, dass der Host vor der Standardisierung in den Wartungsmodus versetzt wird. Virtuelle Maschinen und Appliances können nicht ausgeführt werden, wenn sich ein Host im Wartungsmodus befindet.

Um die Ausfallzeit während der Hoststandardisierung, die auf Kosten der Verfügbarkeit der virtuellen Maschine geht, zu vermindern, können Sie angeben, dass die virtuellen Maschinen und virtuellen Appliances vor der Standardisierung heruntergefahren oder angehalten werden. Wenn Sie in einem DRS-Cluster die virtuellen Maschinen nicht ausschalten, dauert die Standardisierung länger, aber die virtuellen Maschinen stehen während des gesamten Standardisierungsvorgangs zur Verfügung, weil sie mit vMotion auf andere Hosts migriert werden.

- 12 (Optional) Wählen Sie die Option **Versuchen Sie im Falle eines Fehlschlags, erneut in den Wartungsmodus zu wechseln**, und geben Sie die Anzahl an Wiederholungen sowie die Wartezeit zwischen den wiederholten Versuchen an.

Update Manager wartet den Zeitraum der Verzögerung bis zur Wiederholung ab und versucht erneut, den Host in den Wartungsmodus zu versetzen. Dieser Vorgang wird so oft wiederholt, wie dies im Feld **Anzahl an Wiederholungen** angegeben ist.

13 (Optional) Wählen Sie **Alle mit den virtuellen Maschinen auf dem Host verbundenen Wechselmedien trennen.**

Update Manager standardisiert keine Hosts, auf denen sich virtuelle Maschinen befinden, die mit CD-, DVD- oder Diskettenlaufwerken verbunden sind. In einer Clusterumgebung verhindern verbundene Mediengeräte möglicherweise die Ausführung von vMotion, wenn der Zielhost nicht über ein identisches Gerät oder ein gemountetes ISO-Image verfügt, was wiederum den Quellhost daran hindert, in den Wartungsmodus zu wechseln.

Nach der Standardisierung verbindet Update Manager die Wechselmedien neu, sofern diese noch verfügbar sind.

14 (Optional) Aktivieren Sie das Kontrollkästchen unter „ESXi-Patch-Einstellungen“, um Update Manager das Patchen von eingeschalteten, von PXE gestarteten ESXi-Hosts zu ermöglichen.

Diese Option wird nur dann angezeigt, wenn Sie Hosts unter Verwendung von Patch- oder Erweiterungs-Baselines standardisieren.

15 Klicken Sie auf **Weiter.**

16 Bearbeiten Sie die Cluster-Standardisierungsoptionen.

Die Seite „Cluster-Standardisierungsoptionen“ ist nur dann verfügbar, wenn Sie Hosts in einem Cluster standardisieren.

Option	Details
Deaktivieren Sie das Distributed Power Management (DPM), falls es für einen der ausgewählten Cluster aktiviert ist.	Update Manager standardisiert keine Cluster mit aktivem DPM. DPM überwacht die Ressourcennutzung der im Cluster ausgeführten virtuellen Maschinen. Wenn Überkapazitäten vorhanden sind, empfiehlt DPM das Verschieben virtueller Maschinen auf andere Hosts im Cluster und versetzt den ursprünglichen Host in den Standby-Modus, um Energie zu sparen. Das Versetzen von Hosts in den Standby-Modus unterbricht möglicherweise die Standardisierung.
Deaktivieren Sie die High Availability Admission Control, falls sie für einen der ausgewählten Cluster aktiviert ist.	Update Manager standardisiert keine Cluster mit aktiver HA-Zugangssteuerung. Die Zugangssteuerung ist eine von VMware HA verwendete Richtlinie, um die Failover-Kapazität in einem Cluster zu gewährleisten. Wenn die HA-Zugangssteuerung während der Standardisierung aktiviert ist, werden die virtuellen Maschinen in einem Cluster möglicherweise nicht mit vMotion migriert.
Deaktivieren Sie Fault Tolerance (FT), wenn sie für die VMs auf den ausgewählten Hosts aktiviert ist.	Wenn FT für die virtuellen Maschinen auf einem Host aktiviert ist, standardisiert Update Manager diesen Host nicht. Für die Aktivierung von Fault Tolerance müssen die Hosts, auf denen die primären und sekundären virtuellen Maschinen ausgeführt werden, über dieselbe Version verfügen und auf ihnen müssen dieselben Patches installiert sein. Falls Sie unterschiedliche Patches auf diese Hosts anwenden, kann Fault Tolerance (FT) nicht reaktiviert werden.

Option	Details
Aktivieren Sie die parallele Standardisierung für die Hosts in den ausgewählten Clustern.	<p>Standardisieren Sie Hosts in Clustern auf parallele Art und Weise. Falls die Einstellung nicht ausgewählt ist, standardisiert Update Manager die Hosts in einem Cluster sequenziell.</p> <p>Bedingt durch den Aufbau kann sich jeweils nur ein Host aus einem Virtual SAN-Cluster im Wartungsmodus befinden. Update Manager standardisiert nacheinander Hosts, die Teil eines Virtual SAN-Clusters sind, auch wenn Sie die Option auswählen, um sie gleichzeitig zu standardisieren.</p> <p>Standardmäßig berechnet Update Manager kontinuierlich die maximale Anzahl an Hosts, die gleichzeitig standardisiert werden können, ohne gegen die DRS-Einstellungen zu verstoßen. Sie können die Anzahl an gleichzeitig standardisierten Hosts auf eine bestimmte Anzahl beschränken.</p> <hr/> <p>Hinweis Update Manager standardisiert nur die Hosts gleichzeitig, auf denen virtuelle Maschinen ausgeschaltet oder angehalten sind. Sie können virtuelle Maschinen über das Menü Betriebszustand im Bereich „Einstellungen für den Wartungsmodus“ auf der Seite „Standardisierungsoptionen für den Host“ ausschalten oder anhalten.</p>
Migrieren Sie ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster, wenn ein Host in den Wartungsmodus wechseln muss.	<p>Update Manager migriert die angehaltenen und ausgeschalteten virtuellen Maschinen von Hosts, die in den Wartungsmodus wechseln müssen, auf andere Hosts im Cluster. Sie können virtuelle Maschinen im Bereich „Einstellungen für den Wartungsmodus“ vor der Standardisierung ausschalten oder anhalten.</p>

17 (Optional) Generieren Sie einen Bericht zu den Cluster-Standardisierungsoptionen, indem Sie auf der Seite „Cluster-Standardisierungsoptionen“ auf **Bericht generieren** und anschließend auf **Weiter** klicken.

18 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Beispiel

Hinweis Im Bereich „Aktuelle Aufgaben“ wird die Standardisierungsaufgabe angezeigt und verbleibt beim größten Teil der Aufgabe bei etwa 22 Prozent. Der Vorgang wird weiterhin ausgeführt und benötigt etwa 15 Minuten, bis er abgeschlossen ist.

Installieren oder Upgraden von Hosts mithilfe eines Skripts

Mithilfe von automatischen Skriptinstallationen oder -Upgrades können Sie ESXi-Hosts schnell bereitstellen. Skriptinstallationen oder -Upgrades bieten eine effiziente Möglichkeit zum Bereitstellen mehrerer Hosts.

Das Installations- oder Upgrade-Skript enthält die Installationseinstellungen für ESXi. Sie können das Skript für alle Hosts anwenden, die eine ähnliche Konfiguration haben sollen.

Für Skriptinstallationen oder -Upgrades müssen Sie die unterstützten Befehle verwenden, um ein Skript zu erstellen. Sie können das Skript bearbeiten, um Einstellungen zu ändern, die für jeden einzelnen Host unterschiedlich sind.

Das Installations- oder Upgrade-Skript kann sich an einem der folgenden Speicherorte befinden:

- FTP-Server
- HTTP/HTTPS-Server
- NFS-Server
- USB-Flash-Laufwerk
- CD-ROM-Laufwerk

Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts

Sie können ein Installations- oder Upgrade-Skript starten, indem Sie Start-Befehlszeilenoptionen in die Start-Befehlszeile des ESXi-Installationsprogramms eingeben.

Beim Starten müssen Sie möglicherweise Optionen zum Aktivieren des Zugriffs auf die Kickstart-Datei angeben. Sie können Startoptionen eingeben, indem Sie im Bootloader Shift+O drücken. Für eine Installation per PXE-Startvorgang können Sie Optionen über die Zeile `kernelopts` der Datei `boot.cfg` übergeben. Siehe [Grundlegende Informationen zur Datei „boot.cfg“](#) und [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#).

Um den Speicherort des Installationsskripts anzugeben, legen Sie die Option `ks=filepath` fest, wobei `filepath` den Speicherort der Kickstart-Datei angibt. Andernfalls kann eine Skriptinstallation bzw. ein Skript-Upgrade nicht starten. Wenn `ks=filepath` ausgelassen wird, wird das Textinstallationsprogramm ausgeführt.

Unterstützte Startoptionen werden in [Startoptionen](#) aufgelistet.

Verfahren

- 1 Starten Sie den Host.
- 2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



- 3 Geben Sie an der `runweasel`-Eingabeaufforderung **`ks=Speicherort des Installationsskripts und die Start-Befehlszeilenoptionen`** ein.

Beispiel: Startoption

Sie geben die folgenden Startoptionen ein:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Startoptionen

Wenn Sie eine Skriptinstallation ausführen, müssen Sie möglicherweise beim Starten Optionen angeben, um auf die Kickstart-Datei zugreifen zu können.

Unterstützte Startoptionen

Tabelle 9-1. Startoptionen für die ESXi-Installation

Startoption	Beschreibung
<code>BOOTIF=hwtype-MAC-Adresse</code>	Ähnlich der Option <code>netdevice</code> , außer dass das PXELINUX-Format verwendet wird, wie in der Option <code>IPAPPEND</code> unter SYSLINUX auf der Website syslinux.zytor.com beschrieben.
<code>gateway=IP-Adresse</code>	Legt dieses Netzwerk-Gateway als Standard-Gateway für den Download des Installationskripts und der Installationsmedien fest.
<code>ip=IP-Adresse</code>	Richtet eine statische IP-Adresse ein, die zum Herunterladen des Installationskripts und der Installationsmedien verwendet wird. Hinweis: Das PXELINUX-Format für diese Option wird auch unterstützt. Weitere Informationen finden Sie unter der Option <code>IPAPPEND</code> unter SYSLINUX auf der Website syslinux.zytor.com .
<code>ks=cdrom:/Pfad</code>	Führt eine Skriptinstallation anhand des Skripts unter <i>Pfad</i> durch, das sich auf der CD im CD-ROM-Laufwerk befindet. Jede CD-ROM wird gemountet und so lange geprüft, bis die Datei, die dem Pfad entspricht, gefunden wird. Wichtig Wenn Sie ein ISO-Image des Installationsprogramms mit einem benutzerdefinierten Installations- oder Upgradeskript erstellt haben, müssen Sie den Skriptpfad in Großbuchstaben eingeben, zum Beispiel <code>ks=cdrom:/KS_CUST.CFG</code> .
<code>ks=file://Pfad</code>	Führt eine Skriptinstallation anhand des Skripts unter <i>Pfad</i> aus.
<code>ks=Protokoll://ServerPfad</code>	Führt eine Skriptinstallation anhand eines Skripts aus, das sich im Netzwerk an der angegebenen URL befindet. <i>Protokoll</i> kann <code>http</code> , <code>https</code> , <code>ftp</code> oder <code>nfs</code> sein. Ein Beispiel für die Verwendung von NFS-Protokollen ist <code>ks=nfs://Host/PortURL-Pfad</code> . Das Format einer NFS-URL wird in RFC 2224 festgelegt.

Tabelle 9-1. Startoptionen für die ESXi-Installation (Fortsetzung)

Startoption	Beschreibung
<code>ks=usb</code>	Führt eine Skriptinstallation anhand eines Skripts auf einem angeschlossenen USB-Laufwerk aus. Sucht nach einer Datei namens <code>ks.cfg</code> . Die Datei muss sich im Stammverzeichnis des Laufwerks befinden. Falls mehrere USB-Flash-Laufwerke angeschlossen sind, werden sie so lange durchsucht, bis die Datei <code>ks.cfg</code> gefunden wird. Nur FAT16- und FAT32-Dateisysteme werden unterstützt.
<code>ks=usb:/Pfad</code>	Führt eine Skriptinstallation anhand der Skriptdatei auf dem angegebenen Pfad durch, der sich auf einem USB-Laufwerk befindet.
<code>ksdevice=Gerät</code>	Versucht, ein Netzwerkadapter- <i>Gerät</i> bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00:50:56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
<code>nameserver=IP-Adresse</code>	Gibt einen DNS-Server an, der zum Herunterladen des Installationsskripts und der Installationsmedien verwendet wird.
<code>netdevice=Gerät</code>	Versucht, ein Netzwerkadapter- <i>Gerät</i> bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00:50:56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
<code>netmask=Subnetzmaske</code>	Gibt die Subnetzmaske für die Netzwerkkarte an, über die das Installationsskript und das Installationsmedium heruntergeladen wird.
<code>vlanid=vlanid</code>	Konfigurieren Sie die Netzwerkkarte, sodass sie auf dem angegebenen VLAN verwendet werden kann.

Grundlegendes zu Installations- und Upgrade-Skripts

Das Installations- bzw. Upgrade-Skript ist eine Textdatei, z. B. `ks.cfg`, die unterstützte Befehle enthält.

Der Befehlsabschnitt des Skripts enthält die ESXi-Installationsoptionen. Dieser Abschnitt ist zwingend. Er muss der erste Abschnitt im Skript sein.

Unterstützte Speicherorte für Installations- oder Upgrade-Skripts

Im Falle von Installationen und Upgrades, die per Skript durchgeführt wurden, kann das ESXi-Installationsprogramm von mehreren Speicherorten aus auf das Installations- bzw. Upgrade-Skript, das auch als Kickstart-Datei bezeichnet wird, zugreifen.

Die folgenden Speicherorte werden für Installations- oder Upgrade-Skripts unterstützt:

- CD/DVD. Weitere Informationen hierzu finden Sie unter [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#).
- USB-Flash-Laufwerk. Weitere Informationen hierzu finden Sie unter [Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts](#).
- Ein Netzwerkspeicherort, auf den mithilfe der folgenden Protokolle zugegriffen werden kann: NFS, HTTP, HTTPS und FTP

Pfad des Installations- oder Upgrade-Skripts

Sie können den Pfad eines Installations- oder Upgrade-Skripts angeben.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` ist der Pfad des ESXi-Installationsskripts, wobei `XXX.XXX.XXX.XXX` die IP-Adresse der Maschine ist, auf der sich das Skript befindet. Weitere Informationen hierzu finden Sie unter [Grundlegendes zu Installations- und Upgrade-Skripts](#).

Zum Starten eines Installationsskripts aus einer interaktiven Installation müssen Sie die Option `ks=` manuell eingeben. Weitere Informationen hierzu finden Sie unter [Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts](#).

Installation und Upgrade von Skriptbefehlen

Um das Standardinstallationsskript zu modifizieren, ein Skript zu aktualisieren oder ein eigenes Skript zu erstellen, verwenden Sie unterstützte Befehle. Verwenden Sie unterstützte Befehle im Installationsskript, das Sie mit einem Startbefehl angeben, wenn Sie das Installationsprogramm starten.

Um festzustellen, auf welcher Festplatte ESXi installiert oder aktualisiert werden soll, benötigt das Installationsskript einen der folgenden Befehle: `install`, `upgrade` oder `installorupgrade`. Der Befehl `install` erstellt die Standardpartitionen mit einem VMFS-Datenspeicher, der den gesamten Speicherplatz belegt, der nach der Erstellung der anderen Partitionen verfügbar ist.

accepteula/vmaccepteula (erforderlich)

Akzeptiert die ESXi-Lizenzvereinbarung.

clearpart (optional)

Löscht alle vorhandenen Partitionen auf der Festplatte. Setzt voraus, dass der Befehl `install` angegeben wird. Bearbeiten Sie den Befehl `clearpart` in Ihren vorhandenen Skripten mit Bedacht.

<code>--drives=</code>	Entfernt Partitionen auf den angegebenen Laufwerken.
<code>--alldrives</code>	Ignoriert die Bedingung <code>--drives=</code> und erlaubt das Löschen von Partitionen auf allen Laufwerken.
<code>--ignoredrives=</code>	Entfernt Partitionen auf allen außer den angegebenen Laufwerken. Erforderlich, es sei denn, das Flag <code>--drives=</code> oder <code>--alldrives</code> wurde angegeben.
<code>--overwritevmfs</code>	Erlaubt das Überschreiben von VMFS-Partitionen auf den angegebenen Laufwerken. Standardmäßig ist das Überschreiben von VMFS-Partitionen nicht erlaubt.
<code>--firstdisk=</code> <i>disk-type1</i> <i>[disk-type2,...]</i>	Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet: <ol style="list-style-type: none"> 1 Lokal angehängter Speicher (<code>local</code>) 2 Netzwerkspeicher (<code>remote</code>) 3 USB-Festplatten (<code>usb</code>) <p>Sie können die Reihenfolge der Festplatten durch eine kommasetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben. Dazu gehören <code>esx</code> für die erste Festplatte, auf der ESXi installiert ist, Modell- und Anbieterinformationen sowie der Name des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den <code>mptsas</code>-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument <code>--firstdisk=ST3120814A,mptsas,local an</code>.</p>

dryrun (optional)

Analysiert und überprüft das Installationsskript. Führt die Installation nicht aus.

Installieren

Gibt an, dass es sich um eine Neuinstallation handelt. Ersetzt den auslaufenden Befehl `autopart` in Skriptinstallationen von ESXi 4.1. Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk=` or `--drive=` Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=diskname` kann der *Festplattenname* eine der folgenden Formen haben:

- Pfad: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- MPX-Name: `--disk=mpx.vmhba1:C0:T0:L0`
- VML-Name: `--disk=vml.000000034211234`
- vmkLUN-UID: `--disk=vmkLUN_UID`

Die Formate der angenommenen Laufwerksnamen finden Sie unter [Festplattengerätenamen](#).

`--firstdisk=`
`disk-type1,`
`[disk-type2,...]`

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

- 1 Lokal angehängter Speicher (`local`)
- 2 Netzwerkspeicher (`remote`)
- 3 USB-Festplatten (`usb`)

Sie können die Reihenfolge der Festplatten durch eine kommasetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den `mptsas`-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local an`.

`--ignoressd`

Schließt Solid-State-Laufwerke aus der Partitionierung aus. Diese Option kann mit dem Befehl `install` und der Option `--firstdisk` verwendet werden. Diese Option hat Vorrang vor der Option `--firstdisk`. Bei der Verwendung der Option `--drive` oder `--disk` und der Befehle `upgrade` und `installorupgrade` ist sie nicht zulässig. Weitere Informationen zum Verhindern der Formatierung

von SSD-Laufwerken während der automatischen Partitionierung finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevsan

Sie müssen die Option `--overwritevsan` verwenden, wenn Sie ESXi auf einer SSD- oder HDD-Festplatte in einer Virtual SAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine Virtual SAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer Virtual SAN-Festplattengruppe gehört, hängt das Ergebnis von der ausgewählten Festplatte ab:

- Wenn Sie ein SSD-Laufwerk auswählen, werden das SSD-Laufwerk und alle untergeordneten Festplatten (HDD) in derselben Festplattengruppe gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe mehr als zwei Festplatten befinden, wird nur die ausgewählte Festplatte gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe maximal zwei Festplatten befinden, werden das SSD-Laufwerk und die ausgewählte Festplatte gelöscht.

Weitere Informationen zur Verwaltung von Virtual SAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevmfs

Wird benötigt, um vor der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte zu überschreiben.

--preservevmfs

Behält während der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte bei.

--novmfsdisk

Verhindert, dass eine VMFS-Partition auf dieser Festplatte erstellt wird. Muss mit `--overwritevmfs` verwendet werden, wenn eine VMFS-Partition bereits auf der Festplatte vorhanden ist.

installorupgrade

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

--disk= or --drive=

Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=diskname` kann der *Festplattenname* eine der folgenden Formen haben:

- Pfad: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- MPX-Name: `--disk=mpx.vmhba1:C0:T0:L0`

- VML-Name: `--disk=vm1.000000034211234`
- vmkLUN-UID: `--disk=vmkLUN_UID`

Die Formate der angenommenen Laufwerksnamen finden Sie unter [Festplattengerätenamen](#).

`--firstdisk=`
`disk-type1,`
`[disk-type2,...]`

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

- 1 Lokal angehängter Speicher (`local`)
- 2 Netzwerkspeicher (`remote`)
- 3 USB-Festplatten (`usb`)

Sie können die Reihenfolge der Festplatten durch eine kommasetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den `mptsas`-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local an`.

`--overwritevsan`

Sie müssen die Option `--overwritevsan` verwenden, wenn Sie ESXi auf einer SSD- oder HDD-Festplatte in einer Virtual SAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine Virtual SAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer Virtual SAN-Festplattengruppe gehört, hängt das Ergebnis von der ausgewählten Festplatte ab:

- Wenn Sie ein SSD-Laufwerk auswählen, werden das SSD-Laufwerk und alle untergeordneten Festplatten (HDD) in derselben Festplattengruppe gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe mehr als zwei Festplatten befinden, wird nur die ausgewählte Festplatte gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe maximal zwei Festplatten befinden, werden das SSD-Laufwerk und die ausgewählte Festplatte gelöscht.

Weitere Informationen zur Verwaltung von Virtual SAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevmfs

Installieren Sie ESXi, wenn eine VMFS-Partition auf der Festplatte zur Verfügung steht, aber keine ESX- oder ESXi-Installation vorhanden ist. Wenn diese Option nicht vorhanden ist, schlägt das Installationsprogramm fehl, wenn eine VMFS-Partition auf der Festplatte zur Verfügung steht, aber keine ESX- oder ESXi-Installation vorhanden ist.

keyboard (optional)

Legt den Tastaturtyp für das System fest.

keyboardType

Legt die Tastaturzuordnung für den ausgewählten Tastaturtyp fest. *keyboardType* muss einer der folgenden Typen sein.

- Belgisch
- Brasilianisch
- Kroatisch
- Tschechoslowakisch
- Dänisch
- Standard
- Estnisch
- Finnisch
- Französisch
- Deutsch
- Griechisch
- Isländisch
- Italienisch
- Japanisch
- Lateinamerikanisch
- Norwegisch
- Polnisch
- Portugiesisch
- Russisch

- Slowenisch
- Spanisch
- Schwedisch
- Französisch (Schweiz)
- Deutsch (Schweiz)
- Türkisch
- US Dvorak
- Ukrainisch
- Großbritannien

serialnum oder vmserialnum (optional)

Auslaufend in ESXi 5.0.x, unterstützt in ESXi 5.1. Konfiguriert die Lizenzierung. Wenn nicht angegeben, erfolgt die ESXi-Installation im Testmodus.

--esx=<license-key> Gibt den zu verwendenden vSphere-Lizenzschlüssel an. Das Format besteht aus fünf Gruppen mit je fünf Zeichen (XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX).

network (optional)

Gibt eine Netzwerkadresse für das System an.

--bootproto=[dhcp|static] Gibt an, ob die Netzwerkeinstellungen von DHCP abgerufen oder manuell festgelegt werden sollen.

--device= Gibt entweder die MAC-Adresse der Netzwerkkarte oder den Gerätenamen im Format `vmnicNN` an, wie z. B. `vmnic0`. Diese Option bezieht sich auf das Uplink-Gerät für den virtuellen Switch.

--ip= Legt eine IP-Adresse für die zu installierende Maschine im Format `xxx.xxx.xxx.xxx` fest. Dies ist für die Option `--bootproto=static` erforderlich und wird ansonsten ignoriert.

--gateway= Legt das Standard-Gateway als IP-Adresse im Format `xxx.xxx.xxx.xxx` fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet.

--nameserver= Legt den primären Namensserver als IP-Adresse fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet. Lassen Sie diese Option weg, falls Sie nicht vorhaben, DNS zu verwenden.

Für die Option `--nameserver` können zwei IP-Adressen angegeben werden. Beispiel: `--nameserver="10.126.87.104[,10.126.87.120]"`

`--netmask=` Legt die Subnetzmaske des installierten Systems im Format `255.xxx.xxx.xxx` fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet.

`--hostname=` Legt den Hostnamen für das installierte System fest.

`--vlanid= vlanid` Gibt das VLAN des Systems an. Wird entweder mit der Option `--bootproto=dhcp` oder `--bootproto=static` verwendet. Legen Sie den Wert auf eine Ganzzahl zwischen 1 und 4096 fest.

`--addvmportgroup=(0|1)` Gibt an, ob die VM-Netzwerkportgruppe, die von virtuelle Maschinen verwendet wird, hinzugefügt werden soll. Der Standardwert ist 1.

paranoid (optional)

Sorgt dafür, dass Warnmeldungen zum Abbruch der Installation führen. Wenn Sie diesen Befehl auslassen, werden Warnmeldungen protokolliert.

part oder partition (optional)

Erstellt auf dem System einen zusätzlichen VMFS-Datenspeicher. Es kann nur ein Datenspeicher pro Festplatte erstellt werden. Kann nicht auf derselben Festplatte wie der `install`-Befehl verwendet werden. Es kann nur eine Partition pro Festplatte angegeben werden. Diese muss eine VMFS-Partition sein.

datastore name Gibt an, wo die Partition gemountet werden soll.

`--ondisk=` or `--ondrive=` Gibt die Festplatte oder das Laufwerk an, wo die Partition erstellt werden soll.

`--firstdisk=`
disk-type1,
[disk-type2,...] Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

- 1 Lokal angehängter Speicher (*local*)
- 2 Netzwerkspeicher (*remote*)
- 3 USB-Festplatten (*usb*)

Sie können die Reihenfolge der Festplatten durch eine kommasetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie

beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local an`.

reboot (optional)

Startet die Maschine nach Abschluss der Skriptinstallation neu.

`<--noeject>` Nach der Installation wird die CD nicht ausgeworfen.

rootpw (erforderlich)

Legt das Root-Kennwort für das System fest.

`--iscrypted` Legt fest, dass das Kennwort verschlüsselt ist.

`password` Legt das Kennwort fest.

Aktualisieren

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk=` or `--drive=` Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=` kann der *Festplattenname* eine der folgenden Formen haben:

- Pfad: `--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`
- MPX-Name: `--disk=mpx.vmhba1:C0:T0:L0`
- VML-Name: `--disk=vm1.000000034211234`
- vmkLUN-UID: `--disk=vmkLUN_UID`

Die Formate der angenommenen Laufwerksnamen finden Sie unter [Festplattengerätenamen](#).

`--firstdisk=`
`disk-type1,`
`[disk-type2,...]` Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

- 1 Lokal angehängter Speicher (`local`)
- 2 Netzwerkspeicher (`remote`)
- 3 USB-Festplatten (`usb`)

Sie können die Reihenfolge der Festplatten durch eine kommasetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local an`.

%include oder include (optional)

Gibt ein anderes zu analysierendes Installationsskript an. Dieser Befehl wird ähnlich wie ein mehrzeiliger Befehl behandelt, er akzeptiert jedoch nur ein Argument.

filename Beispiel: `%include part.cfg`

%pre (optional)

Gibt ein Skript an, das vor der Evaluierung der Kickstart-Konfiguration ausgeführt werden soll. Sie können es z. B. verwenden, um Dateien zur Aufnahme in die Kickstart-Datei zu generieren.

--interpreter Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.
=`[python|busybox]`

%post (optional)

Führt das angegebene Skript nach Abschluss der Paketinstallation aus. Wenn Sie mehrere `%post`-Abschnitte festlegen, werden sie in der Reihenfolge ausgeführt, in der sie im Installationsskript angegeben sind.

--interpreter Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.
=`[python|busybox]`

--timeout=secs Legt eine Zeitüberschreitung für das Ausführen des Skripts fest. Falls die Ausführung des Skripts nicht abgeschlossen ist, wenn die Zeitüberschreitung eintritt, wird es automatisch beendet.

--ignorefailure Bei Angabe von „true“ wird die Installation auch dann als erfolgreich angesehen, wenn das `%post`-Skript fehlerhaft beendet wurde.
=`[true|false]`

%firstboot

Erstellt ein `init`-Skript, das nur während des ersten Startvorgangs ausgeführt wird. Das Skript hat keinen Einfluss auf spätere Startvorgänge. Wenn Sie mehrere `%firstboot`-Abschnitte festlegen, werden sie in der Reihenfolge ausgeführt, in der sie in der Kickstart-Datei angegeben sind.

Hinweis Sie können die Semantik des `%firstboot`-Skripts erst dann prüfen, wenn das System zum ersten Mal gestartet wird. Ein `%firstboot`-Skript enthält möglicherweise potenziell katastrophale Fehler, die erst nach Abschluss der Installation ersichtlich sind.

<code>--interpreter</code>	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung
<code>=python busybox</code>	ist „busybox“.

Hinweis Sie können die Semantik des `%firstboot`-Skripts erst dann prüfen, wenn das System zum ersten Mal gestartet wird. Wenn das Skript Fehler enthält, sind diese erst nach Abschluss der Installation ersichtlich.

Festplattengerätenamen

Die Installationsskriptbefehle `install`, `upgrade` und `installorupgrade` erfordern die Verwendung von Festplattengerätenamen.

Tabelle 9-2. Festplattengerätenamen

Formatieren	Beispiel	Beschreibung
VML	vml.00025261	Der Geräteiname, wie vom VMkernel gemeldet
MPX	mpx.vmhba0:C0:T0:L0	Der Geräteiname

Grundlegende Informationen zur Datei „boot.cfg“

Die Bootloader-Konfigurationsdatei `boot.cfg` gibt den Kernel, die Kerneloptionen und die Boot-Module an, die der Bootloader `mboot.c32` in einer ESXi-Installation verwendet.

Die Datei `boot.cfg` ist im ESXi-Installationsprogramm enthalten. Sie können die Zeile `kernelopt` der Datei `boot.cfg` ändern, um den Speicherort eines Installationsskripts anzugeben oder andere Startoptionen zu übergeben.

Die Datei `boot.cfg` weist die folgende Syntax auf:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
```

```
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Mit den Befehlen in `boot.cfg` wird der Bootloader konfiguriert.

Tabelle 9-3. Befehle in `boot.cfg`.

Befehl	Beschreibung
<code>title=STRING</code>	Stellt den Titel des Bootloaders auf <code>STRING</code> ein.
<code>kernel=FILEPATH</code>	Stellt den Kernelpfad auf <code>FILEPATH</code> ein.
<code>kernelopt=STRING</code>	Hängt <code>STRING</code> an die Kernel-Startoptionen an.
<code>modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn</code>	Listet die zu ladenden Module auf, getrennt durch drei Striche (---).

Weitere Informationen zum Aktualisieren der Datei `boot.cfg` mit Informationen für einen HTTP-Server finden Sie beispielsweise unter [Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von gPXE](#).

Weitere Informationen hierzu finden Sie auch unter [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#), [Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei](#), [Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „isolinux.cfg“](#) und [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#).

Installieren oder Durchführen eines Upgrades von ESXi von einer CD oder DVD mithilfe eines Skripts

Sie können von einem CD-ROM- oder DVD-ROM-Laufwerk aus mithilfe eines Skripts, das die Installations- oder Upgrade-Optionen festlegt, ESXi installieren oder ein Upgrade davon durchführen.

Sie können das Installations- oder Upgrade-Skript starten, indem Sie beim Starten des Hosts eine Startoption eingeben. Sie können auch ein Installer-ISO-Image erstellen, das das Installationsskript enthält. Mit einem Installer-ISO-Image können Sie eine skriptbasierte, unbeaufsichtigte Installation durchführen, wenn Sie das resultierende Installer-ISO-Image starten. Siehe [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#).

Voraussetzungen

Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das System, auf dem Sie das Produkt installieren oder ein Upgrade davon durchführen, erfüllt die Hardwareanforderungen. Siehe [Hardwareanforderungen für ESXi](#).

- Die ISO-Datei des ESXi-Installationsprogramms befindet sich auf einer Installations-CD oder -DVD. Siehe [Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD](#).
- Das System kann auf das Standardinstallations- oder -Upgrade-Skript (`ks.cfg`) oder ein benutzerdefiniertes Installations- oder -Upgrade-Skript zugreifen. Siehe [Grundlegendes zu Installations- und Upgrade-Skripts](#).
- Sie haben einen Startbefehl ausgewählt, um die Installation oder das Upgrade per Skript auszuführen. Siehe [Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts](#). Eine vollständige Liste der Startbefehle finden Sie unter [Startoptionen](#).

Verfahren

- 1 Starten Sie das ESXi-Installationsprogramm vom lokalen CD-ROM- oder DVD-ROM-Laufwerk aus.
- 2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



- 3 Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

Die Startoption hat das Format `ks=`.

- 4 Drücken Sie die Eingabetaste.

Ergebnisse

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Installieren oder Durchführen eines Upgrades von ESXi von einem USB-Flash-Laufwerk mithilfe eines Skripts

Sie können von einem USB-Flash-Laufwerk aus mithilfe eines Skripts, das die Installations- oder Upgrade-Optionen festlegt, ESXi installieren oder ein Upgrade davon durchführen.

Unterstützte Startoptionen werden in [Startoptionen](#) aufgelistet.

Voraussetzungen

Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das System, auf dem Sie ESXi installieren oder aktualisieren, erfüllt die Hardwareanforderungen für die Installation bzw. das Upgrade. Siehe [Hardwareanforderungen für ESXi](#).
- Die ESXi-Installer-ISO-Datei befindet sich auf einem startfähigen USB-Flash-Laufwerk. Siehe [Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades](#).
- Das System kann auf das Standardinstallations- oder -Upgrade-Skript (`ks.cfg`) oder ein benutzerdefiniertes Installations- oder -Upgrade-Skript zugreifen. Siehe [Grundlegendes zu Installations- und Upgrade-Skripts](#).
- Sie haben eine Startoption ausgewählt, um die Installation, das Upgrade oder die Migration per Skript auszuführen. Siehe [Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts](#).

Verfahren

- 1 Starten Sie das ESXi-Installationsprogramm vom USB-Flash-Laufwerk aus.
- 2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



- 3 Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

Die Startoption hat das Format `ks=`.

- 4 Drücken Sie die Eingabetaste.

Ergebnisse

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Ausführen einer Skriptinstallation oder eines Upgrades von ESXi durch Starten des Installationsprogramms per PXE-Startvorgang

ESXi 6.0 bietet viele Optionen zum Starten des Installationsprogramms per PXE-Startvorgang und zum Verwenden eines Installations- oder eines Upgrade-Skripts.

- Weitere Informationen zur Einrichtung einer PXE-Infrastruktur finden Sie unter [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#).
- Weitere Informationen über das Erstellen und Auffinden eines Installationsskripts finden Sie unter [Grundlegendes zu Installations- und Upgrade-Skripts](#).
- Weitere Informationen über bestimmte Prozeduren zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang und zum Verwenden eines Installationsskripts finden Sie in den folgenden Themen:
 - [Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „isolinux.cfg“](#)
 - [Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei](#)
 - [Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von gPXE](#)
- Weitere Informationen über die Verwendung von vSphere Auto Deploy zum Durchführen eines Skript-Upgrades per PXE-Startvorgang finden Sie unter [Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts

Wenn ein Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie Auto Deploy zum erneuten Bereitstellen des Hosts mit einem neuen Image-Profil verwenden, das eine andere Version von ESXi enthält. Mit ESXi Image Builder PowerCLI können Sie Image-Profile erstellen und verwalten.

Hinweis Wenn Sie den Host aktualisieren, sodass ein Image von ESXi 6.0 oder höher verwendet wird, stellt der Auto Deploy-Server für den ESXi-Host Zertifikate bereit, die von VMCA signiert sind. Wenn Sie derzeit benutzerdefinierte Zertifikate verwenden, können Sie den Host so einrichten, dass er die benutzerdefinierten Zertifikate nach dem Upgrade verwendet.

Der Auto Deploy-Server wird automatisch aktualisiert, wenn Sie das entsprechende vCenter Server-System auf Version 6 aktualisieren. Ab Version 6 ist der Auto Deploy-Server immer auf demselben Verwaltungsknoten wie das vCenter Server-System.

Erneute Bereitstellung von Hosts

vSphere Auto Deploy unterstützt mehrere Optionen zur erneuten Bereitstellung. Sie können einen einfachen Neustart durchführen oder mit einem anderen Image- oder Hostprofil erneut bereitstellen.

Bei einem ersten Start mithilfe von Auto Deploy ist es erforderlich, dass Sie Ihre Umgebung einrichten und Regeln zum Regelsatz hinzufügen. Lesen Sie „Vorbereiten von vSphere Auto Deploy“ im *Installations- und Einrichtungshandbuch für vSphere*.

Die folgenden Vorgänge zur erneuten Bereitstellung sind vorhanden.

- Einfacher Neustart.
- Neustart von Hosts, für die der Benutzer Fragen während des Startvorgangs beantwortet hat.
- Erneute Bereitstellung mit einem anderen Image-Profil.
- Erneute Bereitstellung mit einem anderen Hostprofil.

Erneute Bereitstellung von Hosts mit einfachen Neustartvorgängen

Für einen einfachen Neustart eines Hosts, der mit Auto Deploy bereitgestellt wird, müssen nur weiterhin alle Voraussetzungen erfüllt sein. Der Prozess verwendet das zuvor zugewiesene Image-Profil, das Hostprofil und den Speicherort von vCenter Server.

Die Einrichtung umfasst die DHCP-Server-Einrichtung sowie das Schreiben von Regeln und sie stellt der Auto Deploy-Infrastruktur das Image-Profil zur Verfügung.

Voraussetzungen

Stellen Sie sicher, dass die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt hatten, vorhanden ist.

Verfahren

- 1 Überprüfen Sie, ob das Image-Profil und das Hostprofil für den Host immer noch verfügbar sind und ob der Host die Identifizierungsinformationen (Asset-Tag, IP-Adresse) hat, über die er während der vorherigen Startvorgänge verfügte.
- 2 Versetzen Sie den Host in den Wartungsmodus.

Hosttyp	Aktion
Der Host gehört zu einem DRS-Cluster.	vSphere DRS migriert virtuelle Maschinen auf entsprechende Hosts, wenn Sie den Host in den Wartungsmodus versetzen.
Der Host gehört nicht zu einem DRS-Cluster.	Sie müssen alle virtuelle Maschinen auf verschiedene Hosts migrieren und jeden Host in den Wartungsmodus versetzen.

- 3 Starten Sie den Host neu.

Ergebnisse

Der Host wird heruntergefahren. Wenn der Host neu gestartet wird, verwendet er das vom Auto Deploy-Server bereitgestellte Image-Profil. Der Auto Deploy-Server wendet auch das Hostprofil an, das auf dem vCenter Server-System gespeichert ist.

Erneutes Bereitstellen eines Hosts mit einem neuen Image-Profil

Sie können den Host mithilfe eines neuen Image-Profiles, eines Hostprofils oder eines vCenter Server-Speicherorts erneut bereitstellen, indem Sie die Regel für den Host ändern und einen Vorgang zum Testen und zur Reparatur von Übereinstimmungen durchführen.

Es gibt mehrere Optionen zur erneuten Bereitstellung von Hosts.

- Wenn die VIBs, die Sie verwenden möchten, Live-Update unterstützen, können Sie einen `esxcli software vib`-Befehl verwenden. In diesem Fall müssen Sie außerdem den Regelsatz aktualisieren, damit er ein Image-Profil verwendet, das die neuen VIBs enthält.
- Während des Testens können Sie ein Image-Profil auf einen einzelnen Host anwenden, indem Sie das `Apply-EsxImageProfile`-cmdlet verwenden und den Host neu starten, damit die Änderung übernommen wird. Das `Apply-EsxImageProfile`-cmdlet aktualisiert die Verbindung zwischen dem Host und dem Image-Profil, installiert jedoch keine VIBs auf dem Host.
- Verwenden Sie in allen anderen Fällen diese Vorgehensweise.

Voraussetzungen

- Erstellen Sie das Image-Profil, mit dem der Host gestartet werden soll. Verwenden der Image Builder PowerCLI. Lesen Sie „Verwenden von vSphere ESXi Image Builder CLI“ im *Installations- und Einrichtungshandbuch für vSphere*.
- Stellen Sie sicher, dass die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt hatten, vorhanden ist.

Verfahren

- 1 Führen Sie an der PowerShell-Eingabeaufforderung das `Connect-VIServer-PowerCLI`-cmdlet aus, um eine Verbindung zu dem vCenter Server-System herzustellen, bei dem Auto Deploy registriert ist.

Connect-VIServer myVCServer

Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen ausgegeben werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

- 2 Ermitteln Sie den Speicherort eines öffentlichen Software-Depots, das das Image-Profil enthält, das Sie verwenden möchten, oder definieren Sie mithilfe der Image Builder PowerCLI ein eigenes Image-Profil.

- 3 Führen Sie `Add-EsxSoftwareDepot` aus, um das Software-Depot mit dem Image-Profil zur PowerCLI-Sitzung hinzuzufügen.

Depottyp	Cmdlet
Remote-Depot	Führen Sie <code>Add-EsxSoftwareDepot URL_des_Depots</code> aus.
ZIP-Datei	<ol style="list-style-type: none"> Laden Sie die ZIP-Datei in einen lokalen Dateipfad herunter oder erstellen Sie in der PowerCLI-Maschine einen lokalen Mount-Punkt. Führen Sie <code>Add-EsxSoftwareDepot C:\Dateipfad\Mein_Offline-Depot.zip</code> aus.

- 4 Führen Sie `Get-EsxImageProfile` aus, damit eine Liste der Image-Profile angezeigt wird, und entscheiden Sie, welches Profil Sie verwenden möchten.
- 5 Führen Sie `Copy-DeployRule` aus und legen Sie den Parameter `ReplaceItem` fest, um die Regel zu ändern, die ein Image-Profil zu Hosts zuweist.

Das folgende cmdlet ersetzt das aktuelle Image-Profil, das die Regel dem Host mit dem *Mein_neues_Image-Profil*-Profil zuweist. Nachdem das cmdlet beendet wurde, weist `myrule` den Hosts das neue Image-Profil zu. Die alte Version von `myrule` wird umbenannt und ausgeblendet.

`Copy-DeployRule myrule -ReplaceItem Mein_neues_Image-Profil`

- 6 Testen und reparieren Sie die Regelübereinstimmung für jeden Host, auf dem Sie das Image bereitstellen möchten.

Weitere Informationen hierzu finden Sie unter [Testen und Reparieren der Regelübereinstimmung](#).

Ergebnisse

Wenn Sie nach der Übereinstimmungsreparatur die Hosts neu starten, stellt Auto Deploy die Hosts mit dem neuen Image-Profil bereit.

Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts

Auto Deploy kann einem oder mehreren Hosts ein Hostprofil zuweisen. Das Hostprofil enthält möglicherweise Informationen über die Speicherkonfiguration, die Netzwerkkonfiguration oder andere Hostmerkmale. Wenn Sie einen Host zum Cluster hinzufügen, wird das Hostprofil des Clusters verwendet.

In vielen Fällen weisen Sie einem Cluster einen Host zu, anstatt explizit ein Hostprofil anzugeben. Der Host verwendet das Hostprofil des Clusters.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderliche Software. Weitere Informationen finden Sie unter *Installations- und Einrichtungshandbuch für vSphere*.
- Exportieren Sie das Hostprofil, das Sie verwenden möchten.

Verfahren

- 1 Führen Sie das `Connect-VIServer`-Cmdlet vSphere PowerCLI aus, um eine Verbindung mit dem vCenter Server-System herzustellen, bei dem Auto Deploy registriert ist.

```
Connect-VIServer 192.XXX.X.XX
```

Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen ausgegeben werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

- 2 Verwenden Sie den vSphere Web Client, um einen Host mit den von Ihnen gewünschten Einstellungen einzurichten und ein Hostprofil dieses Hosts zu erstellen.
- 3 Sie können den Namen des Hostprofils herausfinden, indem Sie das vSphere PowerCLI-Cmdlet `Get-VMhostProfile` unter Angabe des ESXi-Hosts ausführen, von dem Sie ein Hostprofil erstellen.
- 4 Definieren Sie an der vSphere PowerCLI-Eingabeaufforderung eine Regel, in der Hosts mit bestimmten Attributen, z. B. einem Bereich von IP-Adressen, dem Hostprofil zugewiesen werden.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",  
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Das angegebene Element wird allen Hosts mit den angegebenen Attributen zugewiesen. In diesem Beispiel wird eine Regel namens „Testregel2“ angegeben. Die Regel weist das angegebene Hostprofil `my_host_profile` allen Hosts zu, die eine IP-Adresse innerhalb des angegebenen Bereichs und den Anbieter Acme oder Zven aufweisen.

- 5 Fügen Sie die Regel dem Regelsatz hinzu.

```
Add-DeployRule testrule2
```

Standardmäßig wird der Arbeitsregelsatz zum aktiven Regelsatz und alle Änderungen am Regelsatz werden aktiv, wenn Sie eine Regel hinzufügen. Wenn Sie den Parameter `NoActivate` angeben, wird der Arbeitsregelsatz nicht der aktive Regelsatz.

Nächste Schritte

- Weisen Sie dem neuen Host einen bereits mithilfe von Auto Deploy ausgestatteten Host zu, indem Sie Übereinstimmungstests und Reparaturvorgänge auf diesen Hosts durchführen. Weitere Informationen finden Sie unter [Testen und Reparieren der Regelübereinstimmung](#).
- Schalten Sie noch nicht ausgestattete Hosts ein, um sie mit dem Hostprofil auszustatten.

Testen und Reparieren der Regelübereinstimmung

Wenn Sie eine Regel zum Auto Deploy-Regelsatz hinzufügen oder Änderungen an einer oder mehreren Regeln vornehmen, werden die Hosts nicht automatisch aktualisiert. Auto Deploy

übernimmt die neuen Regeln nur dann, wenn Sie deren Regelübereinstimmung testen und eine Standardisierung durchführen.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderlichen Softwareprodukte.
- Vergewissern Sie sich, dass Ihre Infrastruktur einen oder mehrere ESXi-Hosts enthält, die mit Auto Deploy bereitgestellt wurden, und dass der Host, auf dem vSphere PowerCLI installiert ist, auf diese ESXi-Hosts zugreifen kann.

Verfahren

- 1 Verwenden Sie vSphere PowerCLI, um zu überprüfen, welche Auto Deploy-Regeln derzeit verfügbar sind.

```
Get-DeployRule
```

Das System gibt die Regeln und die zugeordneten Elemente und Muster zurück.

- 2 Nehmen Sie an einer der verfügbaren Regeln eine Änderung vor.

Ändern Sie beispielsweise das Image-Profil und den Namen der Regel.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Sie können keine Regel bearbeiten, die bereits zu einem Regelsatz hinzugefügt wurde. Kopieren Sie stattdessen die Regel und ersetzen Sie das Element oder Muster, das Sie ändern möchten.

- 3 Vergewissern Sie sich, dass Sie auf den Host zugreifen können, dessen Regelsatzübereinstimmung Sie testen möchten.

```
Get-VMHost -Name MyEsxi42
```

- 4 Führen Sie das cmdlet aus, das die Regelsatzübereinstimmung für den Host testet, und binden Sie den Rückgabewert zur späteren Verwendung an eine Variable.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

- 5 Untersuchen Sie die Unterschiede zwischen dem Inhalt des Regelsatzes und der Konfiguration des Hosts.

```
$tr.itemlist
```

Das System gibt eine Tabelle der aktuellen und der erwarteten Elemente zurück.

CurrentItem	ExpectedItem
-----	-----
My Profile 25MyProfileUpdate	

- 6 Standardisieren Sie den Host, sodass er beim nächsten Neustart den überarbeiteten Regelsatz verwendet.

```
Repair-DeployRuleSetCompliance $tr
```

Nächste Schritte

Wenn mit der von Ihnen geänderten Regel der Speicherort für die Bestandsliste angegeben wurde, werden die Änderungen wirksam, wenn Sie die Übereinstimmung reparieren. Starten Sie bei allen anderen Änderungen Ihren Host neu, um die neue Regel mithilfe von Auto Deploy anzuwenden und eine Übereinstimmung zwischen dem Regelsatz und dem Host zu erzielen.

Aktualisieren von Hosts mithilfe von `esxcli`-Befehlen

Mithilfe der vSphere CLI können Sie ein Upgrade des ESXi 5.x-Hosts auf Version 6.0 durchführen und ESXi 5.x- und 6.0-Hosts aktualisieren oder patchen.

Um `esxcli`-Befehle für vCLI verwenden zu können, müssen Sie vSphere CLI (vCLI) installieren. Weitere Informationen zur Installation und Verwendung der CLI finden Sie in den folgenden Dokumenten:

- *Erste Schritte mit vSphere Command-Line Interfaces*
- *Konzepte und Beispiele zur vSphere Command-Line Interface*
- *Referenz zur vSphere Command-Line Interface* ist eine Referenz auf `vicfg-` und bezieht sich auf vCLI-Befehle.

Hinweis Wenn Sie STRG+C drücken, während ein `esxcli`-Befehl ausgeführt wird, wird die Befehlszeilenschnittstelle beendet und eine neue Eingabeaufforderung gestartet, ohne dass eine Meldung angezeigt wird. Der Befehl wird jedoch weiter ausgeführt.

Bei mit vSphere Auto Deploy bereitgestellten ESXi-Hosts muss das Tools-VIB Teil des Basis-Boot-Images sein, das für die anfängliche Auto Deploy-Installation verwendet wird. Das Tools-VIB kann später nicht hinzugefügt werden.

VIBs, Image-Profile und Software-Depots

Zum Aktualisieren von ESXi mit `esxcli`-Befehlen sind Kenntnisse zu VIBs, Image-Profilen und Software-Depots erforderlich.

Die folgenden technischen Begriffe werden in der vSphere-Dokumentation im Zusammenhang mit Installations- und Upgrade-Aufgaben verwendet.

VIB

Ein VIB ist ein ESXi-Software-Paket. Paketlösungen, Treiber, CIM-Anbieter und Anwendungen von VMware und seinen Partnern, die die ESXi-Plattform als VIBs erweitern. VIBs sind in Software-Depots verfügbar. Sie können VIBs zur Erstellung und Anpassung von ISO-Images oder zum Upgrade von ESXi-Hosts verwenden, indem Sie VIBs asynchron auf den Hosts installieren.

Image-Profil

Ein Image-Profil definiert ein ESXi-Image und besteht aus VIBs. Ein Image-Profil enthält immer ein Basis-VIB und umfasst möglicherweise weitere VIBs. Image-Profile werden mithilfe von vSphere ESXi Image Builder untersucht und definiert.

Software-Depot

Ein Software-Depot ist eine Sammlung von VIBs und Image-Profilen. Das Software-Depot ist eine Hierarchie von Dateien und Ordnern und es kann über eine HTTP-URL (Online-Depot) oder eine ZIP-Datei (Offline-Depot) bereitgestellt werden. VMware und VMware-Partner stellen Depots bereit. Unternehmen mit großen VMware-Installationen erstellen möglicherweise interne Depots, um ESXi-Hosts mit vSphere Auto Deploy bereitzustellen oder um eine ISO-Datei für die ESXi-Installation zu exportieren.

Grundlegende Informationen zu Akzeptanzebenen für VIBs und Hosts

Jedes VIB wird mit einer Akzeptanzebene freigegeben, die nicht geändert werden kann. Die Akzeptanzebene des Hosts bestimmt, welche VIBs auf einem Host installiert werden dürfen.

Die Akzeptanzebene gilt für einzelne VIBs, die über die Befehle `esxcli software vib install` und `esxcli software vib update` installiert wurden, für VIBs, die mithilfe von vSphere Update Manager installiert wurden, und für VIBs in Image-Profilen.

Die Akzeptanzebene aller VIBs auf einem Host muss mindestens so hoch wie die Host-Akzeptanzebene sein. Wenn die Akzeptanzebene des Hosts beispielsweise `VMwareAccepted` lautet, können Sie VIBs mit den Akzeptanzebenen `VMwareCertified` und `VMwareAccepted` installieren, Sie können jedoch keine VIBs mit den Akzeptanzebenen `PartnerSupported` oder `CommunitySupported` installieren. Zur Installation eines VIB mit einer weniger restriktiven Akzeptanzebene als der des Hosts können Sie die Akzeptanzebene des Hosts ändern, indem Sie den vSphere Web Client verwenden oder indem Sie `esxcli software acceptance`-Befehle ausführen.

Es wird empfohlen, Host-Akzeptanzebenen festzulegen, um anzugeben, welche VIBs auf einem Host installiert und mit einem Image-Profil verwendet werden können, und welchen Grad der Unterstützung Sie für einen VIB erwarten können. Beispielsweise würden Sie für Hosts in einer Produktionsumgebung eine restriktivere Akzeptanzebene als für Hosts in einer Testumgebung festlegen.

VMware unterstützt die folgenden Akzeptanzebenen.

VMwareCertified

Die Akzeptanzebene „VMwareCertified“ hat die strengsten Anforderungen. VIBs dieser Ebene unterliegen einer gründlichen Prüfung entsprechend den internen VMware-Qualitätssicherungstests für die gleiche Technologie. Zurzeit werden nur Programmtreiber im Rahmen des IOVP (I/O Vendor Program) auf dieser Ebene veröffentlicht. VMware übernimmt Support-Anrufe für VIBs dieser Akzeptanzebene.

VMwareAccepted

VIBs dieser Akzeptanzebene unterliegen einer Verifizierungsprüfung; es wird jedoch nicht jede Funktion der Software in vollem Umfang getestet. Der Partner führt die Tests durch und VMware verifiziert das Ergebnis. Heute gehören CIM-Anbieter und PSA-Plug-Ins zu den VIBs, die auf dieser Ebene veröffentlicht werden. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

PartnerSupported

VIBs mit der Akzeptanzebene „PartnerSupported“ werden von einem Partner veröffentlicht, dem VMware vertraut. Der Partner führt alle Tests durch. VMware überprüft die Ergebnisse nicht. Diese Ebene wird für eine neue oder nicht etablierte Technologie verwendet, die Partner für VMware-Systeme aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATAoE und SSD. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

CommunitySupported

Die Akzeptanzebene „CommunitySupported“ ist für VIBs gedacht, die von Einzelpersonen oder Unternehmen außerhalb der VMware Partner-Programme erstellt wurden. VIBs auf dieser Ebene wurden nicht im Rahmen eines von VMware zugelassenen Testprogramms getestet und werden weder von VMware Technical Support noch von einem VMware-Partner unterstützt.

Tabelle 9-4. Zur Installation auf Hosts erforderliche VIB-Akzeptanzebenen

Host-Akzeptanzebene	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
VMwareCertified	B			
VMwareAccepted	B	B		
PartnerSupported	B	B	B	
CommunitySupported	B	B	B	B

Angleichen einer Host- mit einer Update-Akzeptanzebene

Sie können die Host-Akzeptanzebene ändern, sodass sie mit der Akzeptanzebene für ein VIB oder Image-Profil, das Sie installieren möchten, identisch ist. Die Akzeptanzebene aller VIBs auf einem Host muss mindestens so hoch wie die Host-Akzeptanzebene sein.

Verwenden Sie dieses Verfahren zum Ermitteln der Akzeptanzebenen des Hosts und des zu installierenden VIBs oder Image-Profils sowie zum Ändern der Akzeptanzebene des Hosts für das Update, falls dies erforderlich ist.

Wenn Sie mit **--server=Servername** einen Zielserver angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Rufen Sie die Akzeptanzebene für das VIB oder das Image-Profil ab.

Option	Beschreibung
Informationen für alle VIBs auflisten	<code>esxcli --server=Servername software sources vib list --depot=URL_des_Depots</code>
Informationen für ein bestimmtes VIB auflisten	<code>esxcli --server=Servername software sources vib list --viburl=URL_des_VIBs</code>
Informationen für alle Image-Profile auflisten	<code>esxcli --server=Servername software sources profile list --depot=URL_des_Depots</code>
Informationen für ein bestimmtes Image-Profil auflisten	<code>esxcli --server=Servername software sources profile get --depot=URL_des_Depots --profile=Name_des_Profils</code>

- 2 Ermitteln Sie die Hostakzeptanzebene.

```
esxcli --server=Servername software acceptance get
```

- 3 (Optional) Ist die Akzeptanzebene des VIBs restriktiver als die Akzeptanzebene des Hosts, dann ändern Sie die Akzeptanzebene des Hosts.

```
esxcli --server=Servername software acceptance set --level=Akzeptanzebene
```

Die *Akzeptanzebene* kann `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` oder `CommunitySupported` sein. Bei den Werten für die *Akzeptanzebene* wird zwischen der Klein- und Großschreibung unterschieden.

Hinweis Sie können die Option `--force` für den Befehl `esxcli software vib` oder `esxcli software profile` verwenden, um ein VIB oder Image-Profil mit einer niedrigeren Akzeptanzebene als der des Hosts hinzuzufügen. Es wird eine Warnung angezeigt. Weil Ihr Setup nicht mehr konsistent ist, wird die Warnung wiederholt, wenn Sie VIBs installieren, VIBs entfernen und gewisse andere Vorgänge auf dem Host durchführen.

Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss.

VIBs, die Sie mit einer Live-Installation installieren können, erfordern keinen Neustart des Hosts. Möglicherweise ist es jedoch erforderlich, den Host in den Wartungsmodus zu versetzen. Andere VIBs und Profile erfordern möglicherweise, dass der Host nach der Installation oder dem Update neu gestartet wird.

Wenn Sie mit `--server=Servername` einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI-Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Überprüfen Sie, ob das VIB oder das Image-Profil, das Sie installieren möchten, erfordert, dass der Host in den Wartungsmodus versetzt oder nach der Installation oder dem Update neu gestartet wird.

Führen Sie einen der folgenden Befehle aus.

Option	Beschreibung
Überprüfen Sie das VIB	<code>esxcli --server=Servername software sources vib get -v Absoluter_Pfad_zum_VIB</code>
Überprüfen Sie die VIBs in einem Depot	<code>esxcli --server=Servername software sources vib get --depot=Depotname</code>
Überprüfen Sie das Image-Profil in einem Depot	<code>esxcli --server=Servername software sources profile get --depot=Depotname</code>

2 Überprüfen Sie die Rückgabewerte.

Die Rückgabewerte, die aus den VIB-Metadaten gelesen werden, geben an, ob sich der Host vor der Installation des VIB oder Image-Profiles im Wartungsmodus befinden muss und ob die Installation des VIB oder Profils einen Neustart des Hosts erfordert.

Hinweis vSphere Update Manager ermittelt anhand des `esxupdate/esxcli`-Prüfungsergebnisses, ob der Wartungsmodus erforderlich ist. Wenn Sie ein VIB auf einem Live-System installieren und der Wert für `Live-Install-Allowed` auf „false“ festgelegt ist, weist das Ergebnis des Installationsvorgangs Update Manager an, den Host neu zu starten. Wenn Sie ein VIB von einem Live-System entfernen und der Wert für `Live-Remove-Allowed` auf „false“ festgelegt ist, weist das Ergebnis des Entfernungsvorgangs Update Manager an, den Host neu zu starten. Während des Neustarts versetzt Update Manager in beiden Fällen den Host automatisch in den Wartungsmodus.

Nächste Schritte

Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus. Weitere Informationen hierzu finden Sie unter [Versetzen eines Hosts in den Wartungsmodus](#). Falls ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, müssen Sie vor der Installation oder dem Update den Host aus dem Cluster entfernen oder HA auf dem Cluster deaktivieren.

Versetzen eines Hosts in den Wartungsmodus

Einige Installations- und Update-Vorgänge, die eine Live-Installation verwenden, setzen voraus, dass sich der Host im Wartungsmodus befindet.

Informationen darüber, wie Sie feststellen können, ob sich bei einem Upgrade-Vorgang ein Host im Wartungsmodus befinden muss, finden Sie unter [Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss](#).

Hinweis Wenn der Host Mitglied eines Virtual SAN-Clusters ist und ein VM-Objekt auf dem Host in seiner Speicherrichtlinie die Einstellung „Anzahl der zulässigen Fehler=0“ verwendet, kann es auf dem Host beim Eintreten in den Wartungsmodus zu ungewöhnlichen Verzögerungen kommen. Die Verzögerungen treten auf, weil Virtual SAN dieses Objekt vom Host entfernen muss, um den Wartungsvorgang erfolgreich abschließen zu können.

Wenn Sie mit `--server=Servername` einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Prüfen Sie, ob sich der Host im Wartungsmodus befindet.

```
vicfg-hostops --server=Servername --operation info
```

- 2 Schalten Sie alle virtuellen Maschinen aus, die auf dem ESXi-Host ausgeführt werden.

Option	Befehl
So schalten Sie das Gastbetriebssystem und anschließend die virtuelle Maschine aus	<code>vmware-cmd --server=ServernamePfad_der_VM stop soft</code>
So erzwingen Sie den Ausschaltvorgang	<code>vmware-cmd --server=ServernamePfad_zur_VM stop hard</code>

Alternativ können Sie die virtuellen Maschinen auf einen anderen Host migrieren, um ihr Ausschalten zu verhindern. Weitere Informationen dazu finden Sie im Thema *Migrieren virtueller Maschinen* in der Dokumentation *vCenter Server und Hostverwaltung*.

- 3 Versetzen Sie den Host in den Wartungsmodus.

```
vicfg-hostops --server=Servername --operation enter
```

- 4 Stellen Sie sicher, dass sich der Host im Wartungsmodus befindet.

```
vicfg-hostops --server=Servername --operation info
```

Aktualisieren eines Hosts mit individuellen VIBs

Sie können einen Host mit VIBs aktualisieren, die in einem Software-Depot, auf das über eine URL zugegriffen werden kann, oder in einem Offline-ZIP-Depot gespeichert sind.

Wichtig Wenn Sie ESXi von einem ZIP-Paket eines von VMware bereitgestellten Depots aktualisieren, auf das über die VMware-Website online zugegriffen werden kann oder das lokal heruntergeladen wurde, unterstützt VMware nur die Update-Methode, die für von VMware bereitgestellte Depots im Abschnitt [Upgrade oder Update eines Hosts mit Image-Profilen](#) angegeben ist.

Die Befehle `esxcli software vib update` und `esxcli software vib install` werden für Upgrade-Vorgänge nicht unterstützt. Siehe [Unterschiede zwischen vSphere-Upgrades und -Updates](#) und [Upgrade oder Update eines Hosts mit Image-Profilen](#).

Wenn Sie mit `--server=Servername` einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI-Befehlszeile aus.

Voraussetzungen

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.
- Stellen Sie fest, ob sich zum Anwenden des Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss. Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus.

Weitere Informationen hierzu finden Sie unter [Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss.](#) Weitere Informationen hierzu finden Sie unter [Versetzen eines Hosts in den Wartungsmodus](#).

- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

- 1 Stellen Sie fest, welche VIBs auf dem Host installiert sind.

```
esxcli --server=Servername software vib list
```

- 2 Ermittlung, welche VIBs im Depot verfügbar sind.

Option	Beschreibung
Aus einem Depot über URL-Zugriff	<code>esxcli --server=Servername software sources vib list --depot=http://Webserver/Name_des_Depots</code>
Aus einer lokalen Depot-ZIP-Datei	<code>esxcli --server=Servername software sources vib list --depot=absoluter_Pfad_zur_Depot-Zip-Datei</code>

Mithilfe des Arguments `--proxy` können Sie einen Proxy-Server angeben.

- 3 Aktualisieren der vorhandenen VIBs, sodass sie die VIBs im Depot enthalten, oder Installieren neuer VIBs.

Option	Beschreibung
Aktualisieren von VIBs von einem Depot, auf das über URL zugegriffen werden kann	<code>esxcli --server=Servername software vib update --depot=http://Webserver/Name_des_Depots</code>
Aktualisieren von VIBs von einer lokalen Depot-ZIP-Datei	<code>esxcli --server=Servername software vib update --depot=absoluter_Pfad_zur_Depot-Zip-Datei</code>
Installation aller VIBs von einer ZIP-Datei auf einem angegebenen Offline-Depot (umfasst VMware-VIBs und von Partnern bereitgestellte VIBs)	<code>esxcli --server=Servername software vib install --depot Pfad_zur_VMware_VIB_ZIP_Datei\VMware_VIB_ZIP_Datei --depot Pfad_zur_Partner_VIB_ZIP_Datei\Partner_VIB_ZIP_Datei</code>

Optionen für die Befehle `update` und `install` ermöglichen es Ihnen, einen Testlauf durchzuführen, ein bestimmtes VIB anzugeben, die Verifizierung einer Akzeptanzebene zu umgehen usw. Umgehen Sie die Verifizierung nicht auf Produktionssystemen. Lesen Sie die *esxcli-Referenz* unter <http://www.vmware.com/support/developer/vcli/>.

- 4 Stellen Sie sicher, dass die VIBs auf Ihrem ESXi-Host installiert sind.

```
esxcli --server=Servername software vib list
```

Upgrade oder Update eines Hosts mit Image-Profilen

Sie können Upgrades oder Updates für einen Host mit Image-Profilen durchführen, die in einem Software-Depot, auf das über eine URL zugegriffen werden kann, oder in einem Offline-ZIP-Depot gespeichert sind.

Das Upgrade oder Update eines ESXi-Hosts können Sie mit dem Befehl **esxcli software profile update** oder **esxcli software profile install** ausführen. Informationen über die Unterschiede zwischen Upgrades und Updates finden Sie unter [Unterschiede zwischen vSphere-Upgrades und -Updates](#).

Wenn Sie ein Upgrade oder Update eines Hosts durchführen, wendet der Befehl **esxcli software profile update** bzw. **esxcli software profile install** eine höhere Version (größer oder kleiner) eines vollständigen Image-Profiles auf den Host an. Nach diesem Vorgang und einem Neustart kann der Host einer vCenter Server-Umgebung derselben höheren Version beitreten.

Der Befehl **esxcli software profile update** bringt den gesamten Inhalt des ESXi-Host-Image auf den gleichen Stand wie die entsprechende Upgrade-Methode mit einem ISO-Installationsprogramm. Allerdings führt das ISO-Installationsprogramm vor dem Upgrade eine Überprüfung potenzieller Probleme durch, während die **esxcli**-Upgrade-Methode darauf verzichtet. Das ISO-Installationsprogramm überprüft den Host darauf, ob dieser über ausreichenden Arbeitsspeicher für das Upgrade verfügt und ob keine nicht unterstützten Geräte angeschlossen sind. Weitere Informationen über das ISO-Installationsprogramm und weitere ESXi-Upgrade-Methoden finden Sie unter [Upgrade-Optionen für ESXi 6.0](#).

Wichtig Wenn Sie ein ESXi-Upgrade oder -Update von einem ZIP-Paket eines von VMware bereitgestellten Depots durchführen, auf das über die VMware-Website online zugegriffen werden kann oder das lokal heruntergeladen wurde, unterstützt VMware nur den Update-Befehl `esxcli software profile update --depot=depot_location --profile=profile_name`.

Wenn Sie mit **--server=Servername** einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

Hinweis Optionen für die Befehle `update` und `install` ermöglichen es Ihnen, einen Testlauf durchzuführen, einen bestimmten VIB anzugeben, die Verifizierung einer Akzeptanzebene zu umgehen usw. Umgehen Sie die Verifizierung nicht auf Produktionssystemen. Weitere Informationen dazu finden Sie unter *Referenz zur vSphere Command-Line Interface*.

Voraussetzungen

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)- Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.
- Stellen Sie fest, ob sich zum Anwenden des Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss. Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus.

Weitere Informationen hierzu finden Sie unter [Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss..](#) Siehe [Versetzen eines Hosts in den Wartungsmodus](#).

- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

- 1 Stellen Sie fest, welche VIBs auf dem Host installiert sind.

```
esxcli --server=Servername software vib list
```

- 2 Ermitteln Sie, welche Image-Profile im Depot verfügbar sind.

```
esxcli --server=Servername software sources profile list --depot=http://  
Webserver/Name_des_Depots
```

Mithilfe des Arguments **--proxy** können Sie einen Proxy-Server angeben.

- 3 Aktualisieren Sie das vorhandene Image-Profil, sodass es die VIBs enthält, oder installieren Sie neue VIBs.

Wichtig Der Befehl `software profile update` aktualisiert vorhandene VIBs mit den entsprechenden VIBs des angegebenen Profils, beeinflusst aber keine anderen VIBs, die auf dem Zielsystem installiert sind. Der Befehl `software profile install` installiert die VIBs, die sich momentan im Depot-Image-Profil befinden, und entfernt alle anderen auf dem Zielsystem installierten VIBs.

Option	Beschreibung
Aktualisieren Sie das Image-Profil von einem von VMware bereitgestellten ZIP-Paket eines Depots, auf das über die VMware-Website online zugegriffen wird oder das in ein lokales Depot heruntergeladen wurde.	<pre>esxcli software profile update --depot=Depotstandort --profile=Profilname</pre> <p>Wichtig Dies ist die einzige Update-Methode, die VMware für die von VMware gelieferten ZIP-Pakete bereitstellt.</p> <p>Die Namen der von VMware bereitgestellten ZIP-Pakete haben folgendes Format: VMware-ESXi-6.0.0-Build-Nummer-depot.zip</p> <p>Der Profilname für die von VMware bereitgestellten ZIP-Pakete hat folgendes Format.</p> <ul style="list-style-type: none"> ■ ESXi-6.0.0-Build-Nummer-standard ■ ESXi-6.0.0-Build-Nummer-notools (umfasst nicht die VMware Tools)
Aktualisieren des Image-Profils von einem Depot, auf das per URL zugegriffen werden kann	<pre>esxcli --server=Servername software profile update --depot=http://Webserver/Name_des_Depots --profile=Name_des_Profils</pre>
Aktualisieren des Image-Profils von einer ZIP-Datei, die lokal auf dem Zielsystem gespeichert ist	<pre>esxcli --server=Servername software profile update --depot=file:///<Pfad_zur_Profil_ZIP_Datei>/<Profil_ZIP_Datei> --profile=Name_des_Profils</pre>
Aktualisieren des Image-Profils von einer ZIP-Datei auf dem Zielsystem, die in einen Datenspeicher kopiert wird	<pre>esxcli --server=Servername software profile update --depot="[Name_des_Datenspeichers]Profil_ZIP_Datei" --profile=Name_des_Profils</pre>
Aktualisieren des Image-Profils von einer ZIP-Datei, die lokal auf dem Zielsystem kopiert und angewendet wird	<pre>esxcli --server=Servername software profile update --depot=/Stammverzeichnis/Pfad_zur_Profil_ZIP_Datei/Profil_ZIP_Datei --profile=Name_des_Profils</pre>
Installation aller neuen VIBs eines angegebenen Profils, auf das per URL zugegriffen werden kann	<pre>esxcli --server=Servername software profile install --depot=http://webserver/Name_des_Depots --profile=Name_des_Profils</pre>
Installation aller neuen VIBs in einem angegebenen Profil von einer ZIP-Datei, die lokal auf dem Ziel gespeichert ist	<pre>esxcli --server=Servername software profile install --depot=file:///<Pfad_zur_Profil_ZIP_Datei>/<Profil_ZIP_Datei> --profile=Name_des_Profils</pre>

Option	Beschreibung
Installation aller neuen VIBs von einer ZIP-Datei auf dem Zielsystem, die in einen Datenspeicher kopiert wird	<code>esxcli --server=Servername software profile install --depot="[Name_des_Datenspeichers]Profil_ZIP_Datei" --profile=Name_des_Profils</code>
Installation aller neuen VIBs von einer ZIP-Datei, die lokal auf dem Zielsystem kopiert und angewendet wird	<code>esxcli --server=Servername software profile install --depot=/Stammverzeichnis/Pfad_zur_Profil_ZIP_Datei/Profil_ZIP_Datei --profile=Name_des_Profils</code>

Hinweis Optionen für die Befehle `update` und `install` ermöglichen es Ihnen, einen Testlauf durchzuführen, einen bestimmten VIB anzugeben, die Verifizierung einer Akzeptanzebene zu umgehen usw. Umgehen Sie die Verifizierung nicht auf Produktionssystemen. Weitere Informationen dazu finden Sie unter *Referenz zur vSphere Command-Line Interface*.

- 4 Stellen Sie sicher, dass die VIBs auf Ihrem ESXi-Host installiert sind.

```
esxcli --server=Servername software vib list
```

Aktualisieren von ESXi-Hosts mit ZIP-Dateien

Sie können ein Update von Hosts mit VIBs oder Image-Profilen durch Herunterladen einer ZIP-Datei aus einem Depot vornehmen.

VMware-Partner bereiten VIBs von Drittanbietern so vor, dass sie Verwaltungsagenten oder asynchron freigegebene Treiber bereitstellen.

Wichtig Wenn Sie ESXi von einem ZIP-Paket eines von VMware bereitgestellten Depots aktualisieren, auf das über die VMware-Website online zugegriffen werden kann oder das lokal heruntergeladen wurde, unterstützt VMware nur die Update-Methode, die für von VMware bereitgestellte Depots im Abschnitt [Upgrade oder Update eines Hosts mit Image-Profilen](#) angegeben ist.

Die Befehle `esxcli software vib update` und `esxcli software vib install` werden für Upgrade-Vorgänge nicht unterstützt. Siehe [Unterschiede zwischen vSphere-Upgrades und -Updates](#) und [Upgrade oder Update eines Hosts mit Image-Profilen](#).

Wenn Sie mit `--server=Servername` einen Zielsystem angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI-Befehlszeile aus.

Voraussetzungen

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.
- Laden Sie die ZIP-Datei eines Depot-Pakets von einem Drittanbieter-VMware-Partner herunter.
- Stellen Sie fest, ob sich zum Anwenden des Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss. Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus.

Weitere Informationen hierzu finden Sie unter [Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss.](#) Weitere Informationen hierzu finden Sie unter [Versetzen eines Hosts in den Wartungsmodus](#).

- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

- ◆ Installieren Sie die ZIP-Datei.

```
esxcli --server=Servername software vib update --depot=/Pfad-zu_VIB_ZIP/  
ZIP-Dateiname.zip
```

Entfernen von VIBs von einem Host

Sie können VIBs von Drittanbietern oder VMware-VIBs von Ihren ESXi-Hosts deinstallieren.

VMware-Partner bereiten VIBs von Drittanbietern so vor, dass sie Verwaltungsagenten oder asynchron freigegebene Treiber bereitstellen.

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Voraussetzungen

- Falls für das Entfernen ein Neustart erforderlich ist und der Host Bestandteil eines VMware HA-Clusters ist, deaktivieren Sie HA für den Host.
- Stellen Sie fest, ob sich zum Anwenden des Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss. Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus.

Weitere Informationen hierzu finden Sie unter [Stellen Sie fest, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss.](#) Weitere Informationen hierzu finden Sie unter [Versetzen eines Hosts in den Wartungsmodus](#).

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Schalten Sie alle virtuellen Maschinen aus, die auf dem ESXi-Host ausgeführt werden.

Option	Befehl
So schalten Sie das Gastbetriebssystem und anschließend die virtuelle Maschine aus	<code>vmware-cmd --server=ServernamePfad_der_VM stop soft</code>
So erzwingen Sie den Ausschaltvorgang	<code>vmware-cmd --server=ServernamePfad_zur_VM stop hard</code>

Alternativ können Sie die virtuellen Maschinen auf einen anderen Host migrieren, um ihr Ausschalten zu verhindern. Weitere Informationen dazu finden Sie im Thema *Migrieren virtueller Maschinen* in der Dokumentation *vCenter Server und Hostverwaltung*.

- 2 Versetzen Sie den Host in den Wartungsmodus.

```
vicfg-hostops --server=Servername --operation enter
```

- 3 Fahren Sie, falls erforderlich, die virtuellen Maschinen herunter oder migrieren Sie sie.

- 4 Stellen Sie fest, welche VIBs auf dem Host installiert sind.

```
esxcli --server=Servername software vib list
```

- 5 Entfernen des VIB.

```
esxcli --server=Servername software vib remove --vibname=Name
```

Geben Sie einen oder mehrere zu entfernende VIBs in einem der folgenden Formate an:

- **Name**
- **Name:Version**
- **Hersteller:Name**
- **Hersteller:Name:Version**

Der Befehl zum Entfernen eines VIB, der über Hersteller, Name und Version angegeben wird, hätte beispielsweise das folgende Format:

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

Hinweis Der Befehl `remove` unterstützt verschiedene weitere Optionen. Siehe die Dokumentation zu *Referenz zur vSphere Command-Line Interface*.

Hinzufügen von Erweiterungen von Drittanbietern zu Hosts mit einem esxcli-Befehl

Sie können den Befehl `esxcli software vib` verwenden, um dem System eine Erweiterung von einem Drittanbieter hinzuzufügen, die als VIB-Paket erhältlich ist. Wenn Sie diesen Befehl verwenden, aktualisiert das VIB-System den Firewall-Regelsatz und aktualisiert den Hostdämon, nachdem Sie das System neu gestartet haben.

Andernfalls können Sie eine Firewall-Konfigurationsdatei verwenden, um Portregeln für Hostdienste anzugeben, die Sie für die Erweiterung aktivieren möchten. Die Dokumentation *vSphere-Sicherheit* enthält Erläuterungen über das Hinzufügen, Übernehmen und Aktualisieren eines Firewall-Regelsatzes und listet die Befehle `esxcli network firewall` auf.

Durchführen einer esxcli-Testinstallation oder eines esxcli-Test-Upgrades

Sie können die Option `--dry-run` verwenden, um eine Vorschau der Ergebnisse eines Installations- oder Upgrade-Vorgangs zu erhalten. Bei einer Testinstallation bzw. einem Test-Upgrade werden keine Änderungen vorgenommen. Es werden lediglich die Vorgänge auf VIB-Ebene protokolliert, die durchgeführt würden, wenn Sie die Option `--dry-run` nicht angegeben hätten.

Wenn Sie mit `--server=Servername` einen Zielsystem angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI-Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Geben Sie den Installationsbefehl bzw. den Befehl zum Durchführen des Upgrades zusammen mit der Option `--dry-run` ein.

- `esxcli --server=Servername software vib install --dry-run`
- `esxcli --server=Servername software vib update --dry-run`
- `esxcli --server=Servername software profile install --dry-run`
- `esxcli --server=Servername software profile update --dry-run`

- 2 Prüfen Sie die Ausgabe, die zurückgegeben wird.

Die Ausgabe enthält eine Liste der VIBs, die installiert bzw. entfernt wurden, sowie die Information, ob für die Installation bzw. das Upgrade ein Neustart erforderlich wäre.

Anzeigen der installierten VIBs und Profile, die nach dem nächsten Hostneustart aktiv werden

Sie können die Option `--rebooting-image` verwenden, um die VIBs und Profile aufzulisten, die auf dem Host installiert sind und nach dem nächsten Hostneustart aktiv werden.

Wenn Sie mit `--server=Servername` einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Geben Sie einen der folgenden Befehle ein.

Option	Beschreibung
Für VIBs	<code>esxcli --server=Servername software vib list --rebooting-image</code>
Für Profile	<code>esxcli --server=Servername software profile get --rebooting-image</code>

- 2 Prüfen Sie die Ausgabe, die zurückgegeben wird.

Die Ausgabe zeigt Informationen für das ESXi-Image an, das nach dem nächsten Neustart aktiv wird. Falls das „pending-reboot“-Image noch nicht erstellt wurde, gibt die Ausgabe nichts zurück.

Anzeigen des Image-Profiles und der Akzeptanzebene des Hosts

Sie können den Befehl `software profile get` verwenden, um das derzeit installierte Image-Profil und die Akzeptanzebene für den angegebenen Host anzuzeigen.

Dieser Befehl zeigt darüber hinaus Einzelheiten zum Verlauf des installierten Image-Profiles an, wie z. B. Profiländerungen.

Wenn Sie mit **--server=Servername** einen Zielservers angeben, fordert der Server Sie auf, einen Benutzernamen und ein Kennwort einzugeben. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces* oder führen Sie `esxcli --help` an der vCLI- Befehlszeile aus.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

- 1 Geben Sie den folgenden Befehl ein.

```
esxcli --server=Servername software profile get
```

- 2 Prüfen Sie die Ausgabe.

Interaktives Upgrade von Hosts

Sie können das ESXi-Installationsprogramm von einer CD, DVD oder einem USB-Flash-Laufwerk starten, um ein Upgrade von ESXi 5.x-Hosts auf ESXi 6.0 durchzuführen.

Achten Sie vor dem Upgrade darauf, die Verbindung zum Netzwerkspeicher zu trennen. Dies verkürzt die Zeit, die das Installationsprogramm zur Suche nach verfügbaren Festplattenlaufwerken benötigt. Nach dem Trennen des Netzwerkspeichers stehen alle Dateien auf den getrennten Festplatten nicht für die Installation zur Verfügung. Trennen Sie keine LUN, die eine vorhandene ESXi-Installation enthält.

Voraussetzungen

- Stellen Sie sicher, dass die ISO-Datei des ESXi-Installationsprogramms in einem der folgenden Speicherorte vorhanden ist.
 - Auf CD oder DVD. Wenn Sie nicht über die Installations-CD bzw. -DVD verfügen, können Sie eine erstellen. Siehe [Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD](#).
 - Auf einem USB-Flash-Laufwerk. Siehe [Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades](#).

Hinweis Sie können das ESXi-Installationsprogramm auch per PXE-Startvorgang starten, um eine interaktive Installation oder Skriptinstallation auszuführen. Siehe [Starten des ESXi-Installationsprogramms per PXE-Startvorgang](#).

- Stellen Sie sicher, dass der Server-Hardwaretaktgeber auf UTC eingestellt ist. Diese Einstellung befindet sich im System-BIOS.

- ESXi Embedded darf sich nicht auf dem Host befinden. ESXi Installable und ESXi Embedded dürfen sich nicht auf demselben Host befinden.
- Wenn Sie ein Upgrade eines 5.0.x- oder 5.1.x-Hosts durchführen, werden unterstützte benutzerdefinierte VIBs migriert, die nicht in der ISO-Datei des ESXi-Installationsprogramms enthalten sind. Siehe [Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern](#).
- Informationen zum Ändern der Startreihenfolge finden Sie in der Dokumentation Ihres Hardwareanbieters.

Verfahren

- 1 Legen Sie die CD bzw. DVD des ESXi-Installationsprogramms in das CD-ROM- bzw. DVD-ROM-Laufwerk ein oder schließen Sie das USB-Flash-Laufwerk des Installationsprogramms an und starten Sie die Maschine neu.
- 2 Stellen Sie im BIOS ein, dass vom CD-ROM-Gerät oder vom USB-Flash-Laufwerk gestartet wird.
- 3 Wählen Sie im Bereich „Festplatte auswählen“ das Laufwerk aus, auf dem ESXi installiert oder aktualisiert werden soll, und drücken Sie die Eingabetaste.

Drücken Sie F1, um Informationen zur ausgewählten Festplatte anzuzeigen.

Hinweis Verlassen Sie sich beim Auswählen einer Festplatte nicht auf die Festplattierreihenfolge in der Liste. Die Reihenfolge der Festplatten wird im BIOS festgelegt. Bei Systemen, in denen ständig Laufwerke hinzugefügt und entfernt werden, ist die Reihenfolge möglicherweise durcheinander geraten.

- 4 Aktualisieren oder installieren Sie ESXi, falls das Installationsprogramm eine vorhandene ESXi-Installation und einen vorhandenen VMFS-Datenspeicher findet.

Wenn ein vorhandener VMFS-Datenspeicher nicht beibehalten werden kann, können Sie wahlweise nur ESXi installieren und den vorhandenen VMFS-Datenspeicher überschreiben oder die Installation abbrechen. Wenn Sie wählen, den vorhandenen VMFS-Datenspeicher zu überschreiben, sichern Sie zuerst den Datenspeicher.
- 5 Drücken Sie zur Bestätigung und zum Start des Upgrades F11.
- 6 Entfernen Sie nach Abschluss des Upgrades die Installations-CD/-DVD bzw. das USB-Flash-Laufwerk.
- 7 Drücken Sie die Eingabetaste, um den Host neu zu starten.
- 8 Legen Sie als erstes Startgerät das Laufwerk fest, das Sie zuvor beim Upgrade von ESXi ausgewählt haben.

Nach dem Upgrade von ESXi-Hosts

10

Um ein Host-Upgrade auszuführen, stellen Sie sicher, dass der Host wieder mit seinem verwaltenden vCenter Server-System verbunden wird und bei Bedarf neu konfiguriert wird. Außerdem prüfen Sie, ob der Host korrekt lizenziert ist.

Führen Sie nach dem Aktualisieren eines ESXi-Hosts die folgenden Aktionen aus:

- Prüfen Sie die Upgrade-Protokolle. Sie können vSphere Web Client zum Exportieren der Protokolldateien verwenden.
- Wenn ein vCenter Server-System den Host verwaltet, müssen Sie den Host mit vCenter Server erneut verbinden, indem Sie in der vCenter Server-Bestandsliste mit der rechten Maustaste auf den Host klicken und **Verbinden** wählen.
- Wenn das Upgrade erfolgreich abgeschlossen ist, befindet sich der ESXi-Host im Testmodus. Der Testzeitraum beträgt 60 Tage. Sie müssen eine vSphere 6.0-Lizenz zuweisen, bevor der Testzeitraum abläuft. Sie können vorhandene Lizenzen aktualisieren oder bei Customer Connect neue erwerben. Verwenden Sie vSphere Web Client zum Konfigurieren der Lizenzierung für die Hosts in Ihrer Umgebung. In der Dokumentation *vCenter Server und Hostverwaltung* finden Sie ausführliche Informationen zum Verwalten von Lizenzen in vSphere.
- Die sdX-Hostgeräte sind nach dem Upgrade möglicherweise neu nummeriert. Aktualisieren Sie bei Bedarf alle Skripts, die auf sdX-Geräte verweisen.
- Aktualisieren Sie virtuelle Maschinen auf dem Host. Weitere Informationen hierzu finden Sie unter [Kapitel 11 Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools](#).

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zum ESXi-Testmodus und -Lizenzmodus](#)
- [Anwenden von Lizenzen nach einem Upgrade auf ESXi 6.0](#)
- [Erforderlicher freier Speicherplatz für die Systemprotokollierung](#)
- [Konfiguration von Syslog auf ESXi-Hosts](#)

Grundlegendes zum ESXi-Testmodus und -Lizenzmodus

Mit dem Testmodus können Sie alle Funktionen von ESXi-Hosts kennenlernen. Im Testmodus sind die gleichen Funktionen wie mit einer vSphere Enterprise Plus-Lizenz verfügbar. Vor Ablauf

des Testmodus müssen Sie Ihren Hosts eine Lizenz zuweisen, die alle genutzten Funktionen unterstützt.

Beispielsweise können Sie im Testmodus vSphere vMotion-Technologie, die vSphere HA-Funktion, die vSphere DRS-Funktion und andere Funktionen nutzen. Wenn Sie diese Funktionen weiter nutzen möchten, müssen Sie ihnen eine Lizenz zuweisen, die sie unterstützt.

Die installierbare Version von ESXi-Hosts wird immer im Testmodus installiert. ESXi Embedded wird von Ihrem Hardwareanbieter auf einem internen Speichergerät vorinstalliert. Es ist möglicherweise im Testmodus oder vorlizenziert.

Die Testperiode beträgt 60 Tage und beginnt mit dem Einschalten des ESXi-Host. Während der 60-tägigen Testphase können Sie jederzeit vom lizenzierten Modus in den Testmodus wechseln. Die in der Testperiode verfügbare Zeit wird um die bereits genutzte Zeit reduziert.

Angenommen, Sie haben einen ESXi-Host im Testmodus bereits seit 20 Tagen verwendet und weisen dann dem Host einen vSphere Standard Edition-Lizenzschlüssel zu. Wenn Sie den Host auf den Testmodus zurücksetzen, können Sie alle Funktionen des Hosts während der verbleibenden 40 Tage im Testmodus nutzen.

Informationen zur Lizenzierung für ESXi-Hosts finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Anwenden von Lizenzen nach einem Upgrade auf ESXi 6.0

Nach einem Upgrade auf ESXi 6.0 müssen Sie eine vSphere 6.0-Lizenz anwenden.

Wenn Sie ein Upgrade von ESXi 5.x-Hosts auf ESXi 6.0-Hosts durchführen, gilt für die Hosts ein Testzeitraum von 60 Tagen bis zur Anwendung der eigentlichen vSphere 6.0-Lizenzen. Weitere Informationen hierzu finden Sie unter [Grundlegendes zum ESXi-Testmodus und -Lizenzmodus](#).

Sie können ein Upgrade Ihrer vorhandenen vSphere 5.x-Lizenzen durchführen oder vSphere 6.0-Lizenzen über Customer Connect erwerben. Wenn Sie über vSphere 6.0-Lizenzen verfügen, müssen Sie diese auf alle aktualisierten ESXi 6.0-Hosts mithilfe der Lizenzmanagementfunktion im vSphere Web Client anwenden. Weitere Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*. Wenn Sie für das Upgrade auf ESXi 6.0 die Skriptmethode verwenden, können Sie den Lizenzschlüssel in der Kickstart-Datei (ks) angeben.

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Wenn Sie Auto Deploy für die Installation Ihres ESXi 6.0-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volume eingerichtet haben, müssen Sie möglicherweise die aktuellen Einstellungen für die Protokollgröße und die Rotation ändern, um sicherzustellen, dass ausreichend Speicherplatz für die Systemprotokollierung verfügbar ist.

Alle vSphere-Komponenten verwenden diese Infrastruktur. Die Standardwerte für die Protokollkapazität in dieser Infrastruktur variieren je nach verfügbarem Speicherplatz und je nach Konfiguration der Systemprotokollierung. Hosts, die mit Auto Deploy bereitgestellt werden, speichern Protokolle auf einer RAM-Festplatte. Der verfügbare Speicherplatz für Protokolle ist daher gering.

Wenn Ihr Host mit Auto Deploy bereitgestellt wurde, stehen Ihnen für die Konfiguration des Protokollspeichers folgende Möglichkeiten zur Verfügung:

- Leiten Sie die Protokolle über das Netzwerk zu einem Remote-Controller um.
- Leiten Sie die Protokolle zu einem NAS- oder NFS-Speicher um.

Wenn Sie Protokolle an einen nicht standardmäßigen Speicher umleiten, zum Beispiel an einen NAS- oder NFS-Speicher, können Sie die Größe und Rotation der auf der Festplatte installierten Hosts ebenfalls neu konfigurieren.

Sie müssen den Protokollspeicher für ESXi-Hosts nicht neu konfigurieren, die die Standardkonfiguration verwenden, bei der Protokolle in einem Scratch-Verzeichnis auf dem VMFS-Volume gespeichert werden. Für diese Hosts konfiguriert ESXi 6.0 die Protokolle in optimaler Abstimmung mit Ihrer Installation und bietet ausreichend Speicherplatz für Protokollnachrichten.

Tabelle 10-1. Empfohlene Mindestgröße und Rotationskonfiguration für hostd-, vpxa- und fdm-Protokolle

Protokoll	Maximale Protokolldateigröße	Anzahl der beizubehaltenden Rotationen	Mindestens erforderlicher Festplattenspeicher
Verwaltungs-Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA-Agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

Informationen zum Einrichten und Konfigurieren des Syslog-Protokolls und eines Syslog-Servers und zum Installieren von vSphere Syslog Collector finden Sie in der Dokumentation zu *Installations- und Einrichtungshandbuch für vSphere*.

Konfiguration von Syslog auf ESXi-Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vm syslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Web Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Dienstes verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

Verfahren

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Web Client aus.
- 2 Klicken Sie auf die Registerkarte **Verwalten**.
- 3 Klicken Sie im Bereich „System“ auf **Erweiterte Einstellungen**.
- 4 Suchen Sie den Bereich **Syslog** in der Liste „Erweiterte Systemeinstellungen“.
- 5 Um das Protokollieren global einzurichten, wählen Sie die zu ändernde Einstellung aus und klicken Sie auf das Symbol „Bearbeiten“.

Option	Beschreibung
Syslog.global.defaultRotate	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis <code>/scratch</code> auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format <code>[Datenspeichername] Pfad_zur_Datei</code> aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <code>[storage1] /systemlogs</code> dem Pfad <code>/vmfs/volumes/storage1/systemlogs</code> zuzuordnen.
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von Syslog.global.LogDir angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. <code>ssl://Hostname1:1514</code> . UDP (Standard), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

- 6 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll.
 - a Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten.
 - b Klicken Sie auf das Symbol „Bearbeiten“ und geben Sie die Anzahl der Rotationen und die Protokollgröße an, die Sie verwenden möchten.
- 7 Klicken Sie auf **OK**.

Ergebnisse

Änderungen an der syslog-Option werden sofort wirksam.

Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools

11

Nachdem Sie ein Upgrade der ESXi-Hosts durchgeführt haben, können Sie ein Upgrade der virtuellen Maschinen auf dem Host durchführen, damit Sie die neuen Funktionen nutzen können.

VMware stellt die folgenden Tools für das Durchführen eines Upgrades von virtuelle Maschinen zur Verfügung:

vSphere Web Client

Setzt voraus, dass Sie schrittweise ein Upgrade der virtuellen Maschine durchführen. vSphere Update Manager ist jedoch nicht erforderlich. Weitere Informationen zum Upgrade virtueller Maschinen finden Sie in der *vSphere-Administratorhandbuch für virtuelle Maschinen*-Dokumentation.

vSphere Update Manager

Automatisiert den Upgrade- und Patch-Prozess für die virtuellen Maschinen, wodurch sichergestellt wird, dass die Schritte in der richtigen Reihenfolge stattfinden. Mit dem Update Manager können Sie die Hardwareversion der virtuellen Maschine und VMware Tools direkt aktualisieren. Informationen finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*.

Fehlerbehebung eines vSphere-Upgrades

12

Mit der Installations- und Upgradesoftware können Sie Probleme auf der Hostmaschine aufdecken, die zu einem Fehlschlag der Installation, des Upgrades oder der Migration führen können.

Bei interaktiven Installationen, Upgrades und Migrationen werden die Fehler oder Warnungen im letzten Bereich des Installationsprogramms angezeigt, in dem Sie aufgefordert werden, die Installation oder das Upgrade zu bestätigen oder abubrechen. Bei Skriptinstallationen, -Upgrades oder -Migrationen werden die Fehler oder Warnungen in die Installationsprotokolldatei geschrieben. Darüber hinaus finden Sie Informationen zu bekannten Problemen in den Versionshinweisen zum Produkt.

vSphere Update Manager bietet benutzerdefinierte Meldungen für diese Fehler oder Warnungen. Überprüfen Sie die Update Manager-Protokolldatei `vmware-vum-server-log4cpp.log`, um die ursprünglichen Fehler und Warnungen anzusehen, die während einer Host-Upgrade-Prüfung des Update Managers vom Skript für die Vorabprüfung zurückgegeben wurden.

Im *vSphere-Upgrade-Handbuch* wird die Verwendung von VMware-Produkten und ihrer Funktionen beschrieben. Wenn in diesem Handbuch nicht beschriebene Probleme oder Fehlersituationen auftreten, finden Sie eine Lösung dafür gegebenenfalls in der VMware-Knowledgebase. Sie können auch auf die Community-Foren von VMware zurückgreifen, um nach anderen Anwendern zu suchen, bei denen dasselbe Problem auftritt, oder um Hilfe zu erbitten. Alternativ können Sie eine Supportanfrage öffnen, um Hilfe von den Servicemitarbeitern von VMware zu erhalten.

Dieses Kapitel enthält die folgenden Themen:

- Erfassen von Protokollen für die Fehlerbehebung bei einer vCenter Server-Installation oder einem Upgrade
- Erfassen von Protokollen zur Fehlerbehebung bei ESXi-Hosts
- Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden
- Wiederherstellen von vCenter Server-Diensten bei einem fehlgeschlagenen Upgrade
- Fehler bei VMware Component Manager während des Starts nach dem Upgrade von vCenter Server Appliance

- Eine Microsoft SQL-Datenbank, bei der ein nicht unterstützter Kompatibilitätsmodus festgelegt ist, sorgt dafür, dass das Installieren oder das Upgrade von vCenter Server fehlschlägt

Erfassen von Protokollen für die Fehlerbehebung bei einer vCenter Server-Installation oder einem Upgrade

Sie können Installations- oder Upgrade-Protokolldateien für vCenter Server erfassen. Wenn eine Installation oder ein Upgrade fehlschlägt, kann die Prüfung der Protokolldateien Sie bei der Identifizierung der Fehlerquelle unterstützen.

Sie können die Installationsassistent-Methode oder die manuelle Methode wählen, um Protokolldateien für den Fall eines Installationsfehlers bei vCenter Server für Windows zu speichern und wiederherzustellen.

Sie können auch Bereitstellungsprotokolldateien für vCenter Server Appliance erfassen.

Erfassen von Installationsprotokollen mithilfe des Installationsassistenten

Sie können die Seite für unterbrochenes Setup des Installationsassistenten verwenden, um zu der erstellten .zip-Datei der Installationsprotokolldateien von vCenter Server für Windows zu gehen.

Wenn die Installation fehlschlägt, wird die Seite zum unterbrochenen Setup angezeigt. Darauf sind die Kontrollkästchen für die Protokollerfassung standardmäßig aktiviert.

Verfahren

- 1 Lassen Sie die Kontrollkästchen aktiviert und klicken Sie auf **Fertig stellen**.

Die Installationsdateien werden in einer ZIP-Datei auf Ihrem Desktop abgelegt, zum Beispiel *VMware-VCS-logs-Zeitpunkt-des-Installationsversuchs.zip*; dabei steht *Zeitpunkt-des-Installationsversuchs* für das Jahr, den Monat, den Tag, die Stunde, Minuten und Sekunden des Installationsversuchs.

- 2 Rufen Sie die Protokolldateien aus der .zip-Datei auf dem Desktop ab.

Nächste Schritte

Prüfen Sie die Protokolldateien, um die Fehlerursache zu ermitteln.

Manuelles Abrufen der Installationsprotokolle

Sie können die Installationsprotokolldateien zu Prüfzwecken manuell abrufen.

Verfahren

- 1 Navigieren Sie zu den Speicherorten der Installationsprotokolldateien.
 - Verzeichnis %PROGRAMDATA%\VMware\vCenterServer\logs, in der Regel
C:\Programme\VMware\vCenterServer\logs

- Verzeichnis %TEMP%, in der Regel C:\Users\username\AppData\Local\Temp

Zu den Dateien im Verzeichnis %TEMP% zählen `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log` und `vim-vcs-msi.log`.

- Öffnen Sie die Installationsprotokolldateien in einem Texteditor, um sie zu prüfen.

Erfassen von Installationsprotokollen für die vCenter Server Appliance

Sie können Installationsprotokolldateien erfassen und diese Dateien prüfen, um die Quelle eines Fehlers zu identifizieren, wenn vCenter Server Appliance während des anfänglichen Startvorgangs nicht mehr reagiert.

Verfahren

- Greifen Sie auf die Appliance-Shell zu.

Option	Beschreibung
Wenn Sie direkten Zugriff auf die Appliance haben:	Drücken Sie Alt+F1.
Um eine Remoteverbindung herzustellen:	Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf der Appliance zu starten.

- Geben Sie einen Benutzernamen und ein Kennwort ein, die von der Appliance erkannt werden.
- Führen Sie in der Appliance-Shell den Befehl `pi shell` aus, um auf die Bash-Shell zuzugreifen.
- Führen Sie in der Bash-Shell das Skript `vc-support.sh` aus, um ein Support-Paket zu generieren.

Mit diesem Befehl wird eine `.tgz`-Datei in `/var/tmp` generiert.

- Exportieren Sie das generierte Support-Paket in den Ordner `user@x.x.x.x:/tmp`.

```
scp /var/tmp/vc-etco-vm-vlan11-dhcp-63-151.eng.vmware.com-2014-02-28--21.11.tgz
user@x.x.x.x:/tmp
```

- Prüfen Sie, welches `firstboot`-Skript fehlgeschlagen ist.

```
cat /var/log/firstboot/firstbootStatus.json
```

Nächste Schritte

Um mögliche Fehlerursachen zu identifizieren, prüfen Sie die Protokolldatei des fehlgeschlagenen `firstboot`-Skripts.

Erfassen der Upgradeprotokolle für die Datenbank

Sie können die Protokolldateien für das Datenbank-Upgrade zu Prüfzwecken manuell abrufen.

Sie können die Datenbank-Upgrade-Protokolle abrufen, nachdem Sie den Upgrade-Prozess für vCenter Server abgeschlossen haben.

Voraussetzungen

Verfahren

- 1 Navigieren Sie zu den Speicherorten der Datenbank-Upgrade-Protokolle.
- 2 Öffnen Sie die Datenbank-Upgrade-Protokolle in einem Texteditor, um sie zu prüfen.

Ergebnisse

Sie können die Protokolldateien auf Details zu den Datenbank-Upgrade-Prozessen prüfen.

Beispiel: Datenbank-Upgrade-Speicherorte

- Für Prüfungen vor dem Upgrade prüfen Sie die Datei `%TEMP%\..\vcsUpgrade\vcdb_req.out`.
Die Datei „vcdb_req.err“ verfolgt alle Fehler, die in der Phase vor dem Upgrade identifiziert wurden.
- Exportdetails finden Sie in der Datei `%TEMP%\..\vcsUpgrade\vcdb_export.out`.
Die Datei „vcdb_export.err“ enthält Fehler, die während der Exportphase des Upgrade identifiziert wurden.
- Importdetails finden Sie in der Datei `ProgramData\VMware\CIS\logs\vmware\vpv\vcdb_import.out`.
Die Datei „vcdb_import.err“ enthält Fehler, die während der Importphase des Upgrade-Prozesses identifiziert wurden.
- Details zum aktuellen Upgrade finden Sie in der Datei `ProgramData\VMware\CIS\logs\vmware\vpv\vcdb_inplace.out`.
Die Datei „vcdb_inplace.err“ enthält Fehler des aktuellen Upgrades.

Nächste Schritte

Prüfen Sie die Protokolldateien „vcdb_inplace.*“.

Erfassen von Protokollen zur Fehlerbehebung bei ESXi-Hosts

Sie können die Protokolldateien für Installationen oder Upgrades von ESXi erfassen. Wenn eine Installation oder ein Upgrade fehlschlägt, kann die Prüfung der Protokolldateien Sie bei der Identifizierung der Fehlerquelle unterstützen.

Lösung

- 1 Geben Sie den Befehl `vm-support` über die ESXi Shell oder SSH aus.
- 2 Gehen Sie zum Verzeichnis `/var/tmp/`.
- 3 Rufen Sie die Protokolldateien aus der `.tgz`-Datei ab.

Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden

Das Skript für die Vorabprüfung der Installation und des Upgrades führt Tests durch, um Probleme auf der Hostmaschine aufzudecken, die zu einem Fehlschlag der Installation, des Upgrades oder der Migration führen können.

Bei interaktiven Installationen, Upgrades und Migrationen werden die Fehler oder Warnungen im letzten Bereich des Installationsprogramms angezeigt, in dem Sie aufgefordert werden, die Installation oder das Upgrade zu bestätigen oder abubrechen. Bei Skriptinstallationen, -Upgrades oder -Migrationen werden die Fehler oder Warnungen in die Installationsprotokolldatei geschrieben.

vSphere Update Manager bietet benutzerdefinierte Meldungen für diese Fehler oder Warnungen. Die ursprünglichen Fehler und Warnungen, die während einer Host-Upgrade-Prüfung durch den Update Manager vom Vorabprüfungsskript zurückgegeben wurden, finden Sie in der Update Manager-Protokolldatei `vmware-vum-server-log4cpp.log`.

Tabelle 12-1. Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden

Fehler oder Warnung	Beschreibung
64BIT_LONGMODESTATUS	Der Hostprozessor muss ein 64-Bit-Prozessor sein.
COS_NETWORKING	Warnung. Es wurde eine IPv4-Adresse auf einer aktivierten virtuellen Netzwerkkarte der Servicekonsole gefunden, für die es keine entsprechende Adresse im selben VMkernel-Subnetz gibt. Für jedes Vorkommen wird eine separate Warnung ausgegeben.
CPU_CORES	Der Host muss mindestens zwei Kerne haben.

Tabelle 12-1. Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden (Fortsetzung)

Fehler oder Warnung	Beschreibung
DISTRIBUTED_VIRTUAL_SWITCH	Wenn auf dem Host die Software Cisco Virtual Ethernet Module (VEM) gefunden wird, überprüft der Test, ob das Upgrade VEM ebenfalls enthält. Der Test ermittelt auch, ob das Upgrade die gleiche Version des Virtual Supervisor Module (VSM) wie die auf dem Host vorhandene Version unterstützt. Wenn die Software fehlt oder mit einer anderen Version des VSM kompatibel ist, gibt der Test eine Warnung zurück. Das Ergebnis gibt die Version der VEM-Software, die auf dem Upgrade-ISO-Image erwartet wurde, sowie die gefundenen Versionen, sofern vorhanden, zurück. Sie können ESXi Image Builder CLI zum Erstellen eines benutzerdefinierten Installations-ISO-Image verwenden, das die entsprechende Version der VEM-Software enthält.
HARDWARE_VIRTUALIZATION	Warnung. Wenn der Hostprozessor über keine Hardwarevirtualisierung verfügt oder die Hardwarevirtualisierung nicht im Host-BIOS aktiviert ist, wird die Hostleistung beeinträchtigt. Aktivieren Sie die Hardwarevirtualisierung in den Startoptionen der Hostmaschine. Weitere Informationen finden Sie in der Dokumentation Ihres Hardwareanbieters.
MD5_ROOT_PASSWORD	Dieser Test überprüft, ob das Root-Kennwort im MD5-Format verschlüsselt ist. Wenn ein Kennwort nicht im MD5-Format verschlüsselt ist, sind möglicherweise nur die ersten acht Zeichen signifikant. In diesem Fall werden nach dem Upgrade alle Zeichen nach den ersten acht Zeichen nicht mehr authentifiziert, was zu einem Sicherheitsproblem führen kann. Wie Sie dieses Problem umgehen, erfahren Sie im VMware-Knowledgebase-Artikel 1024500 .
MEMORY_SIZE	Der Host benötigt für das Upgrade die angegebene Menge an Arbeitsspeicher.
PACKAGE_COMPLIANCE	Nur vSphere Update Manager. Dieser Test vergleicht die vorhandene Software auf dem Host mit der Software auf dem Upgrade-ISO-Image, um festzustellen, ob das Upgrade des Hosts ordnungsgemäß durchgeführt wurde. Falls eines der Pakete fehlt oder eine ältere Version als das Paket auf dem Upgrade-ISO-Image aufweist, gibt der Test einen Fehler zurück und gibt an, welche Software auf dem Host und welche Software auf dem Upgrade-ISO-Image gefunden wurde.
PARTITION_LAYOUT	Ein Upgrade oder eine Migration ist nur möglich, wenn es auf der Festplatte, die aktualisiert werden soll, höchstens eine VMFS-Partition gibt und die VMFS-Partition nach Sektor 1843200 beginnt.

Tabelle 12-1. Fehler und Warnungen, die vom Skript für die Vorabprüfung der Installation und des Upgrades zurückgegeben werden (Fortsetzung)

Fehler oder Warnung	Beschreibung
POWERPATH	Das Skript überprüft, ob die EMC PowerPath-Software installiert ist, die aus einem CIM-Modul und einem Kernelmodul besteht. Wenn eine dieser Komponenten auf dem Host gefunden wurde, überprüft der Test, ob die passenden Komponenten (z. B. CIM, VMkernel oder Modul) ebenfalls im Upgrade vorhanden sind. Ist dies nicht der Fall, gibt das Skript eine Warnung zurück mit dem Hinweis, welche PowerPath-Komponenten auf dem Upgrade-ISO erwartet wurden und welche, wenn überhaupt, gefunden wurden.
PRECHECK_INITIALIZE	Dieser Test überprüft, ob das Skript für die Vorabprüfung ausgeführt werden kann.
SANE_ESX_CONF	Die Datei <code>/etc/vmware/esx.conf</code> muss auf dem Host vorhanden sein.
SPACE_AVAIL_ISO	Nur vSphere Update Manager. Die Hostfestplatte muss über genügend freien Speicherplatz verfügen, um den Inhalt der Installations-CD bzw. -DVD zu speichern.
SPACE_AVAIL_CONFIG	Nur vSphere Update Manager. Die Hostfestplatte muss über genügend freien Speicherplatz verfügen, um die 5.x-Konfiguration zwischen Neustarts speichern zu können.
SUPPORTED_ESX_VERSION	Ein Upgrade bzw. eine Migration auf ESXi 6.0 ist nur von ESXi-Hosts Version 5.x möglich.
TBOOT_REQUIRED	Diese Meldung bezieht sich nur auf vSphere Update Manager-Upgrades. Das Upgrade schlägt mit diesem Fehler fehl, wenn das Hostsystem im „Trusted“-Startmodus (tboot) ausgeführt wird, das ESXi-Upgrade-ISO-Image jedoch keine tboot-VIBs enthält. Dieser Test verhindert ein Upgrade, das den Host weniger sicher macht.
UNSUPPORTED_DEVICES	Warnung. Das Skript prüft auf nicht unterstützte Geräte. Einige PCI-Geräte werden von ESXi 6.0 nicht unterstützt.
UPDATE_PENDING	Dieser Test prüft den Host auf VIB-Installationen, die einen Neustart erfordern. Dieser Test schlägt fehl, wenn mindestens ein VIB installiert ist, der Host jedoch noch nicht neu gestartet wurde. Unter diesen Voraussetzungen kann das Skript für die Vorabprüfung nicht zuverlässig ermitteln, welche Pakete derzeit auf dem Host installiert sind. Daher ist es möglicherweise nicht sicher, auf den Rest der Vorabprüfung zu vertrauen, um festzustellen, ob ein Upgrade sicher ist. Falls dieser Fehler auftritt, starten Sie den Host neu und führen Sie das Upgrade erneut durch.

Wiederherstellen von vCenter Server-Diensten bei einem fehlgeschlagenen Upgrade

Wenn ein Upgrade von vCenter Server mit externem Platform Services Controller fehlschlägt, müssen Sie vCenter Inventory Service oder andere vCenter Server-Dienste manuell wiederherstellen bzw. erneut darauf verweisen.

Problem

Wenn das Upgrade von vCenter Server nach der Deinstallationsphase fehlschlägt und die Installation auf den vorherigen Status zurückgesetzt wird (vCenter Server 5.1 oder 5.5), werden vCenter Inventory Service oder andere vCenter Server-Dienste möglicherweise nicht für die vCenter Single Sign On-Instanz von Platform Services Controller 6.0 neu registriert.

Ursache

Die Registrierung von vCenter Inventory Service und anderen vCenter Server-Diensten wird für vCenter Single Sign On 5.1 oder 5.5 während des Upgrades auf vCenter Server 6.0 aufgehoben. Schlägt ein Upgrade fehl, nachdem die Registrierung der Dienste aufgehoben wurde, gehen die Registrierungsinformationen verloren. Wenn das Upgrade auf vCenter Server 6.0 fortgesetzt wird, erkennt das Installationsprogramm nicht registrierte Dienste und lässt sie unregistriert. vCenter Inventory Service oder andere vCenter Server-Dienste müssen für die neu aktualisierte Platform Services Controller 6.0-Instanz manuell registriert bzw. erneut darauf verwiesen werden. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel [2033620](#).

Lösung

- ◆ Befolgen Sie die Anweisungen im Knowledgebase-Artikel, um diese Dienste erneut für vCenter Single Sign On zu registrieren bzw. erneut darauf zu verweisen.

Fehler bei VMware Component Manager während des Starts nach dem Upgrade von vCenter Server Appliance

vCenter Server Appliance Component Manager schlägt bei der erstmaligen Bereitstellung nach einem Upgrade fehl.

Problem

Sie stellen eine vCenter Server Appliance-Instanz bereit und es wird eine Fehlermeldung angezeigt, die so oder ähnlich lautet:

„Fehler beim Ausführen des Skripts zum erstmaligen Laden.“

„Das SSL-Zertifikat stimmt bei Verbindungsherstellung mit vCenter Single Sign On nicht überein: Hostname im Zertifikat stimmt nicht überein: <vcenter-b.domain.com> != <localhost.localdom> ODER <localhost.localdom> ODER <localhost>“

Ursache

Die vCenter Server Appliance-Instanznamen stimmen nicht mit den Namen in den SSL-Zertifikaten überein. Sie müssen die Zertifikate neu generieren, um die ordnungsgemäßen vollqualifizierten Domännennamen zu erhalten.

Lösung

- 1 Aktivieren Sie die vCenter Server Appliance 5.5-Instanz.
- 2 Melden Sie sich bei der VAMI <https://IP:5480> an.
- 3 Stellen Sie sicher, dass in den Netzwerkeinstellungen die richtige IP-Adresse und der richtige Hostname festgelegt sind.
- 4 Aktivieren Sie das Kontrollkästchen Zertifikatsneugenerierung.
- 5 Starten Sie die vCenter Server Appliance 5.5-Instanz neu.

Die Zertifikate für vCenter Server, vSphere Web Client, vami, slapd, vCenter Inventory Service und vCenter Single Sign On werden neu generiert. Dabei enthält ein Zertifikat CN=vcenter-a.domain.com, und SubjectAltName enthält DNS=vcenter-a.domain.com DNS=vcenter-a IP=192.168.2.100. Nicht mehr enthalten in den Zertifikaten ist *vcenter-b.domain.com*.

- 6 Führen Sie das Upgrade von vCenter Server Appliance 6.0 erneut durch.

Lösung

Siehe [Upgrade von vCenter Server Appliance mit eingebetteter vCenter Single Sign-On-Instanz](#).

Eine Microsoft SQL-Datenbank, bei der ein nicht unterstützter Kompatibilitätsmodus festgelegt ist, sorgt dafür, dass das Installieren oder das Upgrade von vCenter Server fehlschlägt

Die vCenter Server-Installation mit einer Microsoft SQL-Datenbank schlägt fehl, wenn die Datenbank so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird.

Problem

Die folgende Fehlermeldung erscheint: Der eingegebene Datenbankbenutzer verfügt nicht über die erforderlichen Berechtigungen zum Installieren und Konfigurieren von vCenter Server mit der ausgewählten Datenbank. Beheben Sie die folgenden Fehler: %s

Ursache

vCenter Server muss die Datenbankversion unterstützen. Wenn die Datenbank so eingestellt ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird, tritt dieser Fehler bei SQL auch dann auf, wenn es sich bei der Datenbank um eine unterstützte Version handelt. Wenn beispielsweise SQL 2008 für die Ausführung im SQL 2000-Kompatibilitätsmodus eingestellt ist, tritt dieser Fehler auf.

Lösung

- ◆ Stellen Sie sicher, dass es sich bei der vCenter Server-Datenbank um eine unterstützte Version handelt und sie nicht so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.