

VMware ESXi-Upgrade

17. APR 2018

VMware vSphere 6.7

VMware ESXi 6.7



vmware®

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

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

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

docfeedback@vmware.com

VMware, Inc.

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

VMware Global, Inc.

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

Copyright © 2018 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

Inhalt

- 1** Grundlegende Informationen zum VMware ESXi-Upgrade 4
- 2** Einführung in das vSphere-Upgrade 5
 - Übersicht über den vSphere-Upgrade-Vorgang 5
- 3** Upgrade der ESXi-Hosts 11
 - Anforderungen für ESXi 11
 - Vor dem Upgrade der ESXi-Hosts 22
 - Interaktives Upgrade von Hosts 37
 - Installieren oder Upgraden von Hosts mithilfe eines Skripts 38
 - Starten des ESXi -Installationsprogramms mit PXE 56
 - Aktualisieren von Hosts mithilfe von esxcli-Befehlen 63
 - Nach dem Upgrade von ESXi -Hosts 78
- 4** Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts 84
 - Einführung in vSphere Auto Deploy 84
 - Vorbereitung für vSphere Auto Deploy 87
 - Erneute Bereitstellung von Hosts 94
- 5** Erfassen von Protokollen zur Fehlerbehebung bei ESXi -Hosts 101

Grundlegende Informationen zum VMware ESXi-Upgrade

1

VMware ESXi-Upgrade beschreibt das Upgrade von VMware ESXi™ auf die aktuelle Version.

Zielgruppe

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

vSphere Web Client und vSphere Client

Die Anweisungen für Aufgaben in diesem Handbuch basieren auf dem vSphere Web Client. Die meisten Aufgaben in diesem Handbuch lassen sich auch mit dem neuen vSphere Client ausführen. Die neue Terminologie, Topologie und der neue Workflow der vSphere Client-Benutzeroberfläche sind eng an denselben Aspekten und Elementen der vSphere Web Client-Benutzeroberfläche ausgerichtet. Sofern nicht anders angegeben, können Sie die Anweisungen zu vSphere Web Client auf den neuen vSphere Client anwenden.

Hinweis In vSphere 6.7 werden die meisten vSphere Web Client-Funktionen im vSphere Client implementiert. Eine aktuelle Liste der nicht unterstützten Funktionen finden Sie im [Handbuch für Funktions-Updates für den vSphere Client](#).

VMware Technical Publications - Glossar

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

Einführung in das vSphere-Upgrade

2

In vSphere 6.7 gibt es viele Möglichkeiten für das Upgrade der vSphere-Bereitstellung. Für ein erfolgreiches Upgrade von vSphere müssen Sie die Upgrade-Optionen, die Konfigurationsdetails, die den Upgrade-Vorgang beeinflussen, sowie die Abfolge der Aufgaben nachvollziehen können.

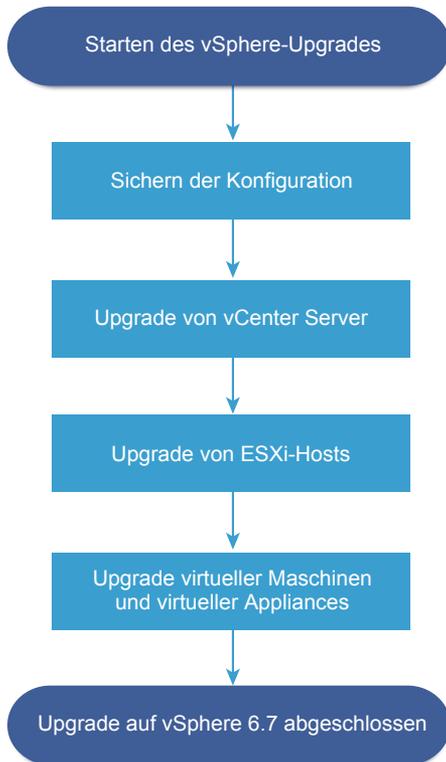
Die zwei Hauptkomponenten von vSphere sind VMware ESXi™ und VMware vCenter Server™. ESXi ist die Virtualisierungsplattform, auf der virtuelle Maschinen erstellt und ausgeführt werden. vCenter Server ist ein Dienst, der als zentraler Administrator für ESXi-Hosts agiert, die in einem Netzwerk verbunden sind. Das vCenter Server-System ermöglicht Ihnen den Zusammenschluss und die Verwaltung der Ressourcen von mehreren Hosts. vCenter Server Appliance ist eine vorkonfigurierte virtuelle Maschine, die auf dem Linux-Betriebssystem basiert, und die für das Ausführen des vCenter Server-Systems und der vCenter Server-Komponenten optimiert ist.

Seit vSphere 6.0 sind wichtige erforderliche Dienste für das Ausführen von vCenter Server und der vCenter Server-Komponenten im Platform Services Controller enthalten.

Basierend auf den vorhandenen vCenter Server-Konfigurationsdetails können Sie ein Upgrade auf einen der folgenden Bereitstellungstypen durchführen:

Übersicht über den vSphere-Upgrade-Vorgang

vSphere ist ein ausgereiftes Produkt mit mehreren Komponenten, für die ein Upgrade durchgeführt werden muss. Das Verständnis der erforderlichen Aufgabenabfolge ist für ein erfolgreiches vSphere-Upgrade entscheidend.

Abbildung 2-1. Übersicht über die vSphere-Upgrade-Aufgaben auf hoher Ebene

Das Upgrade von vSphere umfasst folgende Aufgaben:

- 1 Lesen Sie die vSphere-Versionshinweise.
- 2 Vergewissern Sie sich, dass Sie Ihre Konfiguration gesichert haben.
- 3 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.
- 4 Upgrade von vCenter Server.
Ausführliche Anweisungen finden Sie unter *vCenter Server-Upgrade*
- 5 Falls Sie vSphere Update Manager verwenden, führen Sie ein Upgrade durch. Weitere Informationen erhalten Sie in der VMware vSphere Update Manager-Dokumentation.
- 6 Führen Sie das Upgrade der ESXi-Hosts durch. Siehe [Übersicht über den ESXiHost-Upgrade-Vorgang](#).
- 7 Um ausreichend Datenspeicher für Protokolldateien sicherzustellen, sollten Sie einen Syslog-Server für die Remote-Protokollierung einrichten. 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](#).

- 8 Führen Sie manuell oder unter Verwendung von vSphere Update Manager ein Upgrade Ihrer virtuellen Maschinen und virtuellen Appliances durch, um ein orchestriertes Upgrade vorzunehmen.

Siehe [Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools](#).

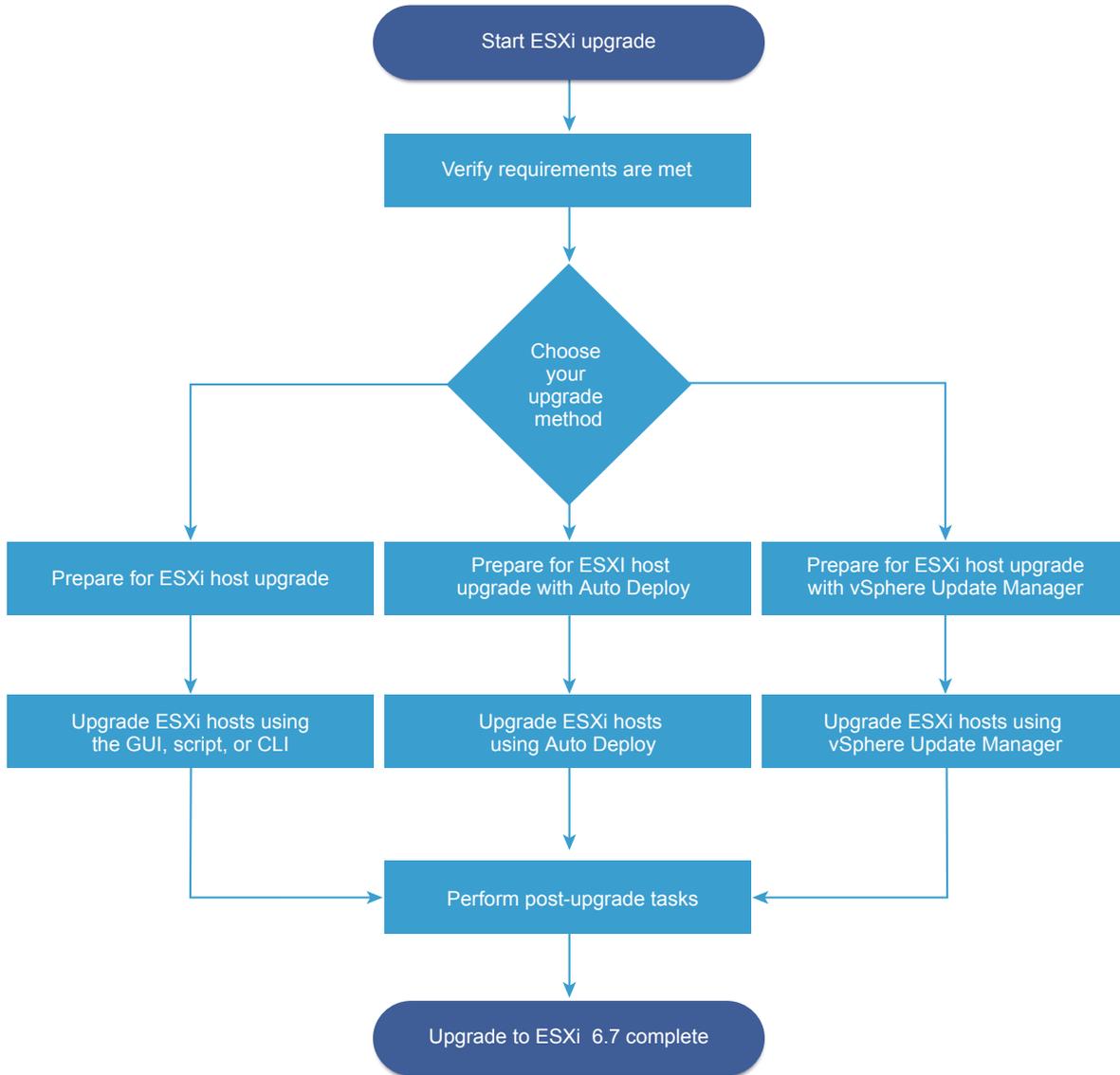
Übersicht über den ESXi Host-Upgrade-Vorgang

VMware bietet mehrere Möglichkeiten für das Upgrade von ESXi-Hosts der Versionen 6.0.x und 6.5.x auf ESXi 6.7.

Die Details und die Ebene der Unterstützung für ein Upgrade auf ESXi 6.7 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-Hosts der Version 6.0 oder 6.5.x, eines asynchronen freigegebenen Treibers oder anderer Drittanbieteranpassungen durchführen oder ein interaktives Upgrade von CD oder DVD, ein Upgrade im Skriptmodus oder ein Upgrade mit vSphere Update Manager durchführen. Wenn Sie ein Upgrade eines ESXi-Hosts der Version 6.0.x oder 6.5.x, der benutzerdefinierte VIBs aufweist, auf Version 6.7 durchführen, werden die benutzerdefinierten VIBs migriert. Weitere Informationen hierzu finden Sie unter [Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern](#).

Abbildung 2-2. Übersicht über den ESXi-Host-Upgrade-Vorgang



Schritte auf hoher Ebene für das Upgrade von ESXi:

- 1 Überprüfen Sie, ob Ihr System die Upgrade-Anforderungen erfüllt. Weitere Informationen hierzu finden Sie unter [Anforderungen für ESXi](#).
- 2 Bereiten Sie Ihre Umgebung für das Upgrade vor. Weitere Informationen hierzu finden Sie unter [Vor dem Upgrade der ESXi-Hosts](#).
- 3 Legen Sie den Speicherort und die Startposition des ESXi-Installationsprogramms fest. Weitere Informationen hierzu finden Sie unter [Medienoptionen für das Starten des ESXi-Installationsprogramms](#). Wenn Sie das Installationsprogramm über PXE starten, überprüfen Sie, ob Ihre Netzwerk-PXE-Infrastruktur ordnungsgemäß eingerichtet ist. Weitere Informationen hierzu finden Sie unter [Starten des ESXi-Installationsprogramms mit PXE](#).
- 4 Führen Sie ein Upgrade von ESXi durch. Siehe [Kapitel 3 Upgrade der ESXi-Hosts](#).

- 5 Nach dem Upgrade von ESXi-Hosts müssen Sie die Hosts erneut mit vCenter Server verbinden und die Lizenzen erneut anwenden. Weitere Informationen hierzu finden Sie unter [Nach dem Upgrade von ESXi-Hosts](#).

Unterstützte Methoden für ein direktes Upgrade auf ESXi6.7:

- Verwenden Sie das interaktive Installationsprogramm der grafischen Benutzeroberfläche von einer CD/DVD oder von einem USB-Laufwerk aus.
- Skript-Upgrade.
- Verwenden Sie die `esxcli`-Befehlszeilenschnittstelle.
- vSphere Auto Deploy. Wenn der ESXi-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host mit einem 6.7-Image erneut bereitzustellen.
- vSphere Update Manager.

Installationsprogramm für grafische Benutzeroberfläche (GUI)

Führen Sie ein interaktives Upgrade mithilfe eines ISO-Images des ESXi-Installationsprogramms auf CD/DVD oder einem USB-Flash-Laufwerk. Sie können das ESXi 6.7-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-Installation enthält, wird der Host auf Version 6.7 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](#).

Durchführen von skriptgesteuerten Upgrades

Sie können für Hosts ein Upgrade von ESXi 6.0.x und ESXi 6.5.x auf ESXi 6.7 durchführen, indem Sie ein Update-Skript ausführen, wodurch ein effizientes, unbeaufsichtigtes Upgrade ermöglicht wird. 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](#).

esxcli-Befehlszeilenschnittstelle

Sie können das `esxcli`-Befehlszeilendienstprogramm für ESXi verwenden, um ein Upgrade von ESXi 6.0.x-Hosts oder ESXi 6.5.x-Hosts auf ESXi 6.7-Hosts durchzuführen. Weitere Informationen hierzu finden Sie unter [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#).

vSphere Auto Deploy

Falls ein ESXi-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 [Kapitel 4 Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

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 vSphere Update Manager verwendet, empfiehlt VMware die Verwendung von vSphere Update Manager. Eine Anleitung zur Durchführung eines koordinierten Upgrades einer virtuellen Maschine finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*.

Die Dienstprogramme esxupdate und vihostupdate werden für ESXi 6.7-Upgrades nicht unterstützt.

Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools

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*.

Upgrade der ESXi-Hosts

Nachdem Sie ein Upgrade von vCenter Server und vSphere Update Manager durchgeführt haben, führen Sie ein Upgrade der ESXi-Hosts durch. Sie können direkt ein Upgrade der ESXi 6.0.x- und 6.5.x-Hosts auf ESXi 6.7 durchführen.

Für das Upgrade von Hosts können Sie die unter [Übersicht über den ESXiHost-Upgrade-Vorgang](#) 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 behandelt die folgenden Themen:

- [Anforderungen für ESXi](#)
- [Vor dem Upgrade der ESXi-Hosts](#)
- [Interaktives Upgrade von Hosts](#)
- [Installieren oder Upgraden von Hosts mithilfe eines Skripts](#)
- [Starten des ESXi-Installationsprogramms mit PXE](#)
- [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#)
- [Nach dem Upgrade von ESXi-Hosts](#)

Anforderungen für ESXi

Für die Installation oder das Upgrade von ESXi 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 6.7 unterstützt werden.

Hardware- und Systemressourcen

Für die Installation bzw. das Upgrade von ESXi 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 6.7 ist eine Hostmaschine mit mindestens zwei CPU-Kernen erforderlich.
- ESXi 6.7 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 6.7 muss das NX/XD-Bit für die CPU im BIOS aktiviert sein.
- ESXi 6.7 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 Netzwerkdaptermodellen 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 und nicht als lokal betrachtet. Diese Festplatten werden standardmäßig nicht als Scratch-Partition verwendet, da sie als remote betrachtet werden.

Hinweis Sie können auf einem ESXi 6.7-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 6.7 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.

Ab vSphere 6.7 unterstützt VMware Auto Deploy den Netzwerkstart und die Bereitstellung von ESXi-Hosts mit UEFI.

ESXi kann von einer Festplatte größer als 2 TB starten, wenn 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 6.7 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 6.7 installiert haben.

Speicheranforderungen für die Installation von bzw. das Upgrade auf ESXi 6.7

Zum Installieren von ESXi 6.7 oder Aktualisieren auf ESXi 6.7 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-Volumen 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, befindet sich die Scratch-Partition `/scratch` auf der Ramdisk des ESXi-Hosts, 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 *Installation und Einrichtung von vCenter Server*-Dokumentation.

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, so dass 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.

ESXi 6.7 -Installation auf M.2 und anderen Nicht-USB-Low-End-Flash-Medien

Im Gegensatz zu USB-Flash-Geräten erstellt das ESXi-Installationsprogramm einen VMFS-Datenspeicher auf M.2 und anderen Nicht-USB-Low-End-Flash-Medien. Wenn Sie eine virtuelle Maschine bereitstellen oder eine virtuelle Maschine auf den Datenspeicher dieses Startgeräts migrieren, kann das Startgerät je nach Lebensdauer des Flash-Geräts und den Eigenschaften der Arbeitslast unter Umständen schnell abgenutzt werden. Sogar schreibgeschützte Arbeitslasten können Probleme auf Low-End-Flash-Geräten erzeugen.

Wichtig Wenn Sie ESXi auf M.2 oder anderen Nicht-USB-Low-End-Flash-Medien installieren, löschen Sie sofort nach der Installation den VMFS-Datenspeicher auf dem Gerät. Weitere Informationen zum Entfernen von VMFS-Datenspeichern finden Sie unter *vSphere-Speicher*.

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 3-1. 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](#).

Tabelle 3-2. 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 3-2. 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 6.7-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 und im VMware Host 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 standardmäßig installierten Dienste. Wenn Sie andere VIBs auf Ihrem Host installieren, stehen Ihnen möglicherweise weitere Dienste und Firewall-Ports zur Verfügung. Die Informationen gelten in erster Linie für Dienste, die im vSphere Web Client sichtbar sind, jedoch sind in der Tabelle auch einige andere Ports enthalten.

Tabelle 3-3. Eingehende Firewall-Verbindungen

Port	Proto- koll	Dienst	Beschreibung
5988	TCP	CIM-Server	Server für CIM (Common Information Model)
5989	TCP	Sicherer CIM-Server	Sicherer Server für CIM
427	TCP, UDP	CIM-SLP	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
546		DHCPv6	DHCP-Client für IPv6
8301, 8302	UDP	DVSSync	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.

Tabelle 3-3. Eingehende Firewall-Verbindungen (Fortsetzung)

Port	Proto- koll	Dienst	Beschreibung
902	TCP	NFC	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.
12345, 23451	UDP	vSAN-Clusterdienst	VMware vSAN-Verzeichnisdienst für Clusterüberwachung und Mitgliedschaft. Verwendet UDP-basiertes IP-Multicast zur Bestimmung von Clustermitgliedern und Verteilung von vSAN-Metadaten an alle Clustermitglieder. Wenn der Dienst deaktiviert ist, wird vSAN nicht ausgeführt.
68	UDP	DHCP-Client	DHCP-Client für IPv4
53	UDP	DNS-Client	DNS-Client
8200, 8100, 8300	TCP, UDP	Fault Tolerance	Datenverkehr zwischen Hosts für vSphere Fault Tolerance (FT)
6999	UDP	NSX Distributed Logical Router-Dienst	NSX Virtual Distributed 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.
2233	TCP	vSAN-Transport	Zuverlässiger vSAN-Datagrammtransport. Nutzt TCP und wird für vSAN-Speicher-E/A verwendet. Wenn der Dienst deaktiviert ist, wird vSAN nicht ausgeführt.
161	UDP	SNMP-Server	Ermöglicht dem Host die Verbindung mit einem SNMP-Server.
22	TCP	SSH-Server	Erforderlich für SSH-Zugriff.
8000	TCP	vMotion	Erforderlich für die VM-Integration mit vMotion. ESXi-Hosts warten an Port 8000 auf TCP-Verbindungen von ESXi-Remotehosts für vMotion-Verkehr.
902, 443	TCP	vSphere Web Client	Client-Verbindungen
8080	TCP	vsanvp	vSAN VASA-Anbieter-Provider. Wird vom Speicherverwaltungsdienst (Storage Management Service, SMS) im Lieferumfang von vCenter für den Zugriff auf Daten zu vSAN-Speicherprofilen, -Funktionen und -Compliance genutzt. Wenn deaktiviert, kann das vSAN Storage Profile Based Management (SPBM) nicht genutzt werden.
80	TCP	vSphere Web Access	Begrüßungsseite mit Downloadlinks für verschiedene Schnittstellen
5900-5964	TCP	RFB-Protokoll	
80, 9000	TCP	vSphere Update Manager	

Tabelle 3-4. Ausgehende Firewall-Verbindungen

Port	Protokoll	Dienst	Beschreibung
427	TCP, UDP	CIM-SLP	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
547	TCP, UDP	DHCPv6	DHCP-Client für IPv6

Tabelle 3-4. Ausgehende Firewall-Verbindungen (Fortsetzung)

Port	Protokoll	Dienst	Beschreibung
8301, 8302	UDP	DVSSync	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.
44046, 31031	TCP	HBR	Wird von vSphere Replication und VMware Site Recovery Manager für den laufenden Replizierungsdatenverkehr verwendet.
902	TCP	NFC	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.
9	UDP	WOL	Verwendet von „Wake on LAN“.
12345 23451	UDP	vSAN-Clusterdienst	Von vSAN verwendeter Clusterüberwachungs-, Mitgliedschafts- und Verzeichnisdienst.
68	UDP	DHCP-Client	DHCP-Client
53	TCP, UDP	DNS-Client	DNS-Client
80, 8200, 8100, 8300	TCP, UDP	Fault Tolerance	Unterstützt VMware Fault Tolerance.
3260	TCP	Software-iSCSI-Client	Unterstützt Software-iSCSI.
6999	UDP	NSX 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.
5671	TCP	rabbitmqproxy	Ein auf dem ESXi-Host ausgeführter Proxy. Dieser Proxy ermöglicht Anwendungen, die innerhalb virtueller Maschinen ausgeführt werden, mit den AMQP-Brokern zu kommunizieren, die in der vCenter-Netzwerkdomäne ausgeführt werden. Die virtuelle Maschine muss sich nicht im Netzwerk befinden, d. h., es ist keine Netzwerkkarte erforderlich. Stellen Sie sicher, dass die IP-Adressen ausgehender Verbindungen mindestens die verwendeten Broker oder künftige Broker enthalten. Sie können Broker zu einem späteren Zeitpunkt hinzufügen, um die Anzahl der Broker zu erhöhen.
2233	TCP	vSAN-Transport	Wird für den RDT-Datenverkehr (Unicast-Peer-to-Peer-Kommunikation) zwischen vSAN-Knoten verwendet.
8000	TCP	vMotion	Erforderlich für die VM-Integration mit vMotion.
902	UDP	VMware vCenter Agent	vCenter Server-Agent
8080	TCP	vsanvp	Wird für Datenverkehr des vSAN-Anbieter-Providers verwendet.
9080	TCP	E/A-Filterdienst	Von der Speicherfunktion für E/A-Filter verwendet

Tabelle 3-5. Firewall-Ports für Dienste, die auf der Benutzeroberfläche standardmäßig nicht angezeigt werden

Port	Proto- koll	Dienst	Kommentar
5900-5964	TCP	RFB-Protokoll	Das RFB-Protokoll ist ein einfaches Protokoll für den Remotezugriff auf grafische Benutzeroberflächen.
8889	TCP	OpenWSMAN-Daemon	Web Services Management (WS-Management ist ein offener DMTF-Standard für die Verwaltung von Servern, Geräten, Anwendungen und Webdiensten.

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Wenn Sie Auto Deploy für die Installation Ihres ESXi 6.7-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volumen 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-Volumen gespeichert werden. Für diese Hosts konfiguriert ESXi 6.7 die Protokolle in optimaler Abstimmung mit Ihrer Installation und bietet ausreichend Speicherplatz für Protokollnachrichten.

Tabelle 3-6. Empfohlene Mindestgröße und Rotationskonfiguration für hostd-, vpxa- und fdm-Protokolle

Protokoll	Maximale Protokolldatei- größe	Anzahl der beizubehal- tenden Rotationen	Mindestens erforderlicher Festplat- tenspeicher
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 *Installation und Einrichtung von vCenter Server*.

Systemanforderungen für VMware Host Client

Stellen Sie sicher, dass Ihr Browser VMware Host Client unterstützt.

Die folgenden Gastbetriebssysteme und Webbrowserversionen werden für VMware Host Client unterstützt.

Unterstützte Browser	Mac OS	Windows	Linux
Google Chrome	50+	50+	50+
Mozilla Firefox	45+	45+	45+
Microsoft Internet Explorer	N/A	11+	N/A
Microsoft Edge	N/A	38+	N/A
Safari	9.0+	N/A	N/A

Kennwörter und Kontosperrung für ESXi

Für ESXi-Hosts müssen Sie ein Kennwort mit vordefinierten Anforderungen verwenden. Mithilfe der erweiterten Option `Security.PasswordQualityControl` können Sie die erforderliche Länge und die erforderliche Zeichenklasse ändern sowie Kennwortsätze erlauben.

ESXi verwendet das Linux-PAM-Modul `pam_passwdqc` für die Verwaltung und Kontrolle der Kennwörter. Ausführliche Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

Hinweis Die Standardanforderungen für ESXi-Kennwörter können versionsabhängig variieren. Mit der erweiterten Option `Security.PasswordQualityControl` können Sie die standardmäßigen Kennwortbeschränkungen prüfen und ändern.

ESXi -Kennwörter

ESXi erzwingt Kennwortanforderungen für den Zugriff über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI), die ESXi Shell, SSH oder den VMware Host Client.

- Beim Erstellen eines Kennworts müssen Sie standardmäßig Zeichen aus vier Zeichenklassen verwenden: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen (z. B. Unter- oder Schrägstriche).
- Standardmäßig beträgt die Kennwortlänge mehr als 7 und weniger als 40 Zeichen.

- Kennwörter dürfen kein Wort aus einem Wörterbuch und keinen Teil eines Worts aus einem Wörterbuch enthalten.

Hinweis Wenn ein Kennwort mit einem Großbuchstaben beginnt, wird dieser bei der Berechnung der verwendeten Zeichenklassen nicht berücksichtigt. Endet ein Kennwort mit einer Ziffer, wird diese bei der Berechnung der verwendeten Zeichenklassen ebenfalls nicht berücksichtigt.

Beispiele für ESXi -Kennwörter

Die folgenden Beispielkennwörter veranschaulichen potenzielle Kennwörter, wenn die Option wie folgt festgelegt ist.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Mit dieser Einstellung sind Kennwörter mit einer oder zwei Zeichenklassen sowie Kennwortsätze nicht zulässig, da die ersten drei Elemente deaktiviert sind. Kennwörter mit drei oder vier Zeichenklassen erfordern sieben Zeichen. Weitere Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

Mit diesen Einstellungen sind die folgenden Kennwörter zulässig.

- `xQaTEhb!`: Enthält acht Zeichen aus drei Zeichenklassen.
- `xQaT3#A`: Enthält sieben Zeichen aus vier Zeichenklassen.

Die folgenden Beispielkennwörter entsprechen nicht den Anforderungen.

- `Xqat3hi`: Beginnt mit einem Großbuchstaben, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.
- `xQaTEh2`: Endet mit einer Ziffer, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.

ESXi -Kennwortsatz

Anstelle eines Kennworts können Sie auch einen Kennwortsatz verwenden. Kennwortsätze sind jedoch standardmäßig deaktiviert. Diesen Standardwert oder sonstige Einstellungen können Sie mithilfe der erweiterten Option `Security.PasswordQualityControl` über den vSphere Web Client ändern.

Beispielsweise können Sie diese Option wie folgt ändern.

```
retry=3 min=disabled,disabled,16,7,7
```

Dieses Beispiel erlaubt Kennwortsätze mit mindestens 16 Zeichen und mindestens 3 Wörtern, getrennt durch Leerzeichen.

Änderungen an der Datei `/etc/pamd/passwd` werden für Legacy-Hosts weiterhin unterstützt, in zukünftigen Versionen ist dies jedoch nicht mehr der Fall. Verwenden Sie stattdessen die erweiterte Option `Security.PasswordQualityControl`.

Ändern der standardmäßigen Kennwortbeschränkungen

Die standardmäßige Beschränkung für Kennwörter oder Kennwortsätze können Sie mithilfe der erweiterten Option `Security.PasswordQualityControl` für Ihren ESXi-Host ändern. Weitere Informationen zum Festlegen der erweiterten ESXi-Optionen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Sie können den Standardwert wie folgt ändern, damit beispielsweise mindestens 15 Zeichen und mindestens vier Wörter erforderlich sind:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Ausführliche Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

Hinweis Nicht alle möglichen Kombinationen der Optionen für `pam_passwdqc` wurden getestet. Führen Sie zusätzliche Tests durch, nachdem Sie Änderungen an den Einstellungen für das Standardkennwort vorgenommen haben.

ESXi -Kontosperrverhalten

Ab vSphere 6.0 wird das Sperren von Konten für den Zugriff über SSH und über das vSphere Web Services SDK unterstützt. Die DCUI und die ESXi Shell unterstützen die Kontosperrung nicht. Standardmäßig wird das Konto nach maximal zehn fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach zwei Minuten entsperrt.

Konfigurieren des Anmeldeverhaltens

Das Anmeldeverhalten für Ihren ESXi-Host können Sie mit den folgenden erweiterten Optionen konfigurieren:

- `Security.AccountLockFailures`. Maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche, bevor das Konto eines Benutzers gesperrt wird. Mit dem Wert „0“ wird das Sperren von Konten deaktiviert.
- `Security.AccountUnlockTime`. Die Anzahl der Sekunden, die ein Benutzer gesperrt wird.

Weitere Informationen zum Festlegen der erweiterten ESXi-Optionen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Vor dem Upgrade der ESXi-Hosts

Damit das Upgrade Ihres ESXi-Hosts erfolgreich verläuft, machen Sie sich mit den einhergehenden Änderungen vertraut und bereiten Sie sich auf diese vor.

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 [Übersicht über den ESXiHost-Upgrade-Vorgang](#), 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. Weitere Informationen hierzu finden Sie unter [Übersicht über den ESXiHost-Upgrade-Vorgang](#).
 - Stellen Sie sicher, dass die Systemhardware die Anforderungen für ESXi erfüllt. Weitere Informationen finden Sie unter [Anforderungen für ESXi](#) 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 Bei Verwendung von Auto Deploy zur Bereitstellung von Hosts muss der Benutzer, der den Prozess ausführt, über lokale Administratorrechte auf dem ESXi-Host verfügen, der bereitgestellt wird. Das Installationsprogramm verfügt standardmäßig über diese Rechte und die Zertifikatbereitstellung erfolgt wie erwartet. Wenn Sie jedoch eine andere Methode als das Installationsprogramm verwenden, müssen Sie diese als Benutzer mit lokalen Administratorrechten ausführen.
- 5 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.
 - Informationen zu einem interaktiven Upgrade von CD, DVD oder USB-Laufwerk finden Sie unter [Interaktives Upgrade von Hosts](#).
 - Informationen zu einem Upgrade im Skriptmodus finden Sie unter [Installieren oder Upgraden von Hosts mithilfe eines Skripts](#).

- Informationen zu vSphere Auto Deploy finden Sie unter [Kapitel 4 Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#). Wenn der ESXi 6.0x- oder 6.5.x-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host mit einem 6.7-Image erneut bereitzustellen.
 - Informationen zur `esxcli`-Befehlmethode finden Sie unter [Aktualisieren von Hosts mithilfe von esxcli-Befehlen](#).
- 6 Planen Sie die Aufgaben, die nach dem Upgrade des ESXi-Hosts durchgeführt werden müssen:
- Testen Sie das System, um sicherzustellen, dass das Upgrade erfolgreich abgeschlossen wurde.
 - Wenden Sie die Lizenzen des Hosts an. Weitere Informationen hierzu finden Sie unter [Anwenden von Lizenzen nach einem Upgrade auf ESXi 6.7](#).
 - 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. Weitere Informationen hierzu finden Sie unter [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 *Installation und Einrichtung von vCenter Server*.
- 7 Wenn das Upgrade fehlgeschlagen ist und Sie den Host gesichert haben, können Sie den Host wiederherstellen.

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-Hosts auf 6.7 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 *Installation und Einrichtung von vCenter Server*.

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 mit PXE](#)
- 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 Installationskript enthält. Weitere Informationen hierzu finden Sie unter [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#).

Vorgehensweise

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

ESXi ist unter „Datacenter- 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 Installationskript 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

Vorgehensweise

- 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
```

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

Vorgehensweise

- 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-Installationskript auf das USB-Flash-Laufwerk.

```
cp ks.cfg /usbdisk
```

- 6 Unmounten Sie das USB-Flash-Laufwerk.

Das USB-Flash-Laufwerk enthält das Installations- oder das Upgrade-Skript für ESXi.

Weiter

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 [PXELINUX-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`.

Vorgehensweise

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 Erstellen Sie das ISO-Image mit dem Befehl mkisofs oder dem Befehl genisoimage neu.

Befehl	Syntax
mkisofs	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 -eltorito-alt-boot -eltorito-platform efi -b efiboot.img -no-emul-boot /esxi_cdrom
genisoimage	genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e efiboot.img -no-emul-boot /esxi_cdrom

Sie können dieses ISO-Image für den regulären Start oder den sicheren Start über UEFI verwenden.

Das ISO-Image enthält Ihr benutzerdefiniertes Installations- bzw. Upgrade-Skript.

Weiter

Installieren Sie ESXi aus dem ISO-Image.

Starten des ESXi -Installationsprogramms mit PXE

Sie können PXE (Preboot Execution Environment) verwenden, um einen Host zu starten. Unter vSphere 6.0 können Sie das ESXi-Installationsprogramm mit PXE über eine Netzwerkschnittstelle auf Hosts starten, die Legacy-BIOS oder UEFI verwenden.

ESXi 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 Legacy-BIOS-Firmware kann nur über IPv4 mit PXE gestartet werden. UEFI-Firmware kann entweder über IPv4 oder IPv6 mit PXE gestartet werden.

DHCP-Beispielkonfigurationen

Der DHCP-Server muss zum Starten des ESXi-Installationsprogramms über PXE die Adresse des TFTP-Servers und den Dateinamen des anfänglichen Bootloaders an den ESXi-Host senden.

Beim ersten Start der Zielmaschine sendet sie ein Paket über das Netzwerk, und es werden Informationen angefordert, damit sie selbst starten kann. Der DHCP-Server antwortet. Der DHCP-Server muss feststellen können, ob die Zielmaschine starten darf. Er muss weiterhin den Speicherort der anfänglichen Bootloader-Binärdatei (normalerweise eine Datei auf einem TFTP-Server) ermitteln.

Vorsicht Richten Sie keinen zweiten 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.

Beispiel für den Start unter Verwendung von TFTP mit IPv4

In diesem Beispiel wird gezeigt, wie ein ISC-DHCP-Server für den Start von ESXi unter Verwendung eines TFTP-Servers mit der IPv4-Adresse `xxx.xxx.xxx.xxx` konfiguriert wird.

```
#
# ISC DHCP server configuration file snippet. This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
    match if substr(option vendor-class-identifier, 0, 9) = "PXEClient";
    next-server xxx.xxx.xxx.xxx;
    if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
        filename = "mboot.efi";
    }
}
```

```

    } else {
        filename = "pxelinux.0";
    }
}

```

Wenn eine Maschine einen Startvorgang über PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `pxelinux.0` oder `mboot.efi` auf dem TFTP-Server zur Verfügung.

Beispiel für den Start unter Verwendung von TFTP mit IPv6

In diesem Beispiel wird gezeigt, wie ein ISC-DHCPv6-Server für den Start von ESXi über einen TFTP-Server mit der IPv6-Adresse `xxxx:xxxx:xxxx:xxxx::xxxx` konfiguriert wird.

```

#
# ISC DHCPv6 server configuration file snippet. This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";

```

Wenn eine Maschine einen Startvorgang über PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `mboot.efi` auf dem TFTP-Server zur Verfügung.

Beispiel für den Start unter Verwendung von HTTP mit IPv4

In diesem Beispiel wird gezeigt, wie ein ISC-DHCP-Server für den Start von ESXi unter Verwendung eines Webserver mit der IPv4-Adresse `xxx.xxx.xxx.xxx` konfiguriert wird. In diesem Beispiel wird gPXELINUX für Legacy-BIOS-Hosts und iPXE für UEFI-Hosts verwendet.

```

#
# ISC DHCPv6 server configuration file snippet. This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
    match if substring(option vendor-class-identifier, 0, 9) = "PXEclient";
    next-server xxx.xxx.xxx.xxx;
    if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
        if exists user-class and option user-class = "iPXE" {
            # Instruct iPXE to load mboot.efi as secondary bootloader
            filename = "mboot.efi";
        } else {
            # Load the snponly.efi configuration of iPXE as initial bootloader
            filename = "snponly.efi";
        }
    }
}

```

```

    } else {
        filename "gpxelinux.0";
    }
}

```

Wenn eine Maschine einen Startvorgang über PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `gpxelinux.0` oder `snponly.efi` auf dem TFTP-Server zur Verfügung. Im UEFI-Fall fordert iPXE dann den DHCP-Server zum Laden der nächsten Datei auf, und dieses Mal gibt der Server `mboot.efi` als den Dateinamen zurück.

Beispiel für den Start unter Verwendung von HTTP mit IPv6

In diesem Beispiel wird gezeigt, wie ein ISC-DHCPv6-Server für den Start von ESXi über einen TFTP-Server mit der IPv6-Adresse `xxxx:xxxx:xxxx:xxxx::xxxx` konfiguriert wird.

```

#
# ISC DHCPv6 server configuration file snippet. This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
    # Instruct iPXE to load mboot.efi as secondary bootloader
    option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
    # Load the snponly.efi configuration of iPXE as initial bootloader
    option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}

```

Wenn eine Maschine einen Startvorgang über PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `snponly.efi` (iPXE) auf dem TFTP-Server zur Verfügung. iPXE fordert dann den DHCP-Server zum Laden der nächsten Datei auf, und dieses Mal gibt der Server `mboot.efi` als den Dateinamen zurück.

PXELINUX-Konfigurationsdateien

Sie benötigen eine PXELINUX-Konfigurationsdatei, um das ESXi-Installationsprogramm auf einem Legacy-BIOS-System zu starten. Durch die Konfigurationsdatei wird das Menü definiert, das auf dem ESXi-Zielhost angezeigt wird, während es gestartet und der TFTP-Server kontaktiert wird, um alle SYSLINUX-Konfigurationen abzurufen, einschließlich PXELINUX und gPXELINUX.

In diesem Abschnitt erhalten Sie allgemeine Informationen zu PXELINUX-Konfigurationsdateien. Ziehen Sie z. B. [DHCP-Beispielkonfigurationen](#) zurate.

Details zur Syntax finden Sie auf der SYSLINUX-Website unter <http://www.syslinux.org/>.

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 in der folgenden Reihenfolge zu laden.

- 1 Sie versucht es mit der MAC-Adresse des ESXi-Zielhosts, der der Code des ARP-Typs, der für Ethernet „01“ lautet, vorangestellt ist.
- 2 Schlägt der Versuch fehl, versucht sie es mit der IP-Adresse des ESXi-Zielsystems in hexadezimaler Schreibweise.
- 3 Letztendlich wird versucht, eine Datei namens `default` zu laden.

Speicherort der PXE-Konfigurationsdatei

Speichern Sie die Datei auf dem TFTP-Server im Verzeichnis `/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 lautet `00-21-5a-ce-40-f6`.

Hintergrundinformationen zum PXE-Startvorgang

Wenn Sie den PXE-Startvorgang nachvollziehen können, kann dies bei der Fehlerbehebung hilfreich sein.

TFTP-Server

Trivial File Transfer Protocol (TFTP) ähnelt dem FTP-Dienst und wird normalerweise nur für Netzwerkartsysteme oder zum Laden der Firmware auf Netzwerkgeräten (z. B. Routern) verwendet. TFTP ist unter Linux und Windows verfügbar.

- 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. Sie können sich einen TFTP-Server auch von einem der verpackten Appliances auf dem VMware Marketplace beschaffen.

- 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/>.

SYSLINUX, PXELINUX und gPXELINUX

Wenn Sie PXE in einer Legacy-BIOS-Umgebung verwenden, müssen Sie die unterschiedlichen Startumgebungen nachvollziehen können.

- SYSLINUX ist eine Open Source-Startumgebung für Maschinen, auf denen Legacy-BIOS-Firmware ausgeführt wird. Der ESXi-Bootloader für BIOS-Systeme `mboot.c.32` wird als ein SYSLINUX-Plug-In ausgeführt. Sie können SYSLINUX für den Start über verschiedene Medientypen einschließlich Festplatte, ISO-Image und Netzwerk konfigurieren. Das SYSLINUX-Paket ist unter <http://www.kernel.org/pub/linux/utils/boot/syslinux/> gespeichert.
- PXELINUX ist eine SYSLINUX-Konfiguration für den Start über einen TFTP-Server gemäß dem PXE-Standard. Wenn Sie PXELINUX für den Start des ESXi-Installationsprogramms verwenden, werden die Binärdatei `pxelinux.0`, `mboot.c32`, die Konfigurationsdatei, der Kernel und weitere Dateien über TFTP übertragen.
- gPXELINUX ist eine Hybrid-Konfiguration, in der PXELINUX und gPXE enthalten ist und mit der der Start über einen Webserver unterstützt wird. gPXELINUX ist im SYSLINUX-Paket enthalten. Wenn Sie gPXELINUX für den Start des ESXi-Installationsprogramms verwenden, werden nur die Binärdatei `gpxelinux.0`, `mboot.c32` und die Konfigurationsdatei über TFTP übertragen. Die übrigen Dateien werden über HTTP übertragen. HTTP ist in der Regel schneller und zuverlässiger als TFTP, insbesondere beim Übertragen großer Datenmengen auf einem stark ausgelasteten Netzwerk.

Hinweis VMware erstellt derzeit das `mboot.c32`-Plug-In für den Einsatz mit der SYSLINUX Version 3.86 und testet den PXE-Start nur mit dieser Version. Andere Versionen sind wahrscheinlich nicht kompatibel. 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.

UEFI PXE und iPXE

Die meisten UEFI-Firmwares enthalten nativ PXE-Unterstützung, die den Start über einen TFTP-Server zulässt. Die Firmware kann den ESXi-Bootloader direkt für UEFI-Systeme, `mboot.efi` laden. Zusätzliche Software wie PXELINUX ist nicht erforderlich.

iPXE kann auch bei UEFI-Systemen hilfreich sein, in deren Firmware PXE nicht enthalten ist, und bei älteren UEFI-Systemen mit Fehlern in der zugehörigen PXE-Unterstützung. In solchen Fällen können Sie versuchen, iPXE auf einem USB-Flash-Laufwerk zu installieren und den Startvorgang von hier aus auszuführen.

Hinweis Apple Macintosh-Produkte enthalten keine Unterstützung für den PXE-Start. Sie enthalten stattdessen Unterstützung für den Netzwerkstart über ein Protokoll speziell für Apple.

Alternative Ansätze für den PXE-Start

Alternative Ansätze für PXE-Start mit verschiedener Software auf unterschiedlichen Hosts sind auch möglich, beispielsweise:

- Konfiguration des DHCP-Servers für die Bereitstellung unterschiedlicher anfänglicher Bootloader-Dateinamen für unterschiedliche Hosts abhängig von MAC-Adressen oder anderen Kriterien. Weitere Informationen finden Sie in der Dokumentation zum DHCP-Server.
- Ansätze unter Verwendung von iPXE als der anfängliche Bootloader mit einer iPXE-Konfigurationsdatei, die den nächsten Bootloader basierend auf der MAC-Adresse oder anderen Kriterien auswählt.

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 „Mein VMware“-Konto unter <https://my.vmware.com/web/vmware/>.

Vorgehensweise

- 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>.

Interaktives Upgrade von Hosts

Um ESXi 6.0-Hosts oder ESXi 6.5-Hosts auf ESXi 6.7 zu aktualisieren, können Sie das ESXi-Installationsprogramm von einer CD, einer DVD oder einem USB-Flash-Laufwerk starten.

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. Weitere Informationen hierzu finden Sie unter [Starten des ESXi-Installationsprogramms mit PXE](#).

- 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 ESXi-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.

Vorgehensweise

- 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 Festplattreihenfolge 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.

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 mit PXE](#).

Um den Speicherort des Installationssskripts 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.

Vorgehensweise

- 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 net-
mask=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 3-7. 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 <code>SYSLINUX</code> 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 <code>SYSLINUX</code> 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 3-7. 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-Gerät bei der Suche nach einem Installationskript 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 Installationskripts und der Installationsmedien verwendet wird.
<code>netdevice=Gerät</code>	Versucht, ein Netzwerkadapter-Gerät bei der Suche nach einem Installationskript 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 Installationskript 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 Skripts 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= disk-type1 [disk-type2,...]</code>	<p>Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:</p> <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 <code>ST3120814A</code> und alle Festplatten bevorzugen, die den <code>mptsas</code>-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument <code>--firstdisk=ST3120814A,mptsas,local</code> an. Sie können <code>localesex</code> als lokalen Speicher verwenden, der ein ESXi-Image enthält, oder Sie können <code>remoteesx</code> als Remotespeicher verwenden, der ein ESXi-Image enthält.</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.

<code>--disk=</code> or <code>--drive=</code>	<p>Legt die zu partitionierende Festplatte fest. Im Befehl <code>--disk=diskname</code> kann der <i>Festplattenname</i> eine der folgenden Formen haben:</p> <ul style="list-style-type: none"> ■ Pfad: <code>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</code> ■ MPX-Name: <code>--disk=mpx.vmhba1:C0:T0:L0</code> ■ VML-Name: <code>--disk=vm1.000000034211234</code> ■ vmkLUN-UID: <code>--disk=vmkLUN_UID</code>
---	--

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. Sie können `localesx` als lokalen Speicher verwenden, der ein ESXi-Image enthält, oder Sie können `remotesesx` als Remotespeicher verwenden, der ein ESXi-Image enthält.

`--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 vSAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine vSAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer vSAN-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 vSAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

<code>--overwritevmfs</code>	Wird benötigt, um vor der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte zu überschreiben.
<code>--preservevmfs</code>	Behält während der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte bei.
<code>--novmfsdisk</code>	Verhindert, dass eine VMFS-Partition auf dieser Festplatte erstellt wird. Muss mit <code>--overwritevmfs</code> 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.

<code>--disk=</code> or <code>--drive=</code>	Legt die zu partitionierende Festplatte fest. Im Befehl <code>--disk=diskname</code> kann der <i>Festplattenname</i> eine der folgenden Formen haben: <ul style="list-style-type: none"> ■ Pfad: <code>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</code> ■ MPX-Name: <code>--disk=mpx.vmhba1:C0:T0:L0</code> ■ VML-Name: <code>--disk=vm1.000000034211234</code> ■ vmkLUN-UID: <code>--disk=vmkLUN_UID</code>
---	---

Die Formate der angenommenen Laufwerksnamen finden Sie unter [Festplattengerätenamen](#).

<code>--firstdisk=</code> <code>disk-type1,</code> <code>[disk-type2,...]</code>	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>)
--	---

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. Sie können `localesx` als lokalen Speicher verwenden, der ein ESXi-Image enthält, oder Sie können `remoteesx` als Remotespeicher verwenden, der ein ESXi-Image enthält.

`--overwritevsan`

Sie müssen die Option `--overwritevsan` verwenden, wenn Sie ESXi auf einer SSD- oder HDD-Festplatte in einer vSAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine vSAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer vSAN-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 vSAN-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

- Estnisch
- Finnisch
- Französisch
- Deutsch
- Griechisch
- Isländisch
- Italienisch
- Japanisch
- Lateinamerikanisch
- Norwegisch
- Polnisch
- Portugiesisch
- Russisch
- Slowenisch
- Spanisch
- Schwedisch
- Französisch (Schweiz)
- Deutsch (Schweiz)
- Türkisch
- Ukrainisch
- Großbritannien
- US Default
- US Dvorak

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 (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (optional)

Gibt eine Netzwerkadresse für das System an.

<code>--bootproto=[dhcp static]</code>	Gibt an, ob die Netzwerkeinstellungen von DHCP abgerufen oder manuell festgelegt werden sollen.
<code>--device=</code>	Gibt entweder die MAC-Adresse der Netzwerkkarte oder den Gerätenamen im Format <code>vmnicNN</code> an, wie z. B. <code>vmnic0</code> . Diese Option bezieht sich auf das Uplink-Gerät für den virtuellen Switch.
<code>--ip=</code>	Legt eine IP-Adresse für die zu installierende Maschine im Format <code>xxx.xxx.xxx.xxx</code> fest. Dies ist für die Option <code>--bootproto=static</code> erforderlich und wird ansonsten ignoriert.
<code>--gateway=</code>	Legt das Standard-Gateway als IP-Adresse im Format <code>xxx.xxx.xxx.xxx</code> fest. Wird im Zusammenhang mit der Option <code>--bootproto=static</code> verwendet.
<code>--nameserver=</code>	Legt den primären Namensserver als IP-Adresse fest. Wird im Zusammenhang mit der Option <code>--bootproto=static</code> verwendet. Lassen Sie diese Option weg, falls Sie nicht vorhaben, DNS zu verwenden. Für die Option <code>--nameserver</code> können zwei IP-Adressen angegeben werden. Beispiel: <code>--nameserver="10.126.87.104[,10.126.87.120]"</code>
<code>--netmask=</code>	Legt die Subnetzmaske des installierten Systems im Format <code>255.xxx.xxx.xxx</code> fest. Wird im Zusammenhang mit der Option <code>--bootproto=static</code> verwendet.
<code>--hostname=</code>	Legt den Hostnamen für das installierte System fest.
<code>--vlanid= <i>vlanid</i></code>	Gibt das VLAN des Systems an. Wird entweder mit der Option <code>--bootproto=dhcp</code> oder <code>--bootproto=static</code> verwendet. Legen Sie den Wert auf eine Ganzzahl zwischen 1 und 4096 fest.
<code>--addvmpportgroup=(0 1)</code>	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.

<i>datastore name</i>	Gibt an, wo die Partition gemountet werden soll.
<code>--ondisk=</code> or <code>--ondrive=</code>	Gibt die Festplatte oder das Laufwerk an, wo die Partition erstellt werden soll.
<code>--firstdisk=</code> <i>disk-type1,</i> <i>[disk-type2, ...]</i>	<p>Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:</p> <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, einschließlich <code>esx</code> 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 <code>ST3120814A</code> und alle Festplatten bevorzugen, die den <code>mptsas</code>-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument <code>--firstdisk=ST3120814A,mptsas,local</code> an. Sie können <code>localesx</code> als lokalen Speicher verwenden, der ein ESXi-Image enthält, oder Sie können <code>remotesesx</code> als Remotespeicher verwenden, der ein ESXi-Image enthält.</p>

reboot (optional)

Startet die Maschine nach Abschluss der Skriptinstallation neu.

<code><--noeject></code>	Nach der Installation wird die CD nicht ausgeworfen.
--------------------------------	--

rootpw (erforderlich)

Legt das Root-Kennwort für das System fest.

<code>--iscrypted</code>	Legt fest, dass das Kennwort verschlüsselt ist.
<i>password</i>	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=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 ESXi 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. Sie können `localesx` als lokalen Speicher verwenden, der ein ESXi-Image enthält, oder Sie können `remotesesx` als Remotespeicher verwenden, der ein ESXi-Image enthält.

`%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 Installationskript 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.

`--interpreter` Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.
`=[python|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 Installationskriptbefehle `install`, `upgrade` und `installorupgrade` erfordern die Verwendung von Festplattengerätenamen.

Tabelle 3-8. Festplattengerätenamen

Formatieren	Beispiel	Beschreibung
VML	vml.00025261	Der Gerätenamen, wie vom VMkernel gemeldet
MPX	mpx.vmhba0:C0:T0:L0	Der Gerätenamen

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` oder `mboot.efi` bei 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 Installationskripts 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
prefix=DIRPATH
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 3-9. Befehle in boot.cfg .

Befehl	Beschreibung
<code>title=STRING</code>	Stellt den Titel des Bootloaders auf <code>STRING</code> ein.
<code>prefix=STRING</code>	(Optional) Setzt <code>DIRPATH/</code> vor jeden <code>FILEPATH</code> in den <code>kernel=</code> - und <code>modules=</code> -Befehlen, die nicht bereits mit <code>/</code> oder mit <code>http://</code> beginnen.
<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 (<code>---</code>).

Siehe [Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript](#) und [Starten des ESXi-Installationsprogramms mit PXE](#).

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](#).

Vorgehensweise

- 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.

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](#).

Vorgehensweise

- 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.

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 6.7 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 mit PXE](#).
- 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 mit PXE unter Verwendung eines Webservers](#)
 - [Starten des ESXi-Installationsprogramms mit PXE unter Verwendung von TFTP](#)
- Weitere Informationen über die Verwendung von vSphere Auto Deploy zum Durchführen eines Skript-Updates per PXE-Startvorgang finden Sie unter [Kapitel 4 Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts](#).

Starten des ESXi -Installationsprogramms mit PXE

Sie können PXE (Preboot Execution Environment) verwenden, um einen Host zu starten. Unter vSphere 6.0 können Sie das ESXi-Installationsprogramm mit PXE über eine Netzwerkschnittstelle auf Hosts starten, die Legacy-BIOS oder UEFI verwenden.

ESXi 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.

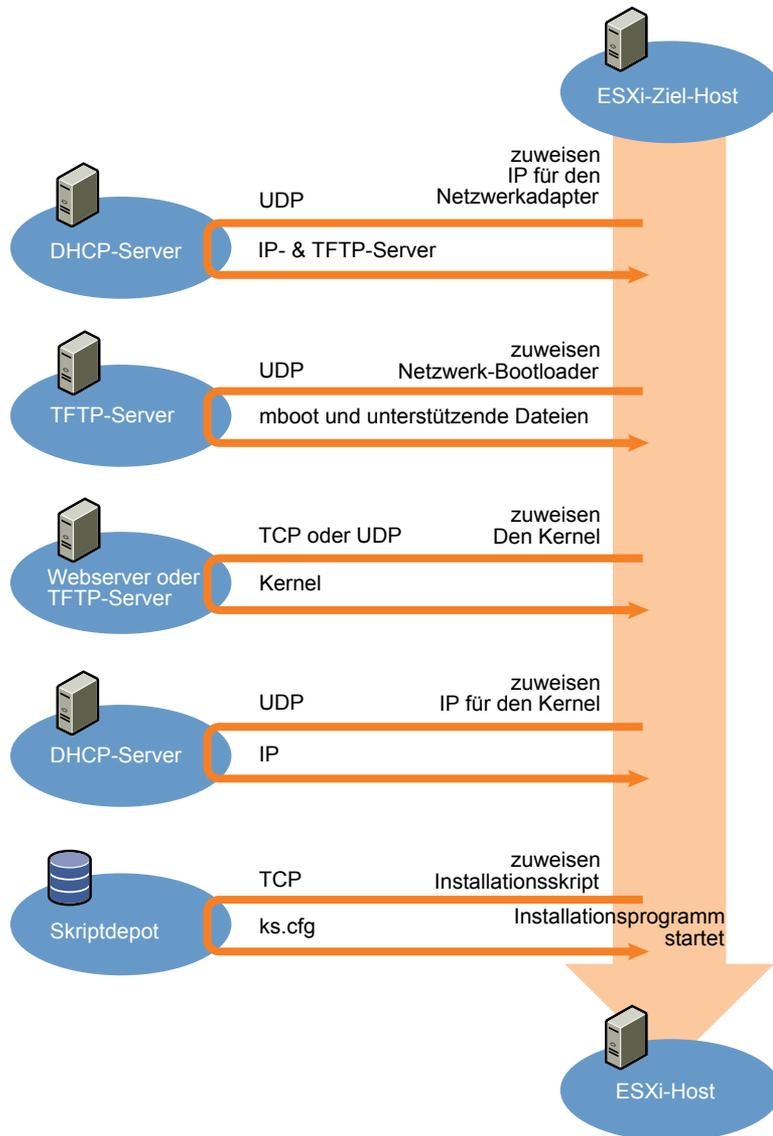
Hinweis Legacy-BIOS-Firmware kann nur über IPv4 mit PXE gestartet werden. UEFI-Firmware kann entweder über IPv4 oder IPv6 mit PXE gestartet werden.

Überblick über den Installationsprozess per PXE-Startvorgang

Bestimmte Details des PXE-Startvorgangs richten sich danach, ob der Zielhost Legacy-BIOS- oder UEFI-Firmware verwendet und ob beim Startvorgang ausschließlich TFTP oder TFTP plus HTTP eingesetzt wird.

Wenn Sie den Zielhost starten, interagiert dieser mit den verschiedenen Servern in der Umgebung, um den Netzwerkadapter, den Bootloader, den Kernel, die IP-Adresse des Kernels und schließlich das Installationskript aufzurufen. Wenn alle Komponenten bereitstehen, startet die Installation wie in folgender Abbildung dargestellt.

Abbildung 3-1. Überblick über den Installationsprozess per PXE-Startvorgang



Die Interaktion zwischen dem ESXi-Host und den anderen Servern verläuft wie folgt:

- 1 Der Benutzer startet den ESXi-Zielhost.
- 2 Der ESXi-Zielhost stellt eine DHCP-Anforderung.
- 3 Der DHCP-Server antwortet mit den IP-Informationen und dem Speicherort des TFTP-Servers.
- 4 Der ESXi-Host kontaktiert den TFTP-Server und fordert die vom DHCP-Server angegebene Datei an.
- 5 Der TFTP-Server sendet den Netzwerk-Bootloader und der ESXi-Host führt ihn aus. Der ursprüngliche Bootloader lädt unter Umständen zusätzliche Bootloader-Komponenten vom TFTP-Server.
- 6 Der Bootloader sucht nach einer Konfigurationsdatei auf dem TFTP-Server, lädt den Kernel und andere ESXi-Komponenten vom HTTP- oder TFTP-Server herunter und startet den Kernel auf dem ESXi-Host.

- 7 Das Installationsprogramm wird interaktiv ausgeführt oder verwendet ein in der Konfigurationsdatei angegebenes Kickstart-Skript.

Starten des ESXi-Installationsprogramms mit PXE unter Verwendung von TFTP

Sie können einen TFTP-Server verwenden, um das ESXi-Installationsprogramm mit PXE zu starten. Der Prozess unterscheidet sich geringfügig, je nachdem, ob Sie UEFI verwenden oder über ein Legacy-BIOS starten. Da die meisten Umgebungen neben ESXi-Hosts, die UEFI-Starts unterstützen, auch Hosts enthalten, die ausschließlich Legacy-BIOS unterstützen, werden in diesem Thema Voraussetzungen und Schritte für beide Hosttypen behandelt.

- Für Legacy-BIOS-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `pxelinux.0`- oder `gpxelinux.0`-Bootloaders für alle Zielmaschinen, wobei aber je nach MAC-Adresse der Zielmaschine möglicherweise unterschiedliche PXELINUX-Konfigurationsdateien verwendet werden.
- Für UEFI-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `mboot.efi`-Bootloaders für alle Zielmaschinen, wobei aber je nach MAC-Adresse der Zielmaschine möglicherweise unterschiedliche `boot.cfg`-Dateien verwendet werden.

Voraussetzungen

Überprüfen Sie, ob die Umgebung die folgenden Voraussetzungen erfüllt:

- ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- Zielhosts mit einer Hardwarekonfiguration, die für Ihre ESXi-Version unterstützt wird. Weitere Informationen finden Sie im *VMware-Kompatibilitätshandbuch*.
- Netzwerkadapter mit PXE-Unterstützung auf dem ESXi-Zielhost
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Weitere Informationen hierzu finden Sie unter [DHCP-Beispielkonfigurationen](#).
- TFTP-Server.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- Für Legacy-BIOS können Sie nur IPv4-Netzwerke verwenden. Zum Starten von UEFI mit PXE können Sie IPv4- oder IPv6-Netzwerke verwenden.
- (Optional) Installationskript (Kickstart-Datei).
- 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.

Rufen Sie für Legacy-BIOS-Systeme Version 3.86 des SYSLINUX-Pakets unter <https://www.kernel.org/pub/linux/utils/boot/syslinux/> ab.

Vorgehensweise

- 1 Konfigurieren Sie den DHCP-Server für den TFTP-Start.
- 2 (Nur Legacy-BIOS) PXELINUX abrufen und konfigurieren:
 - a Rufen Sie SYSLINUX Version 3.86 ab, entpacken Sie das Programm und kopieren Sie die Datei `pxelinux.0` in das Verzeichnis `/tftpboot` der obersten Ebene auf dem TFTP-Server.
 - b Erstellen Sie eine PXELINUX-Konfigurationsdatei mithilfe des folgenden Codemodells.
 ESXi-6.x.x-XXXXXX ist der Name des TFTP-Unterverzeichnisses, das die Dateien des ESXi-Installationsprogramms enthält.

```

DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2

```

- c Speichern Sie die Datei PXELINUX im Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server mit einem Dateinamen, der angibt, ob alle Hosts dieses Installationsprogramm standardmäßig starten:

Option	Beschreibung
Dasselbe Installationsprogramm	Geben Sie der Datei den Namen <code>default</code> , wenn alle Hosts dieses ESXi-Installationsprogramm standardmäßig starten sollen.
Verschiedene Installationsprogramme	Benennen Sie die Datei mit der MAC-Adresse der Zielhostmaschine (<code>01-mac_address_of_target_ESXi_host</code>), wenn nur ein bestimmter Host mit dieser Datei gestartet werden soll, z. B. <code>01-23-45-67-89-0a-bc</code> .

- 3 (Nur UEFI) Kopieren Sie die Datei `efi/boot/bootx64.efi` aus dem ISO-Image des ESXi-Installationsprogramms in das Verzeichnis `/tftpboot/mboot.efi` auf dem TFTP-Server.

Hinweis Neuere Versionen der Datei `mboot.efi` können in der Regel ältere Versionen von ESXi starten. Ältere Versionen der Datei `mboot.efi` hingegen können neuere Versionen von ESXi unter Umständen nicht starten. Wenn Sie verschiedene Hosts konfigurieren möchten, um unterschiedliche Versionen des ESXi-Installationsprogramms zu starten, verwenden Sie die Datei `mboot.efi` aus der neuesten Version.

- 4 Erstellen Sie ein Unterverzeichnis des obersten `/tftpboot`-Verzeichnisses des TFTP-Servers und benennen Sie es nach der enthaltenen ESXi-Version, z. B. `/tftpboot/ESXi-6.x.x-xxxxx`.
- 5 Kopieren Sie den Inhalt des Images des ESXi-Installationsprogramms in das soeben erstellte Verzeichnis.

6 Bearbeiten Sie die Datei `boot.cfg`.

- a Fügen Sie folgende Zeile hinzu:

```
prefix=ESXi-6.x.x-xxxxxx
```

Hier stellt `ESXi-6.x.x-xxxxxx` den Pfadnamen der Installationsprogrammdateien relativ zum Root-Verzeichnis des TFTP-Servers dar.

- b Wenn die Dateinamen in den `kernel=`- und `modules=`-Zeilen mit einem umgekehrten Schrägstrich (`/`) beginnen, löschen Sie dieses Zeichen.

7 (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 Installationskripts anzugeben.

Verwenden Sie den folgenden Code als Beispiel, wobei `XXX.XXX.XXX.XXX` die IP-Adresse des Servers ist, auf dem sich das Installationskript 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
```

8 (Nur UEFI) Geben Sie an, ob alle UEFI-Hosts dasselbe Installationsprogramm starten sollen.

Option	Beschreibung
Dasselbe Installationsprogramm	Kopieren Sie die Datei <code>boot.cfg</code> in das Verzeichnis <code>/tftpboot/boot.cfg</code> oder verknüpfen Sie sie mit diesem Verzeichnis.
Verschiedene Installationsprogramme	<p>a Erstellen Sie ein Unterverzeichnis von <code>/tftpboot</code>, das nach der MAC-Adresse der Zielhostmaschine (<code>01-mac_address_of_target_ESXi_host</code>) benannt ist, z. B. <code>01-23-45-67-89-0a-bc</code>.</p> <p>b Legen Sie eine Kopie (oder eine Verknüpfung mit) der Datei <code>boot.cfg</code> des Hosts in diesem Verzeichnis ab, z. B. <code>/tftpboot/01-23-45-67-89-0a-bc/boot.cfg</code>.</p>

Starten des ESXi-Installationsprogramms mit PXE unter Verwendung eines Webservers

Sie können einen Webserver verwenden, um das ESXi-Installationsprogramm mit PXE zu starten. Da die meisten Umgebungen neben ESXi-Hosts, die UEFI-Starts unterstützen, auch Hosts enthalten, die ausschließlich Legacy-BIOS unterstützen, werden in diesem Thema Voraussetzungen und Schritte für beide Hosttypen behandelt.

- Für Legacy-BIOS-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `pxelinux.0`- oder `gpxelinux.0`-Bootloaders für alle Zielmaschinen, wobei aber je nach MAC-Adresse der Zielmaschine möglicherweise unterschiedliche PXELINUX-Konfigurationsdateien verwendet werden.

- Für UEFI-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `mboot.efi`-Bootloaders für alle Zielmaschinen, wobei aber je nach MAC-Adresse der Zielmaschine möglicherweise unterschiedliche `boot.cfg`-Dateien verwendet werden.

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- Zielhosts mit einer Hardwarekonfiguration, die für Ihre ESXi-Version unterstützt wird. Weitere Informationen finden Sie im *VMware-Kompatibilitätshandbuch*.
- Netzwerkadapter mit PXE-Unterstützung auf dem ESXi-Zielhost
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Weitere Informationen hierzu finden Sie unter [DHCP-Beispielkonfigurationen](#).
- TFTP-Server.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- Für Legacy-BIOS können Sie nur IPv4-Netzwerke verwenden. Zum Starten von UEFI mit PXE können Sie IPv4- oder IPv6-Netzwerke verwenden.
- (Optional) Installationsskript (Kickstart-Datei).
- 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.

Stellen Sie sicher, dass Ihre Umgebung auch die folgenden Voraussetzungen für den PXE-Start mithilfe eines Webservers erfüllt.

- Stellen Sie sicher, dass die ESXi-Zielhosts auf den HTTP-Webserver zugreifen können.
- (UEFI) Rufen Sie iPXE unter <http://ipxe.org> ab.
- (Legacy-BIOS) Rufen Sie Version 3.86 des SYSLINUX-Pakets unter <https://www.kernel.org/pub/linux/utils/boot/syslinux/> ab.

Vorgehensweise

- 1 Konfigurieren Sie den DHCP-Server für den HTTP-Start.
- 2 (Nur UEFI) iPXE abrufen und konfigurieren:
 - a Rufen Sie den iPXE-Quellcode wie unter <http://ipxe.org/download> beschrieben ab.
 - b Befolgen Sie die Anweisungen auf dieser Seite, aber verwenden Sie den folgenden Make-Befehl:


```
make bin-x86_64-efi/snponly.efi
```
 - c Kopieren Sie die resultierende Datei `snponly.efi` in das Verzeichnis `/tftpboot` auf dem TFTP-Server.

- 3 (Nur UEFI) Kopieren Sie die Datei `efi/boot/bootx64.efi` aus dem ISO-Image des ESXi-Installationsprogramms in das Verzeichnis `/tftpboot/mboot.efi` auf dem TFTP-Server.

Hinweis Neuere Versionen der Datei `mboot.efi` können in der Regel ältere Versionen von ESXi starten. Ältere Versionen der Datei `mboot.efi` hingegen können neuere Versionen von ESXi unter Umständen nicht starten. Wenn Sie verschiedene Hosts konfigurieren möchten, um unterschiedliche Versionen des ESXi-Installationsprogramms zu starten, verwenden Sie die Datei `mboot.efi` aus der neuesten Version.

- 4 (Nur Legacy-BIOS) PXELINUX abrufen und konfigurieren:
 - a Rufen Sie SYSLINUX Version 3.86 ab, entpacken Sie das Programm und kopieren Sie die Datei `gpxelinux.0` in das Verzeichnis `/tftpboot` der obersten Ebene auf dem TFTP-Server.
 - b Erstellen Sie eine PXELINUX-Konfigurationsdatei mithilfe des folgenden Codemodells.
 ESXi-6.x.x-XXXXXX ist der Name des TFTP-Unterverzeichnisses, das die Dateien des ESXi-Installationsprogramms enthält.

```

DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-6.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-6.x.x-XXXXXX/boot.cfg
  IPAPPEND 2

```

- c Speichern Sie die Datei PXELINUX im Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server mit einem Dateinamen, der angibt, ob alle Hosts dieses Installationsprogramm standardmäßig starten:

Option	Beschreibung
Dasselbe Installationsprogramm	Geben Sie der Datei den Namen <code>default</code> , wenn alle Hosts dieses ESXi-Installationsprogramm standardmäßig starten sollen.
Verschiedene Installationsprogramme	Benennen Sie die Datei mit der MAC-Adresse der Zielhostmaschine (<code>01-mac_address_of_target_ESXi_host</code>), wenn nur ein bestimmter Host mit dieser Datei gestartet werden soll, z. B. <code>01-23-45-67-89-0a-bc</code> .

- 5 Erstellen Sie ein Verzeichnis auf dem HTTP-Server mit dem Namen der ESXi-Version, die darin abgelegt werden soll, z. B. `/var/www/html/ESXi-6.x.x-XXXXXX`.
- 6 Kopieren Sie den Inhalt des Images des ESXi-Installationsprogramms in das soeben erstellte Verzeichnis.

7 Bearbeiten Sie die Datei `boot.cfg`.

a Fügen Sie folgende Zeile hinzu:

```
prefix=http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX
```

wobei `http://XXX.XXX.XXX.XXX/ESXi-6.x.x-XXXXXX` den Speicherort der Installationsdateien auf dem HTTP-Server angibt.

b Wenn die Dateinamen in den `kernel=`- und `modules=`-Zeilen mit einem umgekehrten Schrägstrich (`/`) beginnen, löschen Sie dieses Zeichen.

8 (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 Installationskripts anzugeben.

Verwenden Sie den folgenden Code als Beispiel, wobei `XXX.XXX.XXX.XXX` die IP-Adresse des Servers ist, auf dem sich das Installationskript befindet, und `esxi_kfiles` das Verzeichnis, in dem sich die Datei `ks.cfg` befindet.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_kfiles/ks.cfg
```

9 (Nur UEFI) Geben Sie an, ob alle UEFI-Hosts dasselbe Installationsprogramm starten sollen.

Option	Beschreibung
Dasselbe Installationsprogramm	Kopieren Sie die Datei <code>boot.cfg</code> in das Verzeichnis <code>/tftpboot/boot.cfg</code> oder verknüpfen Sie sie mit diesem Verzeichnis.
Verschiedene Installationsprogramme	<p>a Erstellen Sie ein Unterverzeichnis von <code>/tftpboot</code>, das nach der MAC-Adresse der Zielhostmaschine (<code>01-mac_address_of_target_ESXi_host</code>) benannt ist, z. B. <code>01-23-45-67-89-0a-bc</code>.</p> <p>b Legen Sie eine Kopie (oder eine Verknüpfung mit) der Datei <code>boot.cfg</code> des Hosts in diesem Verzeichnis ab, z. B. <code>/tftpboot/01-23-45-67-89-0a-bc/boot.cfg</code>.</p>

Aktualisieren von Hosts mithilfe von `esxcli`-Befehlen

Mithilfe der vSphere CLI können Sie ein Upgrade eines ESXi 6.0-Hosts oder ESXi 6.5-Hosts auf Version 6.7 durchführen und ESXi 6.0-, ESXi 6.5- und ESXi 6.7-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

me aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATA-oE 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 3-10. 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-Profiles sowie zum Ändern der Akzeptanzebene des Hosts für das Update, falls dies erforderlich ist.

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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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.

Feststellen, 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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>

- 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.

Weiter

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 [Feststellen, ob sich zum Anwenden eines Updates der Host im Wartungsmodus befindet oder neu gestartet werden muss](#).

Hinweis Wenn der Host Mitglied eines vSAN-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, da vSAN dieses Objekt vom Host entfernen muss, um den Wartungsvorgang erfolgreich abschließen zu können.

Wenn Sie mit `--server=Servername` einen Zielsever 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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=Servername Pfad_der_VM stop soft</code>
So erzwingen Sie den Ausschaltvorgang	<code>vmware-cmd --server=Servername Pfad_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.

Wenn Sie mit `--server=Servername` einen Zielsever 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. Siehe *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 [Feststellen, 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.

Vorgehensweise

- 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.

Sie können den Befehl `esxcli software profile update` oder `esxcli software profile install` verwenden, um ein Upgrade eines ESXi-Hosts durchzuführen oder um einen ESXi-Host zu aktualisieren.

Wenn Sie ein Upgrade eines Hosts durchführen oder einen Host aktualisieren, wendet der Befehl `esxcli software profile update` oder `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 unter Verwendung eines ISO-Installationsprogramms. Allerdings führt das ISO-Installationsprogramm vor dem Upgrade eine Überprüfung potentieller Probleme durch, während die `esxcli`-Upgrade-Methode darauf verzichtet. Das ISO-Installations-

programm 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 [Übersicht über den ESXi-Host-Upgrade-Vorgang](#).

Wichtig Wenn Sie ein Upgrade eines ESXi von einem ZIP-Paket eines von VMware bereitgestellten Depots durchführen oder 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 werden kann, unterstützt VMware nur den Aktualisierungsbefehl `esxcli software profile update --depot=depot_location --profile=profile_name`.

Wenn Sie mit `--server=Servername` einen Zielsever 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 finden Sie unter *Referenz zur vSphere Command-Line Interface*.

Voraussetzungen

- Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Siehe *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 [Feststellen, 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.

Vorgehensweise

- 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=server_name software sources profile list --depot=http://webserver/depot_name
```

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 des 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=depot_location --profile=profile_name</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: <code>VMware-ESXi-Versionnummer-Build-Nummer-depot.zip</code></p> <p>Der Profilename für die von VMware bereitgestellten ZIP-Pakete hat folgendes Format.</p> <ul style="list-style-type: none"> ■ <code>ESXi-version_number-build_number-standard</code> ■ <code>ESXi-Versionnummer-Build-Nummer-notools</code> (umfasst nicht die VMware Tools)
Aktualisieren des Image-Profiles von einem Depot, auf das per URL zugegriffen werden kann	<pre>esxcli --server=server_name software profile update --depot=http://webserver/depot_name --profile=profile_name</pre>
Aktualisieren des Image-Profiles von einer ZIP-Datei, die lokal auf dem Zielsystem gespeichert ist	<pre>esxcli --server=server_name software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=profile_name</pre>
Aktualisieren des Image-Profiles von einer ZIP-Datei auf dem Zielsystem, die in einen Datenspeicher kopiert wird	<pre>esxcli --server=server_name software profile update --depot="[datastore_name]profile_ZIP_file" --profile=profile_name</pre>
Aktualisieren des Image-Profiles von einer ZIP-Datei, die lokal auf dem Zielsystem kopiert und angewendet wird	<pre>esxcli --server=server_name software profile update --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</pre>
Installation aller neuen VIBs eines angegebenen Profils, auf das per URL zugegriffen werden kann	<pre>esxcli --server=server_name software profile install --depot=http://webserver/depot_name --profile=profile_name</pre>
Installation aller neuen VIBs in einem angegebenen Profil von einer ZIP-Datei, die lokal auf dem Ziel gespeichert ist	<pre>esxcli --server=server_name software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=profile_name</pre>

Option	Beschreibung
Installation aller neuen VIBs von einer ZIP-Datei auf dem Zielsystem, die in einem Datenspeicher kopiert wird	<code>esxcli --server=server_name software profile install --depot="[datastore_name]profile_ZIP_file" --profile=profile_name</code>
Installation aller neuen VIBs von einer ZIP-Datei, die lokal auf den Zielsystem kopiert und angewendet wird	<code>esxcli --server=server_name software profile install --depot=/root_dir/path_to_profile_ZIP_file/profile_ZIP_file --profile=profile_name</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.

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. Siehe *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 [Feststellen, 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.

Vorgehensweise

- ◆ 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. Siehe *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 [Feststellen, 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Zur Fehlerbehebung führen Sie esxcli-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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=Servername Pfad_der_VM stop soft</code>
So erzwingen Sie den Ausschaltvorgang	<code>vmware-cmd --server=Servername Pfad_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 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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 würden, 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 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 Zielsever 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. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

- 1 Geben Sie den folgenden Befehl ein.

```
esxcli --server=Servername software profile get
```

- 2 Prüfen Sie die Ausgabe.

Nach dem Upgrade von ESXi -Hosts

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 6.7-Lizenz zuweisen, bevor der Testzeitraum abläuft. Sie können vorhandene Lizenzen aktualisieren oder bei My VMware 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 [Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools](#).
- Richten Sie den vSphere Authentication Proxy-Dienst ein. Frühere Versionen von vSphere Authentication Proxy sind mit vSphere 6.7 nicht kompatibel. Informationen zum Konfigurieren des vSphere Authentication Proxy-Diensts finden Sie im Handbuch *vSphere-Sicherheit*.

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 6.7

Nach einem Upgrade auf ESXi 6.7 müssen Sie eine vSphere 6.7-Lizenz anwenden.

Beim Upgrade von ESXi 6.0- oder ESXi 6.5-Hosts auf ESXi 6.7-Hosts 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 6.0- oder 6.5-Lizenzen durchführen oder vSphere 6.7-Lizenzen über „My VMware“ erwerben. Wenn Sie über vSphere 6.7-Lizenzen verfügen, müssen Sie diese auf alle aktualisierten ESXi 6.7-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 6.7 die Skriptmethode verwenden, können Sie den Lizenzschlüssel in der Kickstart-Datei (ks) angeben.

Ausführen des Validierungsskripts für den sicheren Start auf einem aktualisierten ESXi -Host

Nach dem Upgrade eines ESXi-Hosts von einer früheren ESXi-Version, die UEFI Secure Boot nicht unterstützt hat, können Sie den sicheren Start aktivieren. Ob Sie den sicheren Start aktivieren können, richtet sich danach, wie Sie das Upgrade durchgeführt haben und ob beim Upgrade alle vorhandenen VIBs ersetzt oder bestimmte VIBs nicht geändert wurden. Sie können nach der Durchführung des Upgrades ein Validierungsskript ausführen, um festzustellen, ob der sichere Start von der aktualisierten Installation unterstützt wird.

Für eine erfolgreiche Durchführung des sicheren Starts müssen die Signaturen aller installierten VIBs auf dem System vorhanden sein. In älteren ESXi-Versionen werden die Signaturen beim Installieren von VIBs nicht gespeichert.

Für den sicheren Start über UEFI müssen die ursprünglichen VIB-Signaturen beibehalten werden. Ältere Versionen von ESXi behalten die Signaturen nicht bei, aber beim Upgrade werden die VIB-Signaturen aktualisiert.

- Wenn Sie das Upgrade mithilfe von ESXCLI-Befehlen durchführen, behalten die aktualisierten VIBs die Signaturen nicht bei. In diesem Fall können Sie keinen sicheren Start für dieses System durchführen.
- Wenn Sie das Upgrade mithilfe der ISO-Datei durchführen, speichert das Upgrade die Signaturen aller neuen VIBs. Dies gilt auch für Upgrades von vSphere Update Manager, die die ISO-Datei verwenden.

Wenn beliebige alte VIBs auf dem System verbleiben, stehen die Signaturen dieser VIBs noch nicht zur Verfügung und ein sicherer Start ist nicht möglich.

Wenn das System beispielsweise einen Drittanbietertreiber verwendet und das VMware-Upgrade keine neue Version des Treiber-VIB enthält, verbleibt das alte VIB nach dem Upgrade auf dem System. In seltenen Fällen stellt VMware die fortlaufende Entwicklung eines bestimmten VIB ein, ohne ein neues VIB bereitzustellen, das das alte ersetzt oder überflüssig macht. In diesem Fall verbleibt das alte VIB nach dem Upgrade auf dem System.

Hinweis

Für den sicheren Start über UEFI ist außerdem ein aktueller Bootloader erforderlich. Mit diesem Skript wird nicht geprüft, ob ein aktueller Bootloader vorhanden ist.

Voraussetzungen

- Stellen Sie sicher, dass die Hardware den sicheren Start über UEFI unterstützt.
- Stellen Sie sicher, dass alle VIBs mindestens mit der Akzeptanzebene „PartnerSupported“ signiert sind. Wenn Sie VIBs auf der Ebene „CommunitySupported“ einbeziehen, können Sie den sicheren Start nicht verwenden.

Vorgehensweise

- 1 Führen Sie ein Upgrade für ESXi durch und führen Sie den folgenden Befehl aus.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

- 2 Prüfen Sie die Ausgabe.

Die Ausgabe enthält entweder `Secure boot can be enabled` oder `Secure boot CANNOT be enabled`.

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Wenn Sie Auto Deploy für die Installation Ihres ESXi 6.7-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volumen 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 6.7 die Protokolle in optimaler Abstimmung mit Ihrer Installation und bietet ausreichend Speicherplatz für Protokollnachrichten.

Tabelle 3-11. 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 *Installation und Einrichtung von vCenter Server*.

Konfiguration von Syslog auf ESXi -Hosts

Sie können den vSphere Web Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Dienstes verwenden.

Informationen zur Verwendung des `esxcli system syslog`-Befehls und anderen vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere Command-Line Interfaces*.

Vorgehensweise

- 1 Wählen Sie den Host im Bestandslistenbereich des vSphere Web Client aus.
- 2 Klicken Sie auf **Konfigurieren**.
- 3 Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
- 4 Filter für **syslog**.
- 5 Um das Protokollieren global einzurichten, wählen Sie die zu ändernde Einstellung aus und klicken Sie auf das Symbol **Bearbeiten**.

Option	Beschreibung
<code>Syslog.global.defaultRotate</code>	Maximale Anzahl der beizubehaltenden Archive. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
<code>Syslog.global.defaultSize</code>	Standardgröße des Protokolls in KB, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.

Option	Beschreibung
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis /scratch auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Geben Sie das Verzeichnis im Format <i>[Datenspeichername] Pfad_zur_Datei</i> an, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad <i>[storage1] /systemlogs</i> dem Pfad <i>/vmfs/volumes/storage1/systemlogs</i> 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. <i>ssl://Hostname1:1514</i> . 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 gewünschte Protokollgröße an.
- 7 Klicken Sie auf **OK**.

Änderungen an der syslog-Option werden sofort wirksam.

Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts

4

Wenn ein Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy zum erneuten Bereitstellen des Hosts mit einem neuen Image-Profil verwenden, das eine andere Version von ESXi enthält. Mit vSphere ESXi Image Builder können Sie Image-Profile erstellen und verwalten.

Hinweis Wenn Sie ein Upgrade des Hosts für die Verwendung eines Images mit ESXi 6.0 oder höher durchführen, stellt der vSphere Auto Deploy-Server den ESXi-Host mit von VMCA signierten Zertifikaten bereit. Wenn Sie derzeit benutzerdefinierte Zertifikate verwenden, können Sie den Host so einrichten, dass er die benutzerdefinierten Zertifikate nach dem Upgrade verwendet. Siehe *vSphere-Sicherheit*.

Das Upgrade des vSphere Auto Deploy-Servers wird automatisch durchgeführt, wenn Sie ein Upgrade des entsprechenden vCenter Server-Systems durchführen. Ab Version 6.0 befindet sich der vSphere Auto Deploy-Server immer im selben Verwaltungsknoten wie das vCenter Server-System.

Dieses Kapitel behandelt die folgenden Themen:

- [Einführung in vSphere Auto Deploy](#)
- [Vorbereitung für vSphere Auto Deploy](#)
- [Erneute Bereitstellung von Hosts](#)

Einführung in vSphere Auto Deploy

Wenn Sie einen physischen Host starten, der für vSphere Auto Deploy eingerichtet ist, verwendet vSphere Auto Deploy eine PXE-Startvorgangsinfrastruktur in Verbindung mit vSphere-Hostprofilen, um diesen Host bereitzustellen und anzupassen. Auf dem Host selbst wird kein Status gespeichert. Stattdessen verwaltet der vSphere Auto Deploy-Server die Statusinformationen für jeden Host.

Statusinformationen für ESXi -Hosts

vSphere Auto Deploy speichert die Informationen für die bereitzustellenden ESXi-Hosts an verschiedenen Speicherorten. Die Informationen über den Speicherort der Image-Profile und Hostprofile wird anfänglich in den Regeln angegeben, die die Maschinen den Image-Profilen und Hostprofilen zuordnen.

Tabelle 4-1. vSphere Auto Deploy speichert Informationen zur Bereitstellung

Informationstyp	Beschreibung	Informationsquelle
Image-Status	Die ausführbare Software zur Ausführung auf einem ESXi-Host	Mit vSphere ESXi Image Builder erstelltes Image-Profil.
Konfigurationsstatus	Die konfigurierbaren Einstellungen, die festlegen, wie der Host konfiguriert wird, z. B. virtuelle Switches und ihre Einstellungen, Treibereinstellungen, Startparameter usw	Hostprofil, das über die Benutzeroberfläche des Hostprofils erstellt wurde. Kommt oft von einem Vorlagen-Host.
Status „Dynamisch“	Der Laufzeitstatus, der von der laufenden Software generiert wird, z. B. generierte private Schlüssel oder Laufzeitdatenbanken	Hostarbeitsspeicher, während des Startvorgangs verloren gegangen
Zustand der virtuellen Maschine	Die virtuellen Maschinen, die auf einem Host gespeichert sind, und Autostartinformationen für virtuelle Maschinen (nur bei nachfolgenden Startvorgängen)	Die VM-Informationen, die vom vCenter Server an vSphere Auto Deploy gesendet werden, müssen verfügbar sein, um vSphere Auto Deploy mit Informationen zur virtuellen Maschine zu versorgen.
Benutzereingabe	Der Status basiert auf der Benutzereingabe. So kann beispielsweise eine IP-Adresse, die der Benutzer beim Systemstart angibt, nicht automatisch in das Hostprofil aufgenommen werden.	<p>Hostanpassungsdaten, gespeichert vom vCenter Server während des ersten Startvorgangs</p> <p>Sie können ein Hostprofil erstellen, das für bestimmte Werte eine Benutzereingabe erfordert.</p> <p>Wenn vSphere Auto Deploy ein Hostprofil anwendet, das vom Benutzer bereitgestellte Informationen erfordert, wird der Host in den Wartungsmodus versetzt. Verwenden Sie die Benutzeroberfläche für Hostprofile, um die Übereinstimmung von Hostprofilen zu prüfen, und antworten Sie auf die Aufforderung zum Anpassen des Hosts.</p>

vSphere Auto Deploy-Architektur

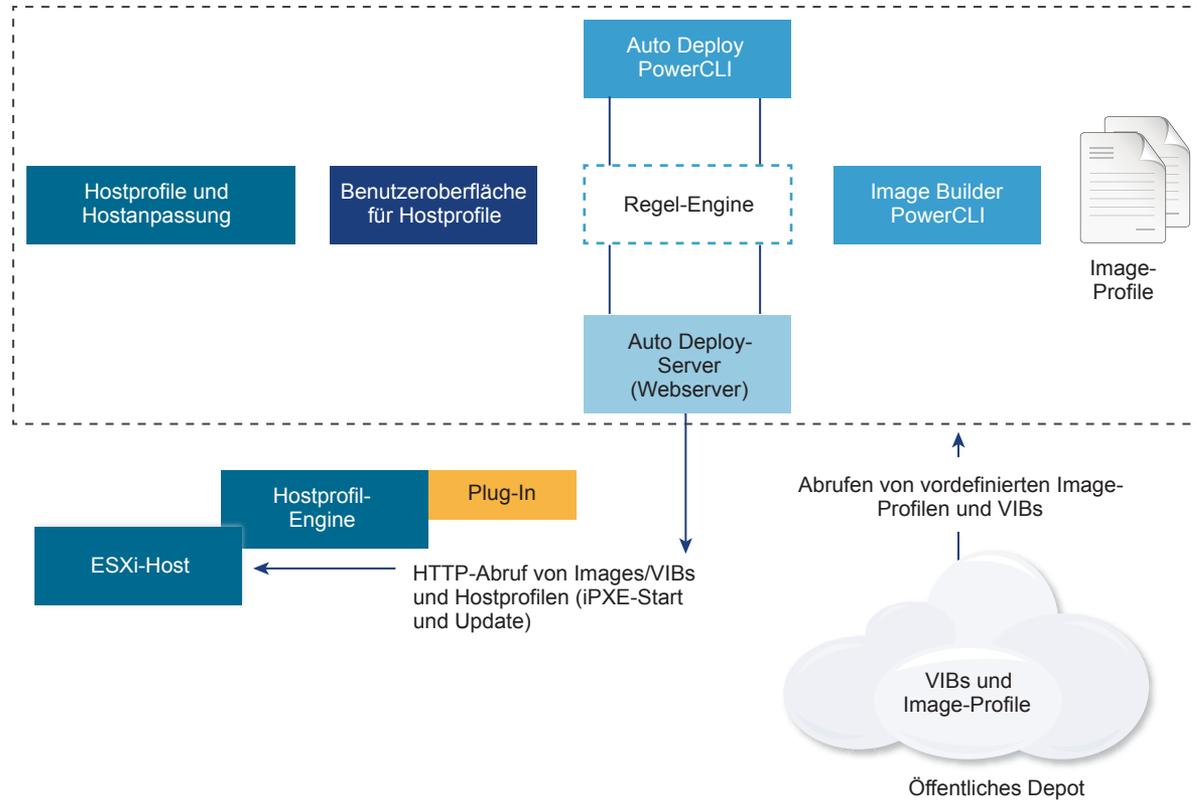
Die vSphere Auto Deploy-Infrastruktur besteht aus mehreren Komponenten.

Weitere Informationen erhalten Sie im Video zur Auto Deploy-Architektur.



Auto Deploy-Architektur (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_auto_deploy_architecture)

Abbildung 4-1. vSphere Auto Deploy-Architektur



vSphere Auto Deploy-Server

Server-Images und Hostprofile auf ESXi-Hosts

vSphere Auto Deploy-Regel-Engine

Sendet Informationen an den vSphere Auto Deploy-Server darüber, welches Image-Profil und welches Hostprofil für welchen Host bereitgestellt werden sollen. Administratoren verwenden vSphere Auto Deploy zur Definition der Regeln, die den Hosts Image-Profile und Hostprofile zuweisen.

Image-Profile

Definieren Sie den VIB-Satz, mit dem die ESXi-Hosts gestartet werden sollen.

- VMware und VMware-Partner stellen Image-Profile und VIBs in öffentlichen Depots zur Verfügung. Verwenden Sie vSphere ESXi Image Builder zur Untersuchung des Depots und die vSphere Auto Deploy-Regel-Engine zur Festlegung, welches Image-Profil welchem Host zugewiesen werden soll.
- VMware-Kunden können ein benutzerdefiniertes Image-Profil auf Basis der öffentlichen Image-Profile und VIBs im Depot erstellen und dieses Image-Profil dem Host zuweisen.

- Hostprofile** Definieren Sie eine maschinenspezifische Konfiguration, wie z. B. ein Netzwerk- oder Speicher-Setup. Erstellen Sie Hostprofile mithilfe der Benutzeroberfläche für Hostprofile. Sie können ein Hostprofil für einen Referenzhost erstellen und dieses Hostprofil auf andere Hosts in Ihrer Umgebung anwenden, um eine konsistente Konfiguration herzustellen.
- Hostanpassung** Speichert Informationen, die der Benutzer angibt, wenn Hostprofile auf den Host angewendet werden. Die Hostanpassung kann möglicherweise eine IP-Adresse oder andere Informationen enthalten, die der Benutzer für diesen Host angegeben hat. Weitere Informationen zu Hostanpassungen finden Sie in der Dokumentation *vSphere-Hostprofile*.
- In früheren Versionen von vSphere Auto Deploy wurde die Hostanpassung „Antwortdatei“ genannt.

Vorbereitung für vSphere Auto Deploy

Sie müssen Ihre Umgebung auf die Verwendung von vSphere Auto Deploy vorbereiten. Sie beginnen mit dem Einrichten des Servers und der Vorbereitung der Hardware. Sie müssen den Starttyp des vSphere Auto Deploy-Diensts in dem vCenter Server-System konfigurieren, das Sie zur Verwaltung der bereitgestellten Hosts verwenden möchten, und PowerCLI installieren.

- [Vorbereiten des Systems für vSphere Auto Deploy](#)

Bevor Sie einen ESXi-Host mit PXE und vSphere Auto Deploy starten können, müssen Sie die erforderliche Software installieren und die DHCP- und TFTP-Server einrichten, mit denen vSphere Auto Deploy interagiert.

- [Verwendung der vSphere Auto Deploy-Cmdlets](#)

vSphere Auto Deploy-Cmdlets werden als Microsoft PowerShell-Cmdlets implementiert und sind in PowerCLI enthalten. Benutzer von vSphere Auto Deploy-Cmdlets haben den Vorteil, alle PowerCLI-Funktionen nutzen zu können.

- [Einrichten der Massenzulassung](#)

Sie können den vSphere Web Client oder die ESXi Shell dazu verwenden, einzelne Lizenzschlüssel anzugeben, oder Sie können die Massenzulassung mithilfe der PowerCLI-Cmdlets einrichten. Die Massenzulassung kann auf allen ESXi-Hosts eingesetzt werden, ist jedoch besonders nützlich für mit vSphere Auto Deploy bereitgestellte Hosts.

Vorbereiten des Systems für vSphere Auto Deploy

Bevor Sie einen ESXi-Host mit PXE und vSphere Auto Deploy starten können, müssen Sie die erforderliche Software installieren und die DHCP- und TFTP-Server einrichten, mit denen vSphere Auto Deploy interagiert.

Eine detaillierte Anleitung und Informationen zur Vorbereitung Ihres Systems für vSphere Auto Deploy finden Sie unter *Installation und Einrichtung von vSphere*.

Voraussetzungen

- Überprüfen Sie, ob die Hosts, die Sie mit vSphere Auto Deploy bereitstellen möchten, den Hardwareanforderungen für ESXi entsprechen. Weitere Informationen hierzu finden Sie unter [Hardwareanforderungen für ESXi](#).
- Stellen Sie sicher, dass die ESXi-Hosts über eine Netzwerkverbindung mit vCenter Server verfügen und alle Portanforderungen erfüllt sind. Siehe *vCenter Server-Upgrade*.
- Wenn Sie in Ihrer vSphere Auto Deploy-Umgebung VLANs verwenden möchten, müssen Sie das End-to-End-Netzwerk ordnungsgemäß einrichten. Wenn der Host per PXE gestartet wird, muss der Firmware-Treiber für das Taggen der Frames mit den richtigen VLAN-IDs konfiguriert werden. Sie müssen diese Konfiguration manuell durchführen, indem Sie über die UEFI/BIOS-Schnittstelle die entsprechenden Änderungen vornehmen. Außerdem müssen die ESXi-Portgruppen mit den richtigen VLAN-IDs konfiguriert werden. Fragen Sie Ihren Netzwerkadministrator, wie VLAN-IDs in Ihrer Umgebung verwendet werden.
- Stellen Sie sicher, dass der Speicher für das vSphere Auto Deploy-Repository ausreicht. Der vSphere Auto Deploy-Server verwendet das Repository zum Speichern der erforderlichen Daten. Dazu zählen die von Ihnen erstellten Regeln und Regelsätze und die VIBs und Image-Profile, die Sie in Ihren Regeln angeben.

Als Best Practice teilen Sie 2 GB zu, damit Sie ausreichend Speicherplatz für vier Image-Profilen bereit und zusätzlichen Speicherplatz in Reserve haben. Für jedes Image-Profil werden ungefähr 350 MB benötigt. Berechnen Sie den Speicherplatzbedarf für das vSphere Auto Deploy-Repository anhand der Anzahl der Image-Profile, die Sie voraussichtlich verwenden werden.

- Verschaffen Sie sich Administratorrechte für den DHCP-Server, der das Netzwerksegment verwaltet, von dem Sie starten möchten. Sie können einen bereits in Ihrer Umgebung vorhandenen DHCP-Server verwenden oder einen DHCP-Server installieren. Ersetzen Sie für Ihre vSphere Auto Deploy-Einrichtung den Dateinamen `gpxelinux.0` durch `snponly64.efi.vmw-hardwired` für UEFI oder `undionly.kpxe.vmw-hardwired` für BIOS. Weitere Informationen zu DHCP-Konfigurationen finden Sie unter [DHCP-Beispielkonfigurationen](#).
- Sichern Sie Ihr Netzwerk wie bei jeder anderen PXE-basierten Bereitstellungsmethode. vSphere Auto Deploy überträgt Daten über SSL, um gelegentliche Störungen und Webspionage zu verhindern. Allerdings wird die Authentizität des Clients oder des vSphere Auto Deploy-Servers während des Startens per PXE-Startvorgang nicht überprüft.
- Wenn Sie vSphere Auto Deploy mit PowerCLI-Cmdlets verwalten möchten, überprüfen Sie, ob Microsoft .NET Framework 4.5 oder 4.5.x und Windows PowerShell 3.0 oder 4.0 auf einem Windows-Computer installiert ist. Sie können PowerCLI auf dem Windows-System installieren, auf dem vCenter Server installiert ist, oder auf einem anderen Windows-System. Weitere Informationen finden Sie im *vSphere PowerCLI-Benutzerhandbuch*.

- Richten Sie einen Remote-Syslog-Server ein. Weitere Informationen zur Konfiguration eines Syslog-Servers finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*. Konfigurieren Sie den ersten Host, den Sie zum Verwenden des Remote-Syslog-Servers starten, und wenden Sie das Hostprofil dieses Hosts auf alle anderen Zielhosts an. Sie können optional vSphere Syslog Collector, ein vCenter Server-Dienstprogramm, das eine einheitliche Architektur für die Systemprotokollierung bietet sowie die Netzwerkprotokollierung und das Kombinieren von Protokollen mehrerer Hosts ermöglicht, installieren und verwenden.
- Installieren Sie ESXi Dump Collector und richten Sie Ihren ersten Host so ein, dass alle Core-Dumps auf ESXi Dump Collector verwiesen werden. Wenden Sie anschließend das Hostprofil von diesem Host auf alle anderen Hosts an.
- Wenn die Hosts, die Sie mit vSphere Auto Deploy bereitstellen möchten, Legacy-BIOS verwenden, stellen Sie sicher, dass der vSphere Auto Deploy-Server über eine IPv4-Adresse verfügt. Legacy-BIOS-Firmware kann nur über IPv4 mit PXE gestartet werden. UEFI-Firmware kann entweder über IPv4 oder IPv6 mit PXE gestartet werden.

Vorgehensweise

- 1 Installieren Sie vCenter Server oder stellen Sie vCenter Server Appliance bereit.
Der vSphere Auto Deploy-Server ist im Verwaltungsknoten enthalten.
- 2 Konfigurieren Sie den Starttyp des vSphere Auto Deploy-Diensts.
 - a Melden Sie sich über vCenter Server beim vSphere Web Client-System an.
 - b Klicken Sie auf der Startseite von vSphere Web Client auf **Verwaltung**.
 - c Klicken Sie unter **Systemkonfiguration** auf **Dienste**.
 - d Wählen Sie **Auto Deploy**, klicken Sie auf das Menü **Aktionen** und wählen Sie **Starttyp bearbeiten**.
 - Unter Windows ist der vSphere Auto Deploy-Dienst deaktiviert. Wählen Sie im Fenster **Starttyp bearbeiten** die Option **Manuell** oder **Automatisch** aus, um vSphere Auto Deploy zu aktivieren.
 - In vCenter Server Appliance ist der vSphere Auto Deploy-Dienst standardmäßig auf **Manuell** gesetzt. Wenn Sie möchten, dass der vSphere Auto Deploy-Dienst beim Start des Betriebssystems automatisch gestartet wird, wählen Sie **Automatisch** aus.

- 3 (Optional) Wenn Sie vSphere Auto Deploy mit dem vSphere Web Client verwalten möchten, konfigurieren Sie den Starttyp des vSphere ESXi Image Builder-Diensts.
 - a Wiederholen Sie [Schritt 2a](#) bis [Schritt 2c](#).
 - b Wählen Sie **ImageBuilder-Dienst** aus, klicken Sie auf das Menü **Aktionen** und wählen Sie **Starttyp bearbeiten** aus.
 - Unter Windows ist der vSphere ESXi Image Builder-Dienst deaktiviert. Wählen Sie im Fenster **Starttyp bearbeiten** die Option **Manuell** oder **Automatisch** aus, um den Dienst zu aktivieren.
 - In vCenter Server Appliance ist der vSphere Auto Deploy-Dienst standardmäßig auf **Manuell** gesetzt. Wenn Sie möchten, dass der vSphere ESXi Image Builder-Dienst beim Start des Betriebssystems automatisch gestartet wird, wählen Sie **Automatisch** aus.
 - c Melden Sie sich beim vSphere Web Client ab und wieder an.
Das Symbol **Auto Deploy** wird auf der Startseite des vSphere Web Client angezeigt.
- 4 (Optional) Wenn Sie vSphere Auto Deploy mit PowerCLI-Cmdlets verwalten möchten, installieren Sie PowerCLI.
 - a Laden Sie die aktuelle Version von PowerCLI von der VMware-Website herunter.
 - b Navigieren Sie zu dem Ordner, der die heruntergeladene Datei PowerCLI enthält und doppelklicken Sie auf die ausführbare Datei.

Wenn der Installationsassistent eine frühere Version von PowerCLI auf Ihrem System erkennt, versucht er, Ihre vorhandene Installation zu aktualisieren.
 - c Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation abzuschließen.
- 5 Konfigurieren Sie den TFTP-Server.
 - a Wechseln Sie in einem vSphere Web Client, der mit dem vCenter Server-System verbunden ist, zur Bestandsliste und wählen Sie das vCenter Server-System aus.
 - b Klicken Sie auf die Registerkarte **Verwalten**, wählen Sie **Einstellungen** und klicken Sie auf **Auto Deploy**.
 - c Klicken Sie auf **TFTP Boot Zip herunterladen**, um die TFTP-Konfigurationsdatei herunterzuladen, und entpacken Sie die Datei in dem Verzeichnis, in dem der TFTP-Server Dateien speichert.
- 6 Richten Sie Ihren DHCP-Server so ein, dass er auf den TFTP-Server verweist, auf dem sich die TFTP-ZIP-Datei befindet.
 - a Geben Sie in DHCP-Option 66 (oft als „next-server“ bezeichnet) die IP-Adresse des TFTP-Servers ein.
 - b Geben Sie den Namen der Startdatei (snponly64.efi.vmw-hardwired) für UEFI oder undionly.kpxe.vmw-hardwired für BIOS in DHCP-Option 67 (oft als boot-filename bezeichnet) an.
- 7 Richten Sie jeden mit vSphere Auto Deploy bereitzustellenden Host für das Starten über das Netzwerk oder per PXE-Startvorgang gemäß den Anweisungen des Anbieters ein.

- 8 (Optional) Wenn Sie Ihre Umgebung für den Einsatz des Fingerabdruckmodus einrichten, können Sie Ihre eigene Zertifizierungsstelle (CA) verwenden, indem Sie das OpenSSL-Zertifikat `rbd-ca.crt` und den privaten OpenSSL-Schlüssel `rbd-ca.key` durch ein eigenes Zertifikat und eine eigene Schlüsseldatei ersetzen.
- Unter Windows befinden sich die Dateien im Unterordner „SSL“ des vSphere Auto Deploy-Installationsverzeichnisses. Unter Windows 7 ist z. B. der Standardordner `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.
 - Auf der vCenter Server Appliance befinden sich die Dateien im Verzeichnis `/etc/vmware-rbd/ssl/`.

Standardmäßig verwendet vCenter Server 6.0 und höher die VMware Certificate Authority (VMCA).

Wenn Sie einen Host einschalten, der für vSphere Auto Deploy eingerichtet ist, kontaktiert der Host den DHCP-Server und wird an den vSphere Auto Deploy-Server verwiesen, der den Host mit dem Image-Profil bereitstellt, das im aktiven Regelsatz angegeben ist.

Weiter

- Definieren Sie eine Regel, die dem Host ein Image-Profil und optionales Hostprofil, einen Hostspeicherort oder ein Skriptpaket zuordnet.
- (Optional) Konfigurieren Sie den ersten Host, den Sie bereitstellen, als Referenzhost. Verwenden Sie die Speicher- und Netzwerkeinstellungen sowie weitere Einstellungen, die Sie auf Ihren Zielhosts freigeben möchten. Erstellen Sie ein Hostprofil für den Referenzhost und schreiben Sie eine Regel, die den Zielhosts sowohl das bereits getestete Image-Profil als auch das Hostprofil zuweist.
- (Optional) Wenn vSphere Auto Deploy die vorhandenen Partitionen überschreiben soll, richten Sie einen Referenzhost für die Durchführung der automatischen Partitionierung ein und wenden Sie das Hostprofil des Referenzhosts auf andere Hosts an.
- (Optional) Wenn Sie hostspezifische Informationen konfigurieren müssen, richten Sie das Hostprofil des Referenzhosts so ein, dass Benutzer zur Eingabe von Informationen aufgefordert werden. Weitere Informationen zu Hostanpassungen finden Sie in der Dokumentation *vSphere-Hostprofile*.

Verwendung der vSphere Auto Deploy-Cmdlets

vSphere Auto Deploy-Cmdlets werden als Microsoft PowerShell-Cmdlets implementiert und sind in PowerCLI enthalten. Benutzer von vSphere Auto Deploy-Cmdlets haben den Vorteil, alle PowerCLI-Funktionen nutzen zu können.

Erfahrene PowerShell-Benutzer können vSphere Auto Deploy-Cmdlets genau wie andere PowerShell-Cmdlets verwenden. Wenn Sie PowerShell und PowerCLI erst seit Kurzem verwenden, sind möglicherweise die folgenden Tipps hilfreich.

Sie können cmdlets, Parameter und Parameterwerte in die PowerCLI-Shell eingeben.

- Sie erhalten Hilfe zu jedem Cmdlet, indem Sie `Get-Helpcmdlet_name` ausführen.
- Beachten Sie, dass bei PowerShell die Groß-/Kleinschreibung nicht beachtet wird.

- Verwenden Sie die Tabulatortaste zum Vervollständigen der cmdlet- und Parameternamen.
- Formatieren Sie die Ausgabe von Variablen und Cmdlets mit `Format-List` oder `Format-Table` bzw. deren Kurzformen `fl` oder `ft`. Um weitere Informationen zu erhalten, führen Sie das Cmdlet `Get-Help Format-List` aus.

Übergeben von Parametern per Name

Sie können in den meisten Fällen Parameter per Name übergeben und Parameterwerte, die Leer- oder Sonderzeichen enthalten, in doppelte Anführungszeichen einschließen.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Bei den meisten Beispielen in der Dokumentation zu *Installation und Einrichtung von vCenter Server* werden Parameter nach Namen übergeben.

Übergeben von Parametern als Objekte

Für Scripting und Automatisierung können Sie Parameter als Objekte übergeben. Das Übergeben von Parametern als Objekte ist sowohl nützlich bei cmdlets, die mehrere Objekte zurückgeben, als auch bei cmdlets, die ein einzelnes Objekt zurückgeben. Betrachten Sie das folgende Beispiel.

- 1 Binden Sie das Objekt, das die Regelsatz-Übereinstimmungsinformationen für einen Host einkapselt, an eine Variable.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

- 2 Zeigen Sie die Eigenschaft `itemlist` des Objekts an, um den Unterschied zu sehen zwischen dem, was sich im Regelsatz befindet, und dem, was der Host aktuell verwendet.

```
$tr.itemlist
```

- 3 Standardisieren Sie den Host, sodass er den überarbeiteten Regelsatz nutzt. Verwenden Sie dazu mit der Variablen das Cmdlet `Repair-DeployRuleSetCompliance`.

```
Repair-DeployRuleSetCompliance $tr
```

Im Beispiel wird der Host standardisiert, wenn Sie ihn das nächste Mal starten.

Einrichten der Massenzulassung

Sie können den vSphere Web Client oder die ESXi Shell dazu verwenden, einzelne Lizenzschlüssel anzugeben, oder Sie können die Massenzulassung mithilfe der PowerCLI-Cmdlets einrichten. Die Massenzulassung kann auf allen ESXi-Hosts eingesetzt werden, ist jedoch besonders nützlich für mit vSphere Auto Deploy bereitgestellte Hosts.

Die Zuweisung von Lizenzschlüsseln über den vSphere Web Client und die Zuweisung von Lizenzen mithilfe von PowerCLI-Cmdlets funktionieren unterschiedlich.

Zuweisen von Lizenzschlüsseln mit dem vSphere Web Client

Sie können einem Host Lizenzschlüssel zuweisen, wenn Sie den Host zum vCenter Server-System hinzufügen oder wenn der Host von einem vCenter Server-System verwaltet wird.

Zuweisen von Lizenzschlüsseln mit LicenseDataManager PowerCLI

Sie können mehrere Lizenzschlüssel angeben, die zu mehreren Hosts hinzugefügt werden sollen. Die Lizenzschlüssel werden zur vCenter Server-Datenbank hinzugefügt. Jedes Mal, wenn ein Host zum vCenter Server-System hinzugefügt wird oder sich erneut damit verbindet, wird dem Host ein Lizenzschlüssel zugewiesen. Ein Lizenzschlüssel, der über die PowerCLI zugewiesen wird, wird als Standardlizenzschlüssel angesehen. Wenn ein nicht lizenziertes Host hinzugefügt oder erneut verbunden wird, wird ihm der Standardlizenzschlüssel zugewiesen. Wenn ein Host bereits lizenziert ist, behält er seinen Lizenzschlüssel bei.

Im folgenden Beispiel werden allen Hosts in einem Datacenter Lizenzen zugewiesen. Sie können auch Lizenzen mit Hosts und Clustern verknüpfen.

Das folgende Beispiel richtet sich an fortgeschrittene PowerCLI-Benutzer, die mit der Verwendung von PowerShell-Variablen vertraut sind.

Voraussetzungen

[Vorbereiten des Systems für vSphere Auto Deploy.](#)

Vorgehensweise

- 1 Stellen Sie in einer PowerCLI-Sitzung eine Verbindung mit dem gewünschten vCenter Server-System her und binden Sie den zugeordneten Lizenz-Manager an eine Variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password $licenseDataManager = Get-LicenseDataManager
```

- 2 Führen Sie ein cmdlet aus, das das Datacenter abrufen, in dem sich die Hosts befinden, für die Sie die Massenzulassungsfunktion verwenden möchten.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

Sie können auch ein cmdlet ausführen, das einen Cluster abrufen, wobei die Massenzulassung für alle darin enthaltenen Hosts durchgeführt werden soll, oder das einen Ordner abrufen, wobei die Massenzulassung für alle Hosts dieses Ordners durchgeführt werden soll.

- 3 Erstellen Sie ein neues LicenseData-Objekt und ein LicenseKeyEntry-Objekt mit zugewiesener Typ-ID und Lizenzschlüssel.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData $licenseKeyEntry = New-Object VMware.VimAutomation.License.Types.LicenseKeyEntry $licenseKeyEntry.TypeId = "vmware-vmware" $licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

- 4 Verknüpfen Sie das `LicenseKeys`-Attribut des `LicenseData`-Objekts, das Sie in Schritt 3 erstellt haben, mit dem `LicenseKeyEntry`-Objekt.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

- 5 Aktualisieren Sie die Lizenzdaten für das Datacenter mit dem `LicenseData`-Objekt und stellen Sie sicher, dass die Lizenz dem Host-Container zugeordnet ist.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData) $licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

- 6 Stellen Sie einen oder mehrere Hosts mit vSphere Auto Deploy bereit und weisen Sie sie dem Datacenter oder dem Cluster zu, denen Sie die Lizenzdaten zugewiesen haben.
- 7 Mit dem vSphere Web Client können Sie sicherstellen, dass der Host erfolgreich der Standardlizenz XXXXX-XXXXX-XXXXX-XXXXX-XXXXX zugewiesen wurde.

Alle Hosts, die Sie dem Datacenter zugewiesen haben, werden nun automatisch lizenziert.

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 vSphere 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 vSphere 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.

Voraussetzungen

- Überprüfen Sie, ob die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt haben, vorhanden ist.

- Überprüfen Sie, ob alle verknüpften Elemente verfügbar sind. Bei einem Element kann es sich um ein Image-Profil, ein Hostprofil, ein benutzerdefiniertes Skript oder einen vCenter Server-Bestandslisten-Speicherort handeln.
- Überprüfen Sie, ob der Host die Identifizierungsinformationen (Asset-Tag, IP-Adresse) hat, über die er während der vorherigen Startvorgänge verfügte.

Vorgehensweise

- 1 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 virtuellen Maschinen auf verschiedene Hosts migrieren und jeden Host in den Wartungsmodus versetzen.

- 2 Starten Sie den Host neu.

Der Host wird heruntergefahren. Wenn der Host neu gestartet wird, verwendet er das vom vSphere Auto Deploy-Server bereitgestellte Image-Profil. Der vSphere 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 unter Verwendung von PowerCLI

Sie können vSphere Auto Deploy verwenden, um einen Host mit einem neuen Image-Profil in einer PowerCLI-Sitzung erneut bereitzustellen, indem Sie die Regel für den Host ändern und einen Vorgang zum Testen und Reparieren 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

- Überprüfen Sie, ob das Image-Profil, das Sie für die erneute Bereitstellung des Hosts verwenden möchten, verfügbar ist. Verwenden Sie vSphere ESXi Image Builder in einer PowerCLI-Sitzung. Lesen Sie „Verwenden von vSphere ESXi Image Builder CLI“ im *Installations- und Einrichtungshandbuch für vSphere*.

- Überprüfen Sie, ob die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt haben, vorhanden ist.

Vorgehensweise

- 1 Führen Sie an der PowerShell-Eingabeaufforderung das PowerCLI-Cmdlet `Connect-VIServer` aus, um eine Verbindung zum vCenter Server-System herzustellen, bei dem vSphere Auto Deploy registriert ist.

```
Connect-VIServer ipv4_or_ipv6_address
```

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 gewünschte Image-Profil enthält, oder definieren Sie mithilfe von vSphere ESXi Image Builder 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 <i>depot_url</i></code> aus.
ZIP-Datei	<ol style="list-style-type: none"> a Laden Sie die ZIP-Datei in einen lokalen Dateipfad herunter oder erstellen Sie für die PowerCLI-Maschine einen lokalen Mount-Punkt. b 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 my_new_imageprofile
```

- 6 Testen Sie die Regelübereinstimmung für jeden Host, auf dem Sie das Image bereitstellen möchten.
- a Vergewissern Sie sich, dass Sie auf den Host zugreifen können, dessen Regelsatzübereinstimmung Sie testen möchten.

```
Get-VMHost -Name ESXi_hostname
```

- b 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 ESXi_hostname
```

- c 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, wenn der Host, dessen Übereinstimmung mit der neuen Regel Sie testen möchten, mit dem aktiven Regelsatz kompatibel ist.

CurrentItem	ExpectedItem
-----	-----
<i>my_old_imageprofile</i>	<i>my_new_imageprofile</i>

- d Standardisieren Sie den Host, sodass er beim nächsten Neustart den überarbeiteten Regelsatz verwendet.

```
Repair-DeployRuleSetCompliance $tr
```

- 7 Starten Sie den Host neu, um ihn mit dem neuen Image-Profil bereitzustellen.

Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts

vSphere 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 VMware PowerCLI und alle erforderliche Software. Weitere Informationen finden Sie unter *Installation und Einrichtung von vCenter Server*.
- Exportieren Sie das Hostprofil, das Sie verwenden möchten.

Vorgehensweise

- 1 Führen Sie in einer PowerCLI-Sitzung das `Connect-VIServer`-cmdlet aus, um eine Verbindung zum vCenter Server-System herzustellen, mit dem vSphere Auto Deploy registriert ist.

```
Connect-VIServer ipv4_or_ipv6_address
```

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 cmdlet `Get-VMhostProfile` PowerCLI unter Angabe des ESXi-Hosts ausführen, von dem Sie ein Hostprofil erstellen.
- 4 Definieren Sie an der 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.

Weiter

- Weisen Sie dem neuen Host einen bereits mithilfe von vSphere Auto Deploy bereitgestellten 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 vSphere Auto Deploy-Regelsatz hinzufügen oder Änderungen an einer oder mehreren Regeln vornehmen, werden die Hosts nicht automatisch aktualisiert. vSphere Auto Deploy übernimmt die neuen Regeln nur dann, wenn Sie deren Regelübereinstimmung testen und eine Standardisierung durchführen.

Voraussetzungen

- [Vorbereiten des Systems für vSphere Auto Deploy](#)
- Vergewissern Sie sich, dass Ihre Infrastruktur einen oder mehrere ESXi-Hosts enthält, die mit vSphere Auto Deploy bereitgestellt wurden, und dass der Host, auf dem PowerCLI installiert ist, auf diese ESXi-Hosts zugreifen kann.

Vorgehensweise

- 1 Führen Sie in einer PowerCLI-Sitzung das `Connect-VIServer`-cmdlet aus, um eine Verbindung zum vCenter Server-System herzustellen, mit dem vSphere Auto Deploy registriert ist.

```
Connect-VIServer ipv4_or_ipv6_address
```

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 PowerCLI, um zu überprüfen, welche vSphere Auto Deploy-Regeln derzeit verfügbar sind.

```
Get-DeployRule
```

Das System gibt die Regeln und die zugeordneten Elemente und Muster zurück.

- 3 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 zum aktiven Regelsatz hinzugefügt wurde. Kopieren Sie stattdessen die Regel und ersetzen Sie das Element oder Muster, das Sie ändern möchten.

- 4 Vergewissern Sie sich, dass Sie auf den Host zugreifen können, dessen Regelsatzübereinstimmung Sie testen möchten.

```
Get-VMHost -Name MyEsxi42
```

- 5 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
```

- 6 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, wenn der Host, dessen Übereinstimmung mit der neuen Regel Sie testen möchten, mit dem aktiven Regelsatz kompatibel ist.

CurrentItem	ExpectedItem
-----	-----
<i>My Profile 25</i>	<i>MyNewProfile</i>

- 7 Standardisieren Sie den Host, sodass er beim nächsten Neustart den überarbeiteten Regelsatz verwendet.

```
Repair-DeployRuleSetCompliance $tr
```

Weiter

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 vSphere Auto Deploy anzuwenden und eine Übereinstimmung zwischen dem Regelsatz und dem Host zu erzielen.

Erfassen von Protokollen zur Fehlerbehebung bei ESXi -Hosts

5

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.