VMware ESXi-Upgrade

Update 3
VMware vSphere 8.0
VMware ESXi 8.0

vmware
by Broadcom

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

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

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

Inhalt

Grundlegende Informationen zum VMware ESXi-Upgrade

1

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

Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Zur Förderung dieses Grundsatzes bei unseren Kunden, Partnern und der internen Community haben wir diesen Leitfaden aktualisiert, indem wir Vorkommen nicht neutraler Sprache entfernt haben.

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.

Upgrade-Optionen in vCenter Server

2

vCenter Server 8.0 bietet zahlreiche Möglichkeiten zum Aktualisieren der vCenter Server-Bereitstellung. Für ein erfolgreiches vCenter Server-Upgrade 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 Sie virtuelle Maschinen und virtuelle Appliances erstellen und ausführen. vCenter Server ist ein Dienst, der als zentraler Administrator für ESXi-Hosts fungiert, die in einem Netzwerk verbunden sind. Das vCenter Server-System ermöglicht Ihnen den Zusammenschluss und die Verwaltung der Ressourcen von mehreren Hosts. Bei der vCenter Server Appliance handelt es sich um eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist.

Sie können vorhandene vCenter Server-Bereitstellungen, die einen eingebetteten oder einen externen Platform Services Controller enthalten, auf eine Bereitstellung aktualisieren, die aus einer vCenter Server Appliance besteht.

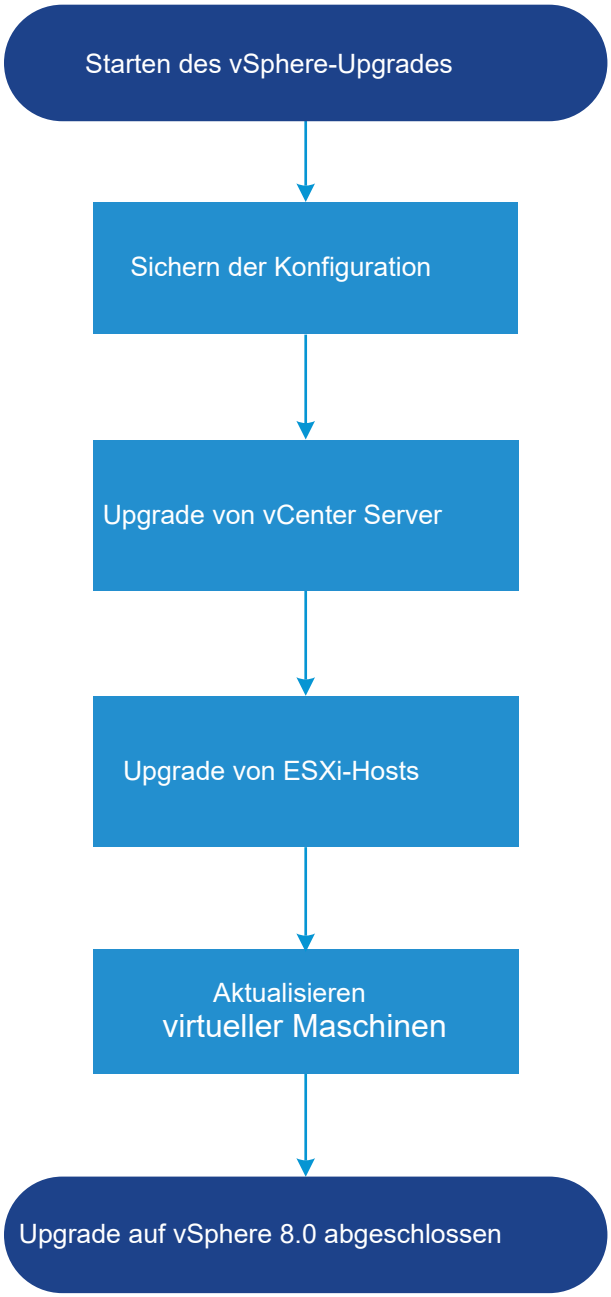
Lesen Sie als Nächstes die folgenden Themen:

- Übersicht über den vSphere-Upgrade-Vorgang

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 vSphere-Upgrade-Aufgaben



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 mit der Version der vCenter Server Appliance kompatibel sind, auf die Sie ein Upgrade durchführen. 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.

   Detaillierte Anweisungen finden Sie unter vCenter Server-Upgrade.

5 Führen Sie das Upgrade der ESXi-Hosts durch. Siehe Übersicht über den ESXiHost-Upgrade-Vorgang.

6 Um ausreichend Datenspeicher für Protokolldateien sicherzustellen, sollten Sie einen Syslog-Server für die Remote-Protokollierung einrichten. Die Einrichtung von Protokollierung auf einem Remotehost ist besonders wichtig für Hosts, die über begrenzten lokalen Speicher verfügen.

   Weitere Informationen hierzu finden Sie unter Erforderlicher freier Speicherplatz für die Systemprotokollierung und Konfiguration von Syslog auf ESXi-Hosts.

7 Aktualisieren Sie Ihre virtuellen Maschinen manuell oder unter Verwendung von vSphere Lifecycle Manager, um ein koordiniertes Upgrade durchzuführen.

   Siehe Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools.

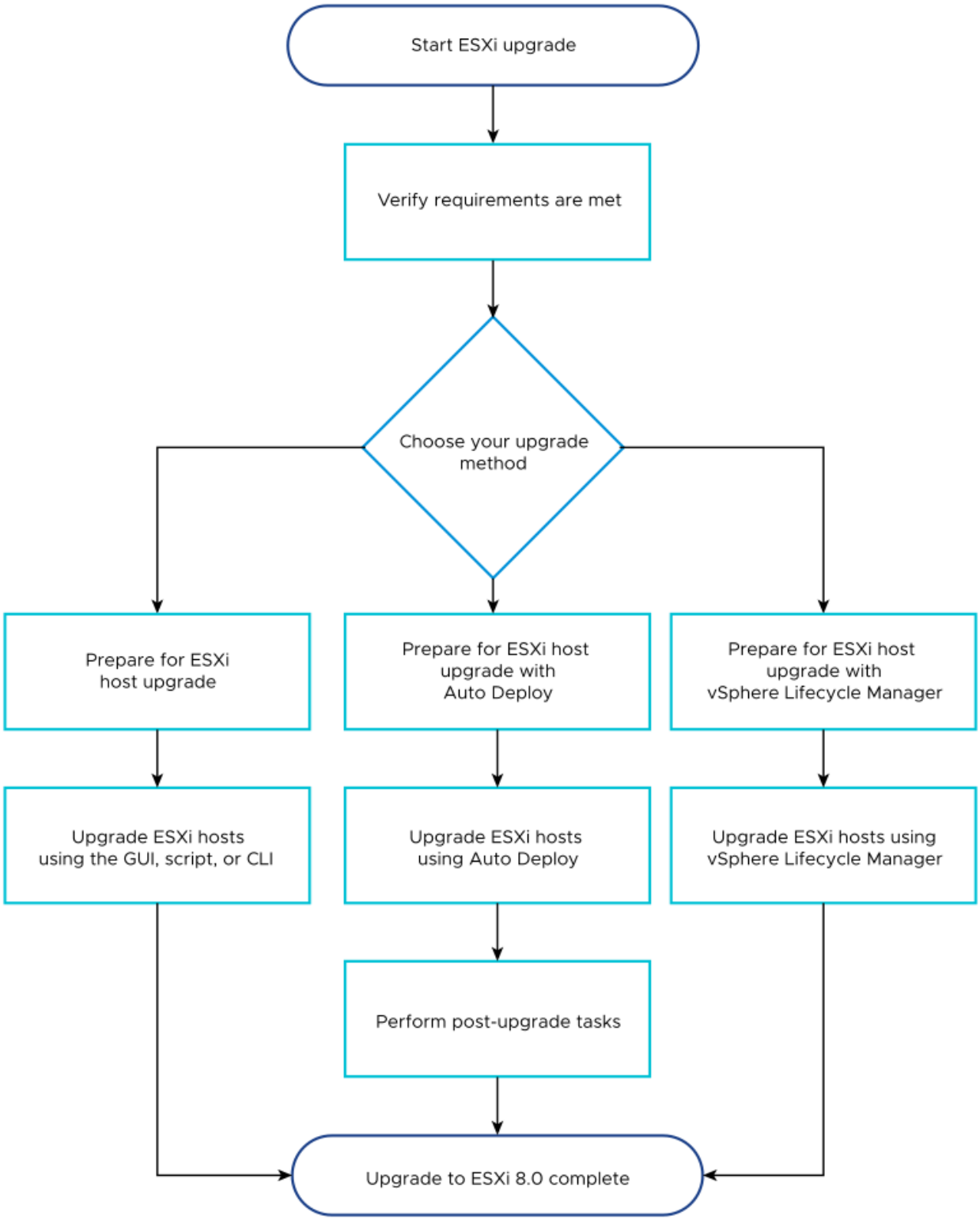
Übersicht über den ESXiHost-Upgrade-Vorgang

VMware bietet mehrere Möglichkeiten für das Upgrade von ESXi-Hosts früherer Versionen auf ESXi-Version 8.0.

Die Details und die Ebene der Unterstützung für ein Upgrade auf ESXi 8.0 hängen vom zu aktualisierenden Host und von der verwendeten Upgrade-Methode ab. Stellen Sie sicher, dass der Upgrade-Pfad von Ihrer aktuellen Version von ESXi auf die Version, auf die Sie ein Upgrade durchführen möchten, unterstützt wird. Weitere Informationen finden Sie in den VMware-Produktinteroperabilitätstabellen unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Sie können ein Upgrade eines ESXi-Hosts auf Version 8.0 durchführen, indem Sie ein interaktives Upgrade von einer CD, einer DVD oder einem USB, ein skriptbasiertes Upgrade, ESXCLI oder vSphere Lifecycle Manager verwenden. Wenn Sie ein Upgrade eines ESXi-Hosts, der benutzerdefinierte VIBs aufweist, auf Version 8.0 durchführen, werden alle unterstützten benutzerdefinierten VIBs migriert. Weitere Informationen finden Sie unter Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern.

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



Die folgenden allgemeinen Schritte gelten 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 das Netzwerk starten, überprüfen Sie, ob Ihre Netzwerkstartinfrastruktur ordnungsgemäß eingerichtet ist. Weitere Informationen hierzu finden Sie unter Netzwerk zum Starten des ESXi-Installationsprogramms.

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.

Die folgenden Methoden werden für ein direktes Upgrade auf ESXi8.0 unterstützt.

- Verwenden Sie das interaktive Installationsprogramm der grafischen Benutzeroberfläche von einer CD/DVD oder von einem USB-Laufwerk aus.
- Führen Sie ein skriptbasiertes Upgrade durch.
- Verwenden Sie ESXCLI.
- Verwenden Sie vSphere Auto Deploy. Wenn der ESXi-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host mit einem 8.0-Image erneut bereitzustellen.
- Verwenden Sie den vSphere Lifecycle Manager.

Installationsprogramm für grafische Benutzeroberfläche (GUI)

Sie können ein interaktives Upgrade durchführen, indem Sie ein ISO-Image des ESXi-Installationsprogramms auf einer CD/DVD oder einem USB-Flash-Laufwerk verwenden oder das Installationsprogramm über das Netzwerk starten. Diese Methode eignet sich für Bereitstellungen mit wenigen Hosts. Wenn Sie während des Installationsvorgangs eine Zielfestplatte auswählen, die eine ESXi-Installation enthält, aktualisiert das Installationsprogramm den Host auf ESXi Version 8.0. 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

Zum Durchführen eines Skript-Upgrades können Sie das ESXi 8.0-Installationsprogramm auf einer CD/DVD oder einem USB-Flash-Laufwerk verwenden oder das Installationsprogramm über das Netzwerk starten. Diese Methode bietet eine effiziente Möglichkeit zum Bereitstellen mehrerer Hosts. Weitere Informationen finden Sie unter Installieren oder Upgraden von Hosts mithilfe eines Skripts.

ESXCLI

Sie können ESXCLI für das Upgrade von ESXi 6.7-Hosts oder ESXi 7.0-Hosts auf ESXi 8.0-Hosts verwenden.

Mit vSphere 8.0 werden Konfigurationsdateien, Komponenten, Basisimages und Add-Ons als neue Softwarelieferungen eingeführt, die Sie zum Aktualisieren oder Patchen von ESXi 8.0-Hosts verwenden können. Informationen zum Verwalten von Komponenten, Basis-Images und Add-Ons auf ESXi finden Sie unter *ESXCLI – Konzepte und Beispiele*.

Zur Verwendung von ESXCLI-Befehlen müssen Sie die eigenständige ESXCLI installieren. Weitere Informationen zur Installation und Verwendung der ESXCLI finden Sie in den folgenden Dokumenten.

- *Erste Schritte mit ESXCLI*
- *ESXCLI – Referenz*

Weitere Informationen hierzu finden Sie unter Aktualisieren von Hosts mithilfe von ESXCLI-Befehlen .

vSphere Auto Deploy

Wenn ein ESXi-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host erneut bereitzustellen und ihn mit einem neuen Image-Profil oder einer auf Clusterebene verwalteten Konfiguration neu zu starten. Ein solches Image-Profil enthält ein ESXi-Upgrade oder einen Patch, ein Hostkonfigurationsprofil und optional Drittanbietertreiber oder Management Agents von VMware-Partnern. Um ESXi-Hosts zu einem Cluster hinzuzufügen, der ESXi-Konfiguration auf Clusterebene verwaltet, erstellen Sie in Auto Deploy eine Regel, die einen solchen Cluster als Hostspeicherort für neu hinzugefügte Hosts zuweist, die dieselben Einstellungen erben und keine manuelle Konfiguration erfordern. Benutzerdefinierte Images können Sie mithilfe von vSphere ESXi Image Builder CLI erstellen. Weitere Informationen finden Sie unter Kapitel 4 Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts .

vSphere Lifecycle Manager

vSphere Lifecycle Manager ist ein vCenter Server-Dienst für die Installation, das Upgrade und das Aktualisieren von ESXi-Hosts. Mithilfe von Images und Baselines ermöglicht vSphere Lifecycle Manager ein zentrales und vereinfachtes Lebenszyklusmanagement für mehrere ESXi-Hosts auf Clusterebene. Weitere Informationen zum Durchführen koordinierter Installationen und Upgrades und Aktualisierungen finden Sie in der *Verwalten des Lebenszyklus von Host und Cluster*-Dokumentation.

Durchführen eines Upgrades für virtuelle Maschinen und VMware Tools

Nachdem Sie ein Upgrade eines ESXi-Hosts durchgeführt haben, können Sie ein Upgrade der virtuellen Maschinen auf dem Host durchführen, damit Sie die neuen Funktionen nutzen können.

Die folgenden Tools sind für das Durchführen eines Upgrades von virtuelle Maschinen verfügbar.

vSphere Client

Sie können den vSphere Client verwenden, um schrittweise ein Upgrade einer virtuellen Maschine durchzuführen. Weitere Informationen zum Upgrade der virtuellen Maschinen finden Sie in der *vSphere-Administratorhandbuch für virtuelle Maschinen*-Dokumentation.

vSphere Lifecycle Manager

Sie können den vSphere Lifecycle Manager verwenden, um die Hardware der virtuellen Maschine und VMware Tools-Versionen der virtuellen Maschinen in Ihrer Umgebung zu aktualisieren. Der vSphere Lifecycle Manager automatisiert den Upgrade-Vorgang und überprüft, ob die Schritte in der richtigen Reihenfolge ausgeführt werden. Weitere Informationen finden Sie in der Dokumentation *Verwalten des Lebenszyklus von Host und Cluster*.

Upgrade der ESXi-Hosts

3

Nachdem Sie vCenter Server aktualisiert haben, führen Sie ein Upgrade Ihrer ESXi-Hosts durch. Sie können ESXi 6.7- und 7.0-Hosts direkt auf ESXi 8.0 aktualisieren.

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 zuerst ein Upgrade von vCenter Server und dann ein Upgrade der ESXi-Hosts durchführen. Wenn Sie Ihre Umgebung nicht in der richtigen Reihenfolge upgraden, kommt es möglicherweise zu Datenverlust und einer Unterbrechung des Serverzugriffs.

Lesen Sie als Nächstes die folgenden Themen:

- Anforderungen für ESXi
- Vor dem Upgrade der ESXi-Hosts
- Aktualisieren von Hosts mit benutzerdefinierten VIBs von Drittanbietern
- Upgrade von ESXi-Hosts in einer Umgebung mit VMware NSX
- Medienoptionen für das Starten des ESXi-Installationsprogramms
- Herunterladen des ESXi-Installationsprogramms
- Name und Bezeichner von ESXi-Speichergerät
- Interaktives Upgrade von Hosts
- Installieren oder Upgraden von Hosts mithilfe eines Skripts
- Starten eines ESXi-Hosts über ein Netzwerkgerät
- Vorgehensweise für das Upgrade 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.

Übersicht über ESXi-Systemspeicher

ESXi 8.0 verfügt über ein Systemspeicherlayout, das eine flexible Verwaltung von Partitionen und Drittanbieterkomponenten ermöglicht und gleichzeitig das Debugging erleichtert.

ESXi-Systemspeicher

Das Layout des ESXi 8.0-Systemspeichers besteht aus vier Partitionen:

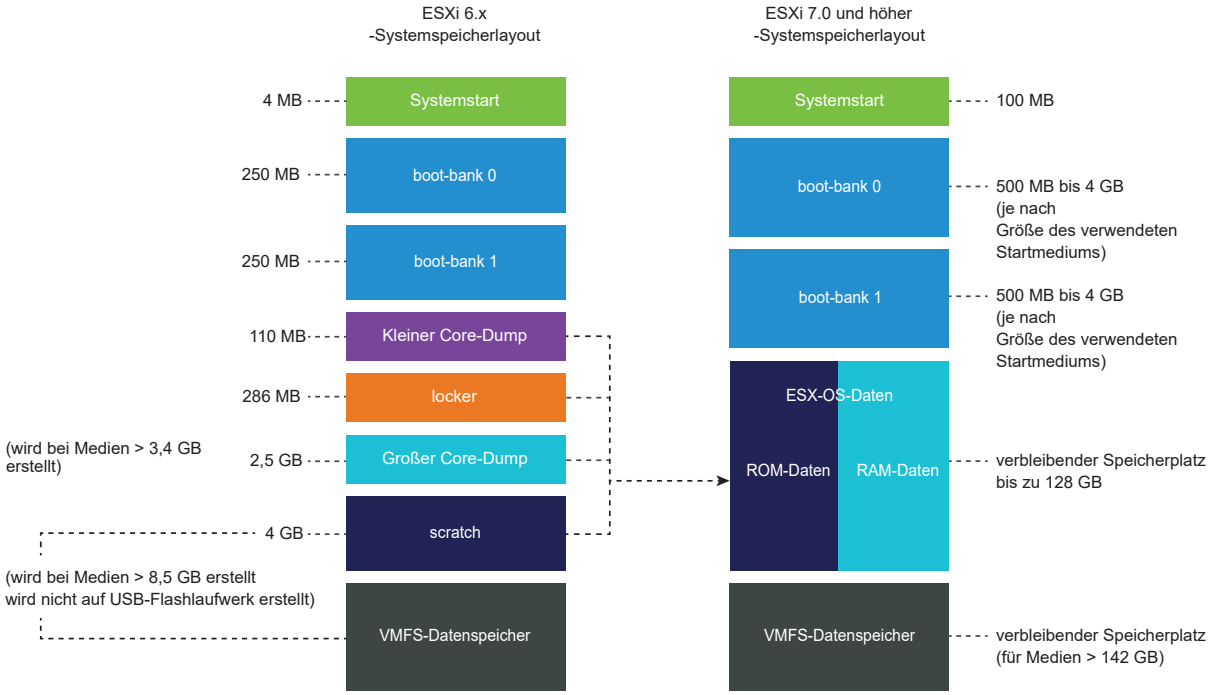
Tabelle 3-1. ESXi-Systemspeicherpartitionen:

Partition	Verwenden	Typ
Systemstart	Speichert Bootloader und EFI-Module.	FAT16
Boot-bank 0	Systemspeicher zum Speichern von ESXi-Startmodulen.	FAT16
Boot-bank 1	Systemspeicher zum Speichern von ESXi-Startmodulen.	FAT16
ESX-OSData	Fungiert als einheitlicher Speicherort zum Speichern zusätzlicher Module. Wird weder für Startvorgänge noch für virtuelle Maschinen verwendet. Fasst die `/scratch`-Legacy-Partition, Locker-Partition für VMware Tools und Core-Dump-Ziele zusammen. **Vorsicht** Falls es sich bei dem Installationsmedium um ein USB- oder SD-Kartengerät handelt, sollten Sie ESX-OSData-Partitionen auf einem persistenten Speichergerät erstellen, das nicht von ESXi-Hosts gemeinsam genutzt wird.	VMFS-L

Das ESX-OSData-Volume ist in zwei allgemeine Datenkategorien – persistente und nicht persistente Daten – unterteilt. Persistente Daten bestehen aus selten geschriebenen Daten, wie z. B. VMware Tools-ISOs, Konfigurationen und Core-Dumps.

Nicht persistente Daten bestehen aus häufig geschriebenen Daten, wie z. B. Protokolle, globale VMFS-Traces, vSAN EPD-Daten (Entry Persistence Daemon), vSAN-Traces und Echtzeitdatenbanken.

Abbildung 3-1. Konsolidierter Systemspeicher in ESXi 8.0



Größen des ESXi-Systemspeichers

Partitionsgrößen (mit Ausnahme der Systemstartpartitionen) können je nach Größe des verwendeten Startmediums variieren. Wenn es sich um ein High Endurance-Startmedium mit einer Kapazität von mehr als 142 GB handelt, wird der VMFS-Datenspeicher automatisch zum Speichern von VM-Daten erstellt.

Sie können die Kapazität des Startmediums und die automatische Dimensionierung überprüfen, die mithilfe des ESXi-Installationsprogramms konfiguriert wurden, indem Sie den vSphere Client verwenden und zur Ansicht **Partitionsdetails** navigieren. Alternativ können Sie auch ESXCLI verwenden, wie z. B. den Befehl `esxcli storage filesystem list`.

Tabelle 3-2. Größen des ESXi-Systemspeichers je nach verwendetem Startmedium und dessen Kapazität.

Größe des Startmediums	8-10 GB	10-32 GB	32-128 GB	>128 GB
Systemstart	100 MB	100 MB	100 MB	100 MB
Boot-bank 0	500 MB	1 GB	4 GB	4 GB
Boot-bank 1	500 MB	1 GB	4 GB	4 GB

Tabelle 3-2. Größen des ESXi-Systemspeichers je nach verwendetem Startmedium und dessen Kapazität. (Fortsetzung)

Größe des Startmediums	8-10 GB	10-32 GB	32-128 GB	>128 GB
ESX-OSData	Verbleibender Speicherplatz	Verbleibender Speicherplatz	Verbleibender Speicherplatz	Maximal 128 GB
VMFS-Datenspeicher				Verbleibende Speicherplatz für Mediengröße > 142 GB

Sie können die Startoption für das ESXi-Installationsprogramm `systemMediaSize` verwenden, um die Größe der Systemspeicherpartitionen auf den Startmedien zu begrenzen. Wenn Ihr System einen geringen Speicherplatzbedarf hat, der nicht die maximale Größe von 128 GB Systemspeicher benötigt, können Sie ihn auf mindestens 32 GB begrenzen. Der Parameter `systemMediaSize` akzeptiert die folgenden Werte:

- Minimum (32 GB, für einzelne Festplatte oder eingebettete Server)
- Klein (64 GB, für Server mit mindestens 512 GB RAM)
- Standardwert (128 GB)
- Maximum (verbrauchen Sie den gesamten verfügbaren Speicherplatz, für Multi-Terabyte-Server)

Der ausgewählte Wert muss dem Zweck Ihres Systems entsprechen. Beispielsweise muss ein System mit 1 TB Arbeitsspeicher das Minimum von 64 GB für die Systemspeicherung verwenden. Informationen zum Festlegen der Startoption zur Installationszeit, z. B. `systemMediaSize=small`, finden Sie unter Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts. Weitere Informationen finden Sie im Knowledgebase-Artikel 81166.

Links des ESXi-Systemspeichers

Die Subsysteme, die Zugriff auf die ESXi-Partitionen benötigen, können mithilfe der folgenden symbolischen Links auf diese Partitionen zugreifen:

Tabelle 3-3. Symbolische Links des ESXi-Systemspeichers.

Systemspeicher-Volume	Symbolischer Link
Boot-bank 0	`/bootbank`
Boot-bank 1	`/altbootbank`

Tabelle 3-3. Symbolische Links des ESXi-Systemspeichers. (Fortsetzung)

Systemspeicher-Volume	Symbolischer Link

Persistente Daten	`/productLocker`
	`/locker`
	`/var/core`
	`/usr/lib/vmware/isoimages`
	`/usr/lib/vmware/floppies`

Nicht persistente Daten	`/var/run`
	`/var/log`
	`/var/vmware`
	`/var/tmp`
	`/scratch`

Speicherverhalten

Wenn Sie ESXi einschalten, wird der Host in eine Autokonfigurationsphase versetzt, während der die Systemspeichergeräte mit Standardwerten konfiguriert werden.

Wenn Sie nach der Installation des ESXi-Images den ESXi-Host neu starten, konfiguriert der Host die Systemspeichergeräte mit Standardwerten. Ab ESXi 7.0 können Sie die Option `autoPartition` aktivieren, mit der automatisch alle verfügbaren leeren Geräte mit VMFS formatiert werden, mit Ausnahme von Legacy-SD- und USB-Geräten. Die Standardeinstellung ist `autoPartition=FALSE`. Dabei werden mit VMFS nur Startgeräte mit einer Größe von mehr als 128 GB formatiert. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 77009.

Vorsicht ESXi überschreibt alle Festplatten, die leer erscheinen. Festplatten werden als leer betrachtet, wenn sie über keine gültigen Partitionstabellen oder Partitionen verfügen. Wenn Sie Software verwenden, die solche Festplatten einsetzt - vor allem, wenn Sie einen logischen Volume-Manager (LVM) anstelle von (oder zusätzlich zu) herkömmlichen Partitionsschemata verwenden, kann dies dazu führen, dass ESXi den lokalen LVM neu formatiert. Erstellen Sie vor dem erstmaligen Starten von ESXi zunächst eine Sicherung Ihrer Systemdaten.

Die Formatierungssoftware sorgt dafür, dass auf der Festplatte oder dem USB-Gerät, von dem der ESXi-Host gestartet wird, vorhandene, vom Hardwareanbieter erstellte Diagnosepartitionen beibehalten werden. Im restlichen Speicher erstellt die Software die Partitionen wie unten beschrieben.

Von ESXi auf dem Hostlaufwerk erstellte Partitionen

Für Neuinstallationen werden mehrere neue Partitionen für den Systemstart, Startbanken und ESX-OSData erstellt. Neue ESXi Installationen verwenden GUID-Partitionstabellen (GPT) anstatt der MSDOS basierten Partitionierung. Das Installationsprogramm erstellt je nach Festplattengröße Startbanken unterschiedlicher Größe. Weitere Informationen zur Scratch-Partition finden Sie unter Grundlegendes zur Scratch-Partition.

Das Installationsprogramm hat nur Auswirkungen auf die Installationsfestplatte. Das Installationsprogramm wirkt sich nicht auf andere Festplatten des Servers aus. Wenn Sie auf einer Festplatte installieren, überschreibt das Installationsprogramm die gesamte Festplatte. Wenn das Installationsprogramm den Speicher automatisch konfiguriert, überschreibt es die Partitionen der Hardwareanbieter nicht.

Zum Erstellen des VMFS-Datenspeichers benötigt das ESXi-Installationsprogramm mindestens 128 GB freien Speicherplatz auf der Installationsfestplatte.

Sie können dieses Standardverhalten außer Kraft setzen, wenn Ihre Richtlinie beispielsweise vorsieht, dass gemeinsam genutzter anstatt lokaler Speicher verwendet werden soll. Um die automatische Festplattenformatierung zu verhindern, trennen Sie die lokalen Speichergeräte unter folgenden Bedingungen vom Host:

- Bevor Sie den Host erstmalig starten.
- Bevor Sie den Host nach dem Zurücksetzen des Hosts auf die Standardwerte für die Konfiguration starten.

Zum Überschreiben der VMFS-Formatierung (wenn die automatische Festplattenformatierung bereits gestartet ist) können Sie den Datenspeicher entfernen. Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Grundlegendes zur Scratch-Partition

Bei Neuinstallationen von ESXi wird während der automatischen Konfigurationsphase eine Scratch-Partition als Teil der ESX-OSDATA-Partition erstellt.

Hinweis Die Partitionierung für Hosts, die von früheren Versionen auf ESXi 7.0 und höher aktualisiert werden, unterscheidet sich deutlich von der Partitionierung für neue Installationen von ESXi. Der Upgrade-Prozess auf ESXi 7.0 und höher partitioniert das Startgerät neu und konsolidiert die ursprünglichen Core-Dump-, Locker- und Scratch-Partitionen auf dem ESX-OSData-Volume.

Die Scratch-Partition wird zum Speichern von Systemprotokollen verwendet, die beim Erstellen eines Support-Pakets benötigt werden. Wenn die Scratch-Partition nicht vorhanden ist, werden Systemprotokolle auf einer Ramdisk gespeichert. Wenn keine Scratch-Partition erstellt wurde, können Sie eine konfigurieren. Sie können die Standardkonfiguration zudem außer Kraft setzen.

Sie können die Scratch-Partition in einem SAN- oder NFS-gemounteten Remoteverzeichnis erstellen.

Festlegen der Scratch-Partition vom vSphere Client aus

Wenn keine Scratch-Partition eingerichtet wurde, sollten Sie insbesondere dann eine solche Partition konfigurieren, wenn auf dem Host nicht genügend Arbeitsspeicher vorhanden ist. Wenn keine Scratch-Partition vorhanden ist, werden Systemprotokolle auf einer Ramdisk gespeichert.

Voraussetzungen

Das für die Scratch-Partition zu verwendende Verzeichnis muss auf dem Host vorhanden sein.

Verfahren

1 Stellen Sie vom vSphere Client aus eine Verbindung zu vCenter Server her.

2 Wählen Sie den Host in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Konfigurieren**.

4 Wählen Sie **System**.

5 Wählen Sie **Erweiterte Systemeinstellungen**.

   Mit der Einstellung **ScratchConfig.CurrentScratchLocation** wird der aktuelle Speicherort der Scratch-Partition angegeben.

6 Geben Sie im Textfeld **ScratchConfig.ConfiguredScratchLocation** einen Verzeichnispfad ein, der für diesen Host eindeutig ist.

   Beispiel: **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.

7 Starten Sie den Host neu, damit die Änderungen wirksam werden.

Hardwareanforderungen für ESXi

Stellen Sie sicher, dass der Host die Mindestanforderungen an die Hardwarekonfiguration erfüllt, die von ESXi 8.0 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 8.0 ist ein Host mit mindestens zwei CPU-Kernen erforderlich.
- ESXi 8.0 unterstützt eine breite Palette von x86-Prozessoren mit 64 Bit und mehreren Kernen. Eine vollständige Liste der unterstützten Prozessoren finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility.
- Für ESXi 8.0 muss das NX/XD-Bit für die CPU im BIOS aktiviert sein.
- ESXi 8.0 benötigt mindestens 8 GB an physischem Arbeitsspeicher. Stellen Sie mindestens 12 GB RAM zum Ausführen virtueller Maschinen in typischen Produktionsumgebungen bereit.
- Um virtuelle 64-Bit-Maschinen zu unterstützen, muss auf x64-CPUs die Unterstützung für die Hardwarevirtualisierung (Intel VT-x oder AMD RVI) aktiviert sein.
- Ein oder mehr Gigabit oder schnellere Ethernet-Controller. Eine Liste mit unterstützten Netzwerkadaptermodellen finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.
- ESXi 8.0 erfordert eine Startfestplatte mit mindestens 32 GB dauerhaftem Speicher wie HDD, SSD oder NVMe. Ein Startgerät darf von ESXi-Hosts nicht gemeinsam genutzt werden.

- 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 kein SATA-CD-ROM-Gerät mit einer virtuellen Maschine auf einem ESXi-Host 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. Ab ESXi 8.0 können Sie keine Softwareadapter für Fibre Channel over Ethernet (FCoE) verwenden, sondern nur Hardware-FCoE-Adapter.

Startanforderungen für ESXi

In vSphere 8.0 ist die Unterstützung für Legacy-BIOS begrenzt und das Starten von ESXi-Hosts über die Unified Extensible Firmware Interface (UEFI) wird empfohlen. Mithilfe von UEFI können Sie Systeme von Festplatten, CD-ROM-Laufwerken oder USB-Medien aus starten. vSphere Auto Deploy unterstützt den Netzwerkstart und die Bereitstellung von ESXi-Hosts mit UEFI. Wenn Ihr System über unterstütze Datenverarbeitungseinheiten (DPU) verfügt, können Sie UEFI nur verwenden, um ESXi auf den DPUs zu installieren und zu starten. Weitere Informationen zu den Plänen von VMware, die Unterstützung für Legacy-BIOS in Serverplattformen einzustellen, finden Sie im Knowledgebase-Artikel https://kb.vmware.com/s/article/84233.

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.

Speicheranforderungen für die Installation von bzw. das Upgrade auf ESXi 8.0

Verwenden Sie für eine optimale Leistung der ESXi 8.0-Installation ein persistentes Speichergerät mit mindestens 32 GB für Startgeräte. Für ein Upgrade auf ESXi 8.0 ist ein Startgerät mit mindestens 8 GB erforderlich. Beim Starten über eine lokale Festplatte (SAN oder iSCSI LUN) wird eine Festplatte mit mindestens 32 GB benötigt, damit Systemspeichervolumes erstellt werden können, die eine Startpartition, Startoptionen und ein VMFS-L-basiertes ESX-OSData-Volume enthalten. Das ESX-OSData-Volume übernimmt die Rolle der `/scratch`-Legacy-Partition, der Locker-Partition für VMware Tools und des Core-Dump-Ziels.

Hinweis In ESXi 8.0 wird das ESX-OSData-Volume als einheitliche Partition betrachtet, und die separaten Komponenten, wie z. B. `/scratch` und VMware Tools, werden in einer einzelnen persistenten OSDATA-Partition konsolidiert.

Zu den weiteren Optionen für eine optimale Leistung der ESXi 8.0-Installation gehören:

- Eine lokale Festplatte mit mindestens 128 GB für eine optimale Unterstützung von ESX-OSData. Die Festplatte enthält die Startpartition, ESX-OSData-Volume und einen VMFS-Datenspeicher.
- Ein Gerät, das mindestens 128 TBW (Terabytes Written) unterstützt.
- Ein Gerät, das mindestens 100 MB/s sequenzielle Schreibgeschwindigkeit liefert.
- Um Ausfallsicherheit im Falle eines Geräteausfalls zu bieten, wird ein gespiegeltes RAID 1-Gerät empfohlen.

Legacy-SD- und USB-Geräte werden mit den folgenden Einschränkungen unterstützt:

- SD- und USB-Geräte werden für Startbankpartitionen unterstützt. Die Verwendung von SD- und USB-Geräten zum Speichern von ESX-OSData-Partitionen ist veraltet, und es wird empfohlen, ein separates persistentes lokales Gerät mit mindestens 32 GB zum Speichern des ESX-OSData-Volumes bereitzustellen. Das persistente lokale Boot-Gerät kann ein branchenüblicher M.2-Flash (SLC und MLC), SAS, SATA, HDD, SSD oder ein NVMe-Gerät sein. Die optimale Kapazität für persistente lokale Geräte beträgt 128 GB.
- Wenn Sie keinen persistenten Speicher bereitstellen, wird ein Alarm angezeigt, wie z. B. `Sekundäres persistentes Gerät nicht gefunden. Verschieben Sie die Installation in den persistenten Speicher, da die Unterstützung der Konfiguration nur für SD-Karte/USB eingestellt wird.`
- Sie müssen ein SD-Flash-Gerät verwenden, das vom Serveranbieter für das jeweilige Servermodell genehmigt wurde, auf dem Sie ESXi auf einem SD-Flash-Speichergerät installieren möchten. Sie finden eine Liste validierter Geräte auf partnerweb.vmware.com.
- Im Knowledgebase-Artikel 85685 finden Sie aktualisierte Anweisungen für Umgebungen auf Basis von SD-Karten oder USB.
- Informationen zur Auswahl eines geeigneten SD- oder USB-Startgeräts finden Sie im Knowledgebase-Artikel 82515.

Beim Upgrade auf ESXi 8.0 von Versionen vor 7.x wird das Startgerät neu partitioniert. Die ursprünglichen Core-Dump-, Locker- und Scratch-Partitionen werden im ESX-OSData-Volume konsolidiert.

Die folgenden Ereignisse treten während der Neupartitionierung auf:

- Wenn kein benutzerdefiniertes Core-Dump-Ziel konfiguriert ist, stellt der standardmäßige Core-Dump-Speicherort eine Datei im ESX-OSData-Volume dar.
- Wenn der Syslog-Dienst zum Speichern von Protokollen auf der 4 GB VFAT-Scratch-Partition konfiguriert ist, werden die Protokolldateien in `var/run/log` auf das ESX-OSData-Volume migriert.
- VMware Tools wird aus der Locker-Partition migriert, und die Partition wird gelöscht.

- Die Core-Dump-Partition wird gelöscht. Die auf der Scratch-Partition gespeicherten Core-Dump-Dateien der Anwendung werden gelöscht.

Hinweis Ein Rollback von ESXi 8.x auf eine Version von ESXi vor 7.x ist aufgrund des Neupartitionierungsvorgangs des Startgeräts nicht möglich. Um nach dem Upgrade auf Version 8.0 eine frühere Version als 7.x von ESXi verwenden zu können, müssen Sie vor dem Upgrade eine Sicherung des Startgeräts erstellen und das ESXi-Startgerät von der Sicherung wiederherstellen. Ein Rollback von ESXi 8.x auf 7.x ist möglich, solange keine Änderungen an den Bootbank-Partitionen vorgenommen wurden und keine beschädigte Partition erkannt wird.

Wenn Sie USB- oder SD-Geräte verwenden, um ein Upgrade durchzuführen, sollten Sie am besten eine ESX-OSData-Region auf einer verfügbaren persistenten Festplatte oder einer SAN-LUN zuteilen. Wenn persistenter Speicher oder eine SAN-LUN nicht verfügbar sind, wird ESX-OSData automatisch auf einer RAM-Festplatte erstellt. VMFS kann auch für ESX-OSData-Partition verwendet werden.

Wenn sich ESX-OSData nach dem Upgrade auf einer RAM-Festplatte befindet und bei nachfolgenden Startvorgängen ein neues persistentes Gerät gefunden wird und dieses Gerät die Einstellung `autoPartition=True` aufweist, wird ESX-OSData automatisch auf dem neuen persistenten Gerät erstellt. ESX-OSData wird nicht automatisch zwischen persistentem Speicher verschoben. Sie können den ESX-OSData-Standort in einem unterstützten Speicher manuell ändern.

Weitere Informationen zum Neukonfigurieren der `/scratch`-Partition finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

Sie können die Option `systemMediaSize` verwenden, um die Größe von ESXi-Systempartitionen zu konfigurieren. Weitere Informationen finden Sie im Knowledgebase-Artikel https://kb.vmware.com/s/article/81166.

Bei Auto Deploy-Installationen versucht das Installationsprogramm, einen Scratch-Bereich auf einer verfügbaren lokalen Festplatte oder einem lokalen Datenspeicher zuzuteilen. Wenn keine lokale Festplatte oder kein lokaler Datenspeicher gefunden wird, schlägt die Installation fehl.

Für Umgebungen, die über ein SAN-Gerät starten oder Auto Deploy verwenden, muss das ESX-OSData-Volume für jeden ESXi-Host auf einer separaten SAN-LUN eingerichtet werden.

Verwenden von Anwendungen für die Remoteverwaltung

Mit Remoteverwaltungsanwendungen können Sie ESXi auf Servern an Remotestandorten installieren.

Zu den für die Installation unterstützten Remoteverwaltungsanwendungen gehören HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM Management Module (MM) und Remote Supervisor Adapter II (RSA II). Support zu Remoteverwaltungsanwendungen erhalten Sie beim jeweiligen Anbieter.

Sie können Remoteverwaltungsanwendungen sowohl für interaktive Installationen als auch für Skriptinstallationen von ESXi im Remotemodus verwenden.

Wenn Sie Remoteverwaltungsanwendungen für die Installation von ESXi nutzen, treten auf der virtuellen CD bei Systemen oder Netzwerken, die mit maximaler Kapazität betrieben werden, unter Umständen Beschädigungsprobleme auf. Sollte die Remoteinstallation ausgehend von einem ISO-Image nicht funktionieren, schließen Sie die Installation über die physische CD ab.

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 3-4. Unterstützte Remotemanagement-Servermodelle und Mindest-Firmware-Versionen

Remotemanagement-Servermodell	Firmware-Version	Java
Dell DRAC 9	6.0.30.00	Nicht verfügbar
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
HP ILO 5	2.72	Nicht verfügbar
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 3-5. Empfehlungen zur Leistungssteigerung

Systemelement	Empfehlung
RAM	ESXi-Hosts benötigen mehr RAM-Speicher als übliche Server. ESXi 8.0 benötigt mindestens 8 GB an physischem RAM. Stellen Sie mindestens 12 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. Der Betrieb von vier virtuellen Maschinen mit Red Hat Enterprise Linux oder Windows XP erfordert mindestens 3 GB RAM für die Baseline-Leistung. Diese Abbildung enthält 1024 MB für die virtuellen Maschinen, mindestens 256 MB für jedes Betriebssystem, wie von den Anbietern empfohlen. Die Ausführung dieser vier virtuellen Maschinen mit jeweils 512 MB RAM erfordert, dass der ESXi-Host 4 GB RAM aufweist, wobei 2048 MB für die virtuellen Maschinen reserviert sind. Bei diesen Berechnungen wurde keine mögliche Einsparung von Arbeitsspeicher durch variable Overhead-Speicherkapazität für die einzelnen virtuellen Maschinen berücksichtigt. Siehe *vSphere-Ressourcenverwaltung*.
Dedizierte schnelle Ethernet-Adapter für virtuelle Maschinen	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.
Festplattenspeicherort	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.

Tabelle 3-5. Empfehlungen zur Leistungssteigerung (Fortsetzung)

Systemelement	Empfehlung
VMFS6-Partitionierung	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 Client. Dadurch wird gewährleistet, dass die Startsektoren der Partitionen für 64 KB ausgerichtet sind, wodurch eine Verbesserung der Speicherleistung erzielt werden kann. **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 Client zum Einrichten von VMFS verwenden.
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-Treibern unterstützt werden. Weitere Informationen finden Sie im *Hardware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Öffnen und schließen Sie die Firewall-Ports für jeden Dienst, indem Sie entweder den vSphere Client oder den VMware Host Client verwenden.

ESXi enthält eine Firewall, die standardmäßig aktiviert ist. Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme des Datenverkehrs für Dienste, die im Sicherheitsprofil des Hosts aktiviert sind, der ein- und ausgehende Datenverkehr blockiert wird. Eine Liste der unterstützten Ports und Protokolle in der ESXi-Firewall finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/.

Im Tool VMware Ports and Protocols werden Portinformationen für Dienste aufgelistet, die standardmäßig installiert sind. 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 Client angezeigt werden. Das Tool VMware Ports and Protocols enthält jedoch auch einige andere Ports.

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Informieren Sie sich zur empfohlenen Mindestgröße und zur Rotationskonfiguration für hostd-, vpxa- und fdm-Protokolle.

Wenn Sie Auto Deploy für die Installation Ihres ESXi 8.0-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volume eingerichtet haben, müssen Sie möglicherweise die aktuellen Einstellungen für die Protokollgröße und die Rotation ändern, um sicherzustellen, dass ausreichend Speicherplatz für die Systemprotokollierung verfügbar ist. Alle vSphere-Komponenten verwenden diese Infrastruktur. Die Standardwerte für die Protokollkapazität in dieser Infrastruktur variieren je nach verfügbarem Speicherplatz und je nach Konfiguration der Systemprotokollierung. Hosts, die mit Auto Deploy bereitgestellt werden, speichern Protokolle auf einer RAM-Festplatte. Der verfügbare Speicherplatz für Protokolle ist daher gering.

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

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

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

Sie müssen den Protokollspeicher für ESXi-Hosts nicht neu konfigurieren, die die Standardkonfiguration verwenden, bei der Protokolle in einem Scratch-Verzeichnis auf dem VMFS-Volume gespeichert werden. Für diese Hosts konfiguriert ESXi 8.0 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 Protokolldateigröße	Anzahl der aufzubewahrenden Protokolldateien	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

Sie können optional VMware vCenter Log Insight installieren, das Protokollaggregation und -analysen bereitstellt.

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 32-Bit und 64-Bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	Nicht verfügbar
Safari	9.0+	Nicht verfügbar	Nicht verfügbar

Kennwörter und Kontosperrung für ESXi

Für ESXi-Hosts müssen Sie ein Kennwort mit vordefinierten Anforderungen verwenden. Mithilfe der erweiterten Systemeinstellung `Security.PasswordQualityControl` können Sie die erforderliche Länge und die erforderliche Zeichenklasse ändern sowie Kennwortsätze erlauben. Sie können auch die Anzahl der Kennwörter festlegen, die für jeden Benutzer gespeichert werden soll. Verwenden Sie dazu die erweiterte Systemeinstellung `Security.PasswordHistory`.

Hinweis Die Standardanforderungen für ESXi-Kennwörter können versionsabhängig variieren. Mit der erweiterten Systemeinstellung `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 darin standardmäßig Zeichen aus drei der vier folgenden Zeichenklassen enthalten sein: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen (z. B. Unter- oder Schrägstriche).
- Standardmäßig besteht ein Kennwort aus mindestens 7 und weniger als 40 Zeichen.
- Kennwörter dürfen kein Wort aus einem Wörterbuch und keinen Teil eines Worts aus einem Wörterbuch enthalten.
- Kennwörter dürfen den Benutzernamen oder Teile des Benutzernamens nicht 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. Ein Wort aus einem Wörterbuch, das in einem Kennwort verwendet wird, verringert die Sicherheit des Kennworts.

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 wird ein Benutzer bis zu drei Mal (retry=3) zur Eingabe eines neuen Kennworts aufgefordert, wenn ein Kennwort nicht ausreichend stark ist oder das Kennwort zweimal nicht korrekt eingegeben wurde. Kennwörter mit einer oder zwei Zeichenklassen und Kennwortsätzen sind nicht zulässig, da die ersten drei Elemente deaktiviert sind. Kennwörter mit drei oder vier Zeichenklassen erfordern sieben Zeichen. Weitere Informationen zu weiteren Optionen, wie z. B. `max`, `passphrase` und so weiter, finden Sie auf der `pam_passwdqc`-Manpage.

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. Die erweitere Einstellung oder sonstige Einstellungen können Sie mithilfe der erweiterten Standardeinstellung `Security.PasswordQualityControl` über den vSphere Client ändern.

Beispielsweise können Sie diese Option wie folgt ändern.

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

In diesem Beispiel sind Passphrasen mit mindestens 16 Zeichen und mindestens drei Wörtern zulässig.

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

Ändern der standardmäßigen Kennwortbeschränkungen

Die standardmäßige Beschränkung für Kennwörter oder Kennwortsätze können Sie mithilfe der erweiterten Systemeinstellung `Security.PasswordQualityControl` für Ihren ESXi-Host ändern. In der *vCenter Server und Hostverwaltung*-Dokumentation finden Sie Informationen zum Ändern der erweiterten Systemeinstellungen ESXi.

Sie können den Standardwert wie folgt ändern, damit beispielsweise mindestens 15 Zeichen und mindestens vier Wörter (`passphrase=4`) 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 von Kennwortoptionen wurden getestet. Führen Sie Tests durch, nachdem Sie Änderungen an den Einstellungen für das Standardkennwort vorgenommen haben.

In diesem Beispiel wird die Kennwortkomplexität auf acht Zeichen aus vier Zeichenklassen festgelegt, wobei ein erheblicher Unterschied zwischen den Kennwörtern, eine gespeicherter Verlauf von fünf Kennwörtern und eine 90-tägige Rotationsrichtlinie erzwungen wird:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

ESXi-Kontosperrverhalten

Das Sperren von Konten für den Zugriff über SSH und das vSphere Web Services SDK wird unterstützt. Die DCUI und die ESXi Shell unterstützen die Kontosperrung nicht. Standardmäßig wird das Konto nach maximal fünf fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach 15 Minuten entsperrt.

Konfigurieren des Anmeldeverhaltens

Das Anmeldeverhalten für Ihren ESXi-Host können Sie mit den folgenden erweiterten Systemeinstellungen 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.
- `Security.PasswordHistory`. Anzahl der für jeden Benutzer zu speichernden Kennwörter. Ab vSphere 8.0 Update 1 ist die Standardeinstellung fünf. Mit dem Wert „0“ wird der Kennwortverlauf deaktiviert.

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 6.7x- oder 7.0.x-Host mit vSphere Auto Deploy bereitgestellt wurde, können Sie vSphere Auto Deploy verwenden, um den Host mit einem 8.0-Image erneut bereitzustellen.
- Informationen zur `esxcli`-Befehlsmethode 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 Lizenzierung von ESXi-Hosts nach dem Upgrade.
   - 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. Sie können optional VMware vCenter Log Insight installieren, das Protokollaggregation und -analysen bereitstellt. Weitere Informationen hierzu finden Sie unter Erforderlicher freier Speicherplatz für die Systemprotokollierung.
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 Installation Bundles (VIBs) installiert sein, z. B. Drittanbietertreiber oder Management-Agents.

Beim Upgrade eines ESXi-Hosts auf 8.0 werden alle unterstützten benutzerdefinierten VIBs migriert. Dabei spielt es keine Rolle, ob die VIBs im ISO-Image des Installationsprogramms enthalten sind. Falls der Host oder das ISO-Image des Installationsprogramms ein VIB enthält, das einen Konflikt verursacht und das Upgrade verhindert, wird in einer Fehlermeldung das VIB angegeben, das den Konflikt verursacht hat. Führen Sie eine der folgenden Aktionen aus, um ein Upgrade für den Host durchzuführen:

- Entfernen Sie das VIB, das den Konflikt verursacht hat, vom ESXi-Host und führen Sie das Upgrade erneut durch. Sie können ein VIB aus dem Host mit `esxcli`-Befehlen 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 zu vSphere ESXi Image Builder CLI finden Sie in der *Installation und Einrichtung von vCenter Server*-Dokumentation.

Upgrade von ESXi-Hosts in einer Umgebung mit VMware NSX

Stellen Sie in einem VMware NSX-Setup vor einem Upgrade auf ESXi 8.0 und höher sicher, dass das NSX Kernelmodul Teil der Image- oder Upgrade-Baseline ist.

Wenn Ihr vSphere-System VMware NSX enthält, müssen Sie vor dem Start eines Upgrades Ihrer ESXi-Hosts sichergehen, dass das NSX-Kernelmodul Teil der gewünschten Softwarespezifikation oder Baseline ist, die Sie für das Upgrade verwenden. Beim Upgrade eines ESXi-Hosts auf 8.0 oder höher werden alle unterstützten benutzerdefinierten VIBs migriert. Dabei spielt es keine Rolle, ob die VIBs im ISO-Image des Installationsprogramms enthalten sind. Allerdings wird das NSX-Kernelmodul nicht automatisch auf das ISO-Image des Installationsprogramms migriert. Bevor Sie mit dem Upgrade-Vorgang fortfahren, müssen Sie eine der folgenden Aktionen durchführen:

- Erstellen Sie eine Erweiterungs-Baseline mit einem neu hochgeladenen NSX-Kernelmodul. Weitere Informationen finden Sie unter Verwaltung des Host- und Clusterlebenszyklus.
- Erstellen Sie ein benutzerdefiniertes Image-Profil mit dem NSX Kernelmodul. Weitere Informationen finden Sie unter Upgrade von ESXi durch ein benutzerdefiniertes Image-Profil in einem VMware NSX-Setup.
- Verwenden Sie PowerCLI, um ein neues ISO-Image zu erstellen. Weitere Informationen finden Sie unter Upgrade ESXi in einem VMware NSX-Setup mit einem neuen ISO-Image.
- Verwenden Sie ESXCLI. Weitere Informationen finden Sie unter Verwenden von ESXCLI für das Upgrade von ESXi-Hosts in einem VMware NSX-Setup.

Upgrade von ESXi durch ein benutzerdefiniertes Image-Profil in einem VMware NSX-Setup

Stellen Sie in einem VMware NSX-Setup vor dem Upgrade auf ESXi 8.0 und höher sicher, dass das NSX-Kernelmodul Teil der Upgrade-Baseline ist.

Voraussetzungen

Wenn Ihr vSphere-System VMware NSX enthält, müssen Sie vor dem Start eines Upgrades Ihrer ESXi-Hosts von einer früheren Version von ESXi auf 8.0 und höher sicherstellen, dass das NSX-Kernelmodul Teil der Baseline ist, die Sie für das Upgrade verwenden. Zu diesem

Zweck können Sie ein benutzerdefiniertes Image-Profil mit einem ESXi Basisimage und einem neu hochgeladenen NSX Kernelmodul erstellen.

- Laden Sie von VMware Customer Connect die ZIP-Datei `NSX Kernel Module for VMware ESXi 8.0` für die Version von VMware NSX herunter, die in Ihrer Umgebung bereitgestellt wird. Beispiel: `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` für VMware NSX 4.0.1.
- Stellen Sie sicher, dass Auto Deploy und Image Builder in Ihrem vCenter Server-System aktiviert sind.

Verfahren

1. Melden Sie sich bei einem vCenter Server 8.x-System an.
2. Navigieren Sie zu **Startseite > Auto Deploy > Software-Depots**, um ein ESXi 8.x-Basisimage, sofern es noch nicht verfügbar ist, und die ZIP-Datei für das NSX-Kernelmodul in die vSphere ESXi Image Builder-Bestandsliste zu importieren.
3. Erstellen Sie ein Image-Profil, das das VMware NSX-Kernelmodul und das Basisimage für ESX 8.x kombiniert. Detaillierte Schritte finden Sie unter Erstellen eines Image-Profils.
4. Exportieren Sie das benutzerdefinierte Image-Profil in ein ISO-Image.
5. Importieren Sie das ISO-Image in das vSphere Lifecycle Manager-Depot.

   Sie können jetzt mithilfe des vSphere Lifecycle Manager eine Upgrade-Baseline basierend auf dem importierten ISO-Image erstellen. Weitere Informationen zum vSphere Lifecycle Manager-Upgrade-Workflow mit Baselines finden Sie im Handbuch „Verwalten des Lebenszyklus von Host und Cluster“.

Upgrade ESXi in einem VMware NSX-Setup mit einem neuen ISO-Image

Stellen Sie in einem VMware NSX-Setup vor einem Upgrade auf ESXi 8.0 und höher sicher, dass das NSX Kernelmodul Teil der Image- oder Upgrade-Baseline ist.

Voraussetzungen

Wenn Ihr vSphere-System VMware NSX enthält, müssen Sie vor dem Start eines Upgrades Ihrer ESXi-Hosts von einer früheren Version von ESXi auf 8.0 und höher sicherstellen, dass das NSX-Kernelmodul Teil der Softwarespezifikation oder Baseline ist, die Sie für das Upgrade verwenden. Zu diesem Zweck können Sie das PowerCLI-Cmdlet `New-IsoImage` verwenden, um ein neues ISO-Image zu erstellen und das ESXi-Upgrade auf die von Ihnen bevorzugte Weise durchzuführen.

- Laden Sie von VMware Customer Connect die ZIP-Datei `NSX Kernel Module for VMware ESXi 8.0` für die Version von VMware NSX herunter, die in Ihrer Umgebung bereitgestellt wird. Beispiel: `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` für VMware NSX 4.0.1.
- Installieren Sie die PowerCLI und die gesamte erforderliche Software. Informationen finden Sie unter Installation und Verwendung von vSphere ESXi Image Builder.

- Stellen Sie sicher, dass Sie Zugriff auf das Software-Depot haben, das die Softwarespezifikation enthält, die Sie verwenden möchten.

Verfahren

- Führen Sie in einer PowerCLI-Sitzung das Cmdlet `New-IsoImage` aus, um ein ISO-Image zu generieren, indem Sie die Parameter `Depots`, `Destination` und `SoftwareSpec` übergeben. Beispielsweise `PS C:\Users\Administrator> New-IsoImage -Depots "C:\VMware-ESXi-8.x.x-xxx-depot.zip","C:\nsx-lcp-4.0.1.0.0.xxx-esx80.zip", -Destination C:\<your new ISO image name>.iso -SoftwareSpec C:\<your file name>.json`. Mit diesem Befehl wird ein neues ISO-Image erstellt, indem das ESXi-Basisimage und die NSX-Kernel-ZIP-Dateien sowie die Softwarespezifikation Ihres gewünschten Images in einer JSON-Datei verwendet werden. Sie können eine beliebige Anzahl und Kombination aus Software-Depots offline und online verwenden. Für Upgrades auf ESXi 8.0 behält das Cmdlet `New-IsoImage` zusätzliche Metadaten für ESXi 8.0 bei, die vom vSphere Lifecycle Manager benötigt werden.

Nächste Schritte

Verwenden Sie das neue ISO-Image, um das ESXi-Upgrade auf Ihre bevorzugte Weise abzuschließen. Weitere Informationen zu vSphere Lifecycle Manager-Upgrade-Workflow finden Sie im Handbuch „Verwalten des Lebenszyklus von Host und Cluster“.

Verwenden von ESXCLI für das Upgrade von ESXi-Hosts in einem VMware NSX-Setup

Stellen Sie in einem VMware NSX-Setup vor einem Upgrade auf ESXi 8.0 und höher sicher, dass das NSX Kernelmodul Teil der Image- oder Upgrade-Baseline ist.

Um ESXCLI für das Upgrade eines ESXi-Hosts in einem vSphere-System zu verwenden, das NSX-T Data Center enthält, müssen Sie die unter Aktualisieren von Hosts ESXCLI-Befehlen beschriebenen Verfahren befolgen:

Voraussetzungen

Wenn Ihr vSphere-System VMware NSX enthält, müssen Sie vor dem Start eines Upgrades Ihrer ESXi-Hosts von einer früheren Version von ESXi auf 8.0 und höher sicherstellen, dass das NSX-Kernelmodul Teil der Softwarespezifikation oder Baseline ist, die Sie für das Upgrade verwenden. Sie können ESXCLI-Befehle verwenden, um ein Upgrade Ihrer ESXi-Hosts durchzuführen und das NSX Kernelmodul erneut zu installieren.

- Laden Sie von VMware Customer Connect die ZIP-Datei `NSX Kernel Module for VMware ESXi 8.0` für die Version von VMware NSX herunter, die in Ihrer Umgebung bereitgestellt wird. Beispiel: `nsx-lcp-4.0.1.0.0.xxx-esx80.zip` für VMware NSX 4.0.1.

Verfahren

1. Versetzen Sie Ihren ESXi-Host in den Wartungsmodus. Weitere Informationen finden Sie unter Versetzen eines Hosts in den Wartungsmodus.

2 Laden Sie ein ESXi 8.x-Image-Profil in einem Software-Depot herunter, auf das über eine URL zugegriffen werden kann oder das in einem Offline-ZIP-Depot gespeichert ist.

3 Führen Sie den ESXCLI-Befehl `esxcli software profile update --depot <path-to-depot-file> -p ESXi-X.X.X-XXXXXX-standard --allow-downgrades --no-sig-check` aus. Beispiel: `esxcli software profile update --depot /vmfs/volumes/5e8fd197-68bce4dc-f8f1-005056af93cf/VMware-ESXi-8.0.0-xxx-depot.zip -p ESXi-8.0.0-xxx-standard --allow-downgrades --no-sig-check`. Weitere Informationen finden Sie unter Upgrade oder Update eines Hosts mit Image-Profilen.

4 Installieren Sie das NSX-Kernelmodul mithilfe des ESXCLI-Befehls `esxcli software vib install -d <path_to_kernel_module_file> --no-sig-check`. Beispiel: `esxcli software vib install -d /tmp/nsx-lcp-4.0.1.0.0.xxx-esx80.zip`

5 Starten Sie den ESXi-Host neu.

6 Beenden Sie den Wartungsmodus für Ihren ESXi-Host.

Medienoptionen für das Starten des ESXi-Installationsprogramms

Das ESXi-Installationsprogramm muss für das System, auf dem Sie ESXi installieren, erreichbar sein.

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 or 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 aus einem Netzwerk. Siehe Starten des ESXi-Installationsprogramms per Netzwerkstartvorgang.
- Starten aus einem Remotespeicherort mithilfe einer Remoteverwaltungsanwendung. Siehe Verwenden von Anwendungen für die Remoteverwaltung.

Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD or DVD

Wenn Sie über keine ESXi-Installations-CD/DVD verfügen, können Sie eine erstellen.

Sie können auch ein Installer-ISO-Image erstellen, das ein benutzerdefiniertes Installationsskript enthält. Weitere Informationen hierzu finden Sie unter Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript.

Verfahren

1 Befolgen Sie das Verfahren Herunterladen des ESXi-Installationsprogramms.

2 Brennen Sie das ISO-Image auf eine CD oder eine DVD.

Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades

Sie können ein USB-Flash-Laufwerk für das Starten der ESXi-Installation oder des Upgrades formatieren.

Die Anweisungen in diesem Verfahren setzen voraus, dass das USB-Flash-Laufwerk als `/dev/sdb` erkannt wird.

Hinweis Die Datei `ks.cfg` mit dem Installationsskript darf sich nicht in dem USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird. Die Kickstart-Datei hat keine Abhängigkeit vom BIOS- oder UEFI-Start.

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` mit der Datei `isolinux.cfg`

Verfahren

1 Starten Sie Linux, melden Sie sich an und wechseln Sie in den Superuser-Modus, indem Sie einen Befehl vom Typ `su` oder `sudo root` verwenden.

2 Wenn Ihr USB-Flash-Laufwerk nicht als `/dev/sdb` erkannt wird oder Sie nicht genau wissen, wie Ihr USB-Flash-Laufwerk erkannt wird, finden Sie es heraus.

   a Schließen Sie Ihr USB-Flash-Laufwerk an.

   b Führen Sie dazu in der Befehlszeile den Befehl zum Anzeigen der aktuellen Protokollmeldungen aus.

   ```
   tail -f /var/log/messages
   ```

   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.

3 Überschreiben Sie das gesamte USB-Laufwerk mit dem ISO-Image. Dadurch werden die Partitionstabelle und alle vorherigen Inhalte auf dem USB-Laufwerk überschrieben.

```
dd bs=10M if=VMware-VMvisor-Installer-version_number-build_number.x86_64.iso
of=/dev/sdb
```

4 Werfen Sie das USB-Laufwerk aus.

```
eject /dev/sdb
```

Ergebnisse

Sie können das USB-Flash-Laufwerk verwenden, um das ESXi-Installationsprogramm zu starten.

Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts

Sie können ein USB-Flash-Laufwerk zum Speichern des ESXi-Installations- oder -Upgrade-Skripts verwenden, das während der Skriptinstallation bzw. des Skript-Upgrades von ESXi verwendet wird.

Wenn auf der Installationsmaschine mehrere USB-Flash-Laufwerke vorhanden sind, durchsucht die Installationssoftware alle angeschlossenen USB-Flash-Laufwerke nach dem Installations- oder Upgrade-Skript.

Die Anweisungen in diesem Verfahren setzen voraus, dass das USB-Flash-Laufwerk als `/dev/sdb` erkannt wird.

Hinweis Die Datei `ks`, die das Installations- oder Upgrade-Skript enthält, darf sich nicht auf dem selben USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird.

Voraussetzungen

- Linux-Maschine
- Installations- oder Upgrade-Skript für ESXi, die Kickstart-Datei `ks.cfg`
- USB-Flash-Laufwerk

Verfahren

1 Schließen Sie das USB-Flash-Laufwerk an eine Linux-Maschine an, die auf das Installations- bzw. Upgrade-Skript zugreifen kann.

2 Erstellen Sie eine Partitionstabelle.

```
/sbin/fdisk /dev/sdb
```

   a Geben Sie `d` ein, um Partitionen zu löschen, bis alle Partitionen gelöscht sind.

   b Geben Sie `n` ein, um die primäre Partition 1 zu erstellen, die sich über die gesamte Festplatte erstreckt.

c Geben Sie `t` ein, um für den Typ eine passende Einstellung für das Dateisystem FAT32 festzulegen, z. B. **c**.

d Geben Sie `p` ein, um die Partitionstabelle auszugeben.

Das Ergebnis sollte dem folgenden Text ähneln:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         243      1951866  c   W95 FAT32 (LBA)
```

e Geben Sie `w` ein, um die Partitionstabelle zu schreiben und den Vorgang zu beenden.

3 Formatieren Sie das USB-Flash-Laufwerk mit dem FAT32-Dateisystem.

/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1

4 Erstellen Sie ein Zielverzeichnis und mounten Sie das USB-Flash-Laufwerk darauf.

mkdir -p /usbdisk

mount /dev/sdb1 /usbdisk

5 Kopieren Sie das ESXi-Installationsskript auf das USB-Flash-Laufwerk.

cp ks.cfg /usbdisk

6 Unmounten Sie das USB-Flash-Laufwerk.

umount /usbdisk

Ergebnisse

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

Nächste Schritte

Wenn Sie das ESXi-Installationsprogramm starten, verweisen Sie für das Installations- oder Upgrade-Skript auf den Speicherort des USB-Flash-Laufwerks. Siehe Eingeben von Startoptionen zum Ausführen 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 Installieren von ESXi mithilfe eines Skripts und Grundlegende Informationen zur Datei „boot.cfg“ .

Voraussetzungen

- Linux-Maschine
- Das ESXi-ISO-Image `VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso`, wobei *x.x.x* die Version von ESXi ist, die Sie installieren, und *XXXXXX* die Buildnummer des ISO-Images des Installationsprogramms
- Ihr benutzerdefiniertes Installations- oder Upgrade-Skript, die Kickstart-Datei `KS_CUST.CFG`

Verfahren

1. Laden Sie das ESXi-ISO-Image vom Broadcom Support Portal herunter.
2. Mounten Sie das ISO-Image in einen Ordner:

   mount -o loop VMware-VMvisor-Installer-x.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 `esxi_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. Ändern Sie die Datei `boot.cfg` sowohl in `/esxi_cdrom/efi/boot/boot.cfg` (für UEFI-Start) als auch in `/esxi_cdrom/boot.cfg` (für Legacy-BIOS-Start), um den Speicherort des Installations- oder Upgrade-Skripts mithilfe der Option `kernelopt` anzugeben.

   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 Image des ISO-Installationsprogramms für den regulären Start oder den sicheren Start über UEFI verwenden. Der vSphere Lifecycle Manager kann die Prüfsumme eines solchen ISO-Images jedoch nicht überprüfen. Darüber hinaus können Sie dieses Image nicht für Upgrades mithilfe von vSphere Lifecycle Manager-Workflows verwenden.

Ergebnisse

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

Nächste Schritte

Installieren Sie ESXi aus dem ISO-Image.

Herunterladen des ESXi-Installationsprogramms

Sie können die ESXi-Installationssoftware entweder von einem OEM oder vom Broadcom Support Portal erhalten.

Registrieren Sie sich im Broadcom Support Portal. Weitere Informationen finden Sie unter Registrieren für ein Konto in Broadcom Support Portal und Communities.

Anweisungen zum Herunterladen von Produkten finden Sie unter Herunterladen von Broadcom-Produkten und -Software.

Informationen zum Herunterladen von Offline-Paketen mit zip-Dateien für ESXi-Patches und -Updates finden Sie unter Herunterladen von Broadcom PTF-Dateien und -Lösungen.

Weitere Informationen finden Sie unter VMware zu Broadcom Support – Häufig gestellte Fragen.

Name und Bezeichner von ESXi-Speichergerät

In der Umgebung ESXi wird jedes Speichergerät durch mehrere Namen identifiziert.

Gerätebezeichner

Je nach Art der Speicherung verwendet der ESXi-Host unterschiedliche Algorithmen und Konventionen zum Generieren eines Bezeichners für jedes Speichergerät.

Vom Speicher bereitgestellte Bezeichner

Der ESXi-Host fragt ein Ziel-Speichergerät nach den Namen des Geräts ab. Aus den zurückgegebenen Metadaten extrahiert oder generiert der Host einen eindeutigen Bezeichner für das Gerät. Der Bezeichner basiert auf bestimmten Speicher-Standards, ist eindeutig und einheitlich auf allen Hosts und hat einen der folgenden Formate:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Pfadbasierter Bezeichner

Stellt das Gerät keinen Bezeichner zur Verfügung, generiert der Host eine mpx.Name des *Speicherpfads*, wobei *Pfad* den ersten Pfad zu dem Gerät, z. B. `mpx.vmhba1:C0:T1:L3` darstellt. Dieser Bezeichner kann auf dieselbe Weise verwendet werden wie der vom Speicher bereitgestellte Bezeichner.

Der mpx.*path*-Bezeichner wird für lokale Geräte unter der Annahme erstellt, dass ihre Pfadnamen eindeutig sind. Dieser Bezeichner ist nicht eindeutig oder dauerhaft und kann sich nach jedem Neustart des Systems ändern.

In der Regel hat der Pfad zu dem Gerät das folgende Format:

vmhba*Adapter*:C*Kanal*:T*Ziel*:L*LUN*

- vmhba*Adapter* ist der Name des Speicheradapters. Der Name bezieht sich auf den physischen Adapter auf dem Host, nicht auf den SCSI-Controller, den die virtuellen Maschinen verwenden.
- C*Channel* ist die Nummer des Speicherkanals.

  Software-iSCSI-Adapter und abhängige Hardwareadapter verwenden die Kanalnummer, um mehrere Pfade zu demselben Ziel anzuzeigen.
- T*Ziel* ist die Zielnummer. Die Zielnummerierung wird vom Host festgelegt und kann sich ändern, wenn es eine Änderung in der Zuordnung von Zielen gibt, die für den Host sichtbar sind. Von verschiedenen Hosts gemeinsam verwendete Ziele verfügen möglicherweise nicht über dieselbe Zielnummer.
- L*LUN* ist die LUN-Nummer, die die Position der LUN innerhalb des Ziels angibt. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).

Beispielsweise repräsentiert `vmhba1:C0:T3:L1` LUN1 auf Ziel 3, auf die über den Speicheradapter vmhba1 und den Kanal 0 zugegriffen wird.

Legacy-Bezeichner

Zusätzlich zu den vom Speicher bereitgestellten Bezeichnern oder mpx.*path*-Bezeichnern generiert ESXi für jedes Gerät einen alternativen veralteten Namen. Der Bezeichner hat das folgende Format:

vml.*number*

Der Legacy-Bezeichner enthält mehrere Ziffern, die für das Gerät eindeutig sind. Der Bezeichner kann teilweise aus den Metadaten, die über den Befehl SCSI INQUIRY erhalten wurden, abgeleitet werden. Für nicht lokale Geräte, die keine SCSI INQUIRY-Bezeichner bieten, wird der vml.*Nummer*-Bezeichner als einzig verfügbarer eindeutiger Bezeichner verwendet.

Beispiel: Anzeigen von Gerätenamen in der vSphere-CLI

Sie können den Befehl `esxcli storage core device list` verwenden, um alle Gerätenamen in der vSphere-CLI anzuzeigen. Die Ausgabe lautet in etwa wie folgt:

```
# esxcli storage core device list
naa.XXX
      Display Name: DGC Fibre Channel Disk(naa.XXX)
      ...
      Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

Interaktives Upgrade von Hosts

Um ESXi 6.7-Hosts oder ESXi 7.0-Hosts auf ESXi 8.0 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.

Hinweis Interaktives Upgrade wird auf ESXi-Hosts mit einer Datenverarbeitungseinheit (DPU) nicht unterstützt.

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 or 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 Überblick über den Installationsprozess per Netzwerkstartvorgang.
- Stellen Sie sicher, dass der Server-Hardwaretaktgeber auf UTC eingestellt ist. Diese Einstellung befindet sich im System-BIOS oder -UEFI.
- 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.

Verfahren

1 Legen Sie die CD bzw. DVD des ESXi-Installationsprogramms in das CD-ROM- bzw. DVD-ROM-Laufwerk ein oder schließen Sie das USB-Flash-Laufwerk des Installationsprogramms an und starten Sie die Maschine neu.

2 Stellen Sie BIOS oder UEFI so ein, dass vom CD-ROM-Gerät oder vom USB-Flashlaufwerk aus 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 Festplattereihenfolge in der Liste. Die Reihenfolge der Festplatten wird im BIOS oder UEFI 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 zur Bereitstellung 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 eine Skriptinstallation oder ein Skript-Upgrade 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 Ausführen 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.

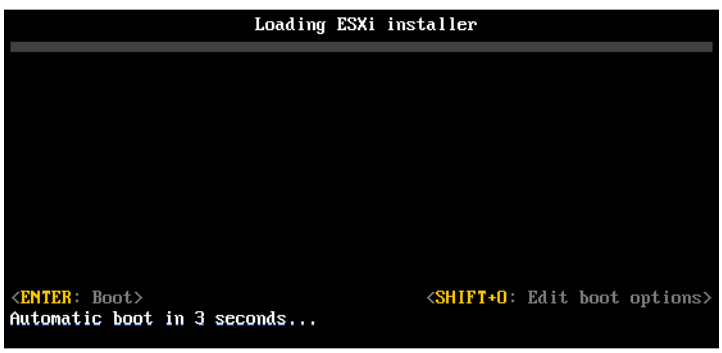
Beim Starten müssen Sie möglicherweise Optionen zum Aktivieren des Zugriffs auf die Kickstart-Datei angeben. Sie können Startoptionen eingeben, indem Sie im Bootloader Shift+O drücken. Für eine Installation per PXE-Startvorgang können Sie Optionen über die Zeile `kernelopts` der Datei `boot.cfg` übergeben. Weitere Informationen finden Sie unter Grundlegende Informationen zur Datei „boot.cfg“ und Starten des ESXi-Installationsprogramms über das Netzwerk.

Um den Speicherort des Installationsskripts anzugeben, legen Sie die Option `ks=`*`filepath`* fest, wobei *filepath* den Speicherort der Kickstart-Datei angibt. Andernfalls kann eine Skriptinstallation bzw. ein Skript-Upgrade nicht starten. Wenn `ks=`*`filepath`* ausgelassen wird, wird das Textinstallationsprogramm ausgeführt.

Unterstützte Startoptionen werden in Startoptionen aufgelistet.

Verfahren

1. Starten Sie den Host.
2. Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3 Geben Sie an der `runweasel`-Eingabeaufforderung **`ks=`*`Speicherort des Installationsskripts und die Start-Befehlszeilenoptionen`*** ein.

Beispiel: Startoption

Sie geben die folgenden Startoptionen ein:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Startoptionen

Wenn Sie eine Skriptinstallation ausführen, müssen Sie möglicherweise beim Starten Optionen angeben, um auf die Kickstart-Datei zugreifen zu können.

Unterstützte Startoptionen

Tabelle 3-7. Startoptionen für die ESXi-Installation

Startoption	Beschreibung
`BOOTIF=`*`hwtype-MAC-Adresse`*	Ähnlich der Option `netdevice`, außer dass das PXELINUX-Format verwendet wird, wie in der Option IPAPPEND unter SYSLINUX auf der Website `syslinux.org` beschrieben.
`gateway=`*`IP-Adresse`*	Legt dieses Netzwerk-Gateway als Standard-Gateway für den Download des Installationsskripts und der Installationsmedien fest.
`ip=`*`IP-Adresse`*	Richtet eine statische IP-Adresse ein, die zum Herunterladen des Installationsskripts und der Installationsmedien verwendet wird. Hinweis: Das PXELINUX-Format für diese Option wird auch unterstützt. Weitere Informationen finden Sie in der Option IPAPPEND unter SYSLINUX auf der Website `syslinux.org`.
`ks=cdrom:/`*`Pfad`*	Führt eine Skriptinstallation anhand des Skripts unter *Pfad* 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 `ks=cdrom:/KS_CUST.CFG`.
`ks=file://`*`Pfad`*	Führt eine Skriptinstallation anhand des Skripts unter *Pfad* aus.
`ks=`*`Protokoll`*`://`*`ServerPfad`*	Führt eine Skriptinstallation mit einem Skript durch, das sich im Netzwerk an der angegebenen URL befindet. Als *Protokoll* kann `http`, `https`, `ftp` oder `nfs` verwendet werden. Ein Beispiel für die Verwendung von NFS-Protokollen ist `ks=nfs://`*`Host/PortURL-Pfad`*. Das Format einer NFS-URL wird in RFC 2224 festgelegt.

Tabelle 3-7. Startoptionen für die ESXi-Installation (Fortsetzung)

Startoption	Beschreibung
`ks=usb`	Führt eine Skriptinstallation anhand eines Skripts auf einem angeschlossenen USB-Laufwerk aus. Sucht nach einer Datei namens `ks.cfg`. Die Datei muss sich im Stammverzeichnis des Laufwerks befinden. Falls mehrere USB-Flash-Laufwerke angeschlossen sind, werden sie so lange durchsucht, bis die Datei `ks.cfg` gefunden wird. Nur FAT16- und FAT32-Dateisysteme werden unterstützt.
`ks=usb:/`*`Pfad`*	Führt eine Skriptinstallation anhand der Skriptdatei auf dem angegebenen Pfad durch, der sich auf einem USB-Laufwerk befindet.
`ksdevice=`*`Gerät`*	Versucht, ein Netzwerkadapter-*Gerät* bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00.50.56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
`nameserver=`*`IP-Adresse`*	Gibt einen DNS-Server an, der zum Herunterladen des Installationsskripts und der Installationsmedien verwendet wird.
`netdevice=`*`Gerät`*	Versucht, ein Netzwerkadapter-*Gerät* bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00.50.56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
`netmask=`*`Subnetzmaske`*	Gibt die Subnetzmaske für die Netzwerkkarte an, über die das Installationsskript und das Installationsmedium heruntergeladen wird.
`vlanid=`*`vlanid`*	Konfigurieren Sie die Netzwerkkarte, sodass sie auf dem angegebenen VLAN verwendet werden kann.
`systemMediaSize=`*`Klein`*	Beschränkt die Größe von Systemspeicherpartitionen auf dem Startmedium. Der ausgewählte Wert muss dem Zweck Ihres Systems entsprechen. Sie können aus den folgenden Werten auswählen: ■ *Minimum* (32 GB, für einzelne Festplatte oder eingebettete Server) ■ *Klein* (64 GB, für Server mit mindestens 512 GB RAM) ■ *Standardwert* (128 GB) ■ *Maximum* (Verbrauch des gesamten verfügbaren Speicherplatzes, für Multi-Terabyte-Server)

Weitere Informationen zur ESXi-Startoptionen nach der Installation finden Sie im VMware-Knowledgebase-Artikel 77009.

Installieren von ESXi mithilfe eines Skripts

Das Installations-/Upgrade-Skript ist eine Textdatei, z. B. `ks.cfg`, die unterstützte Befehle enthält.

Der Befehlsabschnitt des Skripts enthält die ESXi-Installationsoptionen. Dieser Abschnitt ist erforderlich und muss zuerst im Skript angezeigt werden.

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 Installationsskripts anzugeben oder andere Startoptionen zu übergeben.

Die Datei `boot.cfg` weist die folgende Syntax auf:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
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 3-8. Befehle in `boot.cfg`.

Befehl	Beschreibung
`title=`*`STRING`*	Stellt den Titel des Bootloaders auf *`STRING`* ein.
`prefix=`*`STRING`*	(Optional) Setzt *`DIRPATH/`* vor jeden *`FILEPATH`* in den `kernel=`- und `modules=`-Befehlen, die nicht bereits mit / oder mit `http://` beginnen.
`kernel=`*`FILEPATH`*	Stellt den Kernelpfad auf *`FILEPATH`* ein.
`kernelopt=`*`STRING`*	Hängt *`STRING`* an die Kernel-Startoptionen an.
`modules=`*`FILEPATH1 --- FILEPATH2... --- FILEPATHn`*	Listet die zu ladenden Module auf, getrennt durch drei Striche (`---`).

Siehe Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript und Netzwerk zum Starten des ESXi-Installationsprogramms.

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 Installieren von ESXi mithilfe eines 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 Ausführen 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.

Wenn Ihr System mit vSphere 8.0 über unterstützte Datenverarbeitungseinheiten (DPU) verfügt, sollten Sie immer die Installation, Neuinstallation oder das Upgrade von ESXi auf DPUs zusammen mit ESXi auf Hosts in Betracht ziehen. ESXi-Update und -Upgrade auf DPUs werden nicht von der interaktiven oder skriptbasierten Methode unterstützt, Sie können nur vSphere Lifecycle Manager verwenden.

Hinweis Die Verwendung von SD- und USB-Geräten zum Speichern von ESX-OSData-Partitionen wird eingestellt. Sie können SD- und USB-Geräte nur zum Erstellen von Startbankpartitionen, `boot-bank 0` und `boot-bank 1` verwenden. Zusätzlich können Sie eine persistente Festplatte mit mindestens 32 GB bereitstellen, auf der die ESX-OSData-Partition installiert werden soll. Sie definieren solche Festplatten mithilfe des Parameters `systemDisk` im Befehl `install`.

accepteula oder 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.

`--drives=`	Entfernt Partitionen auf den angegebenen Laufwerken.
`--alldrives`	Ignoriert die Bedingung`--drives=` und erlaubt das Löschen von Partitionen auf allen Laufwerken.
`--ignoredrives=`	Entfernt Partitionen auf allen außer den angegebenen Laufwerken. Erforderlich, es sei denn, das Flag `--drives=` oder `--alldrives` wurde angegeben.
`--overwritevmfs`	Erlaubt das Überschreiben von VMFS-Partitionen auf den angegebenen Laufwerken. Standardmäßig ist das Überschreiben von VMFS-Partitionen nicht erlaubt.
`--firstdisk=` ***`disk-type1`*** **`[`*** ***`disk-type2`*** **`,...]`**	**Hinweis** Wenn Ihr vSphere-System eine Version vor 8.0 Update 3 und DPUs aufweist, geben Sie auch einen PCI-Steckplatz an: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Bei Systemen der Version 8.0 Update 3 und höher ist der Parameter `dpupcislots` veraltet. Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet: 1 Lokal angehängter Speicher (`local`)

2 Netzwerkspeicher (`remote`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte 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 `esx` für die erste Festplatte, auf der ESXi installiert ist, Modell- und Anbieterinformationen sowie der Name des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den 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.

dryrun (optional)

Analysiert und überprüft das Installationsskript. Führt die Installation nicht aus.

Installieren

Gibt an, dass es sich um eine Neuinstallation handelt. 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 *diskname* ein Festplattenname oder der vollständige Dateisystempfad einer Festplatte in ESXi sein. Beispiel:

- Festplattenname: `--disk=naa.6d09466044143600247aee55ca2a6405` oder
- Gerätepfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

Die Formate der angenommenen Laufwerksnamen finden Sie unter Festplattengerätenamen.

`--firstdisk=`

`disk-type1,`

`[`*`disk-type2`*`,...]`

Hinweis Wenn Ihr vSphere-System eine Version vor 8.0 Update 3 und DPUs aufweist, geben Sie auch einen PCI-Steckplatz an: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Bei Systemen der Version 8.0 Update 3 und höher ist der Parameter `dpupcislots` veraltet.

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

1 Lokal angehängter Speicher (`local`)

2 Netzwerkspeicher (`remote`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte 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.

`--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 Magnetfestplatte gelöscht.

Weitere Informationen zur Verwaltung von vSAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevmfs Wird benötigt, um vor der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte zu überschreiben.

--preservevmfs Behält während der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte bei.

--novmfsondisk Verhindert, dass eine VMFS-Partition auf dieser Festplatte erstellt wird. Muss mit `--overwritevmfs` verwendet werden, wenn eine VMFS-Partition auf der Festplatte vorhanden ist.

--systemdisk Wenn Sie ein USB- oder SD-Gerät verwenden, gibt `systemDisk` die lokale persistente Festplatte an, auf der die ESX-OSData-Partition installiert werden soll. Zum Beispiel: **`install --firstdisk = usb --systemDisk=<diskID>`**. Dies führt dazu, dass Startbankpartitionen auf dem USB-Gerät abgelegt werden, während sich die OSData-Partition auf der im Parameter `systemDisk` angegebenen Festplatte befindet.

--repartitionsystemdisk Wenn Sie ein USB- oder SD-Gerät verwenden und die lokale Festplatte, die Sie mit dem Parameter `systemDisk` angeben, nicht leer ist oder einen Datenspeicher enthält, können Sie mithilfe von `repartitionSystemDisk` sicherstellen, dass die persistente Festplatte vor der Verwendung neu partitioniert wird.

Hinweis Wenn keine lokale persistente Festplatte verfügbar ist oder die Festplattengröße weniger als 32 GB beträgt, werden Warnmeldungen angezeigt, aber die Installation wird fortgesetzt.

--forceunsupportedinstall Blockiert die Installation von veralteten CPUs.

installorupgrade

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk= or --drive=`

Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=`*`diskname`* kann *diskname* ein Festplattenname oder der vollständige Dateisystempfad einer Festplatte in ESXi sein. Beispiel:

- Festplattenname: `--disk=naa.6d09466044143600247aee55ca2a6405` oder
- Gerätepfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

Die Formate der angenommenen Laufwerksnamen finden Sie unter Festplattengerätenamen.

`--firstdisk=`

`disk-type1,`

`[`*`disk-type2`*`,...]`

Hinweis Wenn Ihr vSphere-System eine Version vor 8.0 Update 3 und DPUs aufweist, geben Sie auch einen PCI-Steckplatz an: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Bei Systemen der Version 8.0 Update 3 und höher ist der Parameter `dpupcislots` veraltet.

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

1 Lokal angehängter Speicher (`local`)

2 Netzwerkspeicher (`remote`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte 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 Magnetfestplatte 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. Bei Nichtvorhandensein dieser Option schlägt das Installationsprogramm fehl, wenn eine VMFS-Partition auf der Festplatte zur Verfügung steht, eine ESX- oder ESXi-Installation aber fehlt.

keyboard (optional)

Legt den Tastaturtyp für das System fest.

`keyboardType`

Gibt die Tastaturkarte für den ausgewählten Tastaturtyp an. *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)

Der Befehl wird in ESXi Version 5.1 und höher unterstützt. 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.

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

paranoid (optional)

Sorgt dafür, dass Warnmeldungen zum Abbruch der Installation führen. Wenn Sie diesen Befehl auslassen, werden Warnmeldungen protokolliert.

part oder partition (optional)

Erstellt auf dem System einen zusätzlichen VMFS-Datenspeicher. Es kann nur ein Datenspeicher pro Festplatte erstellt werden. Kann nicht auf derselben Festplatte wie der `install`-Befehl verwendet werden. Es kann nur eine Partition pro Festplatte angegeben werden. Diese muss eine VMFS-Partition sein.

datastore name — Gibt an, wo die Partition gemountet werden soll.

--ondisk= or --ondrive= — Gibt die Festplatte oder das Laufwerk an, wo die Partition erstellt werden soll.

--onfirstdisk= ***disk-type1,*** **[*disk-type2*,...]**

Hinweis Wenn Ihr vSphere-System eine Version vor 8.0 Update 3 und DPUs aufweist, geben Sie auch einen PCI-Steckplatz an: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Bei Systemen der Version 8.0 Update 3 und höher ist der Parameter `dpupcislots` veraltet.

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

1. Lokal angehängter Speicher (`local`)
2. Netzwerkspeicher (`remote`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte 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 `--onfirstdisk=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.

reboot (optional)

Startet die Maschine nach Abschluss der Skriptinstallation neu.

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

rootpw (erforderlich)

Legt das Root-Kennwort für das System fest.

`--iscrypted` Legt fest, dass das Kennwort verschlüsselt ist.

`password` Legt das Kennwort fest.

Aktualisieren

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk= or --drive=` Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=`*`diskname`* kann *diskname* ein Festplattenname oder der vollständige Dateisystempfad einer Festplatte in ESXi sein. Beispiel:

- Festplattenname: `--disk=naa.6d09466044143600247aee55ca2a6405` oder
- Gerätepfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

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`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte 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.

%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 =[python|busybox]	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.

%post (optional)

Führt das angegebene Skript nach Abschluss der Paketinstallation aus. Wenn Sie mehrere `%post`-Abschnitte festlegen, werden sie in der Reihenfolge ausgeführt, in der sie im Installationsskript angegeben sind.

--interpreter =[python|busybox]	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.
--timeout=secs	Legt eine Zeitüberschreitung für das Ausführen des Skripts fest. Ist das Skript bei Auftreten der Zeitüberschreitung nicht abgeschlossen, wird es zwangsweise beendet.
--ignorefailure =[true|false]	Bei Angabe von „true“ wird die Installation auch dann als erfolgreich angesehen, wenn das `%post`-Skript mit einem Fehler beendet wird.

%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.

Wichtig Das Skript `%firstboot` wird nicht ausgeführt, wenn Secure Boot auf dem ESXi-Host aktiviert ist.

--interpreter	

`=[python|busybox]`	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.

Hinweis Sie können die Semantik des `%firstboot`-Skripts erst dann prüfen, wenn das System zum ersten Mal gestartet wird. Wenn das Skript Fehler enthält, sind diese erst nach Abschluss der Installation ersichtlich.

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

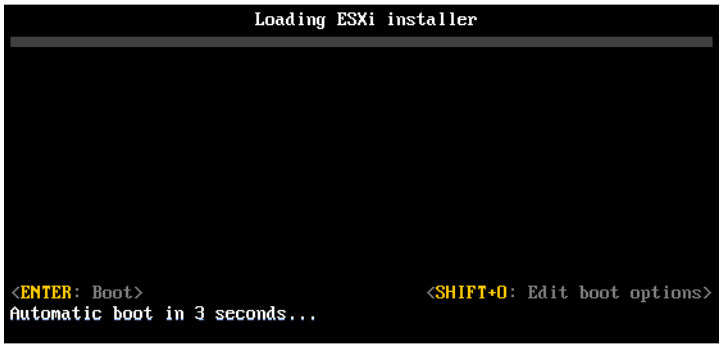
Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- 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 or DVD.
- Das System kann auf das Standardinstallations- oder -Upgrade-Skript (`ks.cfg`) oder ein benutzerdefiniertes Installations- oder -Upgrade-Skript zugreifen. Siehe Installieren von ESXi mithilfe eines Skripts.
- Sie haben einen Startbefehl ausgewählt, um die Installation oder das Upgrade per Skript auszuführen. Siehe Eingeben von Startoptionen zum Ausführen eines Installations- oder Upgrade-Skripts. Eine vollständige Liste der Startbefehle finden Sie unter Startoptionen .

Verfahren

1. Starten Sie das ESXi-Installationsprogramm vom lokalen CD-ROM- oder DVD-ROM-Laufwerk aus.

2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3 Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

   Die Startoption hat das Format `ks=`.

4 Drücken Sie die Eingabetaste.

Ergebnisse

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Installieren oder Durchführen eines Upgrades von ESXi von einem USB-Sticks 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

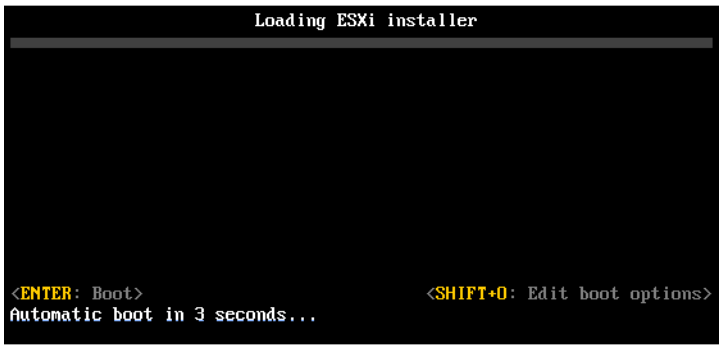
Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das System, auf dem Sie ESXi installieren oder aktualisieren, erfüllt die Hardwareanforderungen für die Installation bzw. das Upgrade. Weitere Informationen hierzu finden Sie unter Hardwareanforderungen für ESXi.
- Die ESXi-Installer-ISO-Datei befindet sich auf einem startfähigen USB-Flash-Laufwerk. Weitere Informationen hierzu finden Sie unter 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. Weitere Informationen hierzu finden Sie unter Installieren von ESXi mithilfe eines Skripts.

- Sie haben eine Startoption ausgewählt, um die Installation, das Upgrade oder die Migration per Skript auszuführen. Weitere Informationen hierzu finden Sie unter Eingeben von Startoptionen zum Ausführen eines Installations- oder Upgrade-Skripts.

Verfahren

1. Starten Sie das ESXi-Installationsprogramm vom USB-Flash-Laufwerk aus.
2. Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3. Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

   Die Startoption hat das Format `ks=`.
4. Drücken Sie die Eingabetaste.

Ergebnisse

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Netzwerk Starten des ESXi-Installationsprogramms für eine Skriptinstallation oder ein Skript-Upgrade

ESXi 8.0 bietet viele Optionen zum Starten des Installationsprogramms über ein Netzwerk und mit Verwendung eines Installations- oder eines Upgrade-Skripts.

- Weitere Informationen zur Einrichtung einer Netzwerkinfrastruktur finden Sie unter Netzwerk zum Starten des ESXi-Installationsprogramms.
- Weitere Informationen über das Erstellen und Auffinden eines Installationsskripts finden Sie unter Installieren von ESXi mithilfe eines Skripts.
- Weitere Informationen über bestimmte Verfahren zum Starten des ESXi-Installationsprogramms per Netzwerkstartvorgang und zum Verwenden eines Installationsskripts finden Sie in den folgenden Themen:
  - Starten des ESXi-Installationsprogramms mithilfe von nativem UEFI-HTTP
  - Starten des ESXi-Installationsprogramms mithilfe von iPXE und HTTP

- Starten des ESXi-Installationsprogramms mithilfe von PXE und TFTP
- Weitere Informationen über die Verwendung von vSphere Auto Deploy zum Durchführen eines Skript-Upgrades per PXE-Startvorgang finden Sie unterKapitel 4 Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts .

Festplattengerätenamen

Die Installationsskriptbefehle `install`, `upgrade` und `installorupgrade` erfordern die Verwendung von Festplattengerätenamen.

Tabelle 3-9. Festplattengerätenamen

Formatieren	Beispiel	Beschreibung
NAA	naa.6d09466044143600247aee55ca2a6405	SCSI-INQUIRY-Bezeichner
EUI	eui.3966623838646463	SCSI-INQUIRY-Bezeichner
T10	t10.SanDisk00Cruzer_Blade000000004C5300 01171118101244	SCSI-INQUIRY-Bezeichner
VML	vml.00025261	Legacy-VMkernel-Bezeichner
MPX	mpx.vmhba0:C0:T0:L0	Pfadbasierter Bezeichner

Weitere Informationen zu Namen für Speichergeräte finden Sie unter *Namen und Bezeichner von Speichergeräten* in der Dokumentation zum *vSphere-Speicher*.

Starten eines ESXi-Hosts über ein Netzwerkgerät

Netzwerk zum Starten des ESXi-Installationsprogramms

Sie können PXE (Preboot Execution Environment) zum Starten eines ESXi-Hosts über ein Netzwerkgerät verwenden, wenn Ihr Host Legacy-BIOS oder UEFI unterstützt.

Wenn der ESXi-Host natives UEFI-HTTP unterstützt können Sie alternativ das HTTP-Protokoll (Hypertext Transfer Protocol) zum Starten des Hosts über ein Netzwerkgerät verwenden. ESXi wird in einem ISO-Format bereitgestellt, das für die Installation auf Flash-Arbeitsspeicher oder auf eine lokale Festplatte verwendet wird. Sie können die Dateien extrahieren und über eine Netzwerkschnittstelle 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.

Natives UEFI-HTTP verwendet DHCP und HTTP zum Starten über ein Netzwerk. UEFI-HTTP-Start erfordert eine Netzwerkinfrastruktur, eine UEFI-Firmware-Version auf dem ESXi-Host, der die HTTP-Startfunktion enthält, und einen Netzwerkadapter, der UEFI-Netzwerke unterstützt.

Startvorgänge mithilfe von HTTP sind schneller und verlässlicher als Startvorgänge mit TFTP. Dies ist auf die Funktionen des TCP-Protokolls zurückzuführen, das dem HTTP-Protokoll zugrunde liegt, wie z. B. integriertes Streaming und Wiederherstellung verlorener Pakete. Wenn Ihre ESXi-Hosts keine Unterstützung für natives UEFI-HTTP bieten, können Sie iPXE-HTTP für den Startvorgang verwenden.

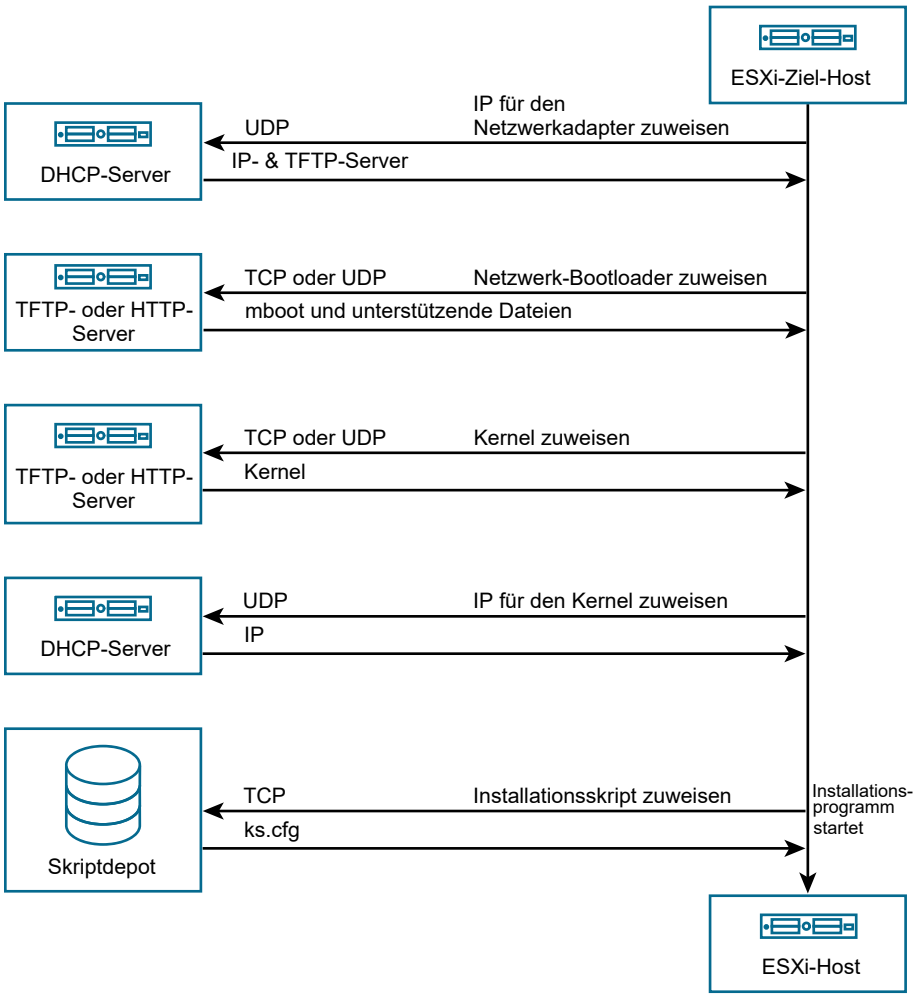
Hinweis Ein Netzwerkstart mit Legacy-BIOS-Firmware kann nur über IPv4 gestartet werden. Ein Netzwerkstart mit UEFI-BIOS-Firmware ist über IPv4 oder IPv6 möglich.

Überblick über den Installationsprozess per Netzwerkstartvorgang

Sie können einen ESXi-Host über eine Netzwerkschnittstelle starten. Der Netzwerkstartvorgang richtet sich danach, ob der Zielhost Legacy-BIOS- oder UEFI-Firmware verwendet und ob beim Startvorgang PXE, TFTP, iPXE HTTP oder UEFI HTTP eingesetzt wird.

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

Abbildung 3-2. 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-Adressen, dem Speicherort des TFTP- oder HTTP-Servers sowie dem Dateinamen oder der URL des anfänglichen Netzwerk-Bootloaders.

4 Der ESXi-Host kontaktiert den TFTP- oder HTTP-Server und fordert den vom DHCP-Server angegebenen Dateinamen oder die URL an.

5 Der TFTP- oder HTTP-Server sendet den Netzwerk-Bootloader, und der ESXi-Host führt ihn aus. Der ursprüngliche Bootloader lädt unter Umständen zusätzliche Bootloader-Komponenten vom Server.

6 Der Bootloader sucht nach einer Konfigurationsdatei auf dem TFTP- oder HTTP-Server, lädt den Kernel und andere ESXi-Komponenten wie in der Konfigurationsdatei angegeben herunter und startet den Kernel auf dem ESXi-Host.

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

Hintergrundinformationen zum Netzwerkstart

Kenntnisse im Hinblick auf Startvorgänge können bei der Fehlerbehebung hilfreich sein.

TFTP-Server

Trivial File Transfer Protocol (TFTP) ähnelt dem FTP-Dienst und wird normalerweise nur für Netzwerkstartsysteme oder zum Laden der Firmware auf Netzwerkgeräten (z. B. Routern) verwendet. 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 wird, müssen Sie tftpd32 Version 2.11 oder höher verwenden. Weitere Informationen hierzu finden Sie unter http://tftpd32.jounin.net/.

SYSLINUX und PXELINUX

Wenn Sie PXE in einer Legacy-BIOS-Umgebung verwenden, müssen Sie mit den unterschiedlichen Startumgebungen vertraut sein.

- SYSLINUX ist eine Open Source-Startumgebung für Maschinen, auf denen Legacy-BIOS-Firmware ausgeführt wird. Der ESXi-Bootloader für BIOS-Systeme (`mboot.c32`) wird als SYSLINUX-Plug-In ausgeführt. Sie können SYSLINUX für den Start über verschiedene Medientypen einschließlich Festplatte, ISO-Image und Netzwerk konfigurieren. Das SYSLINUX-Paket befindet sich unter http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX ist eine SYSXLINUX-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.

Hinweis VMware erstellt 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 möglicherweise nicht kompatibel. *Das Open Source Disclosure-Paket für VMware vSphere Hypervisor* enthält Fehlerkorrekturen für SYSLINUX Version 3.86.

iPXE

iPXE ist eine Open Source-Software, die eine Implementierung von HTTP bereitstellt. Sie können die Software verwenden, um einen anfänglichen Startvorgang durchzuführen. Weitere Informationen finden Sie unter https://ipxe.org/.

VMware enthält einen iPXE-Build als Teil von Auto Deploy. Die Quellstruktur für diesen Build steht im *Open Source Disclosure-Paket für VMware vCenter Server* zur Verfügung.

UEFI-PXE und UEFI-HTTP

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.

Bestimmte UEFI-Firmware unterstützt native UEFI-HTTP-Startvorgänge. Die Funktion wird in Version 2.5 der UEFI-Spezifikation eingeführt. Die Firmware kann den ESXi-Bootloader über einen HTTP-Server ohne zusätzliche Software, wie z. B. iPXE, laden.

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

Alternative Ansätze für den Netzwerkstart

Alternative Ansätze für Netzwerkstarts 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 DCHP-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.

PXELINUX-Konfigurationsdateien

Sie benötigen eine PXELINUX-Konfigurationsdatei, um das ESXi-Installationsprogramm auf einem Legacy-BIOS-System zu starten. Die Konfigurationsdatei definiert das Menü, das dem ESXi-Zielhost angezeigt wird, während er gestartet wird.

In diesem Abschnitt erhalten Sie allgemeine Informationen zu PXELINUX-Konfigurationsdateien.

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 für den 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` versucht in der folgenden Reihenfolge, eine PXE-Konfigurationsdatei 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.

Starten des ESXi-Installationsprogramms mithilfe von PXE und 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.

- Für Legacy-BIOS-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `pxelinux.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

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.

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, den Sie für den PXE-Startvorgang konfigurieren können. 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.

Rufen Sie Version 3.86 des SYSLINUX-Pakets für Legacy-BIOS-Systeme ab. Weitere Informationen finden Sie unter Hintergrundinformationen zum Netzwerkstart.

Verfahren

1. Wenn auf Ihrem ESXi-Host nur Legacy-BIOS-Firmware ausgeführt wird, rufen Sie PXELINUX ab und konfigurieren Sie diese Datei.
   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-8.x.x-XXXXXX` ist der Name des TFTP-Unterverzeichnisses, das die Dateien des ESXi-Installationsprogramms enthält.

      ```
      DEFAULT install
      NOHALT 1
      LABEL install
        KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
        APPEND -c ESXi-8.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 `default`, wenn alle Hosts dieses ESXi-Installationsprogramm standardmäßig starten sollen.
Verschiedene Installationsprogramme	Benennen Sie die Datei mit der MAC-Adresse der Zielhostmaschine (01-*mac_address_of_target_ESXi_host*), wenn nur ein bestimmter Host mit dieser Datei gestartet werden soll, z. B. `01-23-45-67-89-0a-bc`.

2. Wenn auf Ihrem ESXi-Host UEFI-Firmware ausgeführt wird, kopieren Sie die Dateien `efi/boot/bootx64.efi` und `efi/boot/crypto64.efi` aus dem ISO-Image des ESXi-Dienstprogramms in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

3 Benennen Sie die Datei `efi/boot/bootx64.efi` in `mboot.efi` um.

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 Konfigurieren Sie den DHCP-Server.

5 Erstellen Sie ein Unterverzeichnis des obersten `/tftpboot`-Verzeichnisses des TFTP-Servers und benennen Sie es nach der enthaltenen ESXi-Version, z. B. `/tftpboot/ESXi-8.x.x-xxxxx`.

6 Kopieren Sie den Inhalt des Images des ESXi-Installationsprogramms in das neu erstellte Verzeichnis.

7 Bearbeiten Sie die Datei `boot.cfg`.

a Fügen Sie folgende Zeile hinzu:

```
prefix=ESXi-7.x.x-xxxxxx
```

Hier stellt `ESXi-7.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.

c Wenn die `kernelopt=`-Zeile die Zeichenfolge `cdromBoot` enthält, entfernen Sie nur die Zeichenfolge.

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 Installationsskripts anzugeben.

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

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

9 Wenn auf Ihrem ESXi-Host UEFI-Firmware ausgeführt wird, geben Sie an, ob alle UEFI-Hosts dasselbe Dienstprogramm starten sollen.

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

Starten des ESXi-Installationsprogramms mithilfe von iPXE und HTTP

Sie können iPXE zum Starten des ESXi-Installationsprogramms über einen HTTP-Server verwenden.

- Für Legacy-BIOS-Maschinen unterstützt das Verfahren den Start mehrerer verschiedener Versionen des ESXi-Installationsprogramms mithilfe desselben anfänglichen `pxelinux.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

Die Voraussetzungen und Schritte hängen nur von der Unterstützung von UEFI-Start oder Legacy-BIOS ab. Sie können iPXE zum Starten des ESXi-Installationsprogramms über einen HTTP-Server verwenden. Im folgenden Thema werden die Voraussetzungen und Schritte für ESXi-Hosts diskutiert, die UEFI-Start und Hosts unterstützen, die nur Legacy-BIOS unterstützen.

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, den Sie für den PXE-Startvorgang konfigurieren können. 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 HTTP-Servers erfüllt:

- Stellen Sie sicher, dass die ESXi-Zielhosts auf den HTTP-Server zugreifen können.
- Wenn auf Ihrem ESXi-Host nur Legacy-BIOS-Firmware ausgeführt wird, erwerben Sie Version 3.86 des SYSLINUX-Pakets. Weitere Informationen finden Sie unter Hintergrundinformationen zum Netzwerkstart.

Verfahren

1. Rufen Sie iPXE ab und konfigurieren Sie diese Datei.
   a. Rufen Sie den iPXE-Quellcode ab.
   b. Befolgen Sie auf der Downloadseite von iPXE die Anweisungen zum Erstellen, aber führen Sie einen der folgenden Befehle aus.
      - Führen Sie für ESXi-Hosts unter Legacy-BIOS-Firmware den Befehl `make bin/undionly.kpxe` aus.
      - Führen Sie für ESXi-Hosts unter UEFI-Firmware den Befehl `make bin-x86_64-efi/snponly.efi` aus.
   c. Kopieren Sie die Datei `undionly.kpxe` oder `snponly.efi` in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

2 Wenn auf Ihrem ESXi-Host nur Legacy-BIOS-Firmware ausgeführt wird, rufen Sie PXELINUX ab und konfigurieren Sie diese Datei.

   a Rufen Sie SYSLINUX Version 3.86 ab, entpacken Sie das Programm und kopieren Sie die Datei `pxelinux.0` in das Verzeichnis `/tftpboot` auf dem TFTP-Server.

   b Erstellen Sie eine PXELINUX-Konfigurationsdatei mithilfe des folgenden Codemodells.

   `ESXi-8.x.x-XXXXXX` ist der Name des TFTP-Unterverzeichnisses, das die Dateien des ESXi-Installationsprogramms enthält.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-8.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Speichern Sie die PXELINUX-Datei auf dem TFTP-Server im Verzeichnis `/tftpboot/pxelinux.cfg/`.

   Der Dateiname gibt an, ob dieses Installationsprogramm von allen Hosts standardmäßig gestartet wird.

Option	Beschreibung
Dasselbe Installationsprogramm	Geben Sie der Datei den Namen `default`, wenn alle Hosts dieses ESXi-Installationsprogramm standardmäßig starten sollen.
Verschiedene Installationsprogramme	Benennen Sie die Datei mit der MAC-Adresse der Zielhostmaschine (01-*mac_address_of_target_ESXi_host*), wenn diese Datei nur von einem bestimmten Host gestartet werden muss. Beispiel: `01-23-45-67-89-0a-bc`.

3 Wenn auf Ihrem ESXi-Host UEFI-Firmware ausgeführt wird, kopieren Sie die Datei `efi/boot/bootx64.efi` aus dem ISO-Image des ESXi-Dienstprogramms in den Ordner `/tftpboot` auf Ihrem TFTP-Server und benennen Sie die Datei in `mboot.efi` um.

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 Konfigurieren Sie den DHCP-Server.

5 Erstellen Sie ein Verzeichnis auf Ihrem HTTP-Server mit dem gleichen Namen wie die ESXi-Version, die darin enthalten ist. Beispiel: `/var/www/html/ESXi-8.x.x-XXXXXX`.

6 Kopieren Sie den Inhalt des Images des ESXi-Installationsprogramms in das neu erstellte Verzeichnis.

7 Bearbeiten Sie die Datei `boot.cfg`.

   a Fügen Sie folgende Zeile hinzu:

   ```
   prefix=http://XXX.XXX.XXX.XXX/ESXi-8.x.x-XXXXXX
   ```

   wobei `http://XXX.XXX.XXX.XXX/ESXi-8.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.

   c Wenn die `kernelopt=`-Zeile die Zeichenfolge `cdromBoot` enthält, entfernen Sie nur die Zeichenfolge.

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 Installationsskripts anzugeben.

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

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

9 Wenn auf Ihrem ESXi-Host UEFI-Firmware ausgeführt wird, geben Sie an, ob alle UEFI-Hosts dasselbe Dienstprogramm starten sollen.

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

Starten des ESXi-Installationsprogramms mithilfe von nativem UEFI-HTTP

Sie können das ESXi-Installationsprogramm direkt über einen HTTP-Server ohne zusätzliche Software zum Unterstützen des Vorgangs starten.

UEFI-HTTP unterstützt das Starten mehrerer Versionen des ESXi-Installationsprogramms. Verwenden Sie denselben ursprünglichen Bootloader `mboot.efi` für alle Zielmaschinen, aber potenziell unterschiedliche Dateien vom Typ `boot.cfg` je nach MAC-Adresse der Zielmaschine.

Hinweis Mischen Sie während des Startvorgangs keine kein IPv4- oder IPv6-Netzwerke. Verwenden Sie IPv4- oder IPv6-Netzwerke.

Voraussetzungen

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

- ESXi-Host mit UEFI-Firmware, der die HTTP-Startfunktion unterstützt.
- 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 UEFI-Netzwerkunterstützung auf dem ESXi-Zielhost
- DHCP-Server, den Sie für UEFI-HTTP-Startvorgänge konfigurieren können. Siehe DHCP-Beispielkonfigurationen.
- (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.

Verfahren

1. Kopieren Sie die Datei `efi/boot/bootx64.efi` aus dem ISO-Image des ESXi-Installationsprogramms in ein Verzeichnis auf Ihrem HTTP-Server und benennen Sie die Datei in `mboot.efi` um. Beispiel: `http://www.example.com/esxi/mboot.efi`.

   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.

2. Konfigurieren Sie den DHCP-Server.
3. Erstellen Sie ein Verzeichnis auf Ihrem HTTP-Server mit dem gleichen Namen wie die ESXi-Version, die darin enthalten ist. Beispiel: `http://www.example.com/esxi/ESXi-8.x.x-XXXXXX`.
4. Kopieren Sie den Inhalt des Images des ESXi-Installationsprogramms in das neu erstellte Verzeichnis.

5 Ändern Sie die Datei `boot.cfg`.

   a Fügen Sie die folgende Zeile mit der URL des neu erstellten Verzeichnisses hinzu.

   ```
   prefix=http://www.example.com/esxi/ESXi-8.x.x-XXXXXX
   ```

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

   c Wenn die `kernelopt=`-Zeile die Zeichenfolge `cdromBoot` enthält, entfernen Sie nur die Zeichenfolge.

6 (Optional) Fügen Sie für eine Skriptinstallation in der `boot.cfg`-Datei die Option `kernelopt` in die Zeile nach dem Kernelbefehl ein, um den Speicherort des Installationsskripts anzugeben.

   Beispiel: `kernelopt=ks=http://www.example.com/esxi_ksFiles/ks.cfg`

7 (Optional) Sie können die Konfigurationsparameter *networkBootProtocol* und *networkBootUri* der virtuellen Maschine verwenden, um den Startpunkt einer virtuellen Maschine anzugeben. Mit der Einstellung *networkBootProtocol* wird das Startprotokoll (IPv4 oder IPv6) festgelegt. Beispielsweise `networkBootProtocol = httpv4`. Mit der Einstellung *networkBootUri* wird die HTTP-URL für den ESXi-Bootloader (bootx64.efi) festgelegt. Beispiel: `networkBootUri = http://xxx.xxx.xx.x/esxi80uc1/efi/boot/bootx64.efi`.

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

Option	Beschreibung
Dasselbe Installationsprogramm	Fügen Sie die Datei `boot.cfg` zum selben Verzeichnis wie `mboot.efi` hinzu. Beispiel: `http://www.example.com/esxi/boot.cfg`
Verschiedene Installationsprogramme	a Erstellen Sie ein Unterverzeichnis des Verzeichnisses, das die Datei `mboot.efi` enthält. Benennen Sie das Verzeichnis als MAC-Adresse der Zielhostmaschine (01-*mac_address_of_target_ESXi_host*), z. B. `01-23-45-67-89-0a-bc`. b Fügen Sie die benutzerdefinierte Datei `boot.cfg` im Verzeichnis hinzu. Beispiel: `http://www.example.com/esxi/01-23-45-67-89-0a-bc/boot.cfg`.

   Sie können beide Installationsprogrammtypen verwenden. ESXi-Hosts ohne benutzerdefinierte Datei vom Typ `boot.cfg` auf Ihrem HTTP-Server. Führen Sie den Startvorgang über die Standarddatei `boot.cfg` aus.

DHCP-Beispielkonfigurationen

Der DHCP-Server muss die Adresse des TFTP- oder HTTP-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. Außerdem muss er den Speicherort der anfänglichen Bootloader-Binärdatei ermitteln. Für den PXE-Startvorgang ist der Speicherort eine Datei auf einem TFTP-Server. Für den UEFI HTTP-Startvorgang ist der Speicherort eine URL.

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.

Es gibt viele DHCP-Server, die Sie verwenden können. Die folgenden Beispiele gelten für einen ISC-DHCP-Server. 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 PXE und TFTP mit IPv4

In diesem Beispiel wird gezeigt, wie ein ISC-DHCP-Server für den PXE-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 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 {
      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 PXE und TFTP mit IPv6

In diesem Beispiel wird gezeigt, wie ein ISC-DHCPv6-Server für den PXE-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 iPXE und HTTP mit IPv4

In diesem Beispiel wird gezeigt, wie ein ISC-DHCP-Server für den Start von ESXi konfiguriert wird, indem iPXE von einem TFTP-Server mit der IPv4-Adresse `xxx.xxx.xxx.xxx` geladen 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 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 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load pxelinux as secondary bootloader
         filename = "pxelinux.0";
      } else {
         # Load the undionly configuration of iPXE as initial bootloader
         filename = "undionly.kpxe";
   }
}
```

Wenn eine Maschine einen Startvorgang über PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `undionly.kpxe` oder `snponly.efi` auf dem TFTP-Server zur Verfügung. Im Legacy-BIOS-Fall fordert iPXE dann den DHCP-Server zum Laden der nächsten Datei auf, und der Server gibt `pxelinux.0` als den Dateinamen zurück. 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. In beiden Fällen ist iPXE enthalten und das System verfügt über HTTP-Funktionalität. Dies führt dazu, dass das System zusätzliche Dateien von einem HTTP-Server laden kann.

Beispiel für den Start unter Verwendung von iPXE und HTTP mit IPv6

In diesem Beispiel wird gezeigt, wie ein ISC-DHCPv6-Server für den Start von ESXi konfiguriert wird, indem iPXE über einen TFTP-Server mit der IPv6-Adresse `xxxx:xxxx:xxxx:xxxx::xxxx` geladen 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. iPXE ist enthalten, und das System verfügt über HTTP-Funktionalität. Dies führt dazu, dass das System zusätzliche Dateien von einem HTTP-Server laden kann.

Beispiel für den Start unter Verwendung von UEFI HTTP mit IPv4

Dieses Beispiel zeigt, wie Sie einen ISC-DHCP-Server für das Starten von ESXi mithilfe des nativen UEFI HTTP mit IPv4 über den Webserver `www.example.com` konfigurieren.

```
#
# 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 "httpclients" {
   match if substring(option vendor-class-identifier, 0, 10) = "HTTPClient";
   option vendor-class-identifier "HTTPClient";

   if option client-system-arch = 00:10 {
      # x86_64 UEFI HTTP client
      filename = http://www.example.com/esxi/mboot.efi;
   }
}
```

Beispiel für den Start unter Verwendung von UEFI HTTP mit IPv6

Dieses Beispiel zeigt, wie Sie einen ISC-DHCPv6-Server für das Starten von ESXi mithilfe des nativen UEFI HTTP mit IPv6 über den Webserver `www.example.com` konfigurieren.

```
#
# 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.user-class code 15 = { integer 16, string };
option dhcp6.vendor-class code 16 = { integer 32, integer 16, string };

if option dhcp6.client-arch-type = 00:10 {
      # x86_64 HTTP clients
      option dhcp6.vendor-class 0 10 "HTTPClient";
      option dhcp6.bootfile-url "http://www.example.com/esxi/mboot.efi";
}
```

Vorgehensweise für das Upgrade von Hosts mithilfe von ESXCLI-Befehlen

Aktualisieren von Hosts mithilfe von ESXCLI-Befehlen

Mithilfe der ESXCLI können Sie ein Upgrade eines ESXi 6.7- oder ESXi 7.0-Hosts auf Version 8.0 durchführen und ESXi 6.7-, ESXi 7.0- und ESXi 8.0-Hosts aktualisieren oder patchen.

Mit vSphere 8.0 werden Konfigurationsdateien, Komponenten, Basisimages und Add-Ons als neue Softwarelieferungen eingeführt, die Sie zum Aktualisieren oder Patchen von ESXi 8.0-Hosts verwenden können. Informationen zum Verwalten von Komponenten, Basis-Images und Add-Ons auf ESXi finden Sie unter ESXCLI-Konzepte und -Beispiele.

Zur Verwendung von ESXCLI-Befehlen müssen Sie die eigenständige ESXCLI installieren. Weitere Informationen zur Installation und Verwendung der ESXCLI finden Sie in den folgenden Dokumenten.

- Verwenden von ESXCLI
- Erste Schritte mit ESXCLI
- ESXCLI – Referenz

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 Lifecycle Manager installiert wurden, sowie 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 Einstellung des Hosts ändern, indem Sie den vSphere Client verwenden oder `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. Für Hosts in einer Produktionsumgebung legen Sie beispielsweise eine restriktivere Akzeptanzebene als für Hosts in einer Testumgebung fest.

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. Kunden mit Support-Anrufen für VIBs dieser Akzeptanzebene werden von VMware gebeten, sich an die Support-Organisation des Partners zu wenden.

PartnerSupported

VIBs mit der Akzeptanzebene „PartnerSupported“ werden von einem Partner veröffentlicht, dem VMware vertraut. Der Partner führt alle Tests durch. VMware überprüft die Ergebnisse nicht. Diese Ebene wird für eine neue oder nicht etablierte Technologie verwendet, die Partner für VMware-Systeme aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATAoE und

SSD. Kunden mit Support-Anrufen für VIBs dieser Akzeptanzebene werden von VMware gebeten, sich an die Support-Organisation des Partners zu wenden.

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 Akzeptanzebene des Hosts so ändern, dass sie mit der Akzeptanzebene für ein VIB oder Image-Profil übereinstimmt, das Sie installieren möchten. 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 VIB oder Image-Profils sowie zum Ändern der Akzeptanzebene des Hosts, wenn dies für das Update erforderlich ist.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Rufen Sie die Akzeptanzebene für das VIB oder das Image-Profil ab.

Option	Beschreibung
Informationen für alle VIBs auflisten	`esxcli --server=<server_name> software sources vib list --depot=<depot_URL>`
Informationen für ein bestimmtes VIB auflisten	`esxcli --server=<server_name> software sources vib list --viburl=<vib_URL>`
Informationen für alle Image-Profile auflisten	`esxcli --server=<server_name> software sources profile list --depot=<depot_URL>`
Informationen für ein bestimmtes Image-Profil auflisten	`esxcli --server=<server_name> software sources profile get --depot=<depot_URL> --profile=<profile_name>`

2 Rufen Sie die Akzeptanzebene des Hosts ab.

```
esxcli --server=<server_name> software acceptance get
```

3 (Optional) Ist die Akzeptanzebene des VIBs restriktiver als die Akzeptanzebene des Hosts, ändern Sie die Akzeptanzebene des Hosts.

```
esxcli --server=<server_name> software acceptance set --level=<acceptance_level>
```

Die *Akzeptanzebene* kann `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` oder `CommunitySupported` lauten. 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. Eine Warnung wird angezeigt. Weil Ihr Setup nicht mehr konsistent ist, wird die Warnung wiederholt, wenn Sie VIBs installieren, VIBs entfernen und bestimmte andere Vorgänge auf dem Host durchführen.

Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist

VIBs, die Sie mit einer Live-Installation installieren können, erfordern keinen Neustart des Hosts. Möglicherweise ist es jedoch notwendig, den Host in den Wartungsmodus zu versetzen.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Andere VIBs und Profile erfordern möglicherweise, dass der Host nach der Installation oder dem Update neu gestartet wird.

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Überprüfen Sie, ob das VIB oder das Image-Profil, das Sie installieren möchten, erfordert, dass der Host in den Wartungsmodus versetzt oder nach der Installation oder dem Update neu gestartet wird.

Führen Sie einen der folgenden Befehle aus.

Option	Beschreibung
Überprüfen Sie das VIB	`esxcli --server=<server_name> software sources vib get -v <absolute_path_to_vib>`
Überprüfen Sie die VIBs in einem Depot	`esxcli --server=<server_name> software sources vib get --depot=<depot_name>`
Überprüfen Sie das Image-Profil in einem Depot	`esxcli --server=<server_name> software sources profile get --depot=<depot_name>`

2 Überprüfen Sie die Rückgabewerte.

Die Rückgabewerte, die aus den VIB-Metadaten gelesen werden, geben an, ob sich der Host vor der Installation des VIB oder Image-Profils im Wartungsmodus befinden muss und ob die Installation des VIB oder Profils einen Neustart des Hosts erfordert.

Hinweis vSphere Lifecycle Manager stützt sich auf eine interne ESXi-API zur Softwareüberprüfung, mit der ermittelt wird, 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 den vSphere Lifecycle Manager an, den Host neu zu starten. Wenn Sie ein VIB aus einem Live-System entfernen und der Wert für `Live-Remove-Allowed` auf „false“ festgelegt ist, weist das Ergebnis des Löschvorgangs vSphere Lifecycle Manager an, den Host neu zu starten. In beiden Fällen versetzt vSphere Lifecycle Manager den Host automatisch in den Wartungsmodus, wenn die Standardisierung gestartet wird.

Nächste Schritte

Versetzen Sie den Host, falls erforderlich, in den Wartungsmodus. Weitere Informationen hierzu finden Sie unter Versetzen eines Hosts in den Wartungsmodus. Falls ein Neustart erforderlich ist und der Host Bestandteil eines VMware HA-Clusters ist, müssen Sie vor der Installation oder dem Update den Host aus dem Cluster entfernen oder HA auf dem Cluster deaktivieren. Versetzen Sie den Host ebenfalls in den Wartungsmodus, um die Aktivität des Startlaufwerks während des Upgrades zu minimieren.

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.

Der Wartungsmodus wird benötigt, wenn für einen Aktualisierungsvorgang ein Neustart erforderlich ist. Der Host wird jedoch nur dann manuell in den Wartungsmodus versetzt, wenn Sie esxcli-Befehle für Aktualisierungs- und Upgrade-Vorgänge verwenden.

Informationen darüber, wie Sie feststellen können, ob sich bei einem Upgrade-Vorgang ein Host im Wartungsmodus befinden muss, finden Sie unter Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist

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 einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Prüfen Sie, ob sich der Host im Wartungsmodus befindet.

```
esxcli --server=<server_name> system maintenanceMode get
```

2 Schalten Sie alle auf dem ESXi-Host ausgeführten virtuellen Maschinen aus.

Hinweis Sie können alle aktiven virtuellen Maschinen auflisten und die World-ID jeder einzelnen Maschine abrufen, indem Sie den folgenden Befehl ausführen.

```
esxcli --server=<server_name> vm process list
```

Option	Befehl
So schalten Sie das Gastbetriebssystem und anschließend die virtuelle Maschine aus	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
So schalten Sie die virtuelle Maschine sofort aus	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`
So erzwingen Sie den Ausschaltvorgang	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

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.

```
esxcli --server=<server_name> system maintenanceMode set --enable true
```

4 Stellen Sie sicher, dass sich der Host im Wartungsmodus befindet.

```
esxcli --server=<server_name> system maintenanceMode get
```

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 über ein 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.

Hinweis Die Befehle `esxcli software vib update` und `esxcli software vib install` werden für Upgrade-Vorgänge nicht unterstützt. Weitere Informationen hierzu finden Sie unter Upgrade oder Update eines Hosts mit Image-Profilen .

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

- Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. 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 Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist. Weitere Informationen hierzu finden Sie unter Versetzen eines Hosts in den Wartungsmodus.
- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

1 Stellen Sie fest, welche VIBs auf dem Host installiert sind.

```
esxcli --server=<server_name> software vib list
```

2 Ermittlung, welche VIBs im Depot verfügbar sind.

Option	Beschreibung
Aus einem Depot, auf das über eine URL zugegriffen werden kann	`esxcli --server=<server_name> software sources vib list --depot=http://<web_server>/<depot_name>`
Aus der ZIP-Datei eines lokalen Depots	`esxcli --server=<server_name> software sources vib list --depot=<absolute_path_to_depot_zip_file>`

Sie können einen Proxy-Server mithilfe der Option `--proxy` 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	`esxcli --server=<server_name> software vib update --depot=http://<web_server>/<depot_name>`
Aktualisieren von VIBs von einer lokalen Depot-ZIP-Datei	`esxcli --server=<server_name> software vib update --depot=<absolute_path_to_depot_ZIP_file>`
Installation aller VIBs von einer ZIP-Datei auf einem angegebenen Offline-Depot (umfasst VMware-VIBs und von Partnern bereitgestellte VIBs)	`esxcli --server=<server_name> software vib install --depot <path_to_VMware_vib_ZIP_file>\<VMware_vib_ZIP_file> --depot <path_to_partner_vib_ZIP_file>\<partner_vib_ZIP_file>`

Mithilfe der Optionen für die Befehle `update` und `install` können Sie einen Testlauf durchführen, ein bestimmtes VIB angeben, die Verifizierung einer Akzeptanzebene umgehen usw. Umgehen Sie die Verifizierung nicht auf Produktionssystemen. Weitere Informationen finden Sie in der *ESXCLI-Referenz*.

4 Stellen Sie sicher, dass die VIBs auf Ihrem ESXi-Host installiert sind.

```
esxcli --server=<server_name> 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 Update oder Upgrade eines ESXi-Hosts durchzuführen.

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 (Haupt- oder Nebenversion) eines vollständigen Image-Profils auf den Host an. Nach diesem Vorgang und einem Neustart kann der Host einer vCenter Server-Umgebung mit derselben oder einer 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 mithilfe eines ISO-Installationsprogramms. Allerdings führt das ISO-Installationsprogramm eine Prüfung vor dem Upgrade auf potenzielle Probleme durch, z. B. nicht genügend Arbeitsspeicher oder nicht unterstützte Geräte. Die **`esxcli`**-Upgrade-Methode führt solche Überprüfungen nur durch, wenn ein Upgrade von ESXi 6.7 Update 1 oder höher auf eine neuere Version durchgeführt wird.

Hinweis Verwenden Sie die Option `--dry-run` nicht für Upgrades von ESXi 6.7.x und ESXi 7.0.x vor 7.0 Update 3i auf ESXi 8.0 und höher. Wenn die Option `--dry-run` entfernt wird, können Sie die esxcli-Upgrade-Methode weiterhin verwenden, um ein Upgrade von ESXi 6.7 Update 1 oder höher auf ESXi 8.0 oder höher durchzuführen. Für ESXi-Versionen vor 6.7 Update 1 müssen Sie zuerst ein Upgrade auf 6.7 Update 1 oder höher und anschließend ein Upgrade auf ESXi 8.0 oder höher durchführen.

Weitere Informationen über ESXi-Upgrade-Vorgang und -Methoden finden Sie unter Übersicht über den ESXiHost-Upgrade-Vorgang.

Wichtig Wenn Sie ESXi mithilfe eines ZIP-Pakets eines von VMware bereitgestellten Depots aktualisieren, auf das über die VMware-Website online zugegriffen oder das lokal heruntergeladen werden kann, unterstützt VMware nur den Aktualisierungsbefehl `esxcli software profile update --depot=<depot_location> --profile=<profile_name>`.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Hinweis Optionen für die Befehle `update` und `install` ermöglichen es Ihnen, einen Testlauf durchzuführen, die Verifizierung einer Akzeptanzebene zu umgehen, Warnungen der Hardwarekompatibilitätsprüfung zu ignorieren und so weiter. Die Option zum Umgehen der Warnungen der Hardwarekompatibilitätsprüfung ist nur für ESXi 6.7 Update 1 oder höher verfügbar. Umgehen Sie die Verifizierung nicht auf Produktionssystemen.

Um Hilfe zu den Optionen zu erhalten, geben Sie `esxcli software profile install --help` oder `esxcli software profile update --help` ein. Eine vollständige Liste der verfügbaren Befehlszeilenoptionen finden Sie unter ESXCLI-Referenz.

Voraussetzungen

- Installieren Sie eine eigenständige ESXCLI. Siehe *Erste Schritte mit ESXCLI*. 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 Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist. Weitere Informationen hierzu finden Sie unter Versetzen eines Hosts in den Wartungsmodus.

Wichtig Bei Verwendung von ESXCLI zum Aktualisieren des Hosts versetzen Sie den Host manuell in den Wartungsmodus, um sicherzustellen, dass die Startfestplatte vor Beginn des Upgrades nicht aktiv verwendet wird.

- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

1 Stellen Sie fest, welche VIBs auf dem Host installiert sind.

```
esxcli --server=<server_name> software vib list
```

2 Ermitteln Sie, welche Image-Profile im Depot verfügbar sind.

```
esxcli --server=<server_name> software sources profile list --depot=http://<web_server>/
<depot_name>
```

Sie können einen Proxy-Server mithilfe der Option `--proxy` 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 Zielserver installiert sind. Der Befehl `software profile install` installiert die VIBs, die sich momentan im Depot-Image-Profil befinden, und entfernt alle anderen auf dem Zielserver installierten VIBs.

Option	Beschreibung
Aktualisieren des Image-Profils aus einem von VMware bereitgestellten ZIP-Paket in einem Depot, auf das über die VMware-Website online zugegriffen werden kann oder das in ein lokales Depot heruntergeladen wurde	`esxcli software profile update --depot=<depot_location> --profile=<profile_name>` **Wichtig** Dies ist die einzige Update-Methode, die VMware für die von VMware gelieferten ZIP-Pakete bereitstellt. Die Namen der von VMware bereitgestellten ZIP-Pakete haben folgendes Format: `VMware-ESXi-<version_number>-<build_number>-depot.zip`. Der Profilname für die von VMware bereitgestellten ZIP-Pakete hat folgendes Format. ■ `ESXi-<version_number>-<build_number>-standard` ■ `ESXi-<version_number>-<build_number>-notools` (umfasst nicht die VMware Tools)
Aktualisieren des Image-Profils von einem Depot, auf das per URL zugegriffen werden kann	`esxcli --server=<server_name> software profile update --depot=http://<web_server>/<depot_name> --profile=<profile_name>`
Aktualisieren des Image-Profils von einer ZIP-Datei, die lokal auf dem Zielserver gespeichert ist	`esxcli --server=<server_name> software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Aktualisieren des Image-Profils von einer ZIP-Datei auf dem Zielserver, die in einen Datenspeicher kopiert wird	`esxcli --server=<server_name> software profile update --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Aktualisieren des Image-Profils von einer ZIP-Datei, die lokal auf dem Zielserver kopiert und angewendet wird	`esxcli --server=<server_name> software profile update --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Installation aller neuen VIBs eines angegebenen Profils, auf das per URL zugegriffen werden kann	`esxcli --server=<server_name> software profile install --depot=http://<web_server>/<depot_name> --profile=<profile_name>`
Installation aller neuen VIBs in einem angegebenen Profil von einer ZIP-Datei, die lokal auf dem Ziel gespeichert ist.	`esxcli --server=<server_name> software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`

Option	Beschreibung
Installation aller neuen VIBs von einer ZIP-Datei auf dem Zielserver, die in einen Datenspeicher kopiert wird	`esxcli --server=<server_name> software profile install --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Installation aller neuen VIBs von einer ZIP-Datei, die lokal auf den Zielserver kopiert und angewendet wird	`esxcli --server=<server_name> software profile install --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`

4 Stellen Sie sicher, dass die VIBs auf Ihrem ESXi-Host installiert sind.

```
esxcli --server=<server_name> 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 ein ESXi-Upgrade oder -Update von einem ZIP-Paket eines von VMware bereitgestellten Depots durchführen, auf das über die VMware-Website online zugegriffen werden kann oder das lokal heruntergeladen wurde, unterstützt VMware die Befehle `esxcli software vib update` und `esxcli software vib install` nicht. VMware unterstützt nur die Update- und Upgrade-Methoden, die für von VMware bereitgestellte Depots im Thema Upgrade oder Update eines Hosts mit Image-Profilen angegeben sind. Wenn das Depot nicht von VMware bereitgestellt wird und über kein Image-Profil verfügt, können Sie die Befehle `esxcli software vib update` und `esxcli software vib install` für einzelne oder mehrere VIB-Updates verwenden, wie unter Aktualisieren eines Hosts mit einzelnen VIBs und dem Verfahren in diesem Thema beschrieben.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

- Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. 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 Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist. Weitere Informationen hierzu finden Sie unter Versetzen eines Hosts in den Wartungsmodus.
- Falls für das Update ein Neustart erforderlich ist und der Host Bestandteil eines vSphere HA-Clusters ist, entfernen Sie den Host aus dem Cluster oder deaktivieren Sie HA auf dem Cluster.

Verfahren

- Installieren Sie die ZIP-Datei.

```
esxcli --server=<server_name> software vib update --depot=/<path_to_vib_ZIP>/
<ZIP_file_name>.zip
```

Entfernen von VIBs von einem Host

Sie können VIBs von Drittanbietern oder VMware-VIBs von Ihrem ESXi-Host deinstallieren, es sei denn, das VIB ist Teil einer Komponente, die für den ESXi-Lebenszyklus oder einen Treiber erforderlich ist.

VMware-Partner bereiten VIBs von Drittanbietern so vor, dass sie Verwaltungsagenten oder asynchron freigegebene Treiber bereitstellen.

Wichtig Ab ESXi 8.0 Update 2 kann das Entfernen einiger VIBs aus ihren Komponenten zu Laufzeitproblemen mit ESXi führen.

Tabelle 3-11. VIBs, die für ESXi Image-Vollständigkeit erforderlich sind.

Komponente	VIBs
ESXi	bmcal
	bmcal-esxio
	clusterstore
	cpu-microcode
	crx
	drivervm-gpu
	esx-base
	esx-dvfilter-generic-fastpath
	esx-ui
	esx-xserver
	esxio
	esxio-base
	esxio-combiner
	esxio-combiner-esxio
	esxio-dvfilter-generic-fastpath
	gc
	gc-esxio
	native-misc-drivers
	infravisor
	native-misc-drivers-esxio
	pensandoatlas
	trx
	vdfs
	vsan
	vsanhealth
esx-update	esx-update
	loadesx
esxio-update	esxio-update
	loadesxio
Intel-ne1000	ne1000

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Voraussetzungen

- Wenn für das Entfernen ein Neustart erforderlich ist und der Host Bestandteil eines vSphere 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.

  Siehe Prüfen, ob für ESXi Host-Update der Wartungsmodus oder ein Neustart erforderlich ist. Weitere Informationen hierzu finden Sie unter Versetzen eines Hosts in den Wartungsmodus.

  Hinweis Versetzen Sie den Host manuell in den Wartungsmodus, um sicherzustellen, dass die Startfestplatte nicht aktiv verwendet wird, wenn Sie ESXCLI zum Aktualisieren des Hosts verwenden.

- Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Schalten Sie alle auf dem ESXi-Host ausgeführten virtuellen Maschinen aus.

Hinweis Sie können alle aktiven virtuellen Maschinen auflisten und die World-ID jeder einzelnen Maschine abrufen, indem Sie den folgenden Befehl ausführen.

```
esxcli --server=<server_name> vm process list
```

Option	Befehl
So schalten Sie das Gastbetriebssystem und anschließend die virtuelle Maschine aus	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
So schalten Sie die virtuelle Maschine sofort aus	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`
So erzwingen Sie den Ausschaltvorgang	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

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.

```
esxcli --server=<server_name> system maintenanceMode set --enable true
```

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=<server_name> software vib list
```

5 Entfernen Sie das VIB.

```
esxcli --server=<server_name> software vib remove --vibname=<name>
```

Geben Sie ein oder mehrere zu entfernende VIBs in einem der folgenden Formate an:

- *<name>*
- *<name>*:*<version>*
- *<vendor>*:*<name>*
- *<vendor>*:*<name>*:*<version>*

Der Befehl zum Entfernen eines VIB, der nach Hersteller, Name und Version angegeben wird, kann beispielsweise folgendes Format aufweisen:

```
esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
```

Hinweis Der Befehl `remove` unterstützt verschiedene weitere Optionen. Weitere Informationen finden Sie unter *ESXCLI – Referenz*.

Hinzufügen von Drittanbietererweiterungen zu Hosts mit einem ESXCLI-Befehl

Sie können den Befehl `esxcli software vib` verwenden, um dem System eine als VIB-Paket freigegebene Drittanbietererweiterung hinzuzufügen.

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 die Ergebnisse eines Installations- oder Upgrade-Vorgangs in der Vorschau anzuzeigen.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Bei einer Testinstallation bzw. einem Test-Upgrade werden keine Änderungen vorgenommen. Es werden lediglich die Vorgänge auf VIB-Ebene protokolliert, die durchgeführt werden, wenn Sie den Befehl ohne die Option `--dry-run` ausführen.

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Geben Sie den Installations- bzw. Upgrade-Befehl zusammen mit der Option `--dry-run` ein.

- `esxcli --server=<server_name> software vib install --dry-run`
- `esxcli --server=<server_name> software vib update --dry-run`
- `esxcli --server=<server_name> software profile install --dry-run`
- `esxcli --server=<server_name> software profile update --dry-run`

2 Prüfen Sie die Ausgabe, die zurückgegeben wird.

Die Ausgabe zeigt die zu installierenden oder zu entfernenden VIBs sowie Informationen dazu an, ob für die Installation bzw. das Upgrade ein Neustart erforderlich ist.

Auflisten der verfügbaren VIBs und Profile nach dem Neustart des Hosts

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 einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Geben Sie einen der folgenden Befehle ein.

Option	Beschreibung
Für VIBs	`esxcli --server=<server_name> software vib list --rebooting-image`
Für Profile	`esxcli --server=<server_name> software profile get --rebooting-image`

2 Prüfen Sie die Ausgabe, die zurückgegeben wird.

Die Ausgabe zeigt Informationen für das ESXi-Image an, das nach dem nächsten Neustart aktiv wird. Wenn das Image „Ausstehender Neustart“ noch nicht erstellt wurde, gibt die Ausgabe nichts zurück.

Anzeigen des Image-Profils 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-Profils an, wie z. B. Profiländerungen.

Wenn Sie einen Zielserver mit `--server=<server_name>` angeben, werden Sie vom Server zu Eingabe eines Benutzernamens und Kennworts aufgefordert. Weitere Verbindungsoptionen, wie z. B. eine Konfigurations- oder Sitzungsdatei, werden unterstützt. Eine Liste der Verbindungsoptionen finden Sie unter Erste Schritte mit ESXCLI. Alternativ können Sie auch `esxcli --help` an der ESXCLI-Befehlszeile ausführen.

Voraussetzungen

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter Erste Schritte mit ESXCLI. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Verfahren

1 Geben Sie den folgenden Befehl ein.

```
esxcli --server=<server_name> 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 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 8.0-Lizenz zuweisen, bevor der Testzeitraum abläuft. Sie können vorhandene Lizenzen aktualisieren oder bei My VMware neue erwerben. Verwenden Sie vSphere 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 8.0 nicht kompatibel. Informationen zum Konfigurieren des vSphere Authentication Proxy-Diensts finden Sie im Handbuch *vSphere-Sicherheit*.

Grundlegendes zum ESXi-Testmodus und -Lizenzmodus

Sie können im Testmodus eine Reihe von Funktionen erkunden, die der vSphere Enterprise Plus-Lizenz entsprechen.

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.

Für ESXi-Hosts führt der Ablauf des Lizenzierungs- oder Testzeitraums dazu, dass die Verbindung mit vCenter Server getrennt wird. Alle eingeschalteten virtuellen Maschinen werden weiterhin ausgeführt, virtuelle Maschinen können jedoch nach dem Ausschalten nicht mehr eingeschaltet werden. Sie können die aktuelle Konfiguration der bereits verwendeten Funktionen ändern. Sie können die Funktionen, die vor dem Ablauf der Lizenz ungenutzt blieben, nicht verwenden.

Informationen zur Lizenzierung für ESXi-Hosts finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Lizenzierung von ESXi-Hosts nach dem Upgrade

Nach einem Upgrade auf ESXi 8.0 müssen Sie eine vSphere 8-Lizenz anwenden.

Wenn Sie einen ESXi-Host auf eine Version aktualisieren, die mit derselben Nummer beginnt, brauchen Sie die vorhandene Lizenz nicht durch eine neue zu ersetzen. Wenn Sie beispielsweise einen Host von ESXi 6.5 auf 6.7 upgraden, können Sie die gleiche Lizenz auf dem Host beibehalten.

Wenn Sie ein Upgrade von ESXi auf eine Version durchführen, die mit einer anderen Nummer beginnt, müssen Sie eine neue Lizenz anwenden. Wenn Sie beispielsweise ein Upgrade eines ESXi-Hosts von Version 7.x auf 8.0 durchführen, müssen Sie den Host mit einer vSphere 8-Lizenz lizenzieren.

Beim Upgrade von ESXi 6.7- oder ESXi 7.0-Hosts auf ESXi 8.0-Hosts gilt für die Hosts ein Testzeitraum von 60 Tagen bis zur Anwendung der eigentlichen vSphere 8-Lizenzen. Weitere Informationen hierzu finden Sie unter Grundlegendes zum ESXi-Testmodus und -Lizenzmodus.

Sie können vSphere 8-Lizenzen von My VMware erwerben. Wenn Sie über vSphere 8-Lizenzen verfügen, müssen Sie diese auf alle aktualisierten ESXi 8.0-Hosts mithilfe der Lizenzmanagementfunktion im vSphere Client anwenden. Weitere Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*. Wenn Sie für das Upgrade auf ESXi 8.0die Skriptmethode verwenden, können Sie den Lizenzschlüssel in der Kickstart-Datei (ks) angeben.

Ausführen des Secure Boot-Validierungsskripts nach dem ESXi-Upgrade

Nach dem Upgrade eines ESXi-Hosts von einer Version, die UEFI Secure Boot nicht unterstützt, müssen Sie überprüfen, ob Sie den sicheren Start aktivieren können.

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.

- Wenn Sie das Upgrade mithilfe von ESXCLI-Befehlen durchführen, führt die alte Version von ESXi die Installation der neuen VIBs durch, sodass ihre Signaturen nicht gespeichert werden und ein sicherer Start (Secure Boot) nicht möglich ist.

- Wenn Sie das Upgrade mithilfe des ISO-Images durchführen, werden die Signaturen der neuen VIBs gespeichert. Dies gilt auch für vSphere Lifecycle Manager-Upgrades, die das ISO-Image verwenden.
- Wenn alte VIBs auf dem System verbleiben, stehen die Signaturen dieser VIBs nicht zur Verfügung und ein sicherer Start ist nicht möglich.
  - Wenn das System 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

Nach dem Upgrade eines ESXi-Hosts von einer früheren ESXi-Version, die UEFI Secure Boot nicht unterstützte, können Sie möglicherweise 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 unverändert belassen wurden. Sie können nach der Durchführung des Upgrades ein Validierungsskript ausführen, um festzustellen, ob der sichere Start von der aktualisierten Installation unterstützt wird.

- 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.

Verfahren

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`.

Konfiguration von Syslog auf ESXi-Hosts

Sie können den vSphere Client, den VMware Host Client oder den Befehl `esxcli system syslog` zum Konfigurieren des Syslog-Diensts verwenden.

Der syslog-Dienst empfängt, kategorisiert und speichert Protokollmeldungen für Analysen, anhand derer Sie vorbeugende Maßnahmen in Ihrer Umgebung ergreifen können.

Festlegen von ESXi Syslog mithilfe des vSphere Client

Sie können den Befehl vSphere Client verwenden, um den Syslog-Dienst global zu konfigurieren und verschiedene erweiterte Einstellungen zu bearbeiten.

Verfahren

1. Navigieren Sie zum ESXi-Host in der Bestandsliste von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten**.
5. Filter für **`syslog`**.
6. Informationen zum globalen Einrichten der Protokollierung und zur Konfiguration verschiedener erweiterter Einstellungen finden Sie unter ESXi-Syslog-Optionen.
7. (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. Geben Sie die Anzahl der Rotationen und die gewünschte Protokollgröße ein.
8. Klicken Sie auf **OK**.

Ergebnisse

Änderungen an den syslog-Optionen werden sofort wirksam.

Hinweis Mithilfe des vSphere Client oder VMware Host Client definierte Einstellungen für Syslog-Parameter werden sofort wirksam. Die meisten mithilfe von ESXCLI definierten Einstellungen benötigen jedoch einen zusätzlichen Befehl, um wirksam zu werden. Weitere Informationen finden Sie unter ESXi-Syslog-Optionen.

Festlegen von ESXi Syslog mithilfe des VMware Host Client

Sie können den VMware Host Client verwenden, um Parameter des Syslog-Diensts auf ESXi-Hosts zu konfigurieren und zu bearbeiten.

Verfahren

1. Klicken Sie im VMware Host Client unter **Host** auf **Verwaltung > System > Erweiterte Einstellungen**.
2. Geben Sie im Bereich **Suche** die zu definierende Syslog-Einstellung ein. Weitere Informationen erhalten Sie unter ESXi Syslog-Optionen.
3. Wählen Sie die Einstellung aus und klicken Sie auf **Option bearbeiten**.
4. Legen Sie den Wert wie in der Parametertabelle unter ESXi Syslog-Optionen beschrieben fest.

5 Klicken Sie auf **Speichern**.

Festlegen von ESXi Syslog mithilfe von ESXCLI

Sie können den Syslog-Dienst auf ESXi-Hosts mithilfe des ESXCLI-Befehls konfigurieren: `esxcli system syslog config set <syslog option>`.

Voraussetzungen

Informationen zur Verwendung des Befehls „esxcli system syslog“ und anderer ESXCLI-Befehle finden Sie unter Erste Schritte mit ESXCLI. Weitere Informationen zum Öffnen der ESXi Firewall für den in jeder Remotehostspezifikation angegebenen Port finden Sie unter Konfigurieren der ESXi Firewall.

Hinweis Für die Verwendung von ESXCLI ist ESXi zum Öffnen von SSH-Anmeldungen erforderlich. Dies stellt ein Sicherheitsrisiko dar und wird daher nicht empfohlen. Wenn Sie ESXCLI verwenden möchten, stellen Sie sicher, dass Sie den Befehl `esxcli system syslog reload` nach dem Festlegen der einzelnen Parameter nutzen. So ist gewährleistet, dass dieser wirksam wird.

Verfahren

- Verwenden Sie den ESXCLI-Befehl `esxcli system syslog config set <syslog option>`, um eine Syslog-Option festzulegen, die Sie aktivieren möchten. Um beispielsweise die Option `Syslog.global.logHost` festzulegen, verwenden Sie den Befehl `esxcli system syslog config set --loghost=<str>`.

  Nach dem Festlegen von `Syslog.global.logHost` öffnen und halten ESXi-Hosts Verbindungen zu den Syslog-Collectors, und die Übertragung von Meldungen beginnt sofort. Wenn ESXi eine Syslog-Meldung generiert, wird sie in die entsprechende Protokolldatei auf dem ESXi-Host geschrieben und an alle konfigurierten Syslog-Collectors weitergeleitet.

ESXi-Syslog-Optionen

Sie können das Verhalten von ESXi-Syslog-Dateien und -Übertragungen mithilfe mehrerer Syslog-Optionen definieren.

Neben den Basiseinstellungen, wie z. B. `Syslog.global.logHost`, steht ab ESXi 7.0 Update 1 eine Liste mit erweiterten Optionen für Anpassungen und NIAP-Konformität zur Verfügung.

Hinweis Konfigurieren Sie dauerhaften Speicher immer, bevor Sie Überwachungsdatensatzparameter oder den `Syslog.global.logDir`-Parameter festlegen.

Hinweis Alle Einstellungen für Überwachungsdatensätze, die mit `Syslog.global.auditRecord` beginnen, werden sofort wirksam. Für andere Einstellungen, die Sie mithilfe von ESXCLI definieren, müssen Sie zum Aktivieren der Änderungen jedoch den Befehl `esxcli system syslog reload` ausführen.

Tabelle 3-12. Legacy-Syslog-Optionen

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logHost`	`esxcli system syslog config set --loghost=<str>`	Definiert eine kommagetrennte Liste mit Remotehosts und Spezifikationen für Meldungsübertragungen. Wenn das Feld `loghost=<str>` leer ist, werden keine Protokolle weitergeleitet. Obwohl es keinen festen Grenzwert für die Anzahl der Remotehosts gibt, die Syslog-Meldungen empfangen, wird dennoch empfohlen, die Anzahl der Remotehosts auf fünf oder weniger zu begrenzen. Das Format einer Remotehostspezifikation lautet: `protocol://hostname|ipv4|'['ipv6']'[:port]`. Als Protokoll muss TCP, UDP oder SSL verwendet werden. Der Wert eines Ports kann eine beliebige Zahl zwischen 1 und 65535 sein. Wenn kein Port angegeben wird, wird 1514 von SSL und TCP verwendet. UDP verwendet 514. Beispiel: `ssl://hostName1:1514`.
`Syslog.global.defaultRotate`	`esxcli system syslog config set --default-rotate=<long>`	Maximale Anzahl alter beizubehaltender Protokolldateien Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen (siehe `Syslog.global.defaultSize`).
`Syslog.global.defaultSize`	`esxcli system syslog config set --default-size=<long>`	Standardgröße der Protokolldateien in KiB. Nachdem eine Datei die Standardgröße erreicht hat, erstellt der Syslog-Dienst eine neue Datei. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.

Tabelle 3-12. Legacy-Syslog-Optionen (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logDir`	`esxcli system syslog config set --logdir=<str>`	Verzeichnis, in dem sich Protokolle befinden. 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 [*Datenspeichername*] *Pfad_zur_Datei* an, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad `[storage1] /systemlogs` dem Pfad `/vmfs/volumes/storage1/systemlogs` zuzuordnen.
`Syslog.global.logDirUnique`	`esxcli system syslog config set --logdir-unique=<bool>`	Gibt den Namen des ESXi-Hosts an, der mit dem Wert von `Syslog.global.logDir` verknüpft werden soll. Diese Einstellung muss aktiviert werden, wenn sich mehrere ESXi-Hosts bei einem gemeinsam genutzten Dateisystem anmelden. 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.certificate.checkSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Erzwingt die Überprüfung von SSL-Zertifikaten bei der Übertragung von Nachrichten an Remotehosts.

Tabelle 3-13. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.auditRecord.storageCapacity`	`esxcli system auditrecords local set --size=<long>`	Gibt die Kapazität des Verzeichnisses zum Speichern von Überwachungsdatensätzen auf dem ESXi-Host in MiB an. Sie können die Kapazität des Überwachungsdatensatzspeichers nicht verringern. Sie können die Kapazität vor oder nach der Aktivierung des Überwachungsdatensatzspeichers erhöhen (siehe `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Ermöglicht das Senden von Überwachungsdatensätzen an Remotehosts. Remotehosts werden mithilfe des Parameters `Syslog.global.logHost` angegeben.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Erstellt ein Verzeichnis zum Speichern von Überwachungsdatensätzen und legt `/scratch/auditLog` als Standardspeicherort fest. Sie dürfen kein Verzeichnis zur Speicherung von Überwachungsdatensätzen manuell erstellen, und das Verzeichnis für den Überwachungsdatensatzspeicher kann nicht geändert werden, solange der Überwachungsdatensatzspeicher aktiviert ist (siehe `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Aktiviert die Speicherung von Überwachungsdatensätzen auf einem ESXi-Host. Wenn das Verzeichnis zum Speichern von Überwachungsdatensätzen nicht vorhanden ist, wird es mit der von `Syslog.global.auditRecord.storageCapacity` angegebenen Kapazität erstellt.

Tabelle 3-13. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Ermöglicht die Überprüfung des Widerrufstatus aller Zertifikate in einer SSL-Zertifikatskette. Ermöglicht die Überprüfung von X.509-CRLs, die in Übereinstimmung mit den Branchenkonventionen nicht standardmäßig überprüft werden. Eine mit NIAP validierte Konfiguration benötigt CRL-Prüfungen. Wenn CRL-Prüfungen aktiviert sind, müssen alle Zertifikate in einer Zertifikatskette aufgrund von Implementierungseinschränkungen einen CRL-Link bereitstellen. Aktivieren Sie die Option `crl-check` nicht für Installationen ohne Bezug zur Zertifizierung, da sich die ordnungsgemäße Konfiguration einer Umgebung, die CRL-Prüfungen verwendet, als schwierig erweist.
`Syslog.global.certificate.strictX509Compliance`	`esxcli system syslog config set --x509-strict=<bool>`	Aktiviert strikte Übereinstimmung mit X.509. Führt während der Überprüfung zusätzliche Gültigkeitsprüfungen für CA-Stammzertifikate durch. Diese Prüfungen werden in der Regel nicht durchgeführt, da CA-Roots inhärent vertrauenswürdig sind und Inkompatibilitäten mit vorhandenen, falsch konfigurierten CA-Roots verursachen können. Eine mit NIAP validierte Konfiguration benötigt CA-Roots sogar, um Validierungen erfolgreich zu durchlaufen. Aktivieren Sie die Option `x509-strict` nicht für Installationen ohne Bezug zur Zertifizierung, da sich die ordnungsgemäße Konfiguration einer Umgebung, die CRL-Prüfungen verwendet, als schwierig erweist.
`Syslog.global.droppedMsgs.fileRotate`	`esxcli system syslog config set --drop-log-rotate=<long>`	Gibt die Anzahl der beizubehaltenden Protokolldateien mit alten gelöschten Meldungen an.
`Syslog.global.droppedMsgs.fileSize`	`esxcli system syslog config set --drop-log-size=<long>`	Gibt die Größer aller Protokolldateien mit gelöschten Meldungen vor dem Wechsel zu einer neuen Datei in KiB an.

Tabelle 3-13. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.logCheckSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Erzwingt die Überprüfung von SSL-Zertifikaten bei der Übertragung von Nachrichten an Remotehosts. **Hinweis** Veraltet. Verwenden Sie `Syslog.global.certificate.checkSSLCerts` in ESXi 7.0 Update 1 und höher.
`Syslog.global.logFilters`	`esxcli system syslog config logfilter [add | remove | set] ...`	Gibt eine oder mehrere Spezifikationen für die Protokollfilterung an. Alle Protokollfilter müssen durch einen doppelten vertikalen Balken (||) getrennt werden. Das Format eines Protokollfilters lautet: `numLogs | ident | logRegexp`. `numLogs` legt die maximale Anzahl von Protokolleinträgen für die angegebenen Protokollmeldungen fest. Nach Erreichen dieses Werts werden die angegebenen Protokollmeldungen gefiltert und ignoriert. `ident` gibt eine oder mehrere Systemkomponenten an, um den Filter auf die Protokollmeldungen anzuwenden, die von diesen Komponenten erzeugt werden. `logRegexp` gibt eine Zeichenfolge unter Beachtung der Groß-/Kleinschreibung mit Python-Syntax für reguläre Ausdrücke an, um die Protokollmeldungen anhand ihres Inhalts zu filtern.
`Syslog.global.logFiltersEnable`		Aktiviert die Verwendung von Protokollfiltern.
`Syslog.global.logLevel`	`esxcli system syslog config set --log-level=<str>`	Gibt die Ebene der Protokollfilterung an. Sie müssen diesen Parameter nur bei der Behebung eines Problems mit dem Syslog-Daemon ändern. Sie können den Wert `debug` für die Ebene mit den meisten Details, den Wert `info` für die Ebene mit Standarddetails, den Wert `warning` für Warnungen bzw. Fehler oder den Wert `error` für Fehler verwenden.
`Syslog.global.msgQueueDropMark`	`esxcli system syslog config --queue-drop-mark=<long>)`	Gibt den Prozentsatz der Kapazität der Meldungswarteschlange an, ab dem Meldungen verworfen werden.

Tabelle 3-13. Verfügbare Syslog-Optionen ab ESXi 7.0 Update 1 (Fortsetzung)

Option	ESXCLI-Befehl	Beschreibung
`Syslog.global.remoteHost.connectRetryDelay`	`esxcli system syslog config set --default-timeout=<long>`	Gibt die Verzögerung in Sekunden vor dem erneuten Versuch einer Verbindungsherstellung mit einem Remotehost an, nachdem ein Verbindungsversuch fehlgeschlagen ist.
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	Für die TCP- und SSL-Protokolle gibt dieser Parameter die maximale Länge einer Syslog-Übertragung vor dem Auftreten von Kürzungen in Byte an. Die maximale Standardlänge für Meldungen von Remotehosts beträgt 1 KiB. Sie können die maximale Nachrichtenlänge auf bis zu 16 KiB erhöhen. Bei einer Erhöhung dieses Werts auf über 1 KiB ist es jedoch möglich, dass lange Übertragungen gekürzt bei einem Syslog-Collector ankommen. Beispiel: Die Syslog-Infrastruktur, die eine Meldung ausgibt, befindet sich außerhalb von ESXi. Diese Einstellung hat keinen Einfluss auf das UDP-Protokoll. RFC 5426 legt die maximale Nachrichtenübertragungslänge für das UDP-Protokoll auf 480 Byte für IPV4 und 1180 Byte für IPV6 fest. Aufgrund dieser Einschränkung und da UDP-Pakete von der Netzwerkinfrastruktur willkürlich verworfen werden können, wird die Verwendung von UDP für die Übertragung kritischer Syslog-Nachrichten nicht empfohlen.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Ermöglicht das Platzieren von Protokolldateien sowie des Verzeichnisses zum Speichern von Überwachungsdatensätzen in einem vSAN-Cluster. Die Aktivierung dieses Parameters kann jedoch dazu führen, dass der ESXi-Host nicht mehr reagiert.

Feinabstimmung von Syslog auf ESXi-Hosts

Durch die Verwendung der richtigen Syslog-Einstellungen können Sie eine proaktive Überwachung Ihrer Umgebung erreichen, Ausfallzeiten reduzieren und vorbeugende Maßnahmen auf Servern ergreifen.

Beim Einrichten von syslog müssen Sie mehrere Parameter berücksichtigen, die sich auf die Aufbewahrung von Protokolldateien, die Syslog-Übertragung, die Übertragungslänge, die Fehlerbehandlung und die Einrichtung von SSL-Zertifikaten für die sichere Syslog-Meldungsübertragung auswirken. Nachfolgend finden Sie Empfehlungen für die Optimierung Ihrer Syslog-Parameter. Eine Beschreibung aller verfügbaren Parameter wird unter ESXi-Syslog-Optionen angezeigt.

Vorgehensweise zum Festlegen der Aufbewahrung von Protokolldateien

Standardmäßig können Protokolldateien nicht über eine konfigurierte Größe hinaus erweitert werden. Sobald eine Protokolldatei die konfigurierte Größe erreicht, wird die Protokollierung zu einer neuen Protokolldatei weitergeleitet und die älteste Protokolldatei wird gelöscht.

Hinweis Es wird empfohlen, die Rotations- und Größeneinstellungen auszugleichen. Durch das Erhöhen der Einstellung „Rotieren“ wird sichergestellt, dass syslog-Dateien oft genug generiert werden, um eine potenzielle Beschädigung oder Zerstörung durch die anderen Protokolldateien zu verhindern. Durch das Erhöhen der Größeneinstellung wird die Zeit für den Wechsel zu einer anderen Protokolldatei reduziert. Optimale Größeneinstellungen sind ein Vielfaches von 1.024 KiB.

Verwenden Sie die Einstellung `Syslog.global.defaultSize`, um die maximale Größe der Protokolldateien in KiB anzugeben, und `Syslog.global.defaultRotate`, um die maximale Anzahl alter Protokolldateien festzulegen, die beibehalten werden sollen, bevor sie in eine neue Protokolldatei rotieren. Um die Parameter für die Aufbewahrung von Protokolldateien für ein bestimmtes Programm zu ändern, verwenden Sie `Syslog.loggers.<progName>.rotate` und `Syslog.loggers.<progName>.size settings`, wobei `<progName>` der Name des Programms ist, dessen Parameter Sie anpassen möchten.

Verwalten von Einstellungen, die sich auf die Protokolldatei der virtuellen Maschine auswirken

Sie können einige Einstellungen, die sich auf die Protokolldatei der virtuellen Maschine, `vmware.log`, auswirken, entweder in der Datei `vmx`-Datei oder in der Datei `/etc/vmware/config` konfigurieren. Sie müssen eine virtuelle Maschine ausschalten, um die Datei `vmx`-Datei bearbeiten zu können. Diese Änderungen werden nur auf dieser virtuellen Maschine wirksam. Wenn Sie die Datei `/etc/vmware/config` verwenden, müssen Sie der Einstellung das Präfix *„vmx“* hinzufügen, z. B. `vmx.log.keepOld = "20"`. Änderungen wirken sich auf alle virtuellen Maschinen auf dem ESXi-Host aus.

Tabelle 3-14. Konfigurierbare Einstellungen für die vmware.log-Datei

Parameter	Beschreibung	Beispiel	Anmerkungen
`logging`	Deaktiviert die gesamte Protokollierung virtueller Maschinen.	Der Standardwert ist `logging = "TRUE"`. So deaktivieren Sie die Protokollierung virtueller Maschinen: `logging = "FALSE"`	Verwenden Sie diese Einstellung nicht, da die Deaktivierung der Protokollierung virtueller Maschinen es extrem schwierig oder unmöglich macht, Unterstützung bei Problemen mit virtuellen Maschinen zu erhalten. Wenn Sie diese Einstellung aus irgendeinem Grund verwenden müssen, können Sie sie nur in der `vmx`-Datei einer virtuellen Maschine ablegen.

`log.throttleBytesPerSec`	Zur Steuerung, wann eine Protokolldatei drosselt. Die Protokolldateidrosselung tritt auf, wenn Schreibvorgänge in `vmware.log` die festgelegte Rate für einen längeren Zeitraum überschreiten. Dies tritt auf, wenn Code innerhalb des VMX-Prozesses, der eine virtuelle Maschine steuert, übermäßig viele Protokollmeldungen erstellt. Der Standardwert für dieser Einstellungen ist 1 KB/s.
	Im Falle von Protokolldrosselungen wird in der Datei `vmware.log` `<<< Protokoll gedrosselt >>>` angezeigt.
		`log.throttleBytesPerSec = "1500"`
		Um die Protokolldrosselung zu deaktivieren, verwenden Sie
		`log.throttleBytesPerSec = "0xFFFFFFFF"`
			Die Protokolldateidrosselung unterdrückt möglicherweise Informationen, die zur Diagnose von Problemen mit der betroffenen virtuellen Maschine erforderlich sind. Wenn Sie die Protokolldrosselung deaktivieren müssen, platzieren Sie die Zeile aus dem Beispiel in der Datei `vmx`-Datei der betroffenen virtuellen Maschine. Entfernen Sie die Zeile, wenn die Debugging-Sitzung beendet ist.

`log.keepOld`	Steuert die Anzahl der aufzubewahrenden älteren `vmware.log`-Dateien.	`log.keepOld = "20"`	Setzen Sie den Wert dieser Einstellung nicht unter den Standardwert (10). Wenn virtuelle Maschinen häufig verändert oder verschoben werden, sollten Sie diese Einstellung auf 20 oder mehr erhöhen.

Tabelle 3-14. Konfigurierbare Einstellungen für die vmware.log-Datei (Fortsetzung)

Parameter	Beschreibung	Beispiel	Anmerkungen

`log.rotateSize`	Steuert die maximale Größe einer `vmware.log`-Datei in Bytes.	`log.rotateSize = "2500000"`
		Um die Beschränkung der maximalen Größe einer `vmware.log`-Datei zu deaktivieren, verwenden Sie
		`log.rotateSize = "0"`
			Ein Wert dieser Einstellung unter 100.000 kann zu einem Verlust relevanter Protokollmeldungen führen und die Leistung der virtuellen Maschine beeinträchtigen. In ESXi 7.x und früher wird die Größe einer `vmware.log`-Datei nicht durch den Standardwert dieser Einstellung begrenzt. In ESXi 8.x und höher ist der Standardwert dieser Einstellung 2048000.

`log.fileName`	Steuert den Namen und den Speicherort der Protokolldateien der virtuellen Maschine.	`log.fileName = "myVMLog"`
		Mit dieser Einstellung wird der Name der Protokolldateien der virtuellen Maschine von vmware.log in `myVMlog` geändert.
		`log.fileName = "/vmfs/volumes/vol1/myVM/myVM.log"`
		Diese Einstellung leitet Protokolldateien der virtuellen Maschine in ein Verzeichnis auf einem anderen VMFS- Volume (vol1) weiter, wobei `myVM` für einen Dateinamen verwendet wird.
			Speichern Sie keine Protokolldatei außerhalb des Verzeichnisses der virtuellen Maschine, um sicherzustellen, dass die Erfassung von Host-Support-Paketen die Protokolldatei übernimmt, was für das Debuggen von Problemen bei virtuellen Maschinen entscheidend sein kann.

Tabelle 3-14. Konfigurierbare Einstellungen für die vmware.log-Datei (Fortsetzung)

Parameter	Beschreibung	Beispiel	Anmerkungen
`log.fileLevel`	Steuert die Mindestebene, auf der Nachrichten in `vmware.log` geschrieben werden. Jeder Protokollmeldung ist eine Ebene zugeordnet. Ebenen unterhalb der angegebenen Einstellung werden keiner Protokolldatei der virtuellen Maschine hinzugefügt. Die Protokollierungsebenen für Nachrichten der virtuellen Maschine (von der am meisten bis zu der am wenigsten eingeschränkten) lauten: ■ Fehler ■ Warnung ■ Hinweis ■ Info (Standard) ■ Ausführlich (erweitert) ■ Debuggen ■ debug1 ■ debug2 ■ debug3 ■ debug4 ■ debug5 ■ debug6 ■ debug7 ■ debug8 ■ debug9 ■ debug10	`log.fileLevel = "debug1"`	Legen Sie die Ebene nicht auf eine eingeschränktere Ebene als „Info“ fest, um das Herausfiltern von Meldungen zu vermeiden, die zum Debuggen von Problemen bei virtuellen Maschinen erforderlich sind. Verringern Sie die Ebene unterhalb von „Info“ nur auf Anforderung durch den lizenzierten Support. Stellen Sie die Einstellung auf „Info“ wieder her, nachdem das Debugging beendet wurde.
`log.filter.minLogLevel.<groupName>`	Steuert die Ausgabe spezieller Debugging-Meldungen.	`log.filter.minLogLevel.disklib = "debug5"`	Verwenden Sie diese Einstellung nur auf Anforderung durch den lizenzierten Support, der einen oder mehrere `<groupName>`-Parameter bereitstellen sollte. Entfernen Sie die Einstellung, nachdem das Debugging beendet wurde.

Tabelle 3-14. Konfigurierbare Einstellungen für die vmware.log-Datei (Fortsetzung)

Parameter	Beschreibung	Beispiel	Anmerkungen
`log.sysogID`	Ermöglicht das Senden von Protokollmeldungen der virtuellen Maschine an die Systemprotokollierung eines ESXi-Hosts, wie z. B. Syslog.	`log.syslogID = "vmx"`	Verwenden Sie "`vmx`" als Wert für diese Einstellung, damit der ESXi-Syslog-Daemon `vmsyslogd` diese Meldungen in eine separate Protokolldatei senden kann.
`log.syslogLevel`	Steuert die Mindestebene, auf der Meldungen an die Systemprotokollierung eines ESXi-Hosts ausgegeben werden, z. B. Syslog.	`log.syslogLevel = "debug"`	Die Ebenen und die Funktionsweise dieser Einstellung sind identisch mit denen für die `log.fileLevel`-Einstellung.

Vorgehensweise zum Festlegen der Nachrichtenübertragung an Remotehosts

Optional können Sie ESXi so konfigurieren, dass syslog-Meldungen an einen oder mehrere Remotehosts gesendet werden, die als Syslog-Collectors bezeichnet werden, wie z. B. VMware vRealize Log Insight (früher vCenter Log Insight), um Syslog-Meldungen zu erfassen.

Hinweis Es wird empfohlen, dass Sie jeden ESXi-Hosts so konfigurieren, dass syslog-Meldungen an mindestens einen Syslog-Collector gesendet werden. Dadurch wird sichergestellt, dass die Meldungen im Falle eines schwerwiegenden Systemereignisses beibehalten werden und Syslog-Meldungen auf verschiedene Arten verarbeitet werden können, wie z. B. Echtzeitkategorisierung und -analyse (z. B. nach Typ, Zeitspanne oder Maschine) oder Archivieren von Meldungen.

Verwenden Sie die Einstellung `Syslog.global.logHost`, um Remotehostspezifikationen zu definieren. Trennen Sie mehrere Remotehostspezifikationen durch ein Komma (,). Nach dem Festlegen von `Syslog.global.logHost` öffnen und halten ESXi-Hosts Verbindungen zu den Syslog-Collectors, und die Übertragung von Meldungen beginnt sofort. Wenn ESXi eine Syslog-Meldung generiert, wird sie in die entsprechende Protokolldatei auf dem ESXi-Host geschrieben und an alle konfigurierten Syslog-Collectors weitergeleitet.

Neben syslog-Meldungen können aus Sicherheitsgründen auch Überwachungsmeldungen an syslog-Collectors übertragen werden. Überwachungsdatensätze verfolgen sicherheitsbezogene Aktivitäten auf dem ESXi-Host. Weitere Informationen zu Überwachungsdatensätzen finden Sie unter Überwachungsdatensätze.

Hinweis Informieren Sie sich beim Sicherheitsteam Ihres Unternehmens, ob und wie Überwachungsdatensätze festgelegt werden. Für zertifizierte Konfigurationen müssen in der Regel Überwachungsdatensätze aktiviert sein.

Nachfolgend finden Sie die Syntax für `Syslog.global.logHost` -Remotehostspezifikationen:

```
protocol://target[:port]
```

Parameter	Beschreibung	Anmerkungen
`protocol`	Gibt das Netzwerkprotokoll an. Gültige Werte sind `udp`, `tcp` und `ssl`.	Das `ssl`-Protokoll legt fest, dass die Übertragung von syslog-Meldungen verschlüsselt ist. Die `tcp`- und `udp`-Protokolle verschlüsseln die Übertragung nicht. **Hinweis** Wenn das Erfassen von Syslog- oder Überwachungsmeldungen für Ihr System von kritischer Bedeutung ist, vermeiden Sie die Verwendung des `udp`-Protokolls, da die Netzwerkinfrastruktur außerhalb ESXi UDP-Meldungen verwerfen kann.
`target`	Gibt den Remotehost an. Sie können entweder eine IPv4- oder IPv6-Adresse oder einen Hostnamen verwenden.	Wenn Sie eine IPv6-Adresse verwenden, müssen Sie sie in eckige Klammern `[xxx]` einbetten, wobei `xxx` die IPv6-Adresse ist.
`port`	(Optional) Gibt den zu verwendenden Remotehostport an. Wenn Sie UDP oder TCP verwenden, lautet der Standardport 1514. Wenn Sie SSL verwenden, lautet der Standardport 514. Wenn Sie andere Ports als 514 oder 1514 verwenden möchten, müssen Sie die ESXi Firewall anpassen, um den Port zu öffnen.	Weitere Informationen zum Öffnen der ESXi Firewall für den in jeder Remotehostspezifikation angegebenen Port finden Sie unter Konfigurieren der ESXi Firewall.

Beispiele für Remote-Maschinenspezifikationen:

Beispiel für eine Syslog.global.logHost-Zeichenfolge	Anmerkungen
tcp://10.176.130.7:12345	Überträgt Syslog-Meldungen über TCP/IP und Port 12345 an 10.176.130.7.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]	Überträgt Syslog-Meldungen über Port 1514 an eine IPv6-Adresse.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:5432	Überträgt Syslog-Meldungen über Port 54321 an eine IPv6-Adresse.
udp://company.com	Überträgt Syslog-Meldungen über UDP und Port 514 an `company.com`.
udp://company.com,tcp://10.20.30.40:1050	Überträgt Syslog-Meldungen an zwei Remotehosts. Der erste Remotehost verwendet UDP für die Kommunikation mit `company.com` über Port 514. Der zweite Remotehost verwendet TCP für die Kommunikation mit der IPv4-Adresse `10.20.30.40` über Port 1050.
ssl://company.com	Überträgt Syslog-Meldungen mithilfe von SSL (TLS) und Port 514 an `company.com`.

Maximale Meldungsübertragungslänge

Wenn Sie UDP verwenden, beträgt die maximale Übertragungslänge für Syslog-Meldungen 480 Byte für IPv4 und 1180 Byte für IPv6.

Für TCP oder SSL beträgt die standardmäßige maximale Übertragungslänge für Syslog-Meldungen 1 Kibibyte (KiB). Sie können diese Länge mithilfe des Parameters `Syslog.global.remoteHost.maxMsgLen` erhöhen. Der Maximalwert beträgt 16 KiB. Meldungen, die länger als 16 KiB sind, werden abgeschnitten.

Hinweis Wenn eine Erhöhung der maximalen Übertragungslänge erforderlich ist, empfiehlt es sich, die Länge nur so stark wie konkret erforderlich zu erhöhen.

Das Erhöhen der maximalen Syslog-Meldungslänge kann zu Problemen führen, wenn das Netzwerk und die syslog-Infrastruktur außerhalb ESXi Meldungen nicht verarbeiten kann, die länger als 1 KiB sind.

Hinweis Es wird empfohlen, dass Sie aufgrund der Einschränkungen der Paketlänge und der Möglichkeit, dass die externe Netzwerkinfrastruktur die Meldungen verworfen hat, kein UDP zum Übertragen von Syslog-Meldungen verwenden.

Überlegungen zu Zertifikaten beim Konfigurieren von SSL-Übertragungen an Remotehosts

Wenn Sie ESXi zum Übertragen von Syslog-Meldungen an Remotehosts mithilfe von SSL konfigurieren, müssen Sie dem CA-Speicher des ESXi-Hosts ein SSL-Zertifikat für jeden Remotehost hinzufügen. Weitere Informationen finden Sie unter Zertifikatsverwaltung für ESXi-Hosts und Manage CA Certificates with ESXCLI.

Hinweis Lesen Sie in der Dokumentation Ihres Syslog Collectors nach, wie Sie den Collector für den sicheren Empfang von Syslog-Meldungen mithilfe von SSL und einem privaten Schlüssel konfigurieren.

Zusätzliche SSL-Übertragungsparameter

Ein ESXi-System, das den Anforderungen der Sicherheitszertifizierung entspricht, erfordert möglicherweise die Aktivierung von X509-CRL-Prüfungen. Sie aktivieren die erweiterten Einstellungen `Syslog.global.certificate.strictX509Compliance` und `Syslog.global.certificate.checkCRL`, indem Sie den Standardwert von `false` in `true` ändern. Wenn Sie CRL-Prüfungen über die Einstellung `Syslog.global.certificate.checkSSLCerts` aktivieren, müssen aufgrund von Implementierungsbeschränkungen alle Zertifikate in einer Zertifikatskette einen CRL-Link bereitstellen. Die Einstellung ist standardmäßig aktiviert. Sie können SSL-Zertifikatsprüfungen deaktivieren, indem Sie die Einstellung in `false` ändern. Dies wird jedoch nicht empfohlen. Bei der Fehlerbehebung für die Kommunikation mit einem Remotehost müssen Sie möglicherweise SSL-Zertifikatsprüfungen deaktivieren, aber nur für eine begrenzte Zeit.

Vorgehensweise zum Auffinden von Fehler- und Statusinformationen zum Syslog-Daemon

Der ESXi Syslog-Daemon verwendet die Protokolldatei `/var/run/log/vmsyslogd.log`, um Status- und Fehlerinformationen, einschließlich verworfener Meldungen, zu speichern. Wenn die Übertragung von Überwachungsdatensätzen aktiviert ist, gibt der Syslog-Daemon auch Überwachungsdatensätze aus, die sich auf seinen Betrieb beziehen, wie z. B. Start-, Stopp- und Fehlerbedingungen des Daemons, wodurch Sie überprüfen können, ob der syslog-Daemon ordnungsgemäß ausgeführt wird.

Vorgehensweise zum Ändern des standardmäßigen Speicherbereichs der Syslog-Protokolldatei

Der standardmäßige Syslog-Protokolldateispeicherbereich ist `/var/run/log`, für jeden ESXi-Host lokal. Verwenden Sie die Syslog-Konfigurationsvariable `Syslog.global.logDir`, um den standardmäßigen Syslog-Protokolldateispeicherbereich zu ändern, solange sich der Speicherort im dauerhaften Speicher befindet. Wenn `Syslog.global.logDir` für einen dauerhaften Speicher konfiguriert ist, der von mehreren ESXi-Hosts zum Speichern ihrer Syslog-Protokolldateien gemeinsam genutzt wird, ändern Sie die Einstellung `Syslog.global.logDirUnique` in `true`, um zu verhindern, dass Protokolle vermischt werden. Die Einstellung `Syslog.global.logDirUnique` stellt sicher, dass jede ESXi-Maschine einen eindeutigen Namen erhält, der dem Pfad `Syslog.global.logDir` hinzugefügt wird, wodurch die Protokolldateien von anderen Hosts getrennt werden.

Syslog-Meldungswarteschlange für Remotehosts und verworfene Meldungen

Nach dem Start der Syslog-Emissionen werden diese nicht mehr angehalten, außer bei ESXi-Neustarts und -Ausfällen oder bei einer zu beendenden Syslog-Neukonfiguration.

ESXi verwendet einen Warteschlangenmechanismus, wenn Syslog-Meldungen an Remotehosts gesendet werden. Dies hilft, das Verwerfen von Meldungen zu vermeiden, wenn Probleme mit der Netzwerkkonnektivität auftreten und behoben werden. Wenn die Konnektivitätsprobleme jedoch länger dauern, als der Warteschlangenmechanismus tolerieren kann, werden Syslog-Meldungen verworfen. Sie können Statistiken zu verworfenen Meldungen in der Protokolldatei des Syslog-Daemons anzeigen.

Sie können verworfene Meldungen unter /var/run/log/vmsyslogd-dropped.log anzeigen. Diese Protokolldatei enthält spezifische Aufbewahrungseinstellungen, ähnlich denen für die programmspezifischen Aufbewahrungsparameter. Die Parameter für die Aufbewahrung der Protokolldatei für verworfene Meldungen sind: `Syslog.global.droppedMsgs.fileRotate` und `Syslog.global.droppedMsgs.fileSize`.

Konfigurieren der Protokollfilterung auf ESXi-Hosts

Mithilfe der Protokollfilterung können Sie die Protokollierungsrichtlinie des Syslog-Diensts ändern, der auf einem ESXi-Host ausgeführt wird.

Ab vSphere 7.0 Update 2 können Sie mithilfe von ESXCLI Protokollfilter hinzufügen und die Protokollfilterung aktivieren. Ein einmal eingerichteter Protokollfilter bleibt bestehen, bis er entfernt wird, auch über ESXi-Neustarts hinweg.

Protokollfilter betreffen alle Protokollereignisse, die vom `vmsyslogd`-Dienst des ESXi-Hosts verarbeitet werden, und zwar unabhängig davon, ob sie in einem Protokollverzeichnis oder auf einem Remote-Syslog-Server aufgezeichnet werden.

Sie müssen die Protokollfilterungsfunktion aktivieren und den Syslog-Daemon erneut laden, um die Protokollfilter auf dem ESXi-Host zu aktivieren.

ESXCLI-Befehle zum Konfigurieren von Protokollfiltern folgen diesem Muster: `esxcli system syslog config logfilter {cmd} [cmd options]`.

Um beispielsweise die Liste der verfügbaren Protokollfilter abzurufen, führen Sie den folgenden Befehl aus: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Verwenden Sie den Befehl `set`, um die Protokollfilterung zu aktivieren oder zu deaktivieren: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Verwenden Sie den Befehl `add`, um einen Protokollfilter hinzuzufügen, und den Befehl `remove`, um einen Protokollfilter zu entfernen.

Verwenden Sie den Befehl `get`, um zu ermitteln, ob die Protokollfilterung aktiviert ist.

Ein Protokollfilter wird von drei Komponenten angegeben und verwendet die folgende Syntax: `numLogs | ident | logRegexp`.

Parameter	Beschreibung
`numLogs`	Gibt die Anzahl der Übereinstimmungen mit dem regulären Python-Ausdruck „logRegexp“ an, die zulässig sind, bevor die Filterung beginnt.
`ident`	Die `ident`-Zeichenfolge gibt an, wie sich eine Anwendung gegenüber der Syslog-Anlage identifiziert. Der `logRegexp`-Filter muss derselben Anwendung zugeordnet sein. Sie finden die `ident`-Zeichenfolge einer Anwendung, indem Sie die Protokolldateien in `/var/run/log` überprüfen. Das dritte Feld jeder Protokolldatei beginnt mit der `ident`-Zeichenfolge und endet mit `[`.
`logRegexp`	Regulärer Python-Ausdruck, der die Meldungen identifiziert, die Sie herausfiltern möchten.

Um beispielsweise alle Meldungen aus dem hostd-Daemon herauszufiltern, die das Wort „mark“ nach dem zehnten Auftreten enthalten, verwenden Sie den folgenden Befehl: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"`.

Um den Protokollfilter zu entfernen, verwenden Sie den Befehl `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

Weitere Informationen finden Sie unter ESXi-Syslog-Optionen.

Voraussetzungen

Sie können Protokollfilter erstellen, um die Anzahl doppelter Einträge in den ESXi-Protokollen zu reduzieren und bestimmte Protokollereignisse komplett auf die Sperrliste zu setzen.

Installieren Sie ESXCLI. Weitere Informationen finden Sie unter *Erste Schritte mit ESXCLI*. Führen Sie zwecks Fehlerbehebung `esxcli`-Befehle in der ESXi Shell aus.

Verwenden von vSphere Auto Deploy zum erneuten Bereitstellen von Hosts

4

Sie können ESXi-Hosts, die unter Verwendung von vSphere Auto Deploy bereitgestellt wurden, mit einem neuen Image-Profil für eine andere ESXi-Version erneut bereitstellen.

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. Weitere Informationen hierzu finden Sie unter *vSphere-Sicherheit*.

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. Sie können vSphere ESXi Image Builder verwenden, um Image-Profile zu erstellen und zu verwalten. 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.

Lesen Sie als Nächstes die folgenden Themen:

- Einführung in vSphere Auto Deploy
- Installieren und Konfigurieren von vSphere Auto Deploy
- Erneute Bereitstellung von Hosts

Einführung in vSphere Auto Deploy

vSphere Auto Deploy verwendet eine PXE-Startinfrastruktur mit Hostprofilen, einem gewünschten Image oder einer Konfiguration auf Clusterebene, um ESXi Hosts bereitzustellen.

Statusinformationen für ESXi-Hosts

Hinweis Sie können Auto Deploy nicht auf ESXi-Hosts verwenden, die als Teil der vSphere Distributed Services Engine-Funktion mit DPUs konfiguriert sind.

Wenn Sie einen physischen Host starten, der für vSphere Auto Deploy eingerichtet ist, verwendet vSphere Auto Deploy die PXE-Startvorgangsinfrastruktur in Verbindung mit vSphere-Hostprofilen, einem gewünschten Image oder einer Konfiguration auf Clusterebene, 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. vSphere Auto Deploy speichert die Informationen für die bereitzustellenden ESXi-Hosts an verschiedenen Speicherorten. Informationen zum Speicherort von Image-Profilen, Hostprofilen oder Clustern, die Sie entweder mit einem einzelnen Image oder mit einer Konfiguration auf Clusterebene verwalten, werden anfänglich in den Regeln angegeben, die Maschinen 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	Image-Profil, das mit vSphere ESXi Image Builder oder einem vSphere Lifecycle Manager-Image erstellt wurde.
Konfigurationsstatus	Die konfigurierbaren Einstellungen, die festlegen, wie der Host konfiguriert wird, z. B. virtuelle Switches und ihre Einstellungen, Treibereinstellungen, Startparameter usw	Hostprofil, das mit der Hostprofil-Benutzeroberfläche erstellt wird, oder eine Konfiguration, die Sie beim Einrichten eines Clusters erstellen, das alle ESXi-Hosteinstellungen auf Clusterebene in der Bestandslisten-Benutzeroberfläche verwaltet.
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.	Hostanpassungsdaten, gespeichert vom vCenter Server während des ersten Startvorgangs Sie können ein Hostprofil erstellen, das für bestimmte Werte eine Benutzereingabe erfordert. 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.

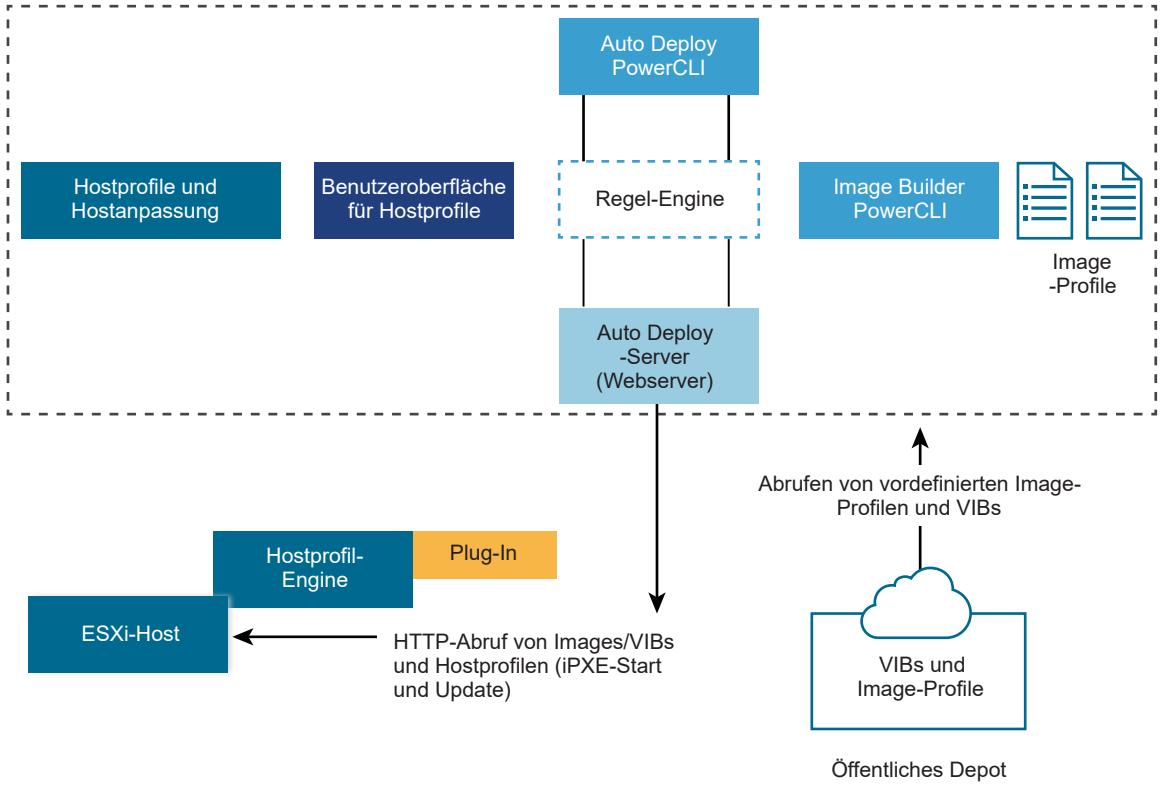
vSphere Auto Deploy-Architektur

Die vSphere Auto Deploy-Infrastruktur besteht aus mehreren Komponenten.

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

(Auto Deploy-Architektur)

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.

Neben Legacy-Image-Profilen, die Sie mit VMware Image Builder erstellen, und Hostprofilen können Sie auch vSphere Auto Deploy-Regeln erstellen, um ESXi mit einem einzelnen vSphere Lifecycle Manager-Image oder einer Konfiguration auf Clusterebene bereitzustellen.

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.
- Mithilfe von vSphere Lifecycle Manager-Images wenden Sie Software- und Firmware-Updates auf die ESXi-Hosts in einem Cluster an. Durch die Verwendung eines einzelnen Images zur Verwaltung aller Hosts in einem Cluster wird die clusterweite Homogenität des Host-Images gewährleistet.
- Mit ESXi 8.0 können Sie einen Cluster einrichten, der alle ESXi-Hosteinstellungen auf Clusterebene verwaltet.
- 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.

Hinweis Wenn Sie mit ESXi 8.0 einen Cluster einrichten, der alle ESXi-Hosteinstellungen auf Clusterebene verwaltet, können Sie keine Hostprofile verwenden.

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.

Auto Deploy-Zertifikate

Standardmäßig stattet der Auto Deploy-Server jeden Host mit Zertifikaten aus, die von der VMware Certificate Authority (VMware CA) signiert wurden. Weitere Informationen finden Sie unter Verwalten von Zertifikaten für ESXi-Hosts.

Wenn Ihre Unternehmensrichtlinien die Verwendung von benutzerdefinierten Zertifikaten vorschreiben, können Sie alternativ den Auto Deploy-Server so einrichten, dass alle Hosts mit benutzerdefinierten Zertifikaten ausgestattet werden, die nicht von der VMware CA signiert sind. Der Auto Deploy-Server wird zu einer Zwischenzertifizierungsstelle Ihrer Drittanbieter-Zertifizierungsstelle. Im Modus „Benutzerdefinierte Zertifizierungsstelle“ sind Sie für die Verwaltung der Zertifikate verantwortlich. Zertifikate können nicht über den vSphere Client

aktualisiert und verlängert werden. In diesem Modus können Sie auch nicht nur eine Gruppe von Hosts auswählen, die mit benutzerdefinierten Zertifikaten bereitgestellt werden sollen, und Sie können benutzerdefinierte Zertifikate nur für statusbehaftete Hosts manuell signieren. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Mit ESXi 8.0 bietet Auto Deploy eine dritte Option, mit der Sie ein Zertifikat außerhalb von vSphere generieren und unabhängig von der Zertifikatsverwaltung in vCenter Server werden können. Beispielsweise können Sie ein benutzerdefiniertes Zertifikat mithilfe eines benutzerdefinierten Skripts oder mithilfe eines Anbieters von Registrierungsdiensten für Domänennamen wie z. B. Verisign generieren. Sie können benutzerdefinierte Zertifikate nur für eine Gruppe von ESXi-Hosts verwenden. Sie können auch benutzerdefinierte Zertifikate für statusfreie Hosts bereitstellen. ESXi-Hosts werden durch die MAC-Adresse der für den Netzwerkstart verwendeten Netzwerkkarte oder durch die BIOS-UUID des ESXi-Hosts identifiziert. Sie aktualisieren den VMware Endpoint Certificate Store (VECS) mit dem benutzerdefinierten Zertifikat, indem Sie PowerCLI verwenden. Weitere Informationen zu den neuen PowerCLI-Cmdlets finden Sie unter vSphere Auto Deploy PowerCLI-Cmdlet – Überblick. Die VMware CA muss den benutzerdefinierten ESXi-Zertifikaten vertrauen, sodass Sie das öffentliche CA-Zertifikat für die benutzerdefinierten Zertifikate zum TRUSTED_ROOTS-Speicher in VECS hinzufügen müssen. Auto Deploy speichert auch die benutzerdefinierten Zertifikate. Wenn ein startender Host mit der entsprechenden MAC-Adresse der für den Netzwerkstart verwendeten Netzwerkkarte oder der BIOS-UUID des ESXi-Hosts erkannt wird, wird automatisch das benutzerdefinierte Zertifikat bereitgestellt. Sie müssen Auto Deploy oder vCenter Server nicht beenden oder neu starten, wenn Sie ein benutzerdefiniertes Zertifikat zu VECS hinzufügen. Starten Sie nur den Host neu, für den Sie ein benutzerdefiniertes Zertifikat hochladen. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Installieren und Konfigurieren von vSphere Auto Deploy

Sie müssen Ihre Umgebung in mehreren Schritten 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 vSphere PowerCLI installieren.

Weitere Themen zum Lesen

- Checkliste vor der Installation von vSphere Auto Deploy

  Bevor Sie mit den Aufgaben in diesem vSphere Auto Deploy-Szenario beginnen können, stellen Sie sicher, dass Ihre Umgebung die Hardware- und Softwareanforderungen erfüllt und Sie über die erforderlichen Berechtigungen für die im Setup enthaltenen Komponenten verfügen.

- 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 vSphere PowerCLI enthalten. Benutzer von vSphere Auto Deploy-Cmdlets haben den Vorteil, alle vSphere PowerCLI-Funktionen nutzen zu können.

- Einrichten der Massenlizenzierung

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

Checkliste vor der Installation von vSphere Auto Deploy

Bevor Sie mit den Aufgaben in diesem vSphere Auto Deploy-Szenario beginnen können, stellen Sie sicher, dass Ihre Umgebung die Hardware- und Softwareanforderungen erfüllt und Sie über die erforderlichen Berechtigungen für die im Setup enthaltenen Komponenten verfügen.

Tabelle 4-2. Checkliste vor der Installation

Erforderliche Software und Hardware	Details
vCenter Server	Der vSphere Auto Deploy-Server ist ein Teil von vCenter Server. Sie müssen den vSphere Auto Deploy-Dienst auf dem vCenter Server-System aktivieren und starten. Sie können viele der Setup-Aufgaben durchführen, indem Sie sich bei vCenter Server anmelden. Weitere Informationen hierzu finden Sie unter Vorbereiten des Systems für vSphere Auto Deploy.
Speicher	Speicher für ESXi-Datenspeicher (NFS, iSCSI oder Fibre Channel) mit Servern und Speicherarrays, die so konfiguriert sind, dass die Server die LUNs erkennen können ■ Eine Liste der Ziel-IP-Adressen für NFS oder iSCSi ■ Eine Liste mit Informationen über Ziel-Volumes für NFS oder iSCSi

Tabelle 4-2. Checkliste vor der Installation (Fortsetzung)

Erforderliche Software und Hardware	Details
Hostinformationen (für vier ESXi-Hosts)	Eine Liste der Ziel-IP-Adressen für NFS oder iSCSi Eine Liste mit Informationen über Ziel-Volumes für NFS oder iSCSi ■ Standardroute, Netzmaske und IP-Adressen für primäre und sekundäre DNS-Server ■ IP-Adresse und Netzmaske für das primäre VMkernel-Verwaltungsnetzwerk ■ IP-Adresse und Netzmaske für andere VMkernel-Netzwerke, wie Speicher, vSphere FT oder VMware vMotion Vorhandene Partitionen werden von vSphere Auto Deploy nicht standardmäßig überschrieben.
vSphere PowerCLI	Weitere Informationen finden Sie unter Installieren von PowerCLI.
ESXi-Softwaredepot	Der Speicherort des ESXi-Softwaredepots auf der Seite „Downloads“ der VMware-Website. Sie verweisen über eine URL auf das dort gespeicherte Image-Profil oder laden eine ZIP-Datei herunter und arbeiten mit einem lokalen Depot. Laden Sie das ESXi-Image nicht herunter.
TFTP-Server	TFTP-Installationssoftware wie zum Beispiel WinAgents TFTP-Server.
DHCP-Server	Der DHCP-Server ist in den vSphere Windows Server-Versionen enthalten.
DNS Server	Ein funktionierender DNS-Server. Sie müssen für jeden Zielhost Einträge in Forward- (A-Datensatz) und Reverse-Zonen (PRT-Datensatz) hinzufügen.

Sie benötigen außerdem Informationen zu sowie Administratorrechte für die Hauptserver der Umgebung. Dazu zählen der Active Directory-Server, der DNS-Server, der DHCP-Server, der NTP-Server usw.

Die Broadcast-Domäne des Subnetzes, in dem Sie das Setup bereitstellen, muss vollständig von Ihnen gesteuert werden können. Stellen Sie sicher, dass sich keine anderen DHCP-, DNS- oder TFTP-Server in diesem Subnetz befinden.

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.

Wenn Sie vSphere Auto Deploy mit PowerCLI-cmdlets verwalten möchten, finden Sie unter *Einrichten von vSphere Auto Deploy und Bereitstellen von Hosts mit vSphere PowerCLI* dazu weitere Informationen.

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 *Upgrade von vCenter Server*.
- Überprüfen Sie, dass Sie über einen TFTP-Server und einen DHCP-Server in Ihrer Umgebung verfügen, um Dateien zu senden und Netzwerkadressen den ESXi-Hosts zuzuweisen, die Auto Deploy bereitstellt. Siehe #unique_86 und #unique_87.
- Stellen Sie sicher, dass die ESXi-Hosts über Netzwerkkonnektivität mit DHCP-, TFTP- und vSphere Auto Deploy-Servern verfügen.
- 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 400 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. 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. Installieren und verwenden Sie optional VMware vCenter Log Insight, das Protokollaggregation und -analysen für VMware und Nicht-VMware-Produkte, virtuell und physisch, mit nahezu echtzeitnaher Suche und Analyse von Protokollereignissen bietet.
- 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.

Verfahren

1 Navigieren Sie zu **Startmenü > Automatischer Einsatz**.

   Standardmäßig verfügt nur die Administratorrolle über Rechte zum Verwenden des vSphere Auto Deploy-Diensts.

2 Wählen Sie auf der Seite **Automatischer Einsatz** Ihre vCenter Server aus dem Dropdown-Menü im oberen Bereich.

3 Klicken Sie auf **Aktivieren von automatischem Einsatz und Image-Builder**, um den Dienst zu aktivieren.

   Wenn der **Image-Builder**-Dienst bereits aktiviert ist, wählen Sie die Registerkarte **Konfigurieren** und klicken Sie auf **Dienst „Automatischer Einsatz“ aktivieren**.

   Die Seite **Software-Depot** wird angezeigt.

4 Konfigurieren Sie den TFTP-Server.

   a Klicken Sie auf die Registerkarte **Konfigurieren**.

   b 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.

   c (Optional) Um einen Proxy-Server zu verwenden, klicken Sie im Bereich *Runtime-Übersicht des automatischen Einsatzes* auf **Hinzufügen** und geben Sie eine Proxyserver-URL in das Textfeld ein.

      Mithilfe von Reverse-Proxy-Servern können die Anforderungen übertragen werden, die an den vSphere Auto Deploy-Server gestellt werden.

5 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.

6 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.

7 (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.

   Die Dateien befinden sich im Verzeichnis `/etc/vmware-rbd/ssl/`.

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

Ergebnisse

Wenn Sie einen ESXi-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.

Nächste Schritte

- Sie können die Standardkonfigurationseigenschaften des **Auto Deploy-Diensts** ändern. Weitere Informationen finden Sie unter in der *vCenter Server und Hostverwaltung*-Dokumentation unter „vCenter Server-Konfiguration“.
- Sie können die Standardkonfigurationseigenschaften des **Image-Builder-Diensts** ändern. Weitere Informationen finden Sie unter in der *vCenter Server und Hostverwaltung*-Dokumentation unter „vCenter Server-Konfiguration“.
- 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 vSphere PowerCLI enthalten. Benutzer von vSphere Auto Deploy-Cmdlets haben den Vorteil, alle vSphere PowerCLI-Funktionen nutzen zu können.

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

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

- Sie erhalten Hilfe zu jedem Cmdlet , indem Sie `Get-Help`*`cmdlet_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 Massenlizenzierung

Sie können den vSphere Client oder die ESXi Shell dazu verwenden, einzelne Lizenzschlüssel anzugeben, oder Sie können die Massenlizenzierung mithilfe der vSphere PowerCLI-Cmdlets einrichten. Die Massenlizenzierung 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 Client und die Zuweisung von Lizenzen mithilfe von vSphere PowerCLI-Cmdlets funktionieren unterschiedlich.

Zuweisen von Lizenzschlüsseln mit dem vSphere 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 vSphere 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 vSphere PowerCLI zugewiesen wird, wird als Standardlizenzschlüssel angesehen. Wenn ein nicht lizenzierter 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 Datencenter Lizenzen zugewiesen. Sie können auch Lizenzen mit Hosts und Clustern verknüpfen.

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

Voraussetzungen

Vorbereiten des Systems für vSphere Auto Deploy.

Verfahren

1 Stellen Sie in einer vSphere 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 zum Abrufen des Datencenters aus, in dem sich die Hosts befinden, für die Sie die Massenlizenzierungsfunktion verwenden möchten.

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

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

3 Erstellen Sie ein `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-vsphere"
$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 Datencenter 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 Datencenter oder dem Cluster zu, denen Sie die Lizenzdaten zugewiesen haben.

7 Mit dem vSphere Client können Sie sicherstellen, dass der Host erfolgreich der Standardlizenz `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` zugewiesen wurde.

Ergebnisse

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

Erneute Bereitstellung von Hosts

Verwenden Sie vSphere Auto Deploy, um ESXi Hosts mit einem anderen Image-Profil oder einem anderen Hostprofil erneut bereitzustellen.

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

Sie können ESXi-Hosts mit dem Image-Profil, dem Hostprofil, dem benutzerdefinierten Skript und dem vCenter Server-Standort, der beim ersten Start zugewiesen wurde, erneut bereitstellen.

Voraussetzungen

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.

- 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.

Verfahren

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.

Ergebnisse

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.

Verwenden von vSphere PowerCLI zum erneuten Bereitstellen eines Hosts

Sie können vSphere Auto Deploy verwenden, um einen Host mit einem neuen Image-Profil in einer vSphere PowerCLI-Sitzung erneut bereitzustellen.

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 update`-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 vSphere 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.

Verfahren

1 Führen Sie an der PowerShell-Eingabeaufforderung das vSphere 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 vSphere PowerCLI-Sitzung hinzuzufügen.

Depottyp	Cmdlet
Remote-Depot	Führen Sie **Add-EsxSoftwareDepot *depot_url*** aus.
ZIP-Datei	a Laden Sie die ZIP-Datei in einen lokalen Dateipfad herunter oder erstellen Sie für die vSphere PowerCLI-Maschine einen lokalen Mount-Punkt. b Führen Sie **Add-EsxSoftwareDepot C:*Dateipfad**Mein_Offline-Depot*.zip** 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
   -----------                          ------------
   my_old_imageprofile                        my_new_imageprofile
   ```

   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 ESXi-Hosts ein Hostprofil zuweisen.

In vielen Fällen weisen Sie einem Cluster einen Host zu, anstatt explizit ein Hostprofil anzugeben. Der Host verwendet das Hostprofil des Clusters.

Voraussetzungen

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.

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

Verfahren

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 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.

Nächste Schritte

- 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

Testen Sie neue oder geänderte Regeln auf Übereinstimmung und reparieren Sie sie entsprechend, da Änderungen im vSphere Auto Deploy-Regelsatz nicht automatisch aktualisiert werden.

Voraussetzungen

Wenn Sie eine Regel zum vSphere Auto Deploy-Regelsatz hinzufügen oder eine oder mehrere Regeln ändern, werden die Hosts nicht automatisch aktualisiert. vSphere Auto Deploy übernimmt die neuen Regeln nur dann, wenn Sie deren Regelübereinstimmung testen und eine Standardisierung durchführen.

- Bereiten Sie das System vor und installieren Sie den Auto Deploy-Server. Weitere Informationen finden Sie unter 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.

Verfahren

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 Ändern Sie eine der verfügbaren Regeln.

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
```

Wenn der Host, für den Sie die neue Regelsatzübereinstimmung testen möchten, mit dem aktiven Regelsatz kompatibel ist, gibt das System eine Tabelle mit aktuellen und erwarteten Elementen zurück.

```
CurrentItem                          ExpectedItem
-----------                          ------------
My Profile 25                        MyNewProfile
```

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

```
Repair-DeployRuleSetCompliance $tr
```

Nächste Schritte

Wenn mit der von Ihnen geänderten Regel der Speicherort für die Bestandsliste angegeben wurde, werden die Änderungen wirksam, wenn Sie die Übereinstimmung reparieren. Starten Sie bei allen anderen Änderungen Ihren Host neu, um die neue Regel mithilfe von 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 Installations- oder Upgrade-Protokolldateien für ESXi erfassen, mit denen Sie die Ursache des Fehlers identifizieren können, wenn eine Installation oder ein Upgrade fehlschlägt.

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.