XenServer

XenServer 8

Contents

Über XenServer 8

April 12, 2024

XenServer ist eine Virtualisierungsplattform, mit der Unternehmen virtualisierte Serverinfrastrukturen erstellen und verwalten können. Es wurde entwickelt, um die Bereitstellung virtueller Windows- und Linux-Maschinen zu optimieren und bietet eine robuste und skalierbare Lösung für die Virtualisierung von Rechenzentren.

XenServer bietet Funktionen wie Live-Migration, Snapshot- und Cloning-Funktionen sowie Ressourcenpooling, die eine effiziente Verwaltung virtualisierter Workloads ermöglichen. Es bietet eine sichere und leistungsstarke Umgebung für die Ausführung von Anwendungen und Diensten und ist damit eine geeignete Wahl für Unternehmen, die ihre Serverinfrastruktur optimieren möchten.

Die Cloud Software Group (CSG) betont die Integration von XenServer in Citrix-Produkte und schafft so eine umfassende Virtualisierungs- und Anwendungsbereitstellungslösung. Unser Ziel ist es, die Flexibilität, Agilität und Wirtschaftlichkeit des IT-Betriebs durch zentralisiertes Management und effiziente Ressourcennutzung zu verbessern. Insgesamt ist XenServer als zuverlässige Virtualisierungslösung für Unternehmen positioniert, die eine leistungsstarke und vielseitige Plattform für ihre Serverumgebungen suchen.

Holen Sie sich XenServer 8 hier.

> **Hinweis:**
>
> Wenn Sie XenServer 8 zuvor als Vorschau verwendet haben, wenden Sie die neuesten Updates an, um nahtlos zur produktionsunterstützten Version überzugehen.
>
> Wenn Sie eine Citrix Virtual Apps and Desktops-Lizenz mit XenServer verwenden, müssen Sie zu einer XenServer Premium Edition-Lizenz wechseln. Weitere Informationen finden Sie unter https://xenserver.com/buy. Bestehende Kunden von Citrix Virtual Apps and Desktops können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Ist XenServer 8 für mich?

XenServer 8 ist die neueste Version von XenServer. Es tritt die Nachfolge von Citrix Hypervisor 8.2 Cumulative Update 1 an und enthält viele neue Funktionen. Weitere Informationen zu diesen Funktionen finden Sie unter Neuigkeiten.

Warum sollten Sie XenServer 8 wählen?

- Sie möchten die neuesten Funktionen von XenServer ausprobieren und können Ihre Hosts und Pools regelmäßig aktualisieren.

  Eine bemerkenswerte Änderung zwischen Citrix Hypervisor 8.2 Cumulative Update 1 und XenServer 8 ist unsere Umstellung auf die kontinuierliche Bereitstellung von Funktionen und Fixes über unseren Mechanismus für häufige Updates. Weitere Informationen finden Sie unter XenServer-Hosts aktualisieren.

- Sie möchten Windows 11-VMs in Ihrer Umgebung verwenden.

  XenServer 8 bietet Unterstützung für Windows 11-VMs und VTPMs. Weitere Informationen finden Sie unter Windows VMs.

- Sie sind ein Benutzer von Citrix Virtual Apps and Desktops und möchten Ihren Workload auf einem Hypervisor ausführen, der viele für Ihre Umgebung optimierte Funktionen enthält.

  Weitere Informationen zu diesen Funktionen finden Sie unter XenServer mit Citrix-Produkten verwenden.

  Informationen darüber, welche Versionen von Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS) mit XenServer 8 unterstützt werden, finden Sie unter Unterstützte Hypervisors für Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS).

  Sie können auch von einer zeitlich begrenzten Aktion profitieren, die kostenlose XenServer-Lizenzen für Citrix-Kunden anbietet. Weitere Informationen

In jedem dieser Fälle ist XenServer 8 das Richtige für Sie. Hier herunterladen.

XenCenter

XenServer 8 benötigt die neueste Version von XenCenter, die eine Versionsnummer in der Form “XenCenter yyyy.x.x”hat. Frühere Versionen von XenCenter, wie XenCenter 8.2.x, werden von XenServer 8 nicht unterstützt.

- Laden Sie das neueste XenCenter herunter
- Sehen Sie sich die Dokumentation an

XenCenter yyyy.x.x wird mit XenServer 8 vollständig unterstützt. XenCenter yyyy.x.x wird noch nicht für den Produktionseinsatz mit Citrix Hypervisor 8.2 CU1 unterstützt.

Häufige Updates im gesamten XenServer 8-Lebenszyklus

Mit XenServer 8 stehen Ihnen in XenCenter häufige Updates zur Verfügung, sodass Sie von einem effizienteren Release-Prozess profitieren können, der neue Funktionen und Bugfixes schneller als bisher

bereitstellt. Mit dieser Funktion können Sie das Modell für häufige Updates zur Verwaltung von Updates für Ihre XenServer-Pools und Hosts kennenlernen.

Während seines Lebenszyklus bietet XenServer 8 einen Strom häufiger und einfach anzuwendender Updates, mit denen Sie neue Funktionen und Bugfixes zum frühestmöglichen Zeitpunkt nutzen können. Sie müssen alle verfügbaren Updates regelmäßig anwenden. Infolgedessen können sich das Verhalten und der Funktionsumfang in XenServer 8 ändern.

Erste Schritte

Schritte zur Verwendung von XenServer 8:

1. Holen Sie sich XenServer 8 von der XenServer-Downloadseite.
2. Installieren Sie die neueste Version von XenCenter.
3. Installieren oder führen Sie ein Upgrade auf XenServer 8 durch.
4. Wenden Sie Updates mithilfe von XenCenter an.

---

layout: doc
description: Discover the features added in the latest version of XenServer.—

Was ist neu

Unser Ziel ist es, XenServer 8-Kunden neue Funktionen und Produktupdates zur Verfügung zu stellen, sobald sie bereit sind. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern. Über den XenServer 8-Release-Stream stellen wir Updates schrittweise in Wellen bereit, um die Produktqualität sicherzustellen und die Verfügbarkeit zu maximieren.

> **Hinweis:**
>
> Wenn Sie XenServer 8 zuvor als Vorschau verwendet haben, wenden Sie die neuesten Updates an, um nahtlos zur produktionsunterstützten Version überzugehen.
>
> Wenn Sie eine Citrix Virtual Apps and Desktops-Lizenz mit XenServer verwenden, müssen Sie zu einer XenServer Premium Edition-Lizenz wechseln. Weitere Informationen finden Sie unter https://xenserver.com/buy. Bestehende Kunden von Citrix Virtual Apps and Desktops können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

XenServer ist zurück

Wir veröffentlichen unser Produkt erneut unter der Marke XenServer. Weitere Informationen finden Sie auf der XenServer-Website.

Im Rahmen dieser Änderung ändern sich auch einige der anderen Namen und Begriffe, die in unserem Produkt und unserer Dokumentation verwendet werden:

Alter Begriff	Neuer Begriff	Hinweise
Citrix Hypervisor	XenServer	
XenServer-Versionsformat `major_version.minor_version`	XenServer-Versionsformat `major_version`	Das XenServer-Versionsformat wurde geändert, sodass nur die Hauptversion angezeigt wird. Während frühere Versionen mit "XenServer 7.6", "Citrix Hypervisor 8.2"usw. nummeriert waren, zeigen diese Version und alle zukünftigen Versionen nur die Hauptversion, z. B. "XenServer 8". XenServer 8 basiert auf derselben Plattform wie Citrix Hypervisor 8.2 CU1 und verwendet daher dieselbe Hauptversion. XenServer 8 ist jedoch die neuere Version des Produkts und enthält die neuesten Funktionen und Fixes.
XenCenter x.x.x	XenCenter JJJJ.x.x	Das Format der XenCenter-Version wurde geändert, sodass es unabhängig von der XenServer-Version ist. Das neue Versionsformat für XenCenter ist. `year.major_version.minor_version`
Citrix VM Tools (zuvor XenServer PV Tools)	XenServer VM-Tools	

Alter Begriff	Neuer Begriff	Hinweise
Poolmeister	Poolkoordinator	Der Haupthost in einem Pool wird jetzt in der Dokumentation und in XenCenter als Poolkoordinator bezeichnet. Der ältere Begriff wird immer noch in einigen Xe-CLI-Befehlen und in der Management-API verwendet.
Pool-Sklave	Pool-Unterstützer	Die untergeordneten Hosts in einem Pool werden jetzt in der Dokumentation und in XenCenter als Poolunterstützer oder unterstützende Hosts bezeichnet. Der ältere Begriff wird immer noch in einigen Xe-CLI-Befehlen und in der Management-API verwendet.
Master-Kennwort	Haupt-Kennwort	
Express-Ausgabe	Test-Ausgabe	

Häufige und einfach anzuwendende Updates

In XenServer 8 hat sich die Art und Weise, wie wir Updates für Sie veröffentlichen, geändert. Regelmäßige Updates werden zur Verfügung gestellt, sodass Sie von einem effizienteren Release-Prozess profitieren können, der neue Funktionen und Bugfixes in einem schnelleren Rhythmus bereitstellt, als dies bisher möglich war. Verwenden Sie XenCenter oder die xe CLI, um diese Updates zu einem für Sie passenden Zeitpunkt auf Ihre XenServer-Hosts und -Pools anzuwenden. Weitere Informationen finden Sie unter XenServer-Hosts aktualisieren.

1. Wir stellen regelmäßige Updates für XenServer 8 in unserem sicheren CDN zur Verfügung.
2. Sehen Sie in XenCenter, wann Updates für Ihren Pool verfügbar sind.
3. Initiieren Sie mit XenCenter oder der xe CLI den Vorgang zum Anwenden von Updates auf Ihren XenServer-Pool.

Weitere Informationen finden Sie unter Anwenden von Updates mithilfe von XenCenter oder Anwenden von Updates mithilfe der XE-CLI.

Eine Liste der neuesten Updates, die für Ihre Early Access- oder Normal-Pools verfügbar sind, finden Sie auf den folgenden Seiten:

- Kanalupdates im Early-Access-Modus
- Normale Kanalupdates

Auf diesen Seiten sind nicht alle Änderungen in den Kanälen Early Access und Normal aufgeführt, sondern nur ein Teil davon. Den vollständigen Satz der verfügbaren Änderungen finden Sie in den Informationen in der XenCenter **Update-Ansicht** .

Windows 11- und vTPM-Unterstützung

Windows 11 wird jetzt auf XenServer unterstützt.

Diese Funktion beinhaltet auch Unterstützung für vTPMs. Sie können ein vTPM erstellen und an eine Windows 10- oder Windows 11-VM anhängen. Weitere Informationen finden Sie unter Windows VMs.

Das vTPM bietet eine TPM 2.0-konforme API für Anwendungen in der VM. TPM 1.2 wird nicht unterstützt.

Änderungen an der Lizenzierung

Das Lizenzverhalten in XenServer 8 unterscheidet sich von dem in früheren Versionen von Citrix Hypervisor und XenServer. Wir haben die Anforderungen für Citrix-Kunden geändert, eine neue Edition hinzugefügt und einige Funktionen für alle verfügbar gemacht.

Weitere Informationen finden Sie unter Lizenzierung.

Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS

In XenServer 8 benötigen Sie eine Premium Edition-Lizenz, um Ihre Workloads auf einem XenServer-Pool oder Host ausführen zu können. Dies ist eine Änderung gegenüber früheren Versionen von Citrix Hypervisor oder XenServer, mit denen Sie Ihre Citrix Virtual Apps and Desktops- oder Citrix DaaS-Lizenz verwenden konnten, um einen kostenlosen Anspruch auf XenServer zu erhalten.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy.

Wenn Sie XenServer oder Citrix Hypervisor bereits zum Hosten Ihrer Citrix Virtual Apps and Desktops-Workloads verwenden, können Sie die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Informationen darüber, welche Versionen von Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS) mit XenServer 8 unterstützt werden, finden Sie unter Unterstützte Hypervisors für Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS).

Test-Ausgabe

Sie können XenServer 8 jetzt kostenlos mit der Trial Edition testen. Mit der Testversion können Sie Funktionen der Premium Edition testen, allerdings in einem Pool mit begrenzter Größe von bis zu 3 Hosts. Weitere Informationen zu den verschiedenen Editionen von XenServer finden Sie unter XenServer-Editionen.

Änderungen an den Funktionen

Die folgenden Funktionen, die in früheren Versionen auf Premium Edition-Kunden beschränkt waren, sind jetzt auch in der Standard Edition verfügbar:

- Automatisierte Updates der Windows-VM-Treiber
- Automatisierte Updates für den Management Agent
- Live-Patching
- XenServer Conversion Manager

Überwachen Sie Host- und Dom0-Ressourcen mit NRPE

> **Hinweis:**
>
> Die NRPE-Funktion ist für XenServer Premium- oder Trial Edition-Kunden verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.

In XenServer 8 können Sie jedes Überwachungstool eines Drittanbieters verwenden, das Nagios Remote Plugin Executor (NRPE) unterstützt, um Host- und Dom0-Ressourcen zu überwachen, z. B. Nagios Core. XenServer integriert NRPE in dom0, sodass Sie verschiedene Host- und Dom0-Metriken erfassen können. Weitere Informationen finden Sie unter Überwachen von Host- und Dom0-Ressourcen mit NRPE.

Überwachen Sie Host- und Dom0-Ressourcen mit SNMP

> **Hinweis:**
>
> Die SNMP-Funktion ist für XenServer Premium- oder Trial Edition-Kunden verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die

> XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.

Sie können jetzt SNMP und jedes NMS Ihrer Wahl verwenden, um die von XenServer verbrauchten Ressourcen remote zu überwachen. Mit dieser Funktion können Sie auch Traps zur Überwachung Ihrer XenServer-Hosts konfigurieren. Dabei handelt es sich um vom Agent initiierte Meldungen, die den NMS darauf hinweisen, dass ein bestimmtes Ereignis in XenServer eingetreten ist. Weitere Informationen finden Sie unter Host- und Dom0-Ressourcen mit SNMP überwachen.

Lokales XFS

Sie können jetzt lokale Speichergeräte mit 4 KB physischen Blöcken verwenden, ohne eine logische Blockgröße von 512 Byte zu benötigen, indem Sie den neuen Thin-Provisioning Local SR-Typ verwenden: XFS. Weitere Informationen finden Sie unter Local XFS.

Änderungen an der Unterstützung des Gastbetriebssystems

Die vollständige Liste der unterstützten Gastbetriebssysteme in XenServer 8 finden Sie unter Unterstützung für Gastbetriebssysteme.

Hinzugefügt

XenServer 8 unterstützt jetzt die folgenden neuen Gäste:

- Debian Bullseye 11 (64 Bit)
- Ubuntu 22.04 (64 Bit)
- Windows 11 (64 Bit)

Entfernt

XenServer 8 unterstützt die folgenden Gäste nicht mehr:

- Debian Jessie 8 (32 bisschen)
- Debian Jessie 8 (64 Bit)
- Debian Stretch 9 (32 Bit)
- Debian Stretch 9 (64 Bit)
- Ubuntu 16.04 (32 Bit)
- Ubuntu 16.04 (64-Bit)
- CoreOS
- SUSE Linux Enterprise Desktop 12 SP3, 12 SP4 (64 Bit)
- SUSE Linux Enterprise Desktop 15 SP3 (64 Bit)

- SUSE Linux Enterprise Server 12 SP3 (64 Bit)
- CentOS 8 (64 Bit)
- Windows 10 (32 Bit)

Veraltet

Die folgenden Gäste sind in XenServer 8 veraltet:

- Ubuntu 18.04 (64 Bit)
- SUSE Linux Enterprise Desktop 12 SP4 (64 Bit)

XenServer Conversion Manager 8.3.1

Mit XenServer Conversion Manager 8.3.1 —der neuesten Version der virtuellen XenServer Conversion Manager-Appliance —können Sie VMs parallel konvertieren, sodass Sie Ihre gesamte VMware-Umgebung schnell und effizient auf XenServer migrieren können. Sie können bis zu 10 VMware ESXi/vCenter VMs gleichzeitig konvertieren.

Weitere Informationen zur Verwendung des XenServer Conversion Managers finden Sie unter XenServer Conversion Manager.

Verbesserungen an GFS2

Einige Einschränkungen bei der Verwendung von GFS2 SRs mit Citrix Machine Creation Services wurden aufgehoben.

- Sie können jetzt MCS-Vollklon-VMs mit GFS2-SRs verwenden.
- Sie können jetzt mehrere GFS2-SRs im selben MCS-Katalog verwenden.

Weitere Informationen zur Verwendung von GFS2-SRs finden Sie unter Gemeinsam genutzter GFS2-Blockspeicher mit Thin-Provisioning.

Zertifikatüberprüfung

Die Funktion zur Zertifikatsüberprüfung stellt sicher, dass alle TLS-Kommunikationsendpunkte im Verwaltungsnetzwerk die zur Identifizierung ihrer Peers verwendeten Zertifikate überprüfen, bevor vertrauliche Daten übertragen werden.

Die Zertifikatsüberprüfung ist bei Neuinstallationen von XenServer 8 und höher standardmäßig aktiviert. Wenn Sie ein Upgrade von einer früheren Version von XenServer oder Citrix Hypervisor durchführen, wird die Zertifikatsüberprüfung nicht automatisch aktiviert und Sie müssen sie aktivieren.

XenCenter fordert Sie auf, die Zertifikatsüberprüfung zu aktivieren, wenn Sie das nächste Mal eine Verbindung zum aktualisierten Pool herstellen.

Weitere Informationen finden Sie unter Zertifikatsverifizierung.

Verwendung von Port 80 beschränken

Um die Sicherheit zu verbessern, können Sie mit XenServer 8 jetzt den TCP-Port 80 auf der Verwaltungsschnittstelle schließen und ausschließlich HTTPS über Port 443 für die Kommunikation mit XenServer verwenden. Bevor Sie jedoch Port 80 schließen, überprüfen Sie, ob alle Ihre API-Clients (insbesondere Citrix Virtual Apps and Desktops) HTTPS über Port 443 verwenden können.

Standardmäßig ist Port 80 immer noch geöffnet. Alle internen Verbindungen für die VM-Migration verwenden jetzt jedoch standardmäßig HTTPS über Port 443.

Weitere Informationen zum Schließen von Port 80 finden Sie unter Verwendung von Port 80 einschränken.

Komprimierung des Migrationsdatenstroms

Die Komprimierungsfunktion für Migrationsstreams ermöglicht es Ihnen, die Speicherübertragung in langsamen Netzwerken bei der Live-Migration einer VM zu beschleunigen, indem Sie den Datenstrom zwischen den Hosts komprimieren. Aktivieren Sie es über XenCenter oder die Xe-CLI. Weitere Informationen finden Sie unter Pooleigenschaften —Erweitert und Poolparameter.

Winbind ersetzt PBIS

Winbind hat PBIS ersetzt, um Active Directory (AD) -Benutzer beim AD-Server zu authentifizieren und die Kommunikation mit dem AD-Server zu verschlüsseln. Diese Ersetzung erfolgt automatisch, wenn Sie ein Upgrade durchführen. In dem unwahrscheinlichen Fall, dass die externe Authentifizierung nach dem Upgrade auf XenServer 8 nicht funktioniert, verlassen Sie die AD-Domäne und treten Sie ihr erneut bei.

Infolge dieser Änderung gibt es einige geringfügige Unterschiede im Verhalten:

- Wenn Sie den Befehl `xe pool-enable-external-auth` verwenden, um einer Domäne beizutreten, wird der Parameter `config:disable_modules` jetzt ignoriert. Dieser Parameter ist spezifisch für PBIS.
- Für den Befehl unterstützt der Parameter `config:ou` jetzt eines der folgenden Formate `xe pool-enable-external-auth`, wenn eine Organisationseinheit mit mehreren Layer angegeben wird: `config:ou=a/b/c` oder `config:ou=c,ou=b,ou=a`.

- Winbind aktualisiert das Computerkontokennwort automatisch alle 14 Tage oder wie in der Konfigurationsoption `winbind_machine_pwd_timeout`angegeben.
- Winbind unterstützt die folgenden Szenarien nicht:
  - Leerzeichen am Anfang oder Ende eines Domänenbenutzers oder eines Domänengruppennamens.
  - Domain-Benutzernamen, die mindestens 64 Zeichen enthalten.
  - Domain-Benutzernamen, die eines der Sonderzeichen +<>”=/%@:,; ‘enthalten
  - Domaingruppennamen, die eines der Sonderzeichen,; ‘enthalten

Weitere Informationen finden Sie unter Winbind.

Integrierter PVS-Beschleuniger

In früheren Versionen von XenServer oder Citrix Hypervisor wurde der PVS-Accelerator als ergänzendes Paket bereitgestellt. Der PVS-Accelerator ist jetzt in der XenServer-Basisinstallation enthalten. Das Verhalten des PVS-Accelerators ist ansonsten unverändert und Sie müssen ihn vor der Verwendung konfigurieren.

Weitere Informationen zum PVS-Accelerator finden Sie unter PVS-Accelerator.

Netzwerkstart einer VM über IPv6

Sie können jetzt eine VM über ein IPv6-Netzwerk über ein Netzwerk booten. Diese Funktion wird nur für UEFI-VMs unterstützt, nicht für BIOS-VMs.

Entfernte Features

Die folgenden Funktionen werden in XenServer nicht mehr unterstützt:

- Legacy Partitionslayout
- Systemintegritätsprüfung
- Measured Boot Supplemental Pack
- Virtuelle Linux-Appliance

> **Hinweis:**
>
> Die Protokolle für den Health Check-Dienst werden von Windows zur Problembehandlung aufbewahrt. Um diese Protokolle zu entfernen, löschen Sie sie manuell in `%SystemRoot%\System32\Winevt\Logs` auf dem Windows-Computer, auf dem XenCenter ausgeführt wird.

Änderungen an Komponenten von Drittanbietern

PuTTY ist nicht mehr mit XenCenter gebündelt. Um eine SSH-Konsole mit XenCenter auf einem XenServer-Host zu starten, müssen Sie ein externes SSH-Konsolentool installieren und sicherstellen, dass XenCenter für dessen Verwendung konfiguriert ist. Weitere Informationen finden Sie unter XenCenter für die Verwendung einer externen SSH-Konsole konfigurieren.

Die folgenden Broadcom-Binärdateien sind nicht mehr in der XenServer-Installation enthalten:

- elxocmcore
- elxocmcorelibs
- hbaapiwrapper

Führen Sie die folgenden Schritte aus, um diese Binärdateien von der Broadcom Emulex-Downloadseite herunterzuladen:

1. Gehen Sie zum Abschnitt **Verwaltungssoftware & Tools**.
2. Laden Sie das **Emulex HBA Manager Core Application Kit (CLI) für Citrix XenServer**herunter.

Die folgenden Marvell-Befehlszeilen-Binärdateien sind nicht mehr in der XenServer-Installation enthalten:

- QConvergeConsole CLI für Citrix (QCC)
- QCS

Führen Sie die folgenden Schritte aus, um QCC von der Marvell QLogic-Downloadseite herunterzuladen:

1. Wählen Sie die Registerkarte **Adapter**.
2. Wählen Sie im linken Bereich den Adaptertyp aus.
3. Wählen Sie im mittleren Bereich das Modell Ihres Adapters aus.
4. Wählen Sie im rechten Bereich **Citrix Hypervisor**.
5. Klicken Sie auf **Go**. Sie werden auf eine Seite mit den verfügbaren Downloads weitergeleitet.
6. Laden Sie die **QConvergeConsole CLI für Citrix (**QCC) herunter.

Um diese Anwendung zu installieren, folgen Sie den Anweisungen im QConvergeConsole Command Line Utility User's Guide.

Hinweise zur Kompatibilität

XenServer 8 ist mit den folgenden Komponenten kompatibel:

- Die neueste Version der XenServer VM Tools für Windows
- Die neueste Version der XenServer VM Tools für Linux

- Die neueste Version der virtuellen Workload Balancing-Appliance
- Die neueste Version der virtuellen XenServer Conversion Manager-Appliance

Diese Komponenten sind auf der XenServer-Downloadseiteverfügbar.

---

layout: doc
description: Changes that are available in the Early Access update channel that have not yet progressed to the Normal update channel.—

Kanalupdates im Early-Access-Modus

Die folgenden Funktionen, Vorschaufunktionen, Verbesserungen und Fehlerbehebungen sind im Early-Access-Updatekanal verfügbar. Einige der zuletzt aufgelisteten Einträge sind möglicherweise noch nicht im normalen Kanal verfügbar. Dieser Artikel listet nicht alle Änderungen im Early-Access-Kanal auf, sondern nur eine Teilmenge. Den vollständigen Satz der verfügbaren Änderungen finden Sie in den Informationen in der XenCenter **Update-Ansicht** .

25. März 2024

Diese Updates beinhalten die folgenden Verbesserungen:

- Reduzieren Sie die CPU-Auslastung von QEMU im Leerlauf.
- Aktualisieren Sie den Cisco Enic-Treiber auf 4.5.0.7.
- Aktualisieren Sie den Cisco FNIC-Treiber auf 2.0.0.90.

18. März 2024

Diese Updates beheben das folgende Problem:

- Nach dem Upgrade von Citrix Hypervisor 8.2 CU1 werden die Hintergrundwartungsdienste für GFS2 SRs nicht ordnungsgemäß gestartet.

14. März 2024

Diese Updates beheben die folgenden Probleme:

- Wenn der Poolkoordinator nicht läuft oder der Toolstack neu gestartet wird, schlagen vTPM-Operationen, die vom Benutzer oder von Windows im Hintergrund ausgeführt werden, möglicherweise fehl.
- Korrigieren Sie die Namen einiger SR-Typen in xsconsole.
- Änderungen am Upstream-Code, durch die die Zahl falsch positiver Meldungen für CVE-2023-38545 reduziert werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Upstream-Codeänderungen, die die Zahl falsch positiver Meldungen für CVE-2023-28486 reduzieren können.

12. März 2024

Diese Updates beinhalten die folgenden Änderungen an XenServer:

- Wenn Sie XenServer 8 Preview mit einer Citrix Virtual Apps and Desktops-Lizenz verwenden, ist diese Lizenz veraltet und wird von XenServer 8 nicht mehr unterstützt.

  Um einen Citrix Virtual Apps and Desktops-Workload auf einem XenServer 8-Pool auszuführen, müssen Sie eine XenServer Premium Edition-Lizenz für alle Hosts im Pool erwerben. Weitere Informationen finden Sie auf der XenServer-Website.

Diese Updates beheben das folgende Problem:

- XSA-452 CVE-2023-28746

  Weitere Informationen finden Sie im Security Bulletin: https://support.citrix.com/article/CTX616982.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie die Intel IPU 2024.1 Microcode-Version.

06. März 2024

> **Hinweis:**
>
> Bevor Sie diese Updates anwenden, aktualisieren Sie Ihr XenCenter auf Version 2024.1.0 oder höher. Die neueste Version von XenCenter ist unter https://xenserver.com/downloads verfügbar.

Diese Updates enthalten die folgende Funktion:

- Die Bezeichnung "Vorschau"wurde aus der Windows 11-Vorlage entfernt. Dieses Gastbetriebssystem ist bereit, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion auf die vollständige Unterstützung in der Produktion umgestellt wird.

Diese Updates beheben die folgenden Probleme:

- Bei der Erfassung von Leistungsstatistiken für Hosts und Gäste sind die gesammelten RRD-Dateien oft nicht aktuell.
- In XenServer 8-Clustern mit GFS2-SRs wird beim Sammeln der XenServer-Datenbanken die Cluster-Daemon-Datenbank nicht erfasst.
- Wenn Sie beim Sammeln eines Serverstatusberichts ein vollständiges Bug-Report-Archiv anfordern und die Dateigrößenbeschränkung einer Datenbank für xcp-rrdd-plugins überschritten wird, werden die Logdateien von xcp-rrdd-plugin nicht gesammelt.
- Gehen Sie beim Erfassen eines Serverstatusberichts wie folgt vor, wenn Sie die SSH-Anmeldung verwenden:
  - Der interaktive Modus, in dem Sie einzelne Dateien für die Erfassung bestätigen, funktioniert ohne spezielle Benutzereingaben nicht.
  - Beim Herunterladen unkomprimierter RRD-Daten mit einer veralteten Methode werden die VM-RRDs nicht erfasst.
- CVE-2023-45230 —Pufferüberlauf im DHCPv6-Client über eine lange Server-ID-Option.
- CVE-2023-45231 —Beim Verarbeiten einer ND-Redirect-Nachricht mit verkürzten Optionen werden Werte außerhalb der Grenzen gelesen.
- CVE-2023-45232 —Endlosschleife beim Parsen unbekannter Optionen im Destination Options-Header.
- CVE-2023-45233 —Endlosschleife beim Analysieren einer PAdN-Option im Destination Options-Header.
- CVE-2023-45234 —Pufferüberlauf bei der Verarbeitung der Option DNS-Server in einer DHCPv6-Advertise-Nachricht.
- CVE-2023-45235 —Pufferüberlauf bei der Verarbeitung der Server-ID-Option aus einer DHCPv6-Proxy-Advertise-Nachricht.
- Ein Problem mit der Verwendung von vTPM, während der Toolstack neu gestartet wird.
- Der Status von NIC-Bindungen wird nicht korrekt wiedergegeben.

Diese Updates beinhalten die folgenden Verbesserungen:

- Verbesserungen an der Art und Weise, wie Sie Softwareupdates auf Ihre XenServer-Hosts und -Pools anwenden. Weitere Informationen finden Sie unter Updates anwenden.
- Aktualisieren Sie die für PURE FlashArray SAN verwendete Multipath-Konfiguration, sodass sie den Empfehlungen des Anbieters entspricht.
- Verbessern Sie die Fehlermeldungen, wenn SR-Typen für Dateien schreibgeschützt sind.
- Verbesserungen beim verteilten Tracing.

28. Februar 2024

Diese Updates beheben die folgenden Probleme:

- XSA-451 CVE-2023-46841.
- Ein Migrationsproblem mit VMs, auf denen CMP_LEGACY zuvor aufgetreten ist.

21. Februar 2024

Diese Updates enthalten die folgende neue Funktion:

- Überwachen Sie Host- und Dom0-Ressourcen mit SNMP. Diese Funktion kann ab der nächsten Version von XenCenter verwendet werden. Weitere Informationen finden Sie unter Host- und Dom0-Ressourcen mit SNMP überwachen.

Diese Updates beheben die folgenden Probleme:

- Wenn Sie versuchen, SR-IOV auf einer Intel E810-NIC in XenCenter zu aktivieren, funktioniert die einer VM zugewiesene VF nach dem Start der VM nicht.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisiere Xen von 4.13 auf 4.17.
- Verschiedene Verbesserungen der GFS2-Datenpfadoperationen.

12. Februar 2024

Diese Updates beinhalten die folgende neue Funktion:

- Hinzufügen einer neuen Überprüfung zum NRPE-Dienst (`check_multipath`), um die Überwachung des Multipath-Status zu ermöglichen.

Diese Updates beheben die folgenden Probleme:

- Wenn es innerhalb des IQN separate unabhängige Zielportalgruppen gibt, kann sich XenServer nicht bei allen iSCSI-Portalen anmelden.
- Wenn Sie eine SMB-ISO-SR-Freigabe erstellen, müssen Sie keine Anmeldeinformationen mehr angeben, wenn Sie eine Verbindung zu einem SMB-Server herstellen, der Gastzugriff ermöglicht.
- Ein Teil des Toolstacks wird möglicherweise unerwartet nicht mehr ausgeführt.
- Sie können keine angehaltene Windows 11-VM importieren, die als XVA mit Erhaltung des Energiestatus exportiert wurde.
- Wenn eine VM mit vTPM gestartet oder schnell zwischen Pools hin und her migriert wird, kann eine Rennbedingung auftreten.

- `pool-eject`-Vorgänge, die parallel ausgeführt werden, können zu TLS-Überprüfungsfehlern führen.
- Korrekturen für mehrere Probleme mit GFS2 SRs mit geringer Wahrscheinlichkeit.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Qlogic Fastlinq-Treiber auf 8.74.0.2.
- Verbesserungen beim verteilten Tracing.

29. Januar 2024

Diese Updates beinhalten die folgenden Verbesserungen:

- Unterstützung für UEFI-Boot und Secure Boot für Linux-Gastbetriebssysteme. Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.
- Geben Sie detailliertere Informationen zu den SHA256- und SHA1-TLS-Zertifikaten eines XenServer-Hosts in der Hostkonsolenansicht in XenCenter an.

23. Januar 2024

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX587605.

15. Januar 2024

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie XenServer VM Tools for Linux auf Version 8.4.0-1, die von der XenServer-Downloadseite heruntergeladen werden kann. Ab dieser Version können Sie das Skript `install.sh` verwenden, um XenServer VM Tools für Linux zu deinstallieren. Weitere Informationen finden Sie unter Deinstallieren der XenServer VM Tools für Linux.
- Stellen Sie sicher, dass die XenServer-Willkommensnachricht immer angezeigt wird, wenn Sie eine Verbindung zu einer XenServer-Hostkonsole herstellen, und dass die Nachricht korrekt in Zeilen umbrochen ist.

4. Januar 2024

Diese Updates beheben die folgenden Probleme:

- Manchmal werden die Warnungen der VM nach der Migration einer VM von einem Pool in einen anderen nicht erfolgreich in den Zielpool kopiert oder aus dem Quellpool entfernt.

- Manchmal wird die Pool-Datenbank nicht aus dem Redo-Log wiederhergestellt (Teil der Hochverfügbarkeitsfunktion).

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Microsemi-Smartpqi-Treiber auf 2.1.26_030.
- Aktualisieren Sie den AMD-Mikrocode auf den Drop 2023-12-05.
- Verbesserungen beim verteilten Tracing.

11. Dezember 2023

Diese Updates beheben die folgenden Probleme:

- Wenn Sie Multipathing mit der Firmware v7.x der Dell EqualLogic PS Serie verwenden, werden möglicherweise iSCSI-Protokollfehler angezeigt.

27. November 2023

Diese Updates beheben die folgenden Probleme:

- Manchmal gibt das Redo-Log (Teil der Hochverfügbarkeitsfunktion) nicht alle Datenbankschreibvorgänge wieder.
- Wenn der Befehl `vdi-copy` zum Kopieren eines VDI auf eine SR ausgeführt wird, meldet XenServer den Fortschritt des Vorgangs nicht korrekt.
- In XenCenter kann das Anpassen einer Vorlage und das anschließende Exportieren und erneute Importieren dazu führen, dass die Vorlage nicht importiert werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Treiber für Dell PERC12 hinzugefügt (Treiberversion: mpi3mr 8.1.4.0.0).
- Allgemeine API-Verbesserungen.
- Die Bezeichnung “Preview”wurde aus der vTPM-Unterstützung entfernt. Dies bedeutet, dass vTPM bereit ist, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion zur vollständigen Unterstützung in der Produktion wechselt.

15. November 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Das Label “Vorschau”wurde aus der Ubuntu 22.04-Vorlage entfernt. Dieses Gastbetriebssystem ist bereit, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion auf die vollständige Unterstützung in der Produktion umgestellt wird.

14. November 2023

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX583037/.

6. November 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Allgemeine SDK-Verbesserungen und verbesserte API-Anmeldezeiten.
- Aktualisieren Sie Open vSwitch auf v2.17.7.

3. November 2023

Diese Updates beinhalten allgemeine Korrekturen und Verbesserungen.

25. Oktober 2023

Diese Updates beheben die folgenden Probleme:

- Die Bereitstellung von Windows mithilfe von PXE-Start und Configuration Manager kann dazu führen, dass Windows hängen bleibt.
- Wenn die Uhrzeitsynchronisierung deaktiviert ist, geben Windows-VMs nicht die richtige Uhrzeit zurück.

Diese Updates beinhalten die folgenden Verbesserungen:

- Windows-VMs im UEFI-Startmodus zeigen jetzt beim Booten das Windows-Logo anstelle des Tianocore-Logos.

18. Oktober 2023

Diese Updates beinhalten allgemeine Korrekturen und Verbesserungen.

11. Oktober 2023

Unterstützung für die folgenden Gastbetriebssysteme:

- Debian Bookworm 12
- Rocky Linux 9
- CentOS Stream 9

> **Hinweis:**
>
> Kunden, die diese Gastbetriebssysteme verwenden möchten, müssen auch die XenServer VM Tools für Linux v8.3.1-1 oder höher installieren, die auf der XenServer-Produktdownloadseite heruntergeladen werden können.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Treiber Mellanox mlnx_en auf 5.9-0.5.5.0.

10. Oktober 2023

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX575089/.

2. Oktober 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Unterstützung für das Red Hat Enterprise Linux 9-Betriebssystem. Weitere technische Informationen finden Sie in den Versionshinweisen zu Red Hat Enterprise Linux 9.

> **Hinweis:**
>
> Kunden, die dieses Gastbetriebssystem verwenden möchten, müssen auch Citrix VM Tools für Linux v8.3.1-1 oder höher installieren, die auf der XenServer-Produktdownloadseite heruntergeladen werden können.

18. September 2023

Diese Updates beinhalten allgemeine Korrekturen und Verbesserungen.

11. September 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktivieren Sie den Interrupt-Balancing für Fibre Channel (FC) -PCI-Geräte. Dies verbessert die Leistung schneller FC-HBA-SRs, insbesondere wenn Multipathing verwendet wird.
- Fix für AMD-Errata #1474. Deaktivieren Sie C6 nach 1000 Tagen Betriebszeit auf AMD Zen2-Systemen, um einen Absturz nach ~1044 Tagen zu vermeiden.

31. August 2023

Diese Updates beheben die folgenden Probleme:

- Leistungsmetriken sind für GFS2 SRs und Datenträger auf diesen SRs nicht verfügbar.
- Sie können keine Snapshots oder Checkpoints für eine suspendierte VM erstellen, wenn an diese VM ein vTPM angehängt ist.
- Wenn ein XenServer-Host abstürzt oder abrupt heruntergefahren wird, schlägt das Starten weiterer Windows 11-VMs oder das Migrieren weiterer Windows 11-VMs auf diesen Host schließlich fehl.
- Wenn beim Anschließen von iSCSI-SRs nicht alle möglichen Pfade verfügbar sind (z. B. ist ein Offline-Controller-Remote-Port ausgefallen), werden dem SR keine zusätzlichen iSCSI-Sitzungen hinzugefügt, wenn auf diese Remote-Ports wieder zugegriffen werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Intel Ice-Treiber auf v1.11.17.1.
- Leistungsverbesserungen für GFS2.

---

layout: doc
description: Changes that are available in the Normal update channel after having progressed from the Early Access update channel.—

Normale Kanalupdates

Updates wechseln in regelmäßigen Abständen vom Early-Access-Updatekanal auf Normal. Die folgenden Funktionen, Vorschaufunktionen, Verbesserungen und Fehlerbehebungen sind im normalen Updatekanal verfügbar. In diesem Artikel werden nicht alle Änderungen im Kanal Normal aufgeführt, sondern nur eine Teilmenge. Den vollständigen Satz der verfügbaren Änderungen finden Sie in den Informationen in der XenCenter **Update-Ansicht** .

19. März 2024

Diese Updates beheben die folgenden Probleme:

- Korrigieren Sie die Namen einiger SR-Typen in xsconsole.
- Änderungen am Upstream-Code, durch die die Zahl falsch positiver Meldungen für CVE-2023-38545 reduziert werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Upstream-Codeänderungen, die die Zahl falsch positiver Meldungen für CVE-2023-28486 reduzieren können.

18. März 2024

Diese Updates beheben die folgenden Probleme:

- Wenn der Poolkoordinator nicht läuft oder der Toolstack neu gestartet wird, schlagen vTPM-Operationen, die vom Benutzer oder von Windows im Hintergrund ausgeführt werden, möglicherweise fehl.
- Nach dem Upgrade von Citrix Hypervisor 8.2 CU1 werden die Hintergrundwartungsdienste für GFS2 SRs nicht ordnungsgemäß gestartet.

12. März 2024

Diese Updates beinhalten die folgenden Änderungen an XenServer:

- Wenn Sie XenServer 8 Preview mit einer Citrix Virtual Apps and Desktops-Lizenz verwenden, ist diese Lizenz veraltet und wird von XenServer 8 nicht mehr unterstützt.

  Um einen Citrix Virtual Apps and Desktops-Workload auf einem XenServer 8-Pool auszuführen, müssen Sie eine XenServer Premium Edition-Lizenz für alle Hosts im Pool erwerben. Weitere Informationen finden Sie auf der XenServer-Website.

Diese Updates beheben das folgende Problem:

- XSA-452 CVE-2023-28746

  Weitere Informationen finden Sie im Security Bulletin: https://support.citrix.com/article/CTX616982.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie die Intel IPU 2024.1 Microcode-Version.

07. März 2024

> **Hinweis:**
>
> Bevor Sie diese Updates anwenden, aktualisieren Sie Ihr XenCenter auf Version 2024.1.0 oder höher. Die neueste Version von XenCenter ist unter https://xenserver.com/downloads verfügbar.

Diese Updates enthalten die folgende Funktion:

- Die Bezeichnung “Vorschau”wurde aus der Windows 11-Vorlage entfernt. Dieses Gastbetriebssystem ist bereit, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion auf die vollständige Unterstützung in der Produktion umgestellt wird.

Diese Updates beheben die folgenden Probleme:

- Bei der Erfassung von Leistungsstatistiken für Hosts und Gäste sind die gesammelten RRD-Dateien oft nicht aktuell.
- In XenServer 8-Clustern mit GFS2-SRs wird beim Sammeln der XenServer-Datenbanken die Cluster-Daemon-Datenbank nicht erfasst.
- Wenn Sie beim Sammeln eines Serverstatusberichts ein vollständiges Bug-Report-Archiv anfordern und die Dateigrößenbeschränkung einer Datenbank für xcp-rrdd-plugins überschritten wird, werden die Logdateien von xcp-rrdd-plugin nicht gesammelt.
- Gehen Sie beim Erfassen eines Serverstatusberichts wie folgt vor, wenn Sie die SSH-Anmeldung verwenden:
  - Der interaktive Modus, in dem Sie einzelne Dateien für die Erfassung bestätigen, funktioniert ohne spezielle Benutzereingaben nicht.
  - Beim Herunterladen unkomprimierter RRD-Daten mit einer veralteten Methode werden die VM-RRDs nicht erfasst.
- CVE-2023-45230 —Pufferüberlauf im DHCPv6-Client über eine lange Server-ID-Option.
- CVE-2023-45231 —Beim Verarbeiten einer ND-Redirect-Nachricht mit verkürzten Optionen werden Werte außerhalb der Grenzen gelesen.
- CVE-2023-45232 —Endlosschleife beim Parsen unbekannter Optionen im Destination Options-Header.
- CVE-2023-45233 —Endlosschleife beim Analysieren einer PAdN-Option im Destination Options-Header.
- CVE-2023-45234 —Pufferüberlauf bei der Verarbeitung der Option DNS-Server in einer DHCPv6-Advertise-Nachricht.
- CVE-2023-45235 —Pufferüberlauf bei der Verarbeitung der Server-ID-Option aus einer DHCPv6-Proxy-Advertise-Nachricht.
- Ein Problem mit der Verwendung von vTPM, während der Toolstack neu gestartet wird.
- Der Status von NIC-Bindungen wird nicht korrekt wiedergegeben.

Diese Updates beinhalten die folgenden Verbesserungen:

- Verbesserungen an der Art und Weise, wie Sie Softwareupdates auf Ihre XenServer-Hosts und -Pools anwenden. Weitere Informationen finden Sie unter Updates anwenden.
- Aktualisieren Sie die für PURE FlashArray SAN verwendete Multipath-Konfiguration, sodass sie den Empfehlungen des Anbieters entspricht.
- Verbessern Sie die Fehlermeldungen, wenn SR-Typen für Dateien schreibgeschützt sind.
- Verbesserungen beim verteilten Tracing.

28. Februar 2024

Diese Updates enthalten die folgende neue Funktion:

- Überwachen Sie Host- und Dom0-Ressourcen mit SNMP. Diese Funktion kann ab der nächsten Version von XenCenter verwendet werden.

Diese Updates beheben die folgenden Probleme:

- Wenn Sie versuchen, SR-IOV auf einer Intel E810-NIC in XenCenter zu aktivieren, funktioniert die einer VM zugewiesene VF nach dem Start der VM nicht.
- XSA-451 CVE-2023-46841.
- Ein Migrationsproblem mit VMs, auf denen CMP_LEGACY zuvor aufgetreten ist.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisiere Xen von 4.13 auf 4.17.
- Verschiedene Verbesserungen der GFS2-Datenpfadoperationen.

15. Februar 2024

Diese Updates beinhalten die folgende neue Funktion:

- Hinzufügen einer neuen Überprüfung zum NRPE-Dienst (`check_multipath`), um die Überwachung des Multipath-Status zu ermöglichen.

Diese Updates beheben die folgenden Probleme:

- Wenn es innerhalb des IQN separate unabhängige Zielportalgruppen gibt, kann sich XenServer nicht bei allen iSCSI-Portalen anmelden.
- Wenn Sie eine SMB-ISO-SR-Freigabe erstellen, müssen Sie keine Anmeldeinformationen mehr angeben, wenn Sie eine Verbindung zu einem SMB-Server herstellen, der Gastzugriff ermöglicht.
- Ein Teil des Toolstacks wird möglicherweise unerwartet nicht mehr ausgeführt.
- Sie können keine angehaltene Windows 11-VM importieren, die als XVA mit Erhaltung des Energiestatus exportiert wurde.
- Wenn eine VM mit vTPM gestartet oder schnell zwischen Pools hin und her migriert wird, kann eine Rennbedingung auftreten.
- `pool-eject`-Vorgänge, die parallel ausgeführt werden, können zu TLS-Überprüfungsfehlern führen.
- Korrekturen für mehrere Probleme mit GFS2 SRs mit geringer Wahrscheinlichkeit.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Qlogic Fastlinq-Treiber auf 8.74.0.2.
- Verbesserungen beim verteilten Tracing.

01. Februar 2024

Diese Updates beinhalten die folgenden Verbesserungen:

- Unterstützung für UEFI-Boot und Secure Boot für Linux-Gastbetriebssysteme. Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.
- Geben Sie detailliertere Informationen zu den SHA256- und SHA1-TLS-Zertifikaten eines XenServer-Hosts in der Hostkonsolenansicht in XenCenter an.

23. Januar 2024

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX587605.

18. Januar 2024

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie XenServer VM Tools for Linux auf Version 8.4.0-1, die von der XenServer-Downloadseite heruntergeladen werden kann. Ab dieser Version können Sie das Skript `install.sh` verwenden, um XenServer VM Tools für Linux zu deinstallieren. Weitere Informationen finden Sie unter Deinstallieren der XenServer VM Tools für Linux.
- Stellen Sie sicher, dass die XenServer-Willkommensnachricht immer angezeigt wird, wenn Sie eine Verbindung zu einer XenServer-Hostkonsole herstellen, und dass die Nachricht korrekt in Zeilen umbrochen ist.

8. Januar 2024

Diese Updates beheben die folgenden Probleme:

- Manchmal werden die Warnungen der VM nach der Migration einer VM von einem Pool in einen anderen nicht erfolgreich in den Zielpool kopiert oder aus dem Quellpool entfernt.
- Manchmal wird die Pool-Datenbank nicht aus dem Redo-Log wiederhergestellt (Teil der Hochverfügbarkeitsfunktion).

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Microsemi-Smartpqi-Treiber auf 2.1.26_030.

- Aktualisieren Sie den AMD-Mikrocode auf den Drop 2023-12-05.
- Verbesserungen beim verteilten Tracing.

14. Dezember 2023

Diese Updates beheben die folgenden Probleme:

- Wenn Sie Multipathing mit der Firmware v7.x der Dell EqualLogic PS Serie verwenden, werden möglicherweise iSCSI-Protokollfehler angezeigt.

30. November 2023

Diese Updates beheben die folgenden Probleme:

- Manchmal gibt das Redo-Log (Teil der Hochverfügbarkeitsfunktion) nicht alle Datenbankschreibvorgänge wieder.
- Wenn der Befehl `vdi-copy` zum Kopieren eines VDI auf eine SR ausgeführt wird, meldet XenServer den Fortschritt des Vorgangs nicht korrekt.
- In XenCenter kann das Anpassen einer Vorlage und das anschließende Exportieren und erneute Importieren dazu führen, dass die Vorlage nicht importiert werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Treiber für Dell PERC12 hinzugefügt (Treiberversion: mpi3mr 8.1.4.0.0).
- Allgemeine API-Verbesserungen.
- Die Bezeichnung "Preview"wurde aus der vTPM-Unterstützung entfernt. Dies bedeutet, dass vTPM bereit ist, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion zur vollständigen Unterstützung in der Produktion wechselt.

22. November 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Das Label "Vorschau"wurde aus der Ubuntu 22.04-Vorlage entfernt. Dieses Gastbetriebssystem ist bereit, vollständig unterstützt zu werden, wenn XenServer 8 von der Vorschauversion auf die vollständige Unterstützung in der Produktion umgestellt wird.

15. November 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Allgemeine SDK-Verbesserungen und verbesserte API-Anmeldezeiten.
- Aktualisieren Sie Open vSwitch auf v2.17.7.

14. November 2023

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX583037/.

6. November 2023

Diese Updates beheben die folgenden Probleme:

- Die Bereitstellung von Windows mithilfe von PXE-Start und Configuration Manager kann dazu führen, dass Windows hängen bleibt.
- Wenn die Uhrzeitsynchronisierung deaktiviert ist, geben Windows-VMs nicht die richtige Uhrzeit zurück.

Diese Updates beinhalten die folgenden Verbesserungen:

- Windows-VMs im UEFI-Startmodus zeigen jetzt beim Booten das Windows-Logo anstelle des Tianocore-Logos.

23. Oktober 2023

Diese Updates beinhalten allgemeine Korrekturen und Verbesserungen.

16. Oktober 2023

Diese Updates beinhalten Unterstützung für die folgenden Gastbetriebssysteme:

- Debian Bookworm 12
- Rocky Linux 9
- CentOS Stream 9

> **Hinweis:**
>
> Kunden, die diese Gastbetriebssysteme verwenden möchten, müssen auch die XenServer VM Tools für Linux v8.3.1-1 oder höher installieren, die auf der XenServer-Produktdownloadseiteheruntergeladen werden können.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Treiber Mellanox mlnx_en auf 5.9-0.5.5.0.

10. Oktober 2023

Diese Updates beinhalten Sicherheitskorrekturen. Weitere Informationen finden Sie im Sicherheitsbulletin https://support.citrix.com/article/CTX575089/.

5. Oktober 2023

Diese Updates beinhalten Unterstützung für das Red Hat Enterprise Linux 9-Betriebssystem. Weitere technische Informationen finden Sie in den Versionshinweisen zu Red Hat Enterprise Linux 9.

> **Hinweis:**
>
> Kunden, die dieses Gastbetriebssystem verwenden möchten, müssen auch Citrix VM Tools für Linux v8.3.1-1 oder höher installieren, die auf der XenServer-Produktdownloadseiteheruntergeladen werden können.

21. September 2023

Diese Updates beinhalten allgemeine Korrekturen und Verbesserungen.

14. September 2023

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktivieren Sie den Interrupt-Balancing für Fibre Channel (FC) -PCI-Geräte. Dies verbessert die Leistung schneller FC-HBA-SRs, insbesondere wenn Multipathing verwendet wird.
- Fix für AMD-Errata #1474. Deaktivieren Sie C6 nach 1000 Tagen Betriebszeit auf AMD Zen2-Systemen, um einen Absturz nach ~1044 Tagen zu vermeiden.

4. September 2023

Diese Updates beheben die folgenden Probleme:

- Leistungsmetriken sind für GFS2 SRs und Datenträger auf diesen SRs nicht verfügbar.
- Sie können keine Snapshots oder Checkpoints für eine suspendierte VM erstellen, wenn an diese VM ein vTPM angehängt ist.
- Wenn ein XenServer-Host abstürzt oder abrupt heruntergefahren wird, schlägt das Starten weiterer Windows 11-VMs oder das Migrieren weiterer Windows 11-VMs auf diesen Host schließlich fehl.

- Wenn beim Anschließen von iSCSI-SRs nicht alle möglichen Pfade verfügbar sind (z. B. ist ein Offline-Controller-Remote-Port ausgefallen), werden dem SR keine zusätzlichen iSCSI-Sitzungen hinzugefügt, wenn auf diese Remote-Ports wieder zugegriffen werden kann.

Diese Updates beinhalten die folgenden Verbesserungen:

- Aktualisieren Sie den Intel Ice-Treiber auf v1.11.17.1.
- Leistungsverbesserungen für GFS2.

---

layout: doc
description: This release of XenServer contains a number of fixes to issues that were present in previous releases.—

Behobene Probleme

Die folgenden Probleme wurden in XenServer 8 behoben. Zusätzlich zu diesen behobenen Problemen werden weitere Fixes auf den Update-Kanälen Normal und Early Access veröffentlicht.

Allgemein

- Ein Neustart der VM hat nicht den gleichen Effekt wie das Ausschalten und anschließende Starten der VM. (CA-188042)
- Wenn ein Active Directory Directory-Benutzer die Pool-Admin-Rolle von einer AD-Gruppe erbt, deren Name Leerzeichen enthält, kann sich der Benutzer nicht über SSH bei XenServer 8 anmelden. (CA-363207)
- In Clusterpools kann ein Netzwerkausfall die folgenden Probleme verursachen: Unfähigkeit, nach einem Host-Neustart erneut eine Verbindung zum GFS2-Speicher herzustellen, Unfähigkeit, Hosts in einem Pool hinzuzufügen oder zu entfernen, Schwierigkeiten bei der Verwaltung des Pools. (XSI-1386)

Grafik

- Auf Hardware mit NVIDIA A16/A2-Grafikkarten kann es manchmal vorkommen, dass virtuelle Maschinen mit vGPUs nicht migriert werden und der interne Fehler “Gpumon_interface.Gpumon_error([S(In
“No vGPU available”))])”auftritt. (CA-374118)

Gäste

Windows-Gäste

- Wenn UEFI-Boot-Windows-VMs gestartet werden, zeigen sie ein TianoCore-Logo. (CP-30146)
- Auf einer Windows-VM ist manchmal die IP-Adresse eines SR-IOV-VIF in XenCenter nicht sichtbar. (CA-340227)
- Auf einer Windows-VM mit mehr als 8 vCPUs funktioniert Receive Side Scaling möglicherweise nicht, da der Xenvif-Treiber die Indirektionstabelle nicht einrichten kann. (CA-355277)
- Wenn ein XenServer-Host abstürzt oder abrupt heruntergefahren wird, schlägt das Starten weiterer Windows 11-VMs oder das Migrieren weiterer Windows 11-VMs auf diesen Host schließlich fehl. (CA-375992)

Linux-Gäste

- Die XenServer VM Tools für Linux können einen falschen Wert für den freien Speicher der VM angeben, der höher als der richtige Wert ist. (CA-352996)

Speicher

- Wenn ein iSCSI-LVM-SR mit Multi-Target- und Wildcard-Ziel-IQNs an einen Host angehängt wird, kann der Verbindungsvorgang fehlschlagen, wenn nicht alle Ziele antworten. (CA-375968)
- Wenn auf einer GFS2-SR weniger als 500 MB Speicherplatz vorhanden sind, kann der Vorgang fehlschlagen, wenn Sie versuchen, auf dieser SR gespeicherte Datenträger zu löschen. (CA-379589)
- Beim Versuch, eine Verbindung zu einem schreibgeschützten NFS v3 SR zu reparieren, kann der Vorgang beim ersten Versuch mit dem Fehler “SM hat eine generische Python-Ausnahme ausgelöst”fehlschlagen. Versuchen Sie den Reparaturvorgang erneut, um dieses Problem zu umgehen. Dieses Problem wird durch einen Schreibvorgang beim ersten Reparaturversuch verursacht. (XSI-1374)

Updates

- Während das Installationsupdate für ein Poolmitglied ausgeführt wird, wird möglicherweise der Fehler “Der Vorgang konnte nicht ausgeführt werden, da gerade Updates abgerufen werden” angezeigt. Um diesen Fehler zu beheben, können Sie den Vorgang wiederholen. (CA-381215)

Workload Balancing

- Für eine virtuelle Workload Balancing-Appliance Version 8.2.2 und höher, die kein LVM verwendet, können Sie den verfügbaren Speicherplatz nicht erweitern. (CA-358817)
- In XenCenter ist der im Überwachungsbericht des Workload Balancing-Pools angezeigte Datumsbereich falsch. (CA-357115)
- Während des Wartungsfensters für den Workload Balancing kann der Workload Balancing keine Platzierungsempfehlungen geben. Wenn diese Situation eintritt, wird der Fehler angezeigt: “Die 4010-Pool-Erkennung wurde nicht abgeschlossen. Verwenden des ursprünglichen Algorithmus. “Das Wartungsfenster für den Workload Balancing ist weniger als 20 Minuten lang und standardmäßig um Mitternacht geplant. (CA-359926)

XenCenter

Informationen zu bekannten und behobenen Problemen in XenCenter finden Sie unter XenCenter What’s New.

---

layout: doc
description: These known issues are present in XenServer 8. Workarounds are available for some of the issues.—

Bekannte Probleme

Dieser Artikel enthält Hinweise und kleinere Probleme in der XenServer 8-Version sowie alle Problemumgehungen, die Sie anwenden können.

Allgemein

- Wenn Sie versuchen, über die serielle Konsole eine Verbindung zu einem XenServer-Host herzustellen, akzeptiert die serielle Konsole möglicherweise Tastatureingaben. Wenn Sie warten, bis die Konsole zweimal aktualisiert wurde, akzeptiert die Konsole Tastatureingaben. (CA-311613)
- Wenn das Lesecaching aktiviert ist, ist das Lesen aus dem übergeordneten Snapshot langsamer als aus dem Blatt. (CP-32853)

- Wenn Sie versuchen, sich mit einem falschen Kennwort an der dom0-Konsole anzumelden, wird folgende Fehlermeldung angezeigt: `When trying to update a password , this return status indicates that the value provided as the current password is not correct.` Diese Fehlermeldung wird erwartet, obwohl sie sich auf eine Kennwortänderung und nicht auf eine Anmeldung bezieht. Versuche dich mit dem richtigen Kennwort anzumelden. (CA-356441)
- Wenn ein XenServer-Host unerwartet ausgeschaltet und neu gestartet wird und versucht, VMs wiederherzustellen, an die ein vTPM angehängt war, kann das vTPM manchmal auf der VM fehlen. (CA-379928)

Grafik

- Wenn NVIDIA T4 im Pass-Through-Modus zu einer VM auf einer bestimmten Serverhardware hinzugefügt wurde, wird diese VM möglicherweise nicht eingeschaltet. (CA-360450)

Gäste

- Wenn Sie versuchen, eine virtuelle Maschine mit aktivierter dynamischer Speichersteuerung live auf einen Zielhost zu migrieren, auf dem Ressourcen wie Arbeitsspeicher sehr begrenzt sind, kann die Migration manchmal fehlschlagen. (CA-380607)

Windows-Gäste

- Bei domänenverbundenen Windows 10-VMs (1903 und höher) mit installiertem FireEye-Agent können wiederholte erfolgreiche RDP-Verbindungen dazu führen, dass die VM mit 100%iger CPU-Auslastung bei `ntoskrnl.exe` einfriert. Führen Sie einen harten Neustart auf der VM durch, um sich von diesem Status zu erholen. (CA-323760)
- Wenn Sie eine UEFI-VM erstellen, erfordert die Windows-Installation zum Starten einen Tastendruck. Wenn Sie während des erforderlichen Zeitraums keine Taste drücken, wechselt die VM-Konsole zur UEFI-Shell.

  Um dieses Problem zu umgehen, können Sie den Installationsvorgang auf eine der folgenden Arten neu starten:

  - Geben Sie in der UEFI-Konsole die folgenden Befehle ein.

    ```
    EFI:
    EFI\BOOT\BOOTX64
    ```

  - Starten Sie die VM neu

Wenn der Installationsvorgang neu gestartet wird, achten Sie in der VM-Konsole auf die Installationsaufforderung. Wenn die Eingabeaufforderung erscheint, drücken Sie eine beliebige Taste. (CA-333694)

- Beim Versuch, eine Windows 10-VM von 1909 auf 20H2 oder höher zu aktualisieren, schlägt das Update möglicherweise mit einem blauen Bildschirm fehl, der den Fehler anzeigt: UNZUGÄNGLICHES STARTGERÄT. (XSI-1075)

  Um die Wahrscheinlichkeit zu verringern, dass dieser Fehler auftritt, können Sie die folgenden Schritte ausführen, bevor Sie ein Update durchführen:

  1. Aktualisieren Sie die XenServer VM Tools für Windows auf Ihrer VM auf die neueste Version.
  2. Snapshot der virtuellen Maschine.
  3. Löschen Sie in der VM-Registrierung die folgenden Werte aus dem Schlüssel HKEY_LOCAL_MACHINE\SY
     ActiveDeviceID, ActiveInstanceID und ActiveLocationInformation

- Wenn Sie eine Windows-VM aus einer Vorlage erstellen, die so eingestellt ist, dass ihre Treiber nicht automatisch aktualisiert werden, ist die erstellte VM fälschlicherweise so eingestellt, dass sie ihre Treiber aktualisiert. Führen Sie den folgenden Befehl aus, um dieses Problem zu umgehen: `xe pool-param-set policy-no-vendor-device=true uuid=<pool-uuid>`. Dieser Befehl stellt sicher, dass zukünftige VMs, die anhand der Vorlage erstellt wurden, korrekt so eingestellt sind, dass Treiber nicht automatisch aktualisiert werden. VMs, die zuvor aus der Vorlage generiert wurden, werden nicht geändert. (CA-371529)

- vTPM-Operationen, die vom Benutzer oder von Windows im Hintergrund ausgeführt werden, können in den folgenden Situationen fehlschlagen:

  – Wenn der Toolstack oder der XenServer-Host abstürzt, bevor der Vorgang mit dem Datenträger synchronisiert wird. Fehler beim Schreiben auf den Datenträger werden ignoriert.

  Bei einem solchen Fehler gibt das vTPM einen Fehler an das Betriebssystem zurück. Windows protokolliert diese Fehler im Systemereignisprotokoll.

- Wenn Sie Bitlocker auf einer Windows-VM aktiviert haben und versuchen, diese VM anzuhalten oder fortzusetzen, kann die VM manchmal abstürzen. (CA-368791)

  Darüber hinaus wird Bitlocker nicht für VMs unterstützt, an die ein vTPM angehängt ist.

Linux-Gäste

- Sie können die Funktion Dynamic Memory Control (DMC) nicht auf Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 oder CentOS Stream 9 VMs verwenden, da diese Betriebssysteme kein Memory Ballooning mit dem Xen-Hypervisor unterstützen. (CA-378797)

- Auf einigen Linux-VMs, insbesondere bei stark ausgelasteten Systemen mit ausstehenden Datenträger-I/O, schlagen Versuche, die VM auszusetzen oder live zu migrieren, möglicherweise fehl. Versuchen Sie, den Wert von beispielsweise auf 300000 zu erhöhen `/sys/power/pm_freeze_timeout`, um dieses Problem zu umgehen. Wenn dieser Workaround nicht erfolgreich ist, können Sie den Linux-Kernel der VM auf die neueste Version aktualisieren. (CP-41455)
- Wenn Sie Debian 10 (Buster) über PXE-Netzwerkstarts installieren, fügen Sie den Bootparametern nicht `console=tty0` hinzu. Dieser Parameter kann zu Problemen beim Installationsvorgang führen. Verwenden Sie nur `console=hvc0` in den Bootparametern. (CA-329015)
- Aufgrund eines bekannten Problems mit einigen SUSE Linux-Betriebssystemen schlägt der Vorgang fehl und die VM wird nicht automatisch neu gestartet, wenn Sie versuchen, einen Crash-Dump auf einer SUSE Linux-VM mit 32 oder mehr vCPUs auszulösen. Dieses Problem betrifft die folgenden Betriebssysteme: SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3, 15 SP4. (CA-375759)

Installation

- Wenn Sie ein Upgrade auf oder die Installation von XenServer 8 von einem ISO auf einem IIS-Server durchführen, kann die Installation oder das Upgrade fehlschlagen und Ihre Hosts können nicht neu gestartet werden. Die Remotekonsole zeigt den GRUB-Fehler an: “Datei”/boot/grub/i3860pc/normal.mod ‘nicht gefunden. In den Rettungsmodus wechseln”. Dieses Problem wird durch die IIS-Konfiguration verursacht, die dazu führt, dass Paketdateien fehlen. Um dieses Problem zu umgehen, stellen Sie sicher, dass doppeltes Escaping auf IIS zulässig ist, bevor Sie das Installations-ISO-Image darauf extrahieren. (XSI-1063)

Internationalisierung

- Nicht-ASCII-Zeichen, z. B. Zeichen mit Akzenten, können in der Host-Konsole nicht verwendet werden. (CA-40845)
- In einer Windows-VM, auf der XenServer VM Tools für Windows installiert ist, kann das Kopieren und Einfügen von Doppelbyte-Zeichen fehlschlagen, wenn die Standard-Desktop-Konsole in XenCenter verwendet wird. Die eingefügten Zeichen werden als Fragezeichen (?) angezeigt.

  Um dieses Problem zu umgehen, können Sie stattdessen die Remotedesktop-Konsole verwenden. (CA-281807)

Speicher

- Wenn Sie eine neue Installation von XenServer auf einem Host mit einer lokalen XFS-SR auf einem NVMe-Gerät erstellen, wird Ihr lokaler Speicher beim Booten nicht angehängt. Die Aktion schlägt mit dem Fehler fehl: “Server_Error ausgelöst (SR_BACKEND_FAILURE, [FileNotFoundError; [Errno 2] No such file or directory: ‘/sys/block/nvme0n/queue/scheduler’])”.

  Wenn Sie dieses Problem sehen, kontaktieren Sie uns unter feedback@xenserver.com. Wir arbeiten aktiv an einem Fix, der in einem zukünftigen Update bereitgestellt wird. Stellen Sie sicher, dass Sie Ihren Pool so konfigurieren, dass er die neuesten Updateserhält.
- Wenn Sie GFS2 SRs verwenden und zwei Hosts in Ihrem Clusterpool haben, kann Ihr Cluster während eines Upgrades Quorum und Fencing verlieren. Um diese Situation zu vermeiden, fügen Sie entweder einen Host zu Ihrem Cluster hinzu oder entfernen Sie einen Host aus Ihrem Cluster. Stellen Sie sicher, dass Sie während des Upgrade-Vorgangs entweder einen oder drei Hosts in Ihrem Pool haben. (CA-313222)
- Wenn Sie eine GFS2 SR verwenden und sich Ihr Clusternetzwerk in einem Nicht-Management-VLAN befindet, können Sie Ihrem Clusterpool keine Hosts hinzufügen oder daraus entfernen. (XSI-1604)
- Nach dem Entfernen einer HBA-LUN aus einem SAN werden möglicherweise Protokollmeldungen und E/A-Fehler angezeigt, wenn Informationen zum logischen Volume abgefragt werden. Um dieses Problem zu umgehen, starten Sie den XenServer-Host neu. (XSI-984)
- Sie können den Namen des vom PVS-Accelerator verwendeten Tmpfs-SR nicht festlegen oder ändern. Wenn für `type` die Option `tmpfs` verwendet wird, ignoriert der Befehl `xe sr-create` den für `name-label` gesetzten Wert und verwendet stattdessen einen festen Wert. Wenn Sie versuchen, den Befehl `xe sr-param-set` auszuführen, um den Namen des tmpfs-SRs zu ändern, wird der Fehler SCRIPT_MISSING angezeigt.
- Sie können nicht mehr als 200 PVS-Accelerator-fähige VMs auf einem XenServer-Host ausführen. (CP-39386)

Drittanbieter

- Eine Einschränkung in den neuesten SSH-Clients bedeutet, dass SSH nicht für Benutzernamen funktioniert, die eines der folgenden Zeichen enthalten: `{ } [] | &`. Stellen Sie sicher, dass Ihre Benutzernamen und Active Directory-Servernamen keines dieser Zeichen enthalten.

XenCenter

Informationen zu bekannten und behobenen Problemen in XenCenter finden Sie unter XenCenter What’s New.

Einstellung von Features und Plattformen

April 12, 2024

Die Ankündigungen in diesem Artikel informieren Sie im Voraus über Plattformen, Produkte und Funktionen, die schrittweise eingestellt werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Wir beobachten die Nutzung und das Feedback unserer Kunden, um festzustellen, wann sie zurückgezogen werden. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element.

Informationen zum Produktlebenszyklussupport finden Sie unter Product Lifecycle Support Policy.

Veraltete und entfernte Produkte und Features

Die folgende Tabelle zeigt die Plattformen, Produkte und Funktionen, die veraltet sind oder entfernt wurden.

Veraltete Elemente werden nicht sofort entfernt. Wir unterstützen sie weiterhin in der aktuellen Version, aber sie werden in einer zukünftigen Version entfernt.

Entfernte Elemente werden in XenServer entweder entfernt oder werden nicht mehr unterstützt.

Die **fett** formatierten Datumsangaben weisen auf Änderungen in diesem Release hin.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
XenServer-Anspruch für Kunden von Citrix Virtual Apps and Desktops	**XenServer 8**	**XenServer 8**	Holen Sie sich eine Premium Edition-Lizenz von https://xenserver.com/buy.
BIOS-Startmodus für XenServer-Hosts	**XenServer 8**		Installieren Sie Ihre Hosts stattdessen im UEFI-Startmodus.
XenCenter Verbindungen zu XenServer-Hosts der Version 7.x und früher.	**XenCenter 2023.3.1**	**XenCenter 2023.3.1**	Aktualisieren Sie Ihre nicht unterstützten XenServer-Hosts.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Virtuelle Linux-Appliance - Demo	**XenServer 8**	**XenServer 8**	
Unterstützung für 32-Bit-Windows 10	**XenServer 8**	**XenServer 8**	
Unterstützung für 32-Bit-Debian Bullseye 11	8.2 CU1	**XenServer 8**	
Unterstützung für Bromium Secure Platform in Windows-VMs	8.2 CU1	8.2 CU1	
Systemintegritätsprüfung	XenCenter 8.2.6	XenCenter 8.2.7	
Upload von Serverstatusberichten von XenCenter auf Citrix Insight Services (CIS)	XenCenter 8.2.6	XenCenter 8.2.7	Laden Sie Ihre Statusberichte manuell über die CIS-Website hoch.
PuTTY wurde mit XenCenter installiert	XenCenter 8.2.6	**XenCenter 2023.3.1**	Bei zukünftigen Versionen von XenCenter müssen Sie Ihre eigene Instanz von PuTTY oder OpenSSH auf dem System installieren, auf dem XenCenter installiert ist.
Lokalisierung von XenCenter ins Japanische und vereinfachte Chinesische	XenCenter 8.2.6	**XenCenter 2023.3.1**	
Software-Fibre-Channel über Ethernet (FCoE)	8.2 CU1		
AMD MxGPU	8.2 CU1	**XenServer 8**	

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Intel GVT-g	8.2 CU1		
Separates PVS-Accelerator-Zusatzpaket	8.2 CU1	**XenServer 8**	Diese Funktionen sind jetzt im Kernprodukt enthalten.
Unterstützung für die folgenden Linux-Betriebssysteme: CoreOS, Ubuntu 16.04, Debian Jessie 8, Debian Stretch 9, SUSE Linux Enterprise Server 12 SP3, SUSE Linux Enterprise Desktop 12 SP3, CentOS 8	8.2 CU1	8.2 CU1	Aktualisieren Sie Ihre virtuellen Maschinen auf eine neuere Version ihres Betriebssystems, sofern verfügbar.
Unterstützung für die folgenden Linux-Betriebssysteme: Ubuntu 18.04, SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Desktop 12 SP4	8.2 CU1	8.2 CU1	Aktualisieren Sie Ihre virtuellen Maschinen auf eine neuere Version ihres Betriebssystems, sofern verfügbar.
Unterstützung für Windows Server 2012 R2	8.2 CU1	**XenServer 8**	Aktualisieren Sie Ihre virtuellen Maschinen auf eine neuere Version ihres Betriebssystems.
Unterstützung für Windows Server 2012 und Windows 8.1	8.2 CU1	8.2 CU1	Aktualisieren Sie Ihre virtuellen Maschinen auf eine neuere Version ihres Betriebssystems.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
VM übertragen	8.2 CU1	8.2 CU1 (XenCenter 8.2.3)	Verwenden Sie die neueste Version von XenCenter. Seit XenCenter 8.2.3 wurde der Mechanismus für den OVF-/OVA-Import/-Export und den Import eines einzelnen Disk-Images vereinfacht, und diese Vorgänge werden jetzt ohne Verwendung der Transfer-VM ausgeführt.
Measured Boot Supplemental Pack	8.2 CU1	8.2 CU1	
Zusatzpaket zur Containerverwaltung	8.2	8.2	
Unterstützung für Hewlett-Packard Integrated Lights-Out (iLO)	8.2	8.2	
Unterstützung für die folgenden Legacy-Prozessoren: `Xeon E3/5/7 family - Sandy Bridge`, `Xeon E3/5/7 v2 family - Ivy Bridge`	8.2	8.2	

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Die in der XenServer-Installations-ISO enthaltene Datei `guest-tools.iso`	8.2	8.2	Laden Sie die XenServer VM Tools für Windows oder für Linux von der XenServer-Downloadseiteherunter.
Unterstützung für Windows 7, Windows Server 2008 SP2 und Windows Server 2008 R2 SP1	8.2	8.2	Aktualisieren Sie Ihre virtuellen Maschinen auf eine neuere Version ihres Betriebssystems.
Legacy-SSL-Modus und Unterstützung für das TLS 1.0/1.1-Protokoll	8.2	8.2	
Serverübergreifende private Netzwerke	8.2	8.2	
Die folgenden xe CLI-Protokollbefehle: `diagnostic-db-log`log-set-output`, `log-get-keys`, `log-get`, `log-reopen`	8.2	**XenServer 8**	
Der vSwitch Controller (siehe Hinweise)	8.1	8.2	

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Legacy-Partitionslayouts: DOS-Partitionslayout, altes GPT-Partitionslayout. Beachten Sie, dass durch diese Änderung auch die Unterstützung für Server mit weniger als 46 GB auf dem primären Datenträger entfernt wird.	8.1	**XenServer 8**	
VSS und Momentaufnahmen mit Stillstand	8.1	8.1	
Unterstützung für Ubuntu 14.04	8.1	8.1	

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für alle paravirtualisierten (PV) VMs, einschließlich der folgenden: Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, CentOS 5, CentOS 6, Oracle Enterprise Linux 5, Oracle Enterprise Linux 6, Scientific Linux 6, NeoKylin Linux Advanced Server 6.2, Debian Wheezy 7, SUSE Linux Enterprise Server 11 SP3, SUSE Linux Enterprise Server 11 SP4, SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 12 SP1, SUSE Linux Enterprise Server 12 SP2, SUSE Linux Enterprise Desktop 11 SP3, SUSE Linux Enterprise Desktop 12, SUSE Linux Enterprise Desktop 12 SP1, SUSE Linux Enterprise Desktop 12 SP2	8.1	8.1	Aktualisieren Sie Ihre VMs auf eine neuere Version ihres Betriebssystems, bevor Sie zur neuesten Version von XenServer wechseln.
Legacy-Treiber: `qla4xxx`, `qla3xxx`, `netxen_nic`, `qlge`, `qlcnic`	8.0		

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Das XenCenter-Installationsprogramm ist im Lieferumfang des XenServer-Installationsmediums enthalten.	8.0	8.0	Laden Sie stattdessen das XenCenter Installationsprogramm von der Downloads-Seite herunter .
XenCenter Verbindungen zu XenServer-Hosts der Version 6.x und früher.	8.0	8.0	Aktualisieren Sie Ihre nicht unterstützten XenServer-Hosts.
Unterstützung für die Nutanix-Integration.	8.0	8.0	

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für die folgenden Legacy-Prozessoren: Opteron 13xx BudapestOpteron 23xx/83xx Barcelona, Opteron 23xx/83xx Shanghai, Opteron 24xx/84xx Istanbul, Opteron 41xx Lisbon, Opteron 61xx Magny Cours, Xeon 53xx Clovertown„ Xeon 54xx Harpertown, Xeon 55xx Nehalem, Xeon 56xx Westmere-EP, Xeon 65xx/75xx Nehalem-EX, Xeon 73xx Tigerton, Xeon 74xx Dunnington	8.0	8.0	Informationen zu unterstützten Prozessoren finden Sie in der Hardwarekompatibilitätsliste

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für `qemu-trad`. Es ist nicht mehr möglich, `qemu-trad` durch Einstellen von `platform-devicemodel=qemu-trad` zu verwenden. Alle mit dem Geräteprofil `qemu-trad` erstellten VMs werden automatisch auf das Profil `qemu-upstream-compat` aktualisiert.	8.0	8.0	
Unterstützung für die folgenden Gastvorlagen: Debian 6 Squeeze, Ubuntu 12.04, Legacy Windows, Asianux Server 4.2, 4.4 und 4.5, NeoKylin Linux Security OS 5, Linx Linux 6, Linx Linux 8, GreatTurbo Enterprise Server 12, Yinhe Kylin 4	8.0	8.0	
Legacy-Windows-Treiber aus dem Citrix VM Tools-ISO	8.0	8.0	

Hinweise

Systemintegritätsprüfung

Die Protokolle für den Health Check-Dienst werden von Windows zur Problembehandlung aufbewahrt. Um diese Protokolle zu entfernen, löschen Sie sie manuell in `%SystemRoot%\System32\Winevt\Logs` auf dem Windows-Computer, auf dem XenCenter ausgeführt wird.

Dynamische Speichersteuerung (DMC)

Diese Funktion wurde zuvor als veraltet aufgeführt. Der Veraltungshinweis wurde am 30. Januar 2023 entfernt. DMC wird in zukünftigen Versionen von XenServer unterstützt.

Trennen des vSwitch-Controllers

Der vSwitch Controller wird nicht mehr unterstützt. Trennen Sie den vSwitch Controller von Ihrem Pool, bevor Sie versuchen, ein Update oder ein Upgrade auf die neueste Version von XenServer durchzuführen.

1. Gehen Sie in der vSwitch-Controller-Benutzeroberfläche zur Registerkarte **Sichtbarkeit und Steuerung** .
2. Suchen Sie den zu trennenden Pool in der Tabelle **Alle Ressourcenpools** . Die Pools in der Tabelle werden anhand der IP-Adresse des Poolkoordinators aufgelistet.
3. Klicken Sie auf das Zahnradsymbol und wählen Sie **Pool entfernen**.
4. Klicken Sie zur Bestätigung auf **Entfernen** .

Nach dem Update oder Upgrade finden die folgenden Konfigurationsänderungen statt:

- Serverübergreifende private Netzwerke werden zu privaten Einzelservernetzwerken zurückgesetzt.
- Über die DVSC-Konsole vorgenommene Quality of Service-Einstellungen werden nicht mehr angewendet. Netzwerktarifbegrenzungen werden nicht mehr durchgesetzt.
- ACL-Regeln wurden entfernt. Der gesamte Datenverkehr von virtuellen Rechnern ist zulässig.
- Die Portspiegelung (RSPAN) ist deaktiviert.

Wenn Sie nach dem Update oder Upgrade einen verbleibenden Status über den vSwitch Controller in Ihrem Pool finden, löschen Sie den Status mit dem folgenden CLI-Befehl: `xe pool-set-vswitch-controller address=`

Schneller Einstieg

April 12, 2024

In diesem Artikel wird beschrieben, wie XenServer (früher Citrix Hypervisor) und seine grafische, Windows-basierte Benutzeroberfläche XenCenter installiert und konfiguriert werden. Nach der Installation werden Sie durch die Erstellung virtueller Windows-Maschinen (VMs) und anschließend benutzerdefinierte VM-Vorlagen erstellt, mit denen Sie schnell mehrere ähnliche VMs erstellen können. Schließlich zeigt dieser Artikel, wie Sie einen Host-Pool erstellen, der die Grundlage für die Migration laufender VMs zwischen Hosts mithilfe der Livemigration bildet.

Dieser Artikel konzentriert sich auf die grundlegendsten Szenarien und soll Sie schnell einrichten.

Dieser Artikel richtet sich hauptsächlich an neue Benutzer von XenServer und XenCenter. Es ist für Benutzer gedacht, die XenServer mithilfe von XenCenter verwalten möchten. Informationen zur Verwaltung von XenServer mit den Linux-basierten xe-Befehlen über die XenServer-Befehlszeilenschnittstelle (bekannt als XE-CLI)
finden Sie unter Befehlszeilenschnittstelle.

Terminologie und Abkürzungen

- *Server*: Ein physischer Computer, auf dem XenServer ausgeführt wird.
- *Host*: Eine XenServer-Installation, die virtuelle Maschinen (VMs) hostet.
- *Virtuelle Maschine (VM)*: Ein Computer, der vollständig aus Software besteht und sein eigenes Betriebssystem und eigene Anwendungen ausführen kann, als wäre es ein physischer Computer. Eine VM verhält sich genau wie ein physischer Computer und enthält ihre eigene virtuelle (softwarebasierte) CPU, RAM, Datenträger und NIC.
- *Pool*: Eine einzelne verwaltete Entität, die mehrere XenServer-Hosts und ihre VMs zusammenhält.
- *Poolkoordinator* (früher *Pool-Master*): Haupthost in einem Pool, der eine zentrale Anlaufstelle für alle Hosts im Pool bietet und die Kommunikation nach Bedarf an andere Poolmitglieder weiterleitet.
- *Storage Repository (SR)*: ein Speichercontainer, in dem virtuelle Datenträger gespeichert werden.

Bedeutende Komponenten

XenServer

XenServer ist eine vollständige Servervirtualisierungsplattform mit allen Funktionen, die zum Erstellen und Verwalten einer virtuellen Infrastruktur erforderlich sind. XenServer ist sowohl für virtuelle Windows- als auch für Linux-Server optimiert.

XenServer läuft direkt auf Serverhardware, ohne dass ein zugrunde liegendes Betriebssystem erforderlich ist, was zu einem effizienten und skalierbaren System führt. XenServer abstrahiert Elemente von der physischen Maschine (wie Datenträger, Ressourcen und Ports) und weist sie den darauf laufenden virtuellen Maschinen (VMs) zu.

Mit XenServer können Sie VMs erstellen, VM-Datenträger-Snapshots erstellen und VM-Workloads verwalten.

XenCenter

XenCenter ist eine grafische, Windows-basierte Benutzerschnittstelle. Mit XenCenter können Sie XenServer-Hosts, Pools und gemeinsam genutzten Speicher verwalten. Verwenden Sie XenCenter, um virtuelle Maschinen von Ihrem Windows-Desktop-Computer aus bereitzustellen, zu verwalten und zu überwachen.

Die XenCenter *Online-Hilfe* ist auch eine hervorragende Ressource für die ersten Schritte mit XenCenter. Drücken Sie jederzeit F1, um auf kontextsensitive Informationen zuzugreifen.

Installieren Sie XenServer und XenCenter

In diesem Abschnitt richten Sie eine XenServer-Mindestinstallation ein.

Was du lernen wirst

Du wirst lernen wie man:

- Installieren Sie XenServer auf einem einzelnen physischen Server
- Installieren Sie XenCenter auf einem Windows-Computer
- Verbindung von XenCenter und XenServer zur Bildung der Infrastruktur für die Erstellung und Ausführung virtueller Maschinen (VMs)

Anforderungen

Um loszulegen, benötigen Sie folgende Artikel:

- Ein physischer Computer als XenServer-Host
- Ein Windows-Computer zum Ausführen der XenCenter-Anwendung
- Installationsdateien für XenServer und XenCenter

Der XenServer-Hostcomputer ist ausschließlich der Ausführung von XenServer und dem Hosten von VMs gewidmet und wird nicht für andere Anwendungen verwendet. Der Computer, auf dem XenCenter ausgeführt wird, kann jeder Allzweck-Windows-Computer sein, der die Hardwareanforderungen erfüllt. Mit diesem Computer können Sie auch andere Anwendungen ausführen. Weitere Informationen finden Sie unter Systemanforderungen.

Sie können die Installationsdateien von XenServer Downloads herunterladen.

Installieren Sie den XenServer-Host

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Allen Servern ist mindestens eine IP-Adresse zugeordnet. Um eine statische IP-Adresse für den Host zu konfigurieren (anstatt DHCP zu verwenden), halten Sie die statische IP-Adresse bereit, bevor Sie mit diesem Verfahren beginnen.

> **Tipp:**
>
> Drücken Sie **F12**, um schnell zum nächsten Installationsbildschirm zu gelangen. Für allgemeine Hilfe drücken Sie **F1**.

So installieren Sie den XenServer-Host:

1. Brennen Sie die Installationsdateien für XenServer auf eine CD oder erstellen Sie einen bootfähigen USB-Stick.

   > **Hinweis:**
   >
   > Informationen zur Verwendung von HTTP, FTP oder NFS als Installationsquelle finden Sie unter Installieren von XenServer.

2. Machen Sie ein Backup der Daten, die Sie behalten möchten. Durch die Installation von XenServer werden Daten auf allen Datenträgern überschrieben, die Sie für die Installation auswählen.
3. Legen Sie das Installationsmedium in das System ein.
4. Starten Sie das System neu.

5. Starten Sie vom lokalen Installationsmedium (falls erforderlich, finden Sie Informationen zum Ändern der Startreihenfolge in der Dokumentation Ihres Hardwareanbieters).
6. Wählen Sie nach den ersten Startmeldungen und dem Bildschirm **Willkommen bei XenServer** Ihr Tastaturlayout für die Installation aus.
7. Wenn der Willkommensbildschirm beim **XenServer-Setup** angezeigt wird, wählen Sie **OK**.
8. Lesen und akzeptieren Sie die XenServer-EULA.

   > **Hinweis:**
   >
   > Wenn Sie eine **Systemhardwarewarnung** sehen, stellen Sie sicher, dass die Unterstützung der Hardware-Virtualisierung in Ihrer Systemfirmware aktiviert ist.

9. Wählen Sie **Ok**, um eine Neuinstallation durchzuführen.
10. Wenn Sie mehrere Datenträger haben, wählen Sie einen Primärdatenträger für die Installation. Wählen Sie **Ok**.

    Wählen Sie aus, welche Datenträger Sie für den Speicher der virtuellen Maschine verwenden möchten. Wählen Sie **Ok**.
11. Wählen Sie **Lokales Medium** als Installationsquelle aus.
12. Wählen Sie **Verifizierung überspringen**und dann **Ok**.

    > **Hinweis:**
    >
    > Wenn Sie während der Installation auf Probleme stoßen, überprüfen Sie die Installationsquelle.

13. Erstellen und bestätigen Sie ein Root-Kennwort, mit dem die XenCenter-Anwendung eine Verbindung zum XenServer-Host herstellt.
14. Richten Sie die Verwaltungsschnittstelle für die Verbindung mit XenCenter ein.

    Wenn Ihr Computer über mehrere Netzwerkkarten verfügt, wählen Sie die Netzwerkkarte aus, die Sie für den Verwaltungsverkehr verwenden möchten (normalerweise die erste Netzwerkkarte).
15. Konfigurieren Sie die Verwaltungs-NIC-IP-Adresse mit einer statischen IP-Adresse oder verwenden Sie DHCP.
16. Geben Sie den Hostnamen und die DNS-Konfiguration manuell oder automatisch über DHCP an.

    Wenn Sie das DNS manuell konfigurieren, geben Sie die IP-Adressen Ihrer primären (erforderlichen), sekundären (optional) und tertiären (optionalen) DNS-Server in die dafür vorgesehenen Felder ein.

17. Wähle deine Zeitzone aus.
18. Geben Sie an, wie der Host die Ortszeit ermitteln soll: mithilfe von NTP oder manueller Zeiteingabe. Wählen Sie **Ok**.
    - Wenn Sie NTP verwenden, können Sie angeben, ob DHCP den Zeitserver festlegt. Alternativ können Sie mindestens einen NTP-Hostnamen oder eine IP-Adresse in die folgenden Felder eingeben.
    - Wenn Sie Datum und Uhrzeit manuell festlegen möchten, werden Sie dazu aufgefordert.
19. Wählen Sie **XenServer installieren**.

    Der Installationsvorgang beginnt. Das kann einige Minuten dauern.
20. Im nächsten Bildschirm werden Sie gefragt, ob Sie zusätzliche Packs installieren möchten. Wählen Sie **Nein**, um fortzufahren.
21. Werfen Sie auf dem Bildschirm "**Installation abgeschlossen** "das Installationsmedium aus und wählen Sie dann **Ok** aus, um den Host neu zu starten.

    Nach dem Neustart des Hosts zeigt XenServer **xsconsole an, eine Systemkonfigurationskonsole**.

    > **Hinweis:**
    >
    > Notieren Sie sich die angezeigte IP-Adresse. Sie verwenden diese IP-Adresse, wenn Sie XenCenter mit dem Host verbinden.

Installieren Sie XenCenter

XenCenter ist normalerweise auf Ihrem lokalen System installiert. Sie können das XenCenter-Installationsprogramm von der XenServer-Downloadseite herunterladen.

Um XenCenter zu installieren:

1. Laden Sie das XenCenter Installationsprogramm herunter oder übertragen Sie es auf den Computer, auf dem Sie XenCenter ausführen möchten.
2. Doppelklicken Sie auf die `.msi`-Installationsdatei, um die Installation zu starten.
3. Folgen Sie dem Setup-Assistenten, mit dem Sie den Standardzielordner ändern und anschließend XenCenter installieren können.

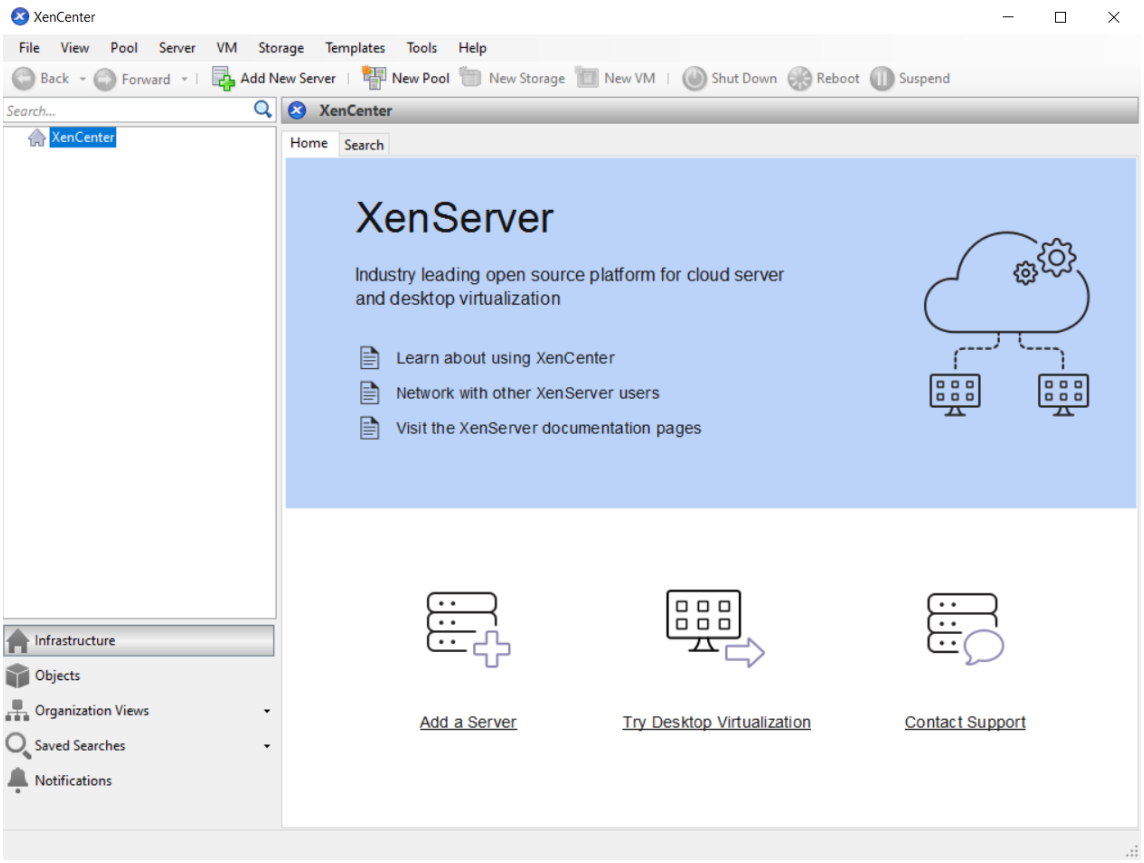
Verbinden Sie XenCenter mit dem XenServer-Host

Mit diesem Verfahren können Sie XenCenter einen Host hinzufügen.

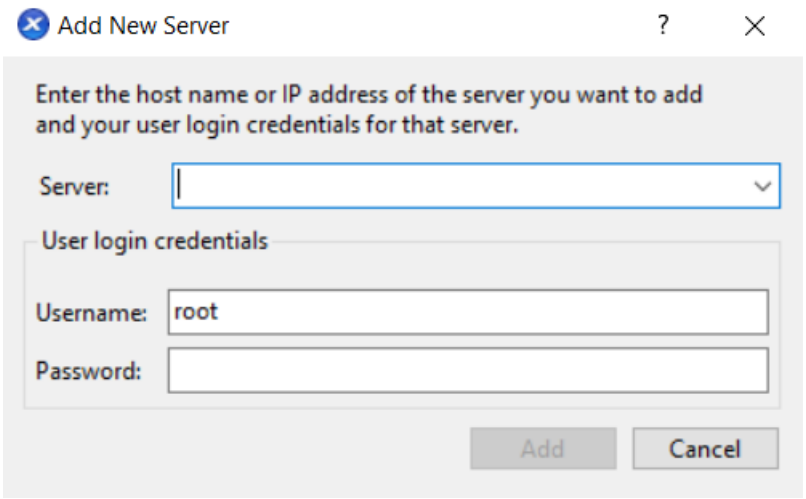
So verbinden Sie XenCenter mit dem XenServer-Host:

1. Starten Sie XenCenter.

   Das Programm öffnet sich auf der Registerkarte **Home** .



2. Klicken Sie auf das Symbol **Neuen Server hinzufügen**, um das Dialogfeld **Neuen Server hinzufügen** zu öffnen.



3. Geben Sie im Feld **Server** die IP-Adresse des Hosts ein. Geben Sie den Root-Benutzernamen und das Kennwort ein, die Sie bei der XenServer-Installation festgelegt haben. Wählen Sie **Hinzufü-**

gen.

> **Hinweis:**
>
> Wenn Sie zum ersten Mal einen Host hinzufügen, wird das Dialogfeld **Verbindungsstatus speichern und wiederherstellen** angezeigt. In diesem Dialogfeld können Sie Ihre Einstellungen für das Speichern Ihrer Hostverbindungsinformationen und das automatische Wiederherstellen von Hostverbindungen festlegen.

XenServer lizenzieren

Sie können XenServer ohne Lizenz verwenden (Trial Edition). Mit der Testversion können Sie Funktionen der Premium Edition testen, allerdings in einem Pool mit begrenzter Größe von bis zu 3 Hosts.

Wenn Sie XenServer zum Ausführen Ihrer Citrix Virtual Apps and Desktops-Workloads verwenden, benötigen Sie eine Premium Edition-Lizenz. Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy. Bestehende Kunden von Citrix Virtual Apps and Desktops können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Wenn Sie eine XenServer-Lizenz haben, wenden Sie sie jetzt an. Weitere Informationen finden Sie unter Lizenzierung.

Erstellen Sie einen Pool von XenServer-Hosts

Ein Ressourcenpool besteht aus mehreren XenServer-Hostinstallationen, die zu einer einzigen verwalteten Einheit zusammengefasst sind.

Mit Ressourcenpools können Sie mehrere Hosts und ihren verbundenen gemeinsamen Speicher als eine einzige vereinheitlichte Ressource anzeigen. Sie können VMs je nach Ressourcenbedarf und Geschäftsprioritäten flexibel im gesamten Ressourcenpool bereitstellen. Ein Pool kann bis zu 64 Hosts enthalten, auf denen dieselbe Version der XenServer-Software auf derselben Patch-Ebene und mit weitgehend kompatibler Hardware ausgeführt wird.

Ein Host im Pool wird als *Poolkoordinator*benannt. Der Poolkoordinator bietet eine zentrale Anlaufstelle für den gesamten Pool und leitet die Kommunikation bei Bedarf an andere Poolmitglieder weiter. Jedes Mitglied eines Ressourcenpools enthält alle Informationen, die erforderlich sind, um bei Bedarf die Rolle des Poolkoordinators zu übernehmen. Der Poolkoordinator ist der erste Host, der für den Pool im Bereich XenCenter Resources aufgeführt ist. Sie können die IP-Adresse des Poolkoordinators ermitteln, indem Sie den Poolkoordinator auswählen und auf die Registerkarte **Suchen** klicken.

In einem Pool mit gemeinsam genutztem Speicher können Sie VMs auf *jedem* Poolmitglied starten, das über ausreichend Arbeitsspeicher verfügt, und die VMs dynamisch zwischen Hosts verschieben.

Die VMs werden während der Ausführung und mit minimalen Ausfallzeiten verschoben. Wenn ein einzelner XenServer-Host einen Hardwarefehler erleidet, können Sie die ausgefallenen VMs auf einem anderen Host im selben Pool neu starten.

Wenn die Hochverfügbarkeitsfunktion aktiviert ist, werden geschützte VMs *automatisch* verschoben, wenn ein Host ausfällt. In einem HA-fähigen Pool wird automatisch ein neuer Poolkoordinator nominiert, wenn der Poolkoordinator heruntergefahren wird.

> **Hinweis:**
>
> Eine Beschreibung der heterogenen Pool-Technologie finden Sie unter Hosts und Ressourcenpools.

Was du lernen wirst

Du wirst lernen wie man:

- Erstellen Sie einen Host-Pool
- Richten Sie ein Netzwerk für den Pool ein
- Bond-NICs
- Richten Sie gemeinsam genutzten Speicher für den Pool ein

XenServer unterstützt zwar viele gemeinsam genutzte Speicherlösungen, dieser Abschnitt konzentriert sich jedoch auf zwei gängige Typen: NFS und iSCSI.

Anforderungen

Um einen Pool mit gemeinsam genutztem Speicher zu erstellen, benötigen Sie die folgenden Elemente:

- Ein zweiter XenServer-Host mit ähnlichem Prozessortyp.
  Verbinden Sie diesen Host mit Ihrer XenCenter Anwendung.
- Ein Speicherrepository für IP-basierten Speicher

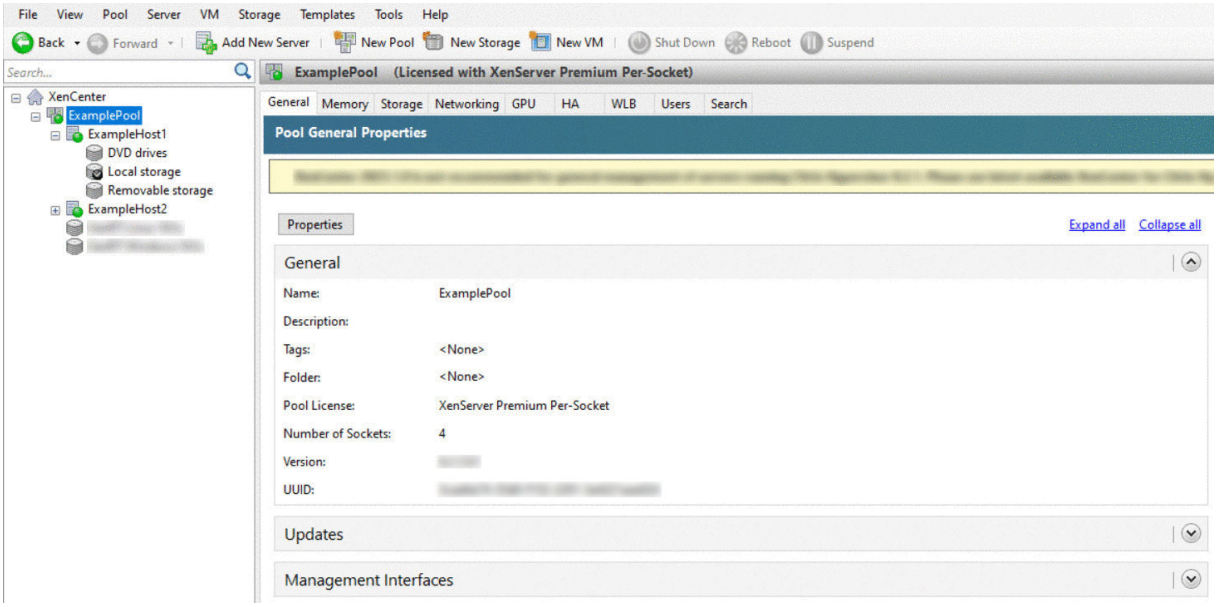
Um Ihnen einen schnellen Einstieg zu ermöglichen, konzentriert sich dieser Abschnitt auf die Erstellung *homogener* Pools. In einem homogenen Pool müssen alle Hosts über kompatible Prozessoren verfügen und dieselbe Version von XenServer unter derselben XenServer-Produktlizenz ausführen. Eine vollständige Liste der Anforderungen an homogene Pools finden Sie unter Systemanforderungen.

Erstellen Sie einen Pool

So erstellen Sie einen Pool:

1. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Neuer Pool** .

2. Geben Sie einen Namen und eine optionale Beschreibung für den neuen Pool ein.
3. Nominieren Sie den Poolkoordinator, indem Sie einen Host aus der **Koordinatorliste** auswählen.
4. Wählen Sie aus der Liste **Zusätzliche Mitglieder** den zweiten Host aus, der in den neuen Pool aufgenommen werden soll.
5. Klicken Sie auf **Pool erstellen**.
   Der neue Pool wird im Bereich **Ressourcen** angezeigt.



Richten Sie Netzwerke für den Pool ein

Wenn Sie XenServer installieren, stellen Sie eine Netzwerkverbindung her, normalerweise auf der ersten Netzwerkkarte im Pool, auf der Sie eine IP-Adresse angegeben haben (während der XenServer-Installation).

Möglicherweise müssen Sie Ihren Pool jedoch mit VLANs und anderen physischen Netzwerken verbinden. Um dies zu tun, müssen Sie diese Netzwerke zum Pool hinzufügen. Sie können XenServer so konfigurieren, dass jede Netzwerkkarte mit einem physischen Netzwerk und zahlreichen VLANs verbunden wird.

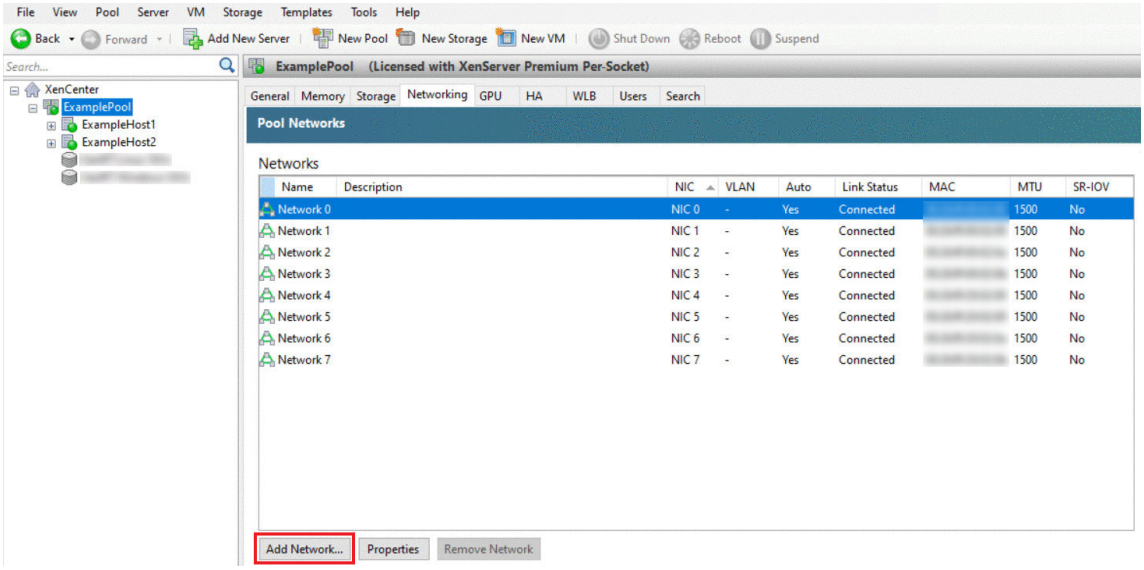
Stellen Sie vor dem Erstellen von Netzwerken sicher, dass die Verkabelung auf jedem Host im Pool übereinstimmt. Schließen Sie die NICs auf jedem Host an dieselben physischen Netzwerke an wie die entsprechenden NICs auf den anderen Poolmitgliedern.

> **Hinweis:**
>
> Wenn die NICs bei der Installation von XenServer nicht an die NICs auf dem Host angeschlossen waren:
>
> - Stecken Sie die NICs ein
> - Wählen Sie in XenCenter die Registerkarte **<your host> > NICs**
> - Klicken Sie auf **Erneut scannen**, damit sie angezeigt werden

Weitere Informationen zur Konfiguration von XenServer-Netzwerken finden Sie unter Netzwerke und Über XenServer-Netzwerke.

Um ein Netzwerk zu XenServer hinzuzufügen:

1. Wählen Sie im Bereich **Ressourcen** in XenCenter den Pool aus.
2. Klicken Sie auf die Registerkarte **Netzwerk** .
3. Klicken Sie auf **Netzwerk hinzufügen**.



4. Wählen Sie auf der Seite **Typ auswählen** **Externes Netzwerk** aus, und klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Name** einen aussagekräftigen Namen für das Netzwerk und eine Beschreibung ein.
6. Geben Sie auf der Seite **Netzwerkeinstellungen** Folgendes an:
   - **NIC:** Wählen Sie die NIC aus, die XenServer zum Senden und Empfangen von Daten aus dem Netzwerk verwenden soll.
   - **VLAN:** Wenn das Netzwerk ein VLAN ist, geben Sie die VLAN-ID (oder das "Tag") ein.

- **MTU:** Wenn das Netzwerk Jumbo-Frames verwendet, geben Sie einen Wert für die Maximum Transmission Unit (MTU) zwischen 1500 und 9216 ein. Lassen Sie andernfalls die MTU-Box auf dem Standardwert von 1500.

Wenn Sie viele virtuelle Maschinen für die Verwendung dieses Netzwerks konfigurieren, können Sie das Kontrollkästchen **Dieses Netzwerk automatisch zu neuen virtuellen Maschinen hinzufügen** aktivieren. Diese Option fügt das Netzwerk standardmäßig hinzu.

7. Klicken Sie auf **Fertigstellen**.

Verbindende NICs

NIC-Bonding kann Ihren Host widerstandsfähiger machen, indem Sie zwei oder mehr physische Netzwerkkarten verwenden, als ob es sich um einen einzigen, leistungsstarken Kanal handeln würde. Dieser Abschnitt bietet nur einen sehr kurzen Überblick über das Bonding, auch bekannt als *NIC-Teaming*. Bevor Sie Bindungen für die Verwendung in einer Produktionsumgebung konfigurieren, empfehlen wir Ihnen, ausführlichere Informationen über die Bindungen zu lesen. Weitere Informationen finden Sie unter Netzwerk.

XenServer unterstützt die folgenden Bond-Modi: Aktiv/Aktiv, Aktiv/Passiv (Aktiv/Backup) und LACP. Active/Active bietet Lastausgleich und Redundanz für VM-basierten Datenverkehr. Für andere Arten von Datenverkehr (Speicherung und Verwaltung) kann aktiv/aktiv den Datenverkehr nicht mit dem Lastenausgleich ausgleichen. Daher sind LACP oder Multipathing die bessere Wahl für den Speicherverkehr. Informationen zum Multipathing finden Sie unter Speicher. Weitere Informationen zum Bonding finden Sie unter Netzwerk.

LACP-Optionen sind nicht sichtbar oder verfügbar, sofern Sie den vSwitch nicht als Netzwerkstapel konfigurieren. Ebenso müssen Ihre Switches den IEEE 802.3ad-Standard unterstützen. Der Switch muss eine separate LAG-Gruppe enthalten, die für jede LACP-Bindung auf dem Host konfiguriert ist. Weitere Informationen zum Erstellen von LAG-Gruppen finden Sie unter Netzwerk.

So binden Sie NICs:

1. Stellen Sie sicher, dass die Netzwerkkarten, die Sie miteinander verbinden möchten, nicht verwendet werden: Fahren Sie alle VMs mit virtuellen Netzwerkschnittstellen mit diesen NICs herunter, bevor Sie die Verbindung herstellen. Nachdem Sie die Bindung erstellt haben, verbinden Sie die virtuellen Netzwerkschnittstellen erneut mit einem geeigneten Netzwerk.
2. Wählen Sie den Host im Bereich **Ressourcen** aus, öffnen Sie dann die Registerkarte **NICs** und klicken Sie auf **Create Bond**.
3. Wählen Sie die Netzwerkkarten aus, die Sie miteinander verbinden möchten. Um eine Netzwerkkarte auszuwählen, aktivieren Sie das entsprechende Kontrollkästchen in der Liste. In

dieser Liste können bis zu vier Netzwerkkarten ausgewählt werden. Deaktivieren Sie das Kontrollkästchen, um die Auswahl einer Netzwerkkarte aufzuheben. Um ein flexibles und sicheres Netzwerk aufrechtzuerhalten, können Sie entweder zwei, drei oder vier Netzwerkkarten verbinden, wenn vSwitch der Netzwerkstapel ist. Sie können jedoch nur zwei Netzwerkkarten verbinden, wenn die Linux-Brücke der Netzwerkstapel ist.

4. Wählen Sie im **Bindungsmodus** die Art der Bindung aus:

   - Wählen Sie **Aktiv-Aktiv**, um einen Aktiv-Aktiv-Bindung zu konfigurieren. Der Verkehr wird zwischen den gebundenen NICs ausgeglichen. Wenn eine Netzwerkkarte innerhalb der Verbindung ausfällt, wird der Netzwerkverkehr des Hosts automatisch über die zweite Netzwerkkarte geleitet.
   - Wählen Sie **Aktiv-Passiv**, um eine aktiv-passive Bindung zu konfigurieren. Der Datenverkehr läuft nur über eine der gebundenen NICs. In diesem Modus wird die zweite Netzwerkkarte nur aktiv, wenn die aktive Netzwerkkarte ausfällt, z. B. wenn sie die Netzwerkkonnektivität verliert.
   - Wählen Sie **LACP mit Lastausgleich basierend auf der Quell-MAC-Adresse** aus, um eine LACP-Bindung zu konfigurieren. Die ausgehende Netzwerkkarte wird basierend auf der MAC-Adresse der VM ausgewählt, von der der Datenverkehr stammt. Verwenden Sie diese Option, um den Datenverkehr in einer Umgebung auszugleichen, in der mehrere VMs auf demselben Host vorhanden sind. Diese Option ist nicht geeignet, wenn weniger virtuelle Schnittstellen (VIFs) als Netzwerkkarten vorhanden sind: da der Lastausgleich nicht optimal ist, da der Datenverkehr nicht auf Netzwerkkarten aufgeteilt werden kann.
   - Wählen Sie **LACP mit Lastausgleich basierend auf IP und Port of Source und Ziel**, um eine LACP-Bindung zu konfigurieren. Die Quell-IP-Adresse, die Quellportnummer, die Ziel-IP-Adresse und die Zielportnummer werden verwendet, um den Datenverkehr über die NICs zuzuweisen. Verwenden Sie diese Option, um den Datenverkehr von VMs in einer Umgebung auszugleichen, in der die Anzahl der Netzwerkkarten die Anzahl der VIFs übersteigt.

     > **Hinweis:**
     >
     > LACP-Bonding ist nur für den vSwitch verfügbar, während Aktiv-Aktiv- und Aktiv-Passiv-Verbindungsmodi sowohl für den vSwitch als auch für die Linux-Brücke verfügbar sind. Informationen zu Netzwerkstapeln finden Sie unter Netzwerk.

5. Um Jumbo-Frames zu verwenden, stellen Sie die Maximum Transmission Unit (MTU) auf einen Wert zwischen 1500 und 9216 ein.
6. Um das neue gebundene Netzwerk automatisch zu neuen VMs hinzuzufügen, die mit dem Assistenten für neue VM erstellt wurden, aktivieren Sie das Kontrollkästchen.

7. Klicken Sie auf **Erstellen**, um die NIC-Bindung zu erstellen und das Dialogfeld zu schließen.

   XenCenter verschiebt automatisch Management- und sekundäre Schnittstellen von sekundären gebündelten NICs auf die Bond-Schnittstelle, wenn die neue Bindung erstellt wird. Ein Host mit seiner Verwaltungsschnittstelle auf einer Bindung darf einem Pool nicht beitreten. Bevor der Host einem Pool beitreten kann, müssen Sie die Verwaltungsschnittstelle neu konfigurieren und sie wieder auf eine physische Netzwerkkarte verschieben.

Einrichten von gemeinsam genutztem Speicher für den Pool

Um die Hosts in einem Pool mit einem Remotespeicher-Array zu verbinden, erstellen Sie eine XenServer-SR. Das SR ist der Speichercontainer, in dem die virtuellen Datenträger einer VM gespeichert sind. SRs sind persistente Objekte auf dem Datenträger, die unabhängig von XenServer existieren. SRs können auf verschiedenen Arten von physischen Speichergeräten existieren, sowohl intern als auch extern. Zu diesen Typen gehören lokale Datenträgergeräte und gemeinsam genutzter Netzwerkspeicher.

Sie können einen XenServer SR für verschiedene Speichertypen konfigurieren, darunter:

- NFS
- iSCSI
- HBA-Hardware
- SMB
- Fibre-Channel
- Software-FCoE (veraltet)

In diesem Abschnitt wird die Einrichtung von zwei Typen gemeinsam genutzter SRs für einen Host-Pool beschrieben: NFS und iSCSI. Bevor Sie ein SR erstellen, müssen Sie Ihr NFS- oder iSCSI-Speicher-Array konfigurieren. Das Setup hängt von der Art der verwendeten Speicherlösung ab. Weitere Informationen finden Sie in der Dokumentation Ihres Anbieters. Bevor Sie beginnen, sollten Sie im Allgemeinen die folgende Einrichtung für Ihre Speicherlösung abschließen:

- **iSCSI SR**: Sie müssen ein Volume und ein LUN auf dem Speicherarray erstellt haben.
- **NFS SR**: Sie müssen das Volume auf dem Speichergerät erstellt haben.
- **Hardware-HBA**: Sie müssen die Konfiguration vorgenommen haben, die erforderlich ist, um die LUN verfügbar zu machen, bevor Sie den Assistenten für neues Speicherrepository ausführen
- **Software FCoE SR**: Sie müssen die Konfiguration, die für die Bereitstellung einer LUN für den Host erforderlich ist, manuell abgeschlossen haben. Dieses Setup umfasst die Konfiguration der FCoE-Fabric und die Zuweisung von LUNs zum Public World Wide Name (PWWN) Ihres SAN.

Wenn Sie ein SR für IP-basierten Speicher (iSCSI oder NFS) erstellen, können Sie eine der folgenden Optionen als Speichernetzwerk konfigurieren: die Netzwerkkarte, die den Verwaltungsdatenverkehr verarbeitet, oder eine neue Netzwerkkarte für den Speicherverkehr. Um eine andere Netzwerkkarte für den Speicherverkehr zu konfigurieren, weisen Sie einer Netzwerkkarte eine IP-Adresse zu, indem Sie eine *Verwaltungsschnittstelle*erstellen.

Wenn Sie eine Verwaltungsschnittstelle erstellen, müssen Sie ihr eine IP-Adresse zuweisen, die die folgenden Kriterien erfüllt:

- Die IP-Adresse befindet sich gegebenenfalls im selben Subnetz wie der Speichercontroller
- Die IP-Adresse befindet sich in einem anderen Subnetz als die IP-Adresse, die Sie bei der Installation von XenServer angegeben haben
- Die IP-Adresse befindet sich nicht im selben Subnetz wie alle anderen Verwaltungsschnittstellen.

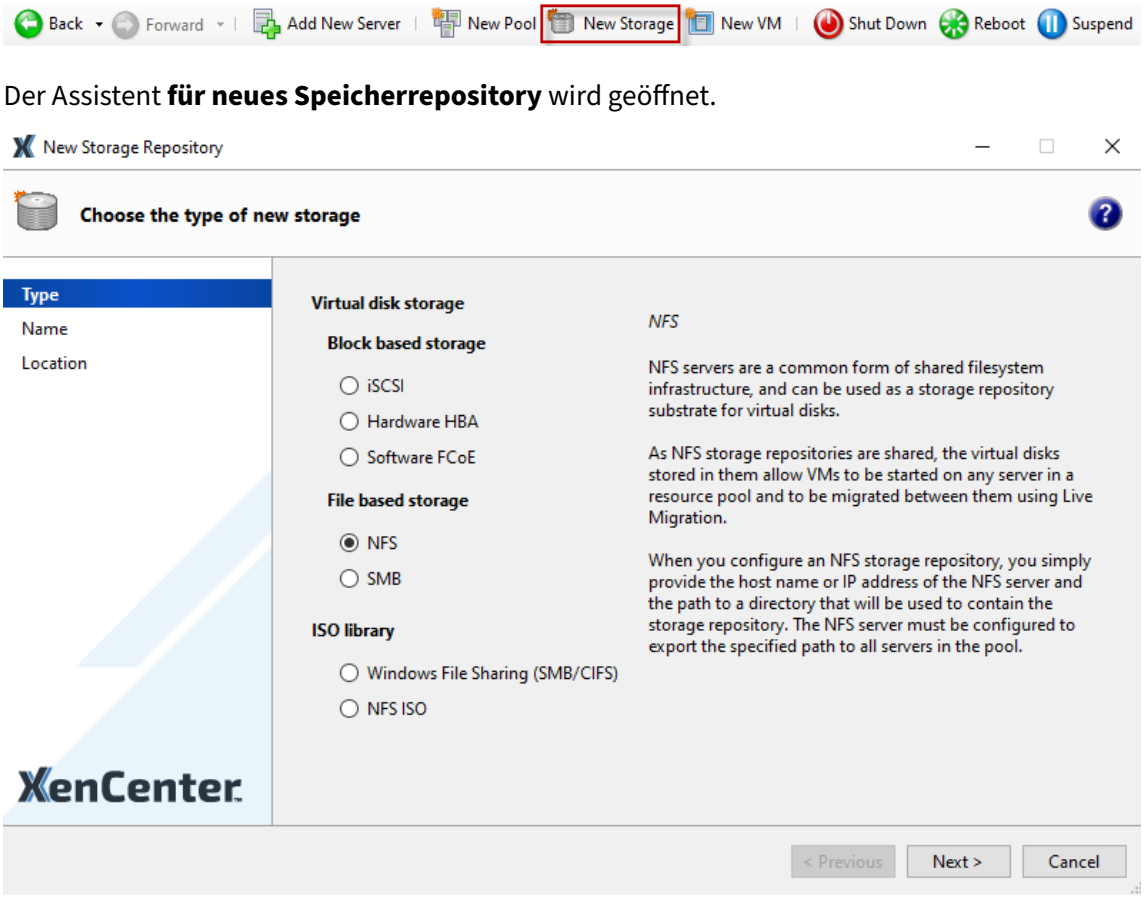
So weisen Sie einer Netzwerkkarte eine IP-Adresse zu:

1. Stellen Sie sicher, dass sich die Netzwerkkarte in einem separaten Subnetz befindet oder dass das Routing entsprechend Ihrer Netzwerktopologie konfiguriert ist. Diese Konfiguration erzwingt den gewünschten Datenverkehr über die ausgewählte Netzwerkkarte.
2. Wählen Sie im **Ressourcenbereich** von XenCenter den Pool (oder den eigenständigen Host) aus. Klicken Sie auf die Registerkarte **Netzwerk**, und klicken Sie dann auf **Konfigurieren** .
3. Klicken **Sie im Dialogfeld "IP-Adresse konfigurieren** "im linken Bereich auf **IP-Adresse hinzufügen**.
4. Geben Sie der neuen Schnittstelle einen aussagekräftigen Namen (z. B. *yourstoragearray_network*). Wählen Sie das mit der **Netzwerkkarte verknüpfte Netzwerk** aus, das Sie für den Speicherverkehr verwenden.
5. Klicken Sie auf **Diese Netzwerkeinstellungen verwenden**. Geben Sie eine statische IP-Adresse ein, die Sie auf der Netzwerkkarte, der Subnetzmaske und dem Gateway konfigurieren möchten. Klicken Sie auf **OK**. Die IP-Adresse muss sich im selben Subnetz wie der Speichercontroller befinden, an den die Netzwerkkarte angeschlossen ist.

> **Hinweis:**
>
> Wann immer Sie einer Netzwerkkarte eine IP-Adresse zuweisen, muss sie sich in einem anderen Subnetz befinden als alle anderen Netzwerkkarten mit IP-Adressen im Pool. Dazu gehört die primäre Verwaltungsschnittstelle.

So erstellen Sie ein neues freigegebenes NFS- oder iSCSI-Speicherrepository:

1. Wählen Sie im Bereich **Ressourcen** den Pool aus. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Neuer Speicher** .



Der Assistent **für neues Speicherrepository** wird geöffnet.

2. Wählen Sie unter virtueller Datenträgerspeicher NFS oder iSCSI als Speichertyp. Klicken Sie zum Fortfahren auf Weiter.
3. Wenn Sie NFS wählen:

   a) Geben Sie einen Namen für das neue SR und den Namen der Freigabe ein, in der es ist. Klicken Sie auf **Scan**, damit der Assistent am angegebenen Speicherort nach vorhandenen NFS-SRs sucht.

   > **Hinweis:**
   >
   > Der NFS-Host muss so konfiguriert sein, dass er den angegebenen Pfad zu allen XenServer-Hosts im Pool exportiert.

   b) Klicken Sie auf **Fertigstellen**.

   Das neue SR wird im Bereich **Ressourcen** innerhalb des Pools angezeigt.

4. Wenn Sie iSCSI wählen:

   a) Geben Sie einen Namen für das neue SR und dann die IP-Adresse oder den DNS-Namen des iSCSI-Ziels ein.

> **Hinweis:**
>
> Das iSCSI-Speicherziel muss so konfiguriert werden, dass jeder XenServer-Host im Pool Zugriff auf eine oder mehrere LUNs hat.

b) Wenn Sie das iSCSI-Ziel für die Verwendung der CHAP-Authentifizierung konfiguriert haben, geben Sie den Benutzernamen und das Kennwort ein.

c) Klicken Sie auf die Schaltfläche **Zielhost scannen**, und wählen Sie dann den iSCSI-Ziel-IQN aus der Liste Ziel-IQN aus.

> **Warnung:**
>
> Das iSCSI-Ziel und alle Hosts im Pool müssen *eindeutige* IQNs haben.

d) Klicken Sie auf **Ziel-LUN**, und wählen Sie dann in der Liste Ziel-LUN die LUN aus, auf der das SR erstellt werden soll.

> **Warnung:**
>
> Jedes einzelne iSCSI-Speicherrepository muss vollständig in einer einzigen LUN enthalten sein und darf sich nicht über mehr als eine LUN erstrecken. Alle auf der ausgewählten LUN vorhandenen Daten werden vernichtet.

e) Klicken Sie auf **Fertigstellen**.

Das neue SR wird im Bereich **Ressourcen** innerhalb des Pools angezeigt.

Das neue gemeinsam genutzte SR wird jetzt zum Standard-SR für den Pool.

Erstellen virtueller Maschinen

Mit XenCenter können Sie virtuelle Maschinen auf verschiedene Arten erstellen, je nach Ihren Anforderungen. Unabhängig davon, ob Sie einzelne VMs mit unterschiedlichen Konfigurationen oder Gruppen mehrerer ähnlicher VMs bereitstellen, XenCenter bringt Sie in nur wenigen Schritten zum Laufen.

XenServer bietet auch eine einfache Möglichkeit, Batches virtueller Maschinen von VMware zu konvertieren. Weitere Informationen finden Sie unter Conversion Manager.

In diesem Abschnitt werden einige Methoden zum Erstellen von Windows-VMs behandelt. Um schnell loszulegen, verwenden die Verfahren das einfachste Setup von XenServer: einen einzelnen XenServer-Host mit lokalem Speicher (nachdem Sie XenCenter mit dem XenServer-Host verbunden haben, wird der Speicher automatisch auf dem lokalen Datenträger des Hosts konfiguriert).

In diesem Abschnitt wird auch gezeigt, wie Sie mithilfe der Live-Migration VMs zwischen Hosts im Pool live migrieren können.

Nachdem Sie erklärt haben, wie Sie Ihre neue VM erstellen und anpassen, wird in diesem Abschnitt beschrieben, wie Sie diese vorhandene VM in eine VM-Vorlage konvertieren. Eine VM-Vorlage behält Ihre Anpassung bei, sodass Sie sie immer verwenden können, um VMs nach denselben (oder ähnlichen) Spezifikationen zu erstellen. Es reduziert auch die Zeit, die zum Erstellen mehrerer VMs benötigt wird.

Sie können auch eine VM-Vorlage aus einem Snapshot einer vorhandenen VM erstellen. Ein Snapshot ist eine Aufzeichnung einer laufenden VM zu einem bestimmten Zeitpunkt. Es speichert die Speicher-, Konfigurations- und Netzwerkinformationen der ursprünglichen VM, wodurch sie für Backupzwecke nützlich ist. Snapshots bieten eine schnelle Möglichkeit, VM-Vorlagen zu erstellen. In diesem Abschnitt wird veranschaulicht, wie Sie einen Snapshot einer vorhandenen VM erstellen und diesen Snapshot dann in eine VM-Vorlage konvertieren. Abschließend wird in diesem Abschnitt beschrieben, wie Sie VMs aus einer VM-Vorlage erstellen.

Was du lernen wirst

Du wirst lernen wie man:

- Erstellen einer Windows 10-VM
- Installieren Sie die XenServer VM Tools für Windows
- Migrieren Sie eine laufende VM zwischen Hosts im Pool
- Erstellen einer VM-Vorlage
- Erstellen einer VM aus einer VM-Vorlage

Anforderungen

Um einen Pool mit gemeinsam genutztem Speicher zu erstellen, benötigen Sie die folgenden Elemente:

- Der XenServer-Pool, den Sie eingerichtet haben
- XenCenter
- Installationsdateien für Windows 10 VM
- Installationsdateien für XenServer VM Tools für Windows

Erstellen einer Windows 10-VM

> **Hinweis:**
>
> Das folgende Verfahren bietet ein Beispiel für die Erstellung einer Windows 10-VM. Die Standardwerte können je nach dem von Ihnen ausgewählten Betriebssystem variieren.

So erstellen Sie eine Windows VM:

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue VM**, um den Assistenten für neue VM zu öffnen.

   Mit dem Assistenten für neue VM können Sie die neue VM konfigurieren und verschiedene Parameter für CPU-, Speicher- und Netzwerkressourcen anpassen.

2. Wählen Sie eine VM-Vorlage und klicken Sie auf **Weiter**.

   Jede Vorlage enthält die Setup-Informationen zum Erstellen einer VM mit einem bestimmten Gastbetriebssystem (OS) und mit optimalem Speicher. Diese Liste spiegelt die Vorlagen wider, die XenServer derzeit unterstützt.

   > **Hinweis:**
   >
   > Wenn das Betriebssystem, das Sie auf Ihrer neuen VM installieren, nur mit der Originalhardware kompatibel ist, aktivieren Sie das Kästchen **Host-BIOS-Zeichenfolgen auf VM kopieren** . Verwenden Sie diese Option beispielsweise für eine Betriebssystem-Installations-CD, die mit einem bestimmten Computer verpackt wurde.
   >
   > Nachdem Sie eine VM zum ersten Mal gestartet haben, können Sie ihre BIOS-Zeichenfolgen nicht ändern. Stellen Sie sicher, dass die BIOS-Zeichenfolgen korrekt sind, bevor Sie die VM zum ersten Mal starten.

3. Geben Sie einen Namen und optional eine Beschreibung der neuen VM ein.

4. Wählen Sie die Quelle der Betriebssystemmedien aus, die auf der neuen VM installiert werden sollen.

   Die Installation von einer CD/DVD ist die einfachste Option für den Einstieg. Wählen Sie die Standardoption für die Installationsquelle (DVD-Laufwerk), legen Sie den Datenträger in das DVD-Laufwerk des XenServer-Hosts ein und klicken Sie auf **Weiter**, um fortzufahren.

   Mit XenServer können Sie auch Betriebssysteminstallationsmedien aus einer Reihe von Quellen abrufen, einschließlich einer bereits vorhandenen ISO-Bibliothek.

   Um eine bereits vorhandene ISO-Bibliothek anzuhängen, klicken Sie auf **Neue ISO-Bibliothek** und geben Sie den Speicherort und den Typ der ISO-Bibliothek an. Sie können dann das spezifische ISO-Medium des Betriebssystems aus der Liste auswählen.

5. Die VM läuft auf dem installierten Host. Wählen Sie **Weiter**, um fortzufahren.

6. Weisen Sie Prozessor- und Speicherressourcen zu.

   Jedes Betriebssystem hat unterschiedliche Konfigurationsanforderungen, die sich in den Vorlagen widerspiegeln. Sie können die Standardeinstellungen bei Bedarf ändern. Klicken Sie zum Fortfahren auf **Weiter**.

7. Weisen Sie eine Grafikprozesseinheit (GPU) zu.

   Der Assistent für **neue VM** fordert Sie auf, der VM eine dedizierte GPU oder virtuelle GPUs zuzuweisen. Mit dieser Option kann die VM die Rechenleistung der GPU nutzen. Es bietet bessere Unterstützung für professionelle High-End-3D-Grafikanwendungen wie CAD-, GIS- und medizinische Bildgebungsanwendungen.

   > **Hinweis:**
   >
   > GPU-Virtualisierung ist für Kunden der XenServer Premium Edition verfügbar.

8. Konfigurieren Sie den Speicher für die neue VM.

   Klicken Sie auf **Weiter**, um die Standardzuweisung und -konfiguration auszuwählen, oder Sie möchten vielleicht:

   a) Ändern Sie den Namen, die Beschreibung oder die Größe Ihres virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.

   b) Fügen Sie einen neuen virtuellen Datenträger hinzu, indem Sie **Hinzufügen**auswählen.

   > **Hinweis:**
   >
   > Wenn Sie einen Pool von XenServer-Hosts erstellen, können Sie zu diesem Zeitpunkt beim Erstellen einer VM gemeinsam genutzten Speicher konfigurieren.

9. Konfigurieren Sie das Netzwerk auf der neuen VM.

   Klicken Sie auf **Weiter**, um die Standard-Netzwerkkarte und -konfigurationen auszuwählen, einschließlich einer automatisch erstellten eindeutigen MAC-Adresse für jede Netzwerkkarte, oder Sie können:

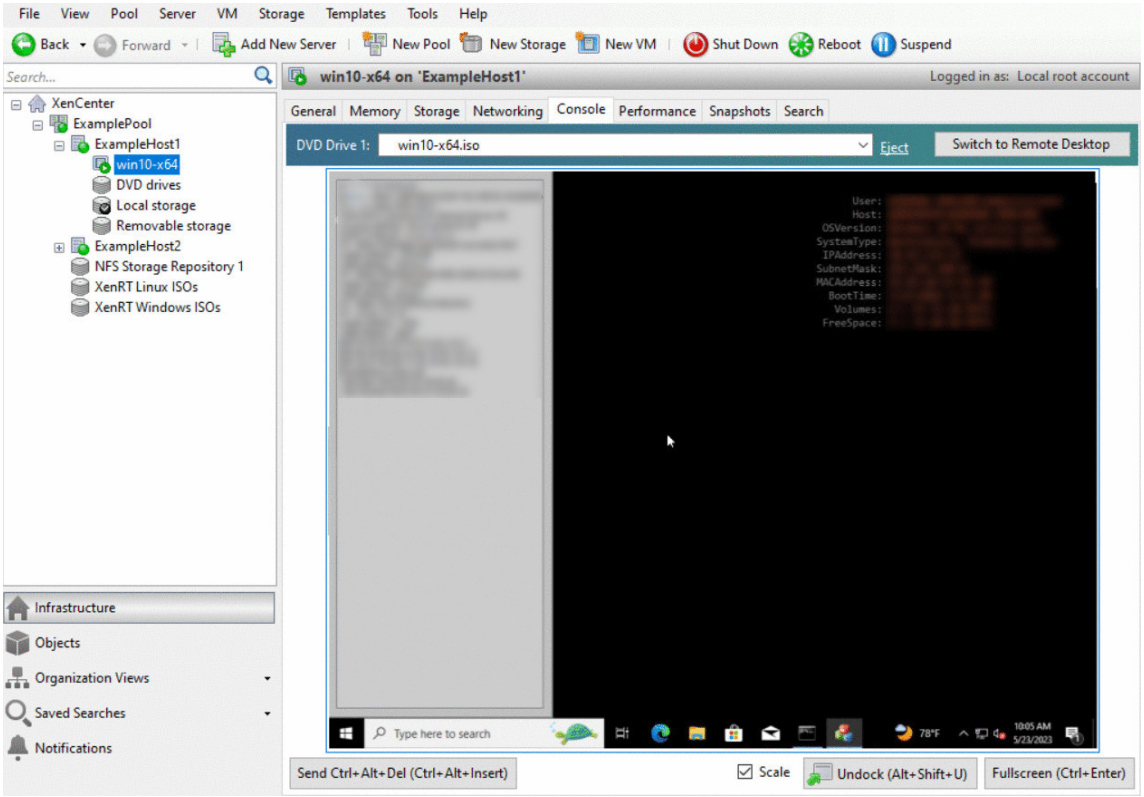
   a) Ändern Sie das physische Netzwerk, die MAC-Adresse oder die Quality of Service (QoS) -Priorität des virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.

   b) Fügen Sie eine neue virtuelle Netzwerkschnittstelle hinzu, indem Sie **Hinzufügen**auswählen.

      XenServer verwendet die virtuelle Netzwerkschnittstelle, um eine Verbindung zum physischen Netzwerk auf dem Host herzustellen. Achten Sie darauf, das Netzwerk auszuwählen, das dem Netzwerk entspricht, das die virtuelle Maschine benötigt. Informationen zum Hinzufügen eines physischen Netzwerks finden Sie unter Netzwerke für den Pool einrichten.

10. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Jetzt erstellen**, um die VM zu erstellen und zur Registerkarte **Suchen** zurückzukehren.

    Ein Symbol für Ihre neue VM wird unter dem Host im Bereich **Ressourcen** angezeigt.



Wählen Sie im Bereich **Ressourcen** die VM aus, und klicken Sie dann auf die Registerkarte **Konsole**, um die VM-Konsole anzuzeigen.

11. Folgen Sie den Installationsbildschirmen des Betriebssystems und treffen Sie Ihre Auswahl.
12. Nachdem die Betriebssysteminstallation abgeschlossen und die VM neu gestartet wurde, installieren Sie die XenServer VM Tools für Windows.

Installieren Sie die XenServer VM Tools für Windows

XenServer VM Tools für Windows bieten leistungsstarke I/O-Dienste ohne den Aufwand herkömmlicher Geräteemulation. XenServer VM Tools für Windows bestehen aus I/O-Treibern (auch bekannt als paravirtualisierte Treiber oder PV-Treiber) und dem Management Agent. XenServer VM Tools für Windows müssen auf jeder Windows-VM installiert sein, damit die VM eine vollständig unterstützte Konfiguration hat. Eine Windows-VM funktioniert ohne sie, aber die Leistung ist beeinträchtigt. XenServer VM Tools für Windows ermöglichen auch bestimmte Funktionen und Features, darunter das saubere Herunterfahren, Neustarten, Anhalten und Live-Migrieren von VMs.

> **Warnung:**
>
> Installieren Sie die XenServer VM Tools für Windows für jede Windows-VM. Das Ausführen von Windows-VMs ohne XenServer VM Tools für Windows wird *nicht* unterstützt.

> Wir empfehlen, dass Sie einen Snapshot Ihrer VM erstellen, bevor Sie die XenServer VM Tools installieren oder aktualisieren.

So installieren Sie die XenServer VM Tools für Windows:

1. Laden Sie die Datei XenServer VM Tools für Windows auf Ihre Windows-VM herunter. Holen Sie sich diese Datei von der XenServer-Downloadseite.
2. Führen Sie die `managementagentx64.msi` Datei aus, um mit der Installation der XenServer VM Tools zu beginnen.
3. Befolgen Sie die Anweisungen im Installationsprogramm.
4. Starten Sie die VM neu, wenn Sie aufgefordert werden, den Installationsvorgang abzuschließen.

> **Hinweis:**
>
> E/A-Treiber werden automatisch auf einer Windows-VM installiert, die Updates von Windows Update erhalten kann. Wir empfehlen jedoch, das Paket XenServer VM Tools für Windows zu installieren, um den Management Agent zu installieren und eine unterstützte Konfiguration beizubehalten. Die folgenden Funktionen sind nur für Kunden der XenServer Premium Edition verfügbar:
>
> - Möglichkeit, I/O-Treiber von Windows Update zu empfangen
> - Automatisches Update des Management Agents

Nachdem Sie die XenServer VM Tools für Windows installiert haben, können Sie Ihre VM anpassen, indem Sie Anwendungen installieren und andere Konfigurationen durchführen. Wenn Sie mehrere VMs mit ähnlichen Spezifikationen erstellen möchten, können Sie dies schnell tun, indem Sie eine Vorlage aus der vorhandenen VM erstellen. Verwenden Sie diese Vorlage, um virtuelle Maschinen zu erstellen. Weitere Informationen finden Sie unter Erstellen von VM-Vorlagen.

Migrieren Sie laufende VMs zwischen Hosts in einem Pool

Mithilfe der Live-Migration können Sie eine laufende VM von einem Host auf einen anderen im selben Pool verschieben, und das praktisch ohne Betriebsunterbrechung. Wohin Sie eine VM migrieren möchten, hängt davon ab, wie Sie die VM und den Pool konfigurieren.

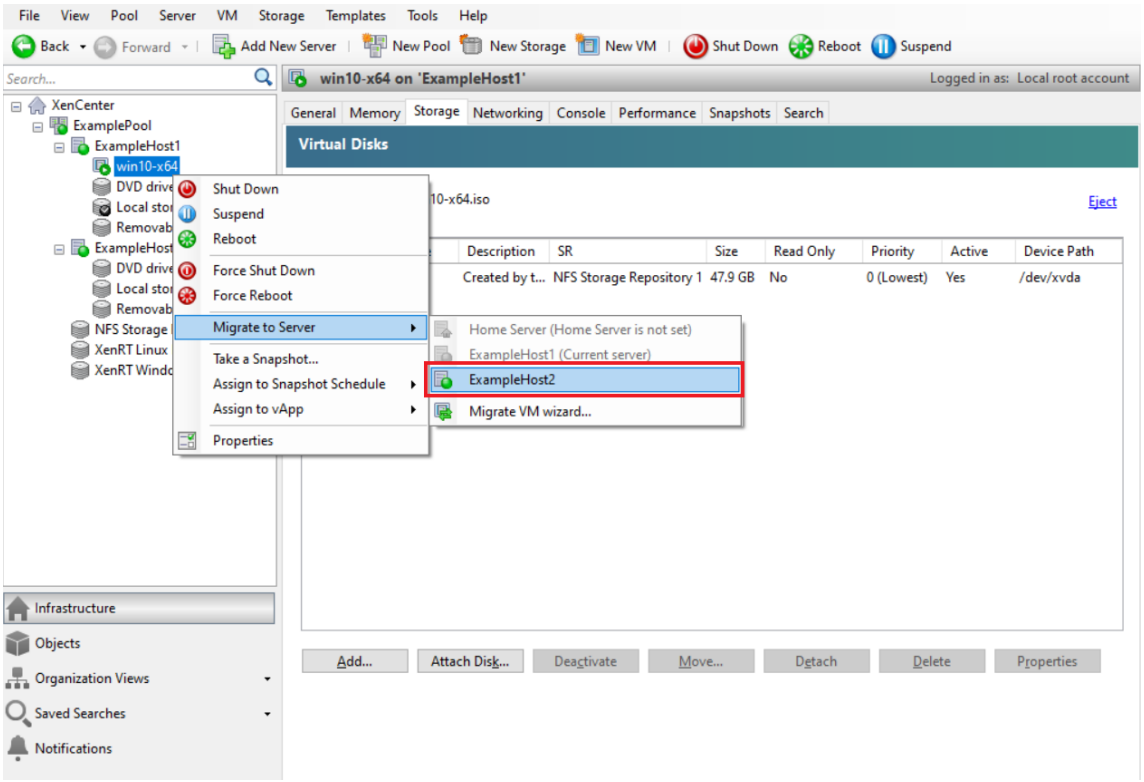
So migrieren Sie eine laufende VM:

1. Wählen Sie im Bereich **Ressourcen** die VM aus, die Sie verschieben möchten.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass die von Ihnen migrierte VM keinen lokalen Speicher hat.

2. Klicken Sie mit der rechten Maustaste auf das VM-Symbol, zeigen Sie **auf Zum Server migrieren**, und wählen Sie dann den neuen VM-Host aus.

> **Tipp:**
>
> Sie können die VM auch auf den Zielhost ziehen.



3. Die migrierte VM wird unter dem neuen Host im Bereich **Ressourcen** angezeigt.

Erstellen von VM-Vorlagen

Es gibt verschiedene Möglichkeiten, eine VM-Vorlage aus einer vorhandenen Windows-VM zu erstellen, jede mit ihren individuellen Vorteilen. Dieser Abschnitt konzentriert sich auf zwei Methoden: Konvertieren einer vorhandenen VM in eine Vorlage und Erstellen einer Vorlage aus einem Snapshot einer VM. In beiden Fällen behält die VM-Vorlage die benutzerdefinierte Konfiguration des ursprünglichen VM- oder VM-Snapshots bei. Die Vorlage kann dann verwendet werden, um schnell neue, ähnliche VMs zu erstellen. In diesem Abschnitt wird veranschaulicht, wie Sie aus diesen Vorlagen neue VMs erstellen können.

Bevor Sie eine Vorlage aus einem vorhandenen VM- oder VM-Snapshot erstellen, empfehlen wir, dass Sie das Windows-Dienstprogramm `Sysprep` auf der ursprünglichen VM ausführen. Im Allgemeinen bereitet `Sysprep` das Ausführen ein Betriebssystem für das Klonen und Wiederherstellen von Datenträgern vor. Windows-Betriebssysteminstallationen enthalten viele eindeutige Elemente pro Installation (einschließlich Sicherheitskennungen und Computernamen). Diese Elemente müssen eindeutig bleiben und dürfen nicht auf neue VMs kopiert werden. Wenn sie kopiert werden, können Verwirrung

und Probleme auftreten. Durch das Ausführen von Sysprep werden diese Probleme vermieden, indem neue, einzigartige Elemente für die neuen VMs generiert werden können.

> **Hinweis:**
>
> Das Ausführen von Sysprep ist für Basisbereitstellungen oder Testumgebungen möglicherweise nicht so erforderlich wie für Produktionsumgebungen.

Weitere Informationen Sysprepzu finden Sie in Ihrer Windows-Dokumentation. Das ausführliche Verfahren zum Ausführen dieses Dienstprogramms kann sich je nach installierter Windows-Version unterscheiden.

Erstellen einer VM-Vorlage aus einer vorhandenen VM So erstellen Sie eine VM-Vorlage aus einer vorhandenen VM:

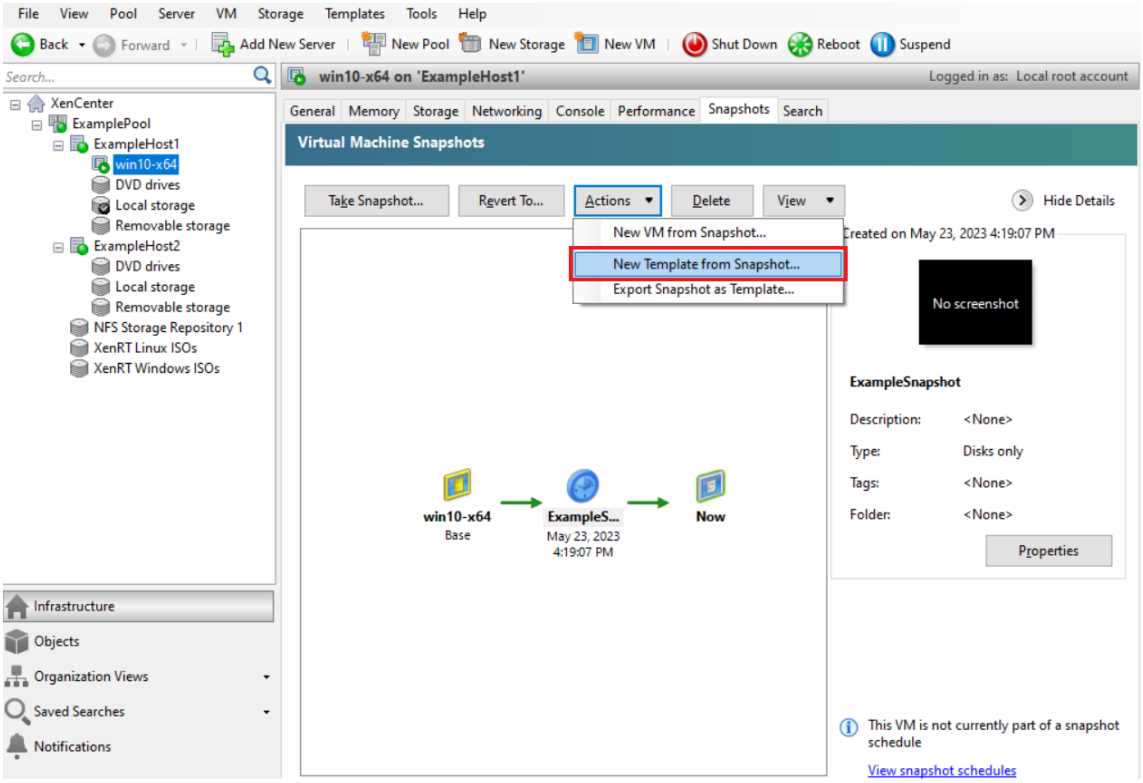
> **Warnung:**
>
> Wenn Sie eine Vorlage aus einer vorhandenen VM erstellen, ersetzt die neue Vorlage die ursprüngliche VM. Die VM existiert nicht mehr.

1. Fahren Sie die VM herunter, die Sie konvertieren möchten.
2. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf die VM, und wählen Sie **In Vorlage konvertieren**aus.
3. Klicken Sie zur Bestätigung auf **Konvertieren** .

   Sobald Sie die Vorlage erstellt haben, wird die neue VM-Vorlage im Bereich **Ressourcen** angezeigt und ersetzt die vorhandene VM.

Erstellen einer VM-Vorlage aus einem VM-Snapshot So erstellen Sie eine Vorlage aus einem Snapshot einer VM:

1. Wählen Sie im Bereich **Ressourcen** die VM aus. Klicken Sie auf die Registerkarte **Snapshots** und dann auf **Snapshot**erstellen.
2. Geben Sie einen Namen und optional eine Beschreibung des neuen Snapshots ein. Klicken Sie auf **Momentaufnahme aufnehmen**
3. Sobald der Snapshot fertig ist und das Symbol auf der Registerkarte **Schnappschüsse** angezeigt wird, wählen Sie das Symbol für den neuen Snapshot aus. Wählen Sie in der Liste **Aktionen** die Option **Neue Vorlage aus Snapshot aus**.



4. Geben Sie einen Namen für die Vorlage ein, und klicken Sie dann auf **Erstellen**.

Erstellen von virtuellen Rechnern aus einer VM-Vorlage

So erstellen Sie eine VM aus einer benutzerdefinierten VM-Vorlage:

1. Klicken Sie im Bereich XenCenter **Resources** mit der rechten Maustaste auf die Vorlage und wählen Sie Assistent für **neue VM** .

   Der Assistent für **neue VM** wird geöffnet.

2. Folgen Sie dem Assistenten für **neue VM**, um eine VM aus der ausgewählten Vorlage zu erstellen.

   > **Hinweis:**
   >
   > Wenn der Assistent Sie zur Eingabe einer Medienquelle für die Betriebssysteminstallation auffordert, wählen Sie den Standardwert aus und fahren Sie fort.

   Die neue VM wird im Bereich **Ressourcen** angezeigt.

Wenn Sie eine Vorlage verwenden, die aus einer vorhandenen VM erstellt wurde, können Sie auch **Quick Create**auswählen. Diese Option führt Sie nicht durch den Assistenten für **neue VM** . Stattdessen erstellt und stellt diese Option sofort eine neue VM mit allen in Ihrer Vorlage angegebenen Konfigurationseinstellungen bereit.

Systemanforderungen

February 24, 2024

XenServer benötigt mindestens zwei separate physische x86-Computer: einer als XenServer-Host und der andere für die Ausführung der XenCenter-Anwendung oder der XenServer-Befehlszeilenschnittstelle (CLI). Der XenServer-Hostcomputer ist ausschließlich der Ausführung von XenServer und dem Hosten von VMs gewidmet und wird nicht für andere Anwendungen verwendet.

> **Warnung:**
>
> XenServer unterstützt nur Treiber und zusätzliche Pakete, die von uns bereitgestellt werden und direkt in der Steuerdomäne des Hosts installiert werden. Treiber, die von Websites Dritter bereitgestellt werden, einschließlich Treiber mit demselben Namen oder derselben Versionsnummer wie die von uns bereitgestellten Treiber, werden nicht unterstützt.
>
> Die folgenden Ausnahmen werden unterstützt:
>
> - Software, die als Zusatzpaket geliefert und von uns ausdrücklich empfohlen wird.
> - Treiber, die NVIDIA zur Aktivierung der vGPU-Unterstützung bereitstellt. Weitere Informationen finden Sie unter NVIDIA vGPU.
>
>   Other drivers provided by NVIDIA, for example, the Mellanox drivers, are not supported with XenServer unless distributed by us.

Verwenden Sie zum Ausführen von XenCenter ein beliebiges Allzweck-Windows-System, das die Hardwareanforderungen erfüllt. Dieses Windows-System kann zum Ausführen anderer Anwendungen verwendet werden.

Wenn Sie XenCenter auf diesem System installieren, wird auch die XenServer-CLI installiert. Eine eigenständige Remote-XenServer-CLI kann auf jeder RPM-basierten Linux-Distribution installiert werden. Weitere Informationen finden Sie unter Befehlszeilenschnittstelle.

XenServer-Hostsystemanforderungen

Obwohl XenServer normalerweise auf Hardware der Serverklasse bereitgestellt wird, ist XenServer auch mit vielen Modellen von Workstations und Laptops kompatibel. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste (HCL).

Im folgenden Abschnitt werden die empfohlenen XenServer-Hardwarespezifikationen beschrieben.

Der XenServer-Host muss eine 64-Bit-x86-Serverklasse-Maschine sein, die für das Hosten von VMs vorgesehen ist. XenServer erstellt eine optimierte und gehärtete Linux-Partition mit einem Xen-

fähigen Kernel. Dieser Kernel steuert die Interaktion zwischen den virtualisierten Geräten, die von VMs erkannt werden, und der physischen Hardware.

XenServer kann verwenden:

- Bis zu 6 TB RAM
- Bis zu 16 physische NICs
- Bis zu 448 logische Prozessoren pro Host.

> **Hinweis:**
>
> Die maximale Anzahl unterstützter logischer Prozessoren ist je nach CPU unterschiedlich. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste (HCL).

Die Systemanforderungen für den XenServer-Host sind:

CPUs

Eine oder mehrere 64-Bit-x86-CPUs, mindestens 1,5 GHz, 2 GHz oder schneller Multicore-CPU empfohlen.

Um VMs mit Windows oder neueren Linux-Versionen zu unterstützen, benötigen Sie ein Intel VT oder AMD-V 64-Bit-x86-basiertes System mit einer oder mehreren CPUs.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die Hardwareunterstützung für Virtualisierung auf dem XenServer-Host aktivieren. Virtualisierungsunterstützung ist eine Option in Ihrer Systemfirmware. Es ist möglich, dass auf Ihrer Hardware die Virtualisierungsunterstützung deaktiviert ist. Weitere Informationen finden Sie in Ihrer Serverdokumentation.

Um VMs zu unterstützen, auf denen unterstütztes paravirtualisiertes Linux ausgeführt wird, benötigen Sie ein standardmäßiges 64-Bit-x86-basiertes System mit einer oder mehreren CPUs.

RAM

Mindestens 2 GB, 4 GB oder mehr empfohlen

Speicherplatz

- Lokal angeschlossener Speicher mit mindestens 46 GB Speicherplatz, 70 GB Speicherplatz empfohlen

- SAN über HBA (nicht über Software) bei der Installation mit Multipath-Boot von SAN.

Eine ausführliche Liste kompatibler Speicherlösungen finden Sie in der Hardwarekompatibilitätsliste (HCL).

Netzwerk

Netzwerkkarte mit 100 Mbit/s oder schneller. Eine oder mehrere GB- oder 10-Gbit-NICs werden für schnellere Export-/Importdatenübertragungen und VM-Livemigration empfohlen.

Aus Gründen der Redundanz empfehlen wir, mehrere Netzwerkkarten zu verwenden. Die Konfiguration der NICs unterscheidet sich je nach Speichertyp. Weitere Informationen finden Sie in der Dokumentation des Anbieters.

XenServer benötigt ein IPv4-Netzwerk für Verwaltung und Speicherverkehr.

> **Hinweise:**
>
> - Stellen Sie sicher, dass die Zeiteinstellung auf Ihrem Server auf die aktuelle Uhrzeit in UTC eingestellt ist.
> - In einigen Supportfällen ist ein serieller Konsolenzugriff für Debug-Zwecke erforderlich. Bei der Einrichtung der XenServer-Konfiguration empfehlen wir, den seriellen Konsolenzugriff zu konfigurieren. Prüfen Sie bei Hosts, die keine physische serielle Schnittstelle haben oder bei denen keine geeignete physische Infrastruktur verfügbar ist, ob Sie ein eingebettetes Verwaltungsgerät konfigurieren können. Zum Beispiel Dell DRAC. Weitere Informationen zum Einrichten des seriellen Konsolenzugriffs finden Sie unter CTX228930 - How to Configure Serial Console Access auf XenServer 7.0 und höher.

XenCenter Systemanforderungen

XenCenter hat die folgenden Systemanforderungen:

- **Betriebssystem:**
  - Windows 10
  - Windows 11
  - Windows Server 2016
  - Windows Server 2019
- **.NET-Framework:** Version 4.8
- **CPU-Geschwindigkeit:** mindestens 750 MHz, 1 GHz oder schneller empfohlen
- **RAM:** mindestens 1 GB, 2 GB oder mehr empfohlen
- **Speicherplatz:** mindestens 100 MB

- **Netzwerk:** 100 Mbit/s oder schneller NIC
- **Bildschirmauflösung:** 1024x768 Pixel, mindestens

Wenn Sie möchten, dass XenCenter eine externe SSH-Konsole starten kann, die eine Verbindung zu Ihrem Server herstellt, installieren Sie eine der folgenden Anwendungen auf dem System:

- PuTTY
- OpenSSH (wird standardmäßig auf einigen Windows-Betriebssystemen installiert)

Weitere Informationen finden Sie unter XenCenter für die Verwendung einer externen SSH-Konsole konfigurieren.

Unterstützte Gastbetriebssysteme

Eine Liste der unterstützten VM-Betriebssysteme finden Sie unter Unterstützung für Gastbetriebssysteme.

Anforderungen an den Pool

Ein Ressourcenpool ist ein homogenes oder heterogenes Aggregat aus einem oder mehreren Hosts, bis zu einem Maximum von 64. Bevor Sie einen Pool erstellen oder einen Host mit einem vorhandenen Pool verbinden, stellen Sie sicher, dass alle Hosts im Pool die folgenden Anforderungen erfüllen.

Hardwareanforderungen

Alle Server in einem XenServer-Ressourcenpool müssen über weitgehend kompatible CPUs verfügen, d. h.:

- Der CPU-Anbieter (Intel, AMD) muss auf allen CPUs auf allen Servern identisch sein.
- Für alle CPUs muss die Virtualisierung aktiviert sein.

Weitere Anforderungen

Zusätzlich zu den zuvor genannten Hardwarevoraussetzungen gibt es noch einige weitere Konfigurationsvoraussetzungen für den Beitritt eines Hosts zu einem Pool:

- Es muss eine konsistente IP-Adresse haben (eine statische IP-Adresse auf dem Host oder eine statische DHCP-Lease). Diese Anforderung gilt auch für Server, die gemeinsam genutzten NFS- oder iSCSI-Speicher bereitstellen.
- Die Systemuhr muss mit dem Poolkoordinator synchronisiert werden (z. B. über NTP).

- Es kann kein Mitglied eines vorhandenen Ressourcenpools sein.
- Es kann keine laufenden oder angehaltenen VMs oder aktive Vorgänge auf seinen VMs wie Herunterfahren oder Exportieren haben. Fahren Sie alle VMs auf dem Host herunter, bevor Sie sie einem Pool hinzufügen.
- Es kann nicht bereits einen gemeinsam genutzten Speicher konfiguriert haben.
- Es kann keine gebundene Verwaltungsschnittstelle haben. Konfigurieren Sie die Verwaltungsschnittstelle neu und verschieben Sie sie auf eine physische Netzwerkkarte, bevor Sie den Host zum Pool hinzufügen. Nachdem der Host dem Pool beigetreten ist, können Sie die Verwaltungsschnittstelle erneut konfigurieren.
- Es muss dieselbe Version von XenServer auf derselben Patch-Ebene ausgeführt werden wie Hosts, die sich bereits im Pool befinden.
- Es muss mit denselben Zusatzpaketen konfiguriert werden wie die Hosts, die sich bereits im Pool befinden. Zusätzliche Pakete werden verwendet, um Zusatzsoftware in der XenServer-Steuerdomäne dom0 zu installieren. Um eine inkonsistente Benutzererfahrung in einem Pool zu verhindern, müssen auf allen Hosts im Pool dieselben Zusatzpakete mit derselben Version installiert sein.
- Es muss dieselbe XenServer-Lizenz haben wie die Hosts, die sich bereits im Pool befinden. Sie können die Lizenz von Poolmitgliedern ändern, nachdem Sie dem Pool beigetreten sind. Der Host mit der niedrigsten Lizenz bestimmt, welche Funktionen allen Mitgliedern im Pool zur Verfügung stehen.

XenServer-Hosts in Ressourcenpools können eine unterschiedliche Anzahl von physischen Netzwerkschnittstellen enthalten und über lokale Speicherrepositorys unterschiedlicher Größe verfügen.

> **Hinweis:**
>
> Server, die gemeinsam genutzten NFS- oder iSCSI-Speicher für den Pool bereitstellen, müssen eine statische IP-Adresse haben oder über DNS adressierbar sein.

Homogene Pools

Ein homogener Ressourcenpool ist ein Aggregat von Servern mit identischen CPUs. CPUs auf einem Server, der einem homogenen Ressourcenpool beitritt, müssen über denselben Anbieter, dasselbe Modell und dieselben Funktionen wie die CPUs auf Servern verfügen, die sich bereits im Pool befinden.

Heterogene Pools

Die Erstellung heterogener Pools wird durch den Einsatz von Technologien in Intel (FlexMigration) und AMD (Extended Migration) CPUs ermöglicht, die *CPU-Maskierung* oder *Leveling*ermöglichen. Mit diesen Funktionen kann eine CPU so konfiguriert werden, dass sie eine andere Marke, ein anderes Modell oder einen anderen Funktionssatz *vorgibt* als sie tatsächlich ist. Mit diesen Funktionen können Sie Pools von Hosts mit unterschiedlichen CPUs erstellen und dennoch Livemigrationen sicher unterstützen.

Informationen zum Erstellen heterogener Pools finden Sie unter Hosts und Ressourcenpools.

Konfigurationslimits

April 12, 2024

Verwenden Sie die folgenden Konfigurationsgrenzen als Richtlinie bei der Auswahl und Konfiguration Ihrer virtuellen und physischen Umgebung für XenServer. Die folgenden getesteten und empfohlenen Konfigurationsgrenzen werden für XenServer vollständig unterstützt.

- Grenzwerte für virtuelle Maschinen
- XenServer-Host-Grenzwerte
- Grenzwerte für Ressourcenpools

Faktoren wie Hardware und Umgebung können die unten aufgeführten Einschränkungen beeinflussen. Weitere Informationen zu unterstützter Hardware finden Sie in der Hardwarekompatibilitätsliste. Konsultieren Sie die dokumentierten Grenzwerte Ihrer Hardwarehersteller, um sicherzustellen, dass Sie die unterstützten Konfigurationsbeschränkungen für Ihre Umgebung nicht überschreiten.

Grenzwerte für virtuelle Maschinen (VM)

Element	Limit
Server	
Virtuelle CPUs pro VM (Linux)	32/64 (siehe Anmerkung 1)
Virtuelle CPUs pro VM (Windows)	32/64 (siehe Anmerkung 1)
Speicher	

Element	Limit
Arbeitsspeicher pro VM	1,5 TiB (siehe Anmerkung 2)
Speicher	
Virtual Disk-Images (VDI) (einschließlich CD-ROM) pro VM	241 (siehe Anmerkung 3)
Virtuelle CD-ROM-Laufwerke pro VM	1
virtuelle Datenträgergröße (NFS)	2040 GiB
virtuelle Datenträgergröße (LVM)	2040 GiB
Größe des virtuellen Laufwerks (GFS2)	16 TiB
Netzwerke	
Virtuelle Netzwerkkarten pro VM	7 (siehe Hinweis 4)
Grafik-Fähigkeit	
vGPUs pro VM	8
GPUs pro VM durchlaufen	1
Geräte	
Passthrough-USB-Geräte	6

Hinweise:

1. Konsultieren Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten. Derzeit unterstützen Red Hat Enterprise Linux 8 und Derivate nicht mehr als 32 vCPUs. Obwohl das Limit bei 64 liegt, empfehlen wir, das Limit auf 32 festzulegen, wenn Ihre VMs möglicherweise nicht vertrauenswürdig sind oder wenn Sie mögliche Auswirkungen auf die Systemverfügbarkeit verhindern möchten.
2. Die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, variiert. Wenn Sie den Speicher auf einen höheren Wert als das vom Betriebssystem unterstützte Limit einstellen, kann dies zu Leistungsproblemen innerhalb Ihres Gastes führen.

3. Die maximale Anzahl unterstützter VDIs hängt vom Gastbetriebssystem ab. Konsultieren Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten.
4. Einige Gastbetriebssysteme haben ein niedrigeres Limit, andere Gäste benötigen die Installation der XenServer VM Tools, um dieses Limit zu erreichen.

XenServer-Host-Grenzwerte

Element	Limit
Server	
Logische Prozessoren pro Host	960 (siehe Hinweis 1)
Gleichzeitige virtuelle Maschinen pro Host	1000 (siehe Hinweis 2)
Gleichzeitige geschützte VMs pro Host mit aktivierter HA	500
Virtuelle GPU-VMs pro Host	128 (siehe Hinweis 3)
Speicher	
Arbeitsspeicher pro Host	6 TB
Speicher	
Gleichzeitige aktive virtuelle Datenträger pro Host	2048 (siehe Anmerkung 4)
Speicherrepositories pro Host (NFS)	400
Netzwerke	
Physische Netzwerkkarten pro Host	16
Physische NICs pro Netzwerkbindung	4
Virtuelle Netzwerkkarten pro Host	512
VLANs pro Host	800
Netzwerk-Bonds pro Host	4
Grafik-Fähigkeit	

Element	Limit
GPUs pro Host	8 (siehe Anmerkung 5)

Hinweise:

1. Die maximale Anzahl der unterstützten logischen physikalischen Prozessoren ist je nach CPU unterschiedlich. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste.
2. Die maximale Anzahl von virtuellen Rechnern pro unterstütztem Host hängt von der VM-Workload, der Systemlast, der Netzwerkkonfiguration und bestimmten Umgebungsfaktoren ab. Wir behalten uns das Recht vor zu bestimmen, welche spezifischen Umweltfaktoren die Höchstgrenze beeinflussen, ab der ein System funktionieren kann. Für größere Pools (über 32 Hosts) empfehlen wir, der Steuerdomäne (Dom0) mindestens 8 GB RAM zuzuweisen. Für Systeme mit über 500 virtuellen Maschinen oder bei Verwendung des PVS Accelerator empfehlen wir, mindestens 16 GB RAM zur Control Domain zuzuweisen. Informationen zum Konfigurieren des Dom0-Speichers finden Sie unter CTX134951 - How to Configure dom0-Speicher.
3. Für NVIDIA vGPU, 128 vGPU-beschleunigte VMs pro Host mit 4xM60-Karten (4x32=128 VMs) oder 2xM10-Karten (2x64=128 VMs). Für Intel GVT-G 7 VMs pro Host mit einer Blendengröße von 1.024 MB. Kleinere Blendengrößen können die Anzahl der pro Host unterstützten GVT-G-VMs weiter einschränken. Diese Zahl könnte sich ändern. Die aktuell unterstützten Grenzwerte finden Sie in der Hardwarekompatibilitätsliste.
4. Die Anzahl der gleichzeitig aktiven virtuellen Datenträger pro Host wird auch durch die Anzahl der SRs begrenzt, die Sie an den Host angehängt haben, und durch die Anzahl der angeschlossenen VDIs, die für jede SR zulässig sind (600). Weitere Informationen finden Sie im Eintrag “Angehängte VDIs pro SR”in den Grenzwerten für Ressourcenpools.
5. Diese Zahl könnte sich ändern. Die aktuell unterstützten Grenzwerte finden Sie in der Hardwarekompatibilitätsliste.

Grenzwerte für Ressourcenpools

Element	Limit
Server	
Virtuelle Rechner pro Ressourcenpool	2400

Element	Limit
Hosts pro Ressourcenpool	64 (siehe Anmerkung 1)
Netzwerke	
VLANs pro Ressourcenpool	800
Notfallwiederherstellung	
Integrierte Site-Recovery-Speicherrepositories pro Ressourcenpool	8
Speicher	
Pfade zu einer LUN	16
Multipath-LUNs pro Host	150 (siehe Anmerkung 2)
Multipathed-LUNs pro Host (wird von Speicherrepositorys verwendet)	150 (siehe Anmerkung 2)
VDIs pro SR (NFS, SMB, EXT, XFS, GFS2)	20000
VDIs pro SR (LVM)	1000
Angehängte VDIs pro SR (alle Typen)	600
Speicherrepositories pro Pool (NFS)	400
Speicher-Repositorys pro Pool (GFS2)	62
Live-Speichermigration	
(Nicht-CDROM) VDIs pro VM	6
Snapshots pro VM	1
Gleichzeitige Übertragungen	3
XenCenter	
Gleichzeitige Vorgänge pro Pool	25

> **Hinweise:**
>
> 1. Clusterpools, die GFS2-Speicher verwenden, unterstützen maximal 16 Hosts im Ressourcenpool.
> 2. Wenn HA aktiviert ist, empfehlen wir, das Standard-Timeout auf mindestens 120 Sekunden zu erhöhen, wenn mehr als 30 Multipath-LUNs auf einem Host vorhanden sind. Informationen zum Erhöhen des HA-Timeouts finden Sie unter CTX139166 - Ändern der Timeout-Einstellungen für Hochverfügbarkeit.

---

layout: doc
description: XenServer provides drivers that enable the product to support a wide range of hardware.
—

Hardware-Treiber

Wir arbeiten mit Partnerorganisationen zusammen, um Treiber und Support für eine Vielzahl von Geräten bereitzustellen. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste.

Zur Unterstützung dieser Hardware enthält Ihre Installation von XenServer 8 Treiber von Drittanbietern, die als kompatibel mit XenServer zertifiziert wurden. Eine Liste der Treiber, die in Ihrer ersten XenServer-Installation enthalten sind, finden Sie im zusammenfassenden Artikel Treiberversionen für XenServer undCitrix Hypervisor.

Updates für Treiber

Wir liefern regelmäßig aktualisierte Versionen dieser Treiber, mit denen neue Hardware aktiviert oder Probleme mit vorhandener Hardware behoben werden können. Die meisten Treiberupdates werden über den Update mechanismus bereitgestellt. Weitere Informationen finden Sie unter XenServer-Hosts aktualisieren.

Einige Treiberupdates werden als ISO-Dateien der Treiberdatenträger auf der Website https://support.citrix.com veröffentlicht. Diese Treiber sind im zusammenfassenden Artikel Treiberversionen für XenServer und Citrix Hypervisoraufgeführt.

Obwohl wir die Treiber und ihren Quellcode an unsere Kunden verteilen, gehören die Treiber-Quelldateien dem Hardwarehersteller.

Unterstützung für Fahrer

XenServer unterstützt nur Treiber, die im Lieferumfang des Produkts enthalten sind oder von https://support.citrix.com heruntergeladen wurden. Treiber, die von Websites Dritter bereitgestellt werden, einschließlich Treiber mit demselben Namen oder derselben Versionsnummer wie die von uns bereitgestellten Treiber, werden nicht unterstützt.

> **Hinweis:**
>
> Die einzige Ausnahme von dieser Einschränkung sind die Treiber, die NVIDIA zur Aktivierung der vGPU-Unterstützung bereitstellt. Weitere Informationen finden Sie unter NVIDIA vGPU.
>
> Andere von NVIDIA bereitgestellte Treiber, zum Beispiel die Mellanox-Treiber, werden von XenServer nur unterstützt, wenn sie von uns vertrieben werden.

Laden Sie keine Treiber von der Website Ihres Hardwareanbieters herunter, auch wenn der Treiber dieselbe Versionsnummer hat wie die von XenServer bereitgestellte. Diese Treiber werden nicht unterstützt.

Bevor ein Treiber mit XenServer unterstützt werden kann, muss er bei uns zertifiziert und über einen der zugelassenen Mechanismen veröffentlicht werden. Dieser Zertifizierungsprozess stellt sicher, dass der Treiber ein Format hat, das für die Installation in einer XenServer-Umgebung erforderlich ist, und dass er mit XenServer 8 kompatibel ist.

Was ist, wenn ein Treiber, den ich benötige, nicht unterstützt wird?

Wenn Ihr Hardwareanbieter Ihnen empfiehlt, eine bestimmte Treiberversion zu installieren, die nicht im Lieferumfang oder auf der Website https://support.citrix.com verfügbar ist, bitten Sie den Anbieter, uns zu kontaktieren, um diese Version des Treibers mit XenServer zu zertifizieren.

Wir stellen den Anbietern Zertifizierungskits zur Verfügung, mit denen sie aktualisierte Versionen ihrer Treiber testen können, die vom gemeinsamen Kundenstamm von Citrix Hypervisor und dem Hardwareanbieter benötigt werden. Nachdem uns der Anbieter die Ergebnisse der Zertifizierungstests zur Verfügung gestellt hat, überprüfen wir, dass diese Ergebnisse keine Probleme oder Regressionen in der aktualisierten Version des Treibers aufweisen. Die Treiberversion ist jetzt mit XenServer zertifiziert und wir veröffentlichen den Treiber mit unseren regulären Updates oder als Treiberdatenträger-ISO unter https://support.citrix.com.

Weitere Informationen über den Zertifizierungsprozess, den der Anbieter befolgen muss, finden Sie im Artikel Hardwarekompatibilitätsliste erklärt.

layout: doc
description: Learn which VM operating systems are supported on XenServer and how much memory and disk space each operating system requires.—

Unterstützung für Gastbetriebssysteme

Befolgen Sie bei der Installation von VMs und der Zuweisung von Ressourcen wie Arbeitsspeicher und Speicherplatz die Richtlinien des Betriebssystems und aller relevanten Anwendungen.

Betriebssystem	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Speicherplatz
Windows 10 (64-Bit)	2 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows 11 (64 Bit)	4 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows Server 2016, Windows Server Core 2016 (64 Bit)	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows Server 2019, Windows Server Core 2019 (64 Bit)	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows Server 2022, Windows Serverkern 2022 (64 Bit)	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
CentOS 7 (64 Bit)	2 GB	1,5 TB	10 GB
CentOS Stream 9 (64-Bit) (Vorschau) (siehe Hinweis 1)	2 GB	1,5 TB	10 GB
Red Hat Enterprise Linux 7 (64 Bit)	2 GB	1,5 TB	10 GB
Red Hat Enterprise Linux 8 (64 Bit)	2 GB	1,5 TB	10 GB
Red Hat Enterprise Linux 9 (64-Bit) (Vorschau) (siehe Hinweis 1)	2 GB	1,5 TB	10 GB
SUSE Linux Enterprise Server 12 SP5 (64 Bit)	1 GB	1,5 TB	8 GB

Betriebssystem	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Speicherplatz
SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5 (64 Bit)	1 GB	1,5 TB	8 GB
SUSE Linux Enterprise Desktop 15 SP4, 15 SP5 (64 Bit)	1 GB	1,5 TB	8 GB
Oracle Linux 7 (64 Bit)	2 GB	1,5 TB	10 GB
Oracle Linux 8 (64 Bit)	2 GB	1,5 TB	10 GB
Wissenschaftliches Linux 7 (64 Bit)	2 GB	1,5 TB	10 GB
Debian Buster 10 (64 Bit)	512 MB	1,5 TB	10 GB
Debian Bullseye 11 (64 Bit)	512 MB	1,5 TB	10 GB
Debian Bookworm 12 (64 Bit) (Vorschau) (siehe Hinweis 1)	1 GB	1,5 TB	10 GB
Ubuntu 20.04 (64 Bit)	512 MB	1,5 TB	10 GB
Ubuntu 22.04 (64 Bit)	1 GB	1,5 TB	10 GB
NeoKylin Linux Advanced Server 7.2 (64-Bit)	1 GB	1,5 TB	10 GB
Gooroom 2 (64 Bit)	1 GB	1,5 TB	10 GB
Rocky Linux 8 (64 Bit)	1 GB	1,5 TB	10 GB
Rocky Linux 9 (64-Bit) (Vorschau) (siehe Hinweis 1)	2 GB	1,5 TB	15 GB

> **Hinweis:**
>
> 1. Kunden, die dieses Gastbetriebssystem verwenden möchten, müssen auch die XenServer VM Tools für Linux v8.3.1-1 oder höher installieren, die auf der XenServer-Produktdownloadseiteheruntergeladen werden können.

- XenServer VM Tools für Linux wird nur auf den oben aufgeführten Linux-Gastbetriebssystemen

unterstützt.

- Alle unterstützten Betriebssysteme laufen im HVM-Modus.
- Einzelne Versionen der Betriebssysteme können auch ihre eigenen Höchstgrenzen für die unterstützte Speichermenge festlegen (z. B. aus Lizenzgründen).
- Überschreiten Sie bei der Konfiguration des Gastspeichers nicht die maximale Menge an physischem Speicher, die Ihr Betriebssystem adressieren kann. Das Festlegen eines Speichermaximums, das über dem vom Betriebssystem unterstützten Limit liegt, kann zu Stabilitätsproblemen innerhalb Ihres Gastes führen.
- Verwenden Sie die folgende Methode, um eine VM mit einer neueren Nebenversion von RHEL als in der vorherigen Tabelle aufgeführt zu erstellen:
  - Installieren Sie die VM von den neuesten unterstützten Medien für die Hauptversion
  - Verwenden Sie `yum update`, um die VM auf die neuere Nebenversion zu aktualisieren

  Dieser Ansatz gilt auch für RHEL-basierte Betriebssysteme wie CentOS und Oracle Linux.
- XenServer unterstützt alle SKUs (Editionen) für die aufgelisteten Versionen von Windows.

Langfristige Unterstützung durch

XenServer umfasst eine Richtlinie zur langfristigen Gastunterstützung (LTS) für Linux-VMs. Mit der LTS-Richtlinie können Sie kleinere Versionsupdates mit einer der folgenden Methoden verwenden:

- Installieren von neuen Gastmedien
- Upgrade von einem vorhandenen unterstützten Gast

Betriebssysteme außerhalb des Supports

Die Liste der unterstützten Gastbetriebssysteme kann Betriebssysteme enthalten, die zum Zeitpunkt der Veröffentlichung dieser Version von XenServer von ihren Anbietern unterstützt wurden, aber jetzt nicht mehr von ihren Anbietern unterstützt werden.

Wir bieten keinen Support mehr für diese Betriebssysteme an (auch wenn sie in der Tabelle der unterstützten Gäste aufgeführt bleiben oder ihre Vorlagen auf Ihren XenServer-Hosts verfügbar bleiben). Beim Versuch, ein gemeldetes Problem zu beheben und zu lösen, prüfen wir, ob das Problem direkt mit einem Betriebssystem auf einer VM zusammenhängt, das nicht unterstützt wird. Um Ihnen bei dieser Entscheidung zu helfen, bitten wir Sie möglicherweise, zu versuchen, ein Problem mit einer unterstützten Version des Gastbetriebssystems zu reproduzieren. Wenn das Problem mit dem Betriebssystem zusammenhängt, das nicht mehr unterstützt wird, werden wir das Problem nicht weiter untersuchen.

> **Hinweis:**
>
> Windows-Versionen, die von Microsoft als Teil eines LTSB-Zweigs unterstützt werden, werden von XenServer unterstützt.
> Windows-Versionen, die nicht mehr unterstützt werden, aber Teil einer Vereinbarung über erweiterte Sicherheitsupdates (ESU) sind, werden von XenServer nicht unterstützt.

---

layout: doc
description: If your XenServer traffic traverses network components such as firewalls or proxy servers, open these ports to ensure communication flow.—

Konnektivitätsanforderungen

Dieser Artikel bietet einen Überblick über Domänen und allgemeine Ports, die von XenServer-Komponenten verwendet werden und als Teil der Netzwerkarchitektur betrachtet werden müssen, insbesondere wenn der Kommunikationsverkehr Netzwerkkomponenten wie Firewalls oder Proxyserver durchquert, wo Ports geöffnet oder Domänen zu einer Zulassungsliste hinzugefügt werden müssen, um den Kommunikationsfluss sicherzustellen.

Externe Domänen, auf die von XenServer-Produktkomponenten zugegriffen wird

Konfigurieren Sie Ihre Firewall je nach Ihrer Bereitstellung und Ihren Anforderungen so, dass diese XenServer-Komponenten auf die aufgelisteten Domänen zugreifen können.

XenServer-Hosts

Ihre XenServer-Hosts greifen auf die folgenden Domänen zu:

Domäne	Port	Richtung	Details
repo.ops.xenserver.com	443	Ausgehend	Der XenServer-Poolkoordinator lädt verfügbare Updates für XenServer 8 von diesem Ort herunter. Weitere Informationen finden Sie unter Updates.
repo-src.ops.xenserver.com	443	Ausgehend	Der XenServer-Poolkoordinator lädt die Quelldateien für XenServer 8-Updates von diesem Speicherort herunter. Weitere Informationen finden Sie unter Updates.
telemetry.ops.xenserver.com	443	Ausgehend	Der XenServer-Poolkoordinator sammelt Telemetriedaten und lädt sie regelmäßig an diesen Standort hoch. Weitere Informationen finden Sie unter Telemetrie.

Wenn Sie Ihre XenServer-Pools für den Empfang von Updates konfigurieren, können Sie einen Proxyserver konfigurieren, den der Poolkoordinator zum Herunterladen der Updates verwendet. Weitere Informationen finden Sie unter Updates für Ihren Pool konfigurieren.

XenCenter

Die XenCenter Management Console greift auf die folgenden Domänen zu:

Domäne	Port	Richtung	Details
`updates.ops.xenserver.com`	443	Ausgehend	XenCenter fragt Informationen auf dieser Site ab, um festzustellen, ob Updates für XenCenter- und XenServer 8-Hosts verfügbar sind. Weitere Informationen finden Sie unter Aktualisieren Ihrer XenServer-Hosts
`citrix.com` und Unterdomänen	443	Ausgehend	Wenn Sie XenCenter verwenden, um Citrix Hypervisor 8.2 Cumulative Update 1-Hosts und -Pool zu verwalten, greift XenCenter auf Unterdomänen in der Domäne `citrix.com` zu, um über Hotfixes informiert zu werden und diese herunterzuladen. Weitere Informationen finden Sie unter Aktualisieren der Citrix Hypervisor-Hosts

Sie können einen Proxyserver konfigurieren, den XenCenter durchläuft, um nach Updates zu suchen und diese herunterzuladen. Weitere Informationen finden Sie unter Proxyserver.

Windows-VMs

Wenn Sie Ihre Windows-VMs so eingerichtet haben, dass sie Updates für den XenServer VM Tools Management Agent erhalten, greift Ihre Windows-VM auf die folgenden Domänen zu:

Domäne	Port	Richtung	Details
pvupdates.vmd.citrix.com	443	Ausgehend	Die XenServer VM Tools für Windows fragen Informationen auf dieser Site ab, um festzustellen, ob Updates für den Management Agent verfügbar sind.
downloadns.citrix.com.edgesuite.net	443	Ausgehend	Die XenServer VM Tools für Windows laden die Installationsdateien für den Management Agent von diesem Speicherort herunter.

Wenn Sie nicht möchten, dass Ihre Windows-VM auf diese Domänen zugreift, können Sie Management-Agent-Updates an einen internen Webserver umleiten. Weitere Informationen finden Sie unter Umleiten der Management Agent-Updates .

Von den XenServer-Produktkomponenten verwendete Kommunikationsports

Die in der folgenden Tabelle aufgeführten Ports sind die allgemeinen Ports, die von XenServer-Komponenten verwendet werden. Je nach Bereitstellung und Anforderungen müssen nicht alle Ports offen sein.

Quelle	Ziel	Typ	Port	Details
XenServer-Hosts	XenServer-Hosts	TCP	80, 443	Host-interne Kommunikation zwischen Mitgliedern eines Ressourcenpools mithilfe der Management-API

Quelle	Ziel	Typ	Port	Details
	Citrix Lizenzserver	TCP	27000	Verwaltet die Erstverbindung für Lizenzanfragen
		TCP	7279	Ein-/Auschecken von Lizenzen
	NTP-Dienst	TCP, UDP	123	Zeit-Synchronisierung
	DNS-Dienst	TCP, UDP	53	DNS-Suchvorgänge
	Domänencontroller	TCP, UDP	389	LDAP (für die Active Directory-Benutzerauthentifizierung)
		TCP	636	LDAP über SSL (LDAPS)
	FileServer (mit SMB-Speicher)	TCP, UDP	139	ISOStore:NetBIOSSessionServi
		TCP, UDP	445	ISOStore:Microsoft-DS
	SAN-Controller	TCP	3260	iSCSI-Speicher
	NAS-Kopf-/Dateiserver	TCP	2049	NFSv4-Speicher
		TCP, UDP	2049	NFSv3-Speicher. TCP ist die Standardeinstellung
		TCP, UDP	111	NFSv3 Storage - Verbindung zu rpcbind
		TCP, UDP	Dynamisch	NFSv3-Speicher - ein dynamischer Satz von Ports, der vom Filer ausgewählt wird
	Syslog	UDP	514	Sendet Daten zum Zusammenstellen an einen zentralen Ort

Quelle	Ziel	Typ	Port	Details
	Clustering	TCP	8892, 8896, 21064	Kommunikation zwischen allen Poolmitgliedern in einem Clusterpool
		UDP	5404, 5405	
XenCenter	XenServer-Hosts	TCP	22	SSH
		TCP	443	Verwaltung mithilfe der Management-API
	Virtuelle Maschine	TCP	5900	VNC für Linux-VMs
		TCP	3389	RDP für Windows-VMs
Virtuelle Appliance für den Workloadausgle-ich	XenServer-Hosts	TCP	8012	Standardmäßig verwendet der Workload Balancing-Server 8012. Wenn Sie jedoch bei der Einrichtung des Workload Balancing einen anderen Port angeben, stellen Sie sicher, dass die Kommunikation auf diesem Port zulässig ist.

Quelle	Ziel	Typ	Port	Details
Andere Kunden	XenServer-Hosts	TCP	80, 443	Jeder Client, der die Management-API für die Kommunikation mit XenServer-Hosts verwendet

XenServer arbeitet mit verschiedenen Citrix-Produkten zusammen. Weitere Informationen zu den von diesen Produkten verwendeten Ports finden Sie unter Von Citrix verwendete Kommunikationsports.

> **Hinweis:**
>
> - Um die Sicherheit zu verbessern, können Sie den TCP-Port 80 auf der Verwaltungsschnittstelle von XenServer-Hosts schließen. Weitere Informationen zum Schließen von Port 80 finden Sie unter Verwendung von Port 80 einschränken.
> - Wenn FQDN anstelle von IP als Ressource verwendet wird, stellen Sie sicher, dass er auflösbar ist.

Active Directory-Integration

Wenn Sie Active Directory in Ihrer Umgebung verwenden, stellen Sie sicher, dass die folgenden Firewallports für ausgehenden Datenverkehr geöffnet sind, damit XenServer auf die Domänencontroller zugreifen kann.

Port	Protokoll	Verwenden
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS-Namensdienst
139	TCP	NetBIOS-Sitzung (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB über TCP

Port	Protokoll	Verwenden
464	UDP/TCP	Kennwortänderungen für
636	UDP/TCP	LDAP über SSL
3268	TCP	Globale Katalogsuche

Weitere Informationen finden Sie unter Active Directory-Integration

Citrix Provisioning Services

Wenn Sie Citrix Provisioning Services in Ihrer Umgebung verwenden, stellen Sie sicher, dass auf die folgenden Firewall-Ports zugegriffen werden kann:

Port	Protokoll	Verwenden
6901, 6902, 6905	UDP	Provisioning der ausgehenden Kommunikation mit dem Server (Pakete, die für das Zielgerät bestimmt sind)
6910	UDP	Anmeldung am Zielgerät mit Citrix Provisioning Services
6901	UDP	Konfigurierbarer Zielgerät-Anschluss. Der Standardport ist 6901.
6910–6930	UDP	Konfigurierbarer Serverportbereich. Der Standardbereich ist 6910—6930.

Weitere Informationen finden Sie unter Citrix Provisioning Services und von Citrix verwendete Kommunikationsports.

---

layout: doc
description: Learn more about XenServer (formerly Citrix Hypervisor) concepts, components, and features.—

Technische Übersicht

XenServer (ehemals Citrix Hypervisor) ist eine branchenführende Plattform für kostengünstige Desktop-, Server- und Cloud-Virtualisierungsinfrastrukturen. XenServer ermöglicht es Unternehmen jeder Größe und Art, Rechenressourcen zu konsolidieren und in virtuelle Workloads für die heutigen Rechenzentrumsanforderungen umzuwandeln. In der Zwischenzeit wird ein nahtloser Weg zum Verschieben von Workloaden in die Cloud sichergestellt.

Die wichtigsten Funktionen von XenServer sind:

- Konsolidierung mehrerer virtueller Maschinen (VMs) auf einem physischen Server
- Reduzierung der Anzahl der zu verwaltenden separaten Disk-Images
- Einfache Integration mit vorhandenen Netzwerk- und Speicherinfrastrukturen
- So können Sie Wartungsarbeiten ohne Ausfallzeiten planen, indem Sie VMs live zwischen XenServer-Hosts migrieren
- Sicherstellung der Verfügbarkeit von VMs durch Verwendung von Hochverfügbarkeit zur Konfiguration von Richtlinien, die VMs auf einem anderen Host neu starten, falls einer ausfällt
- Erhöhung der Portabilität von VM-Images, da ein VM-Image auf einer Reihe von Bereitstellungsinfrastrukturen funktioniert

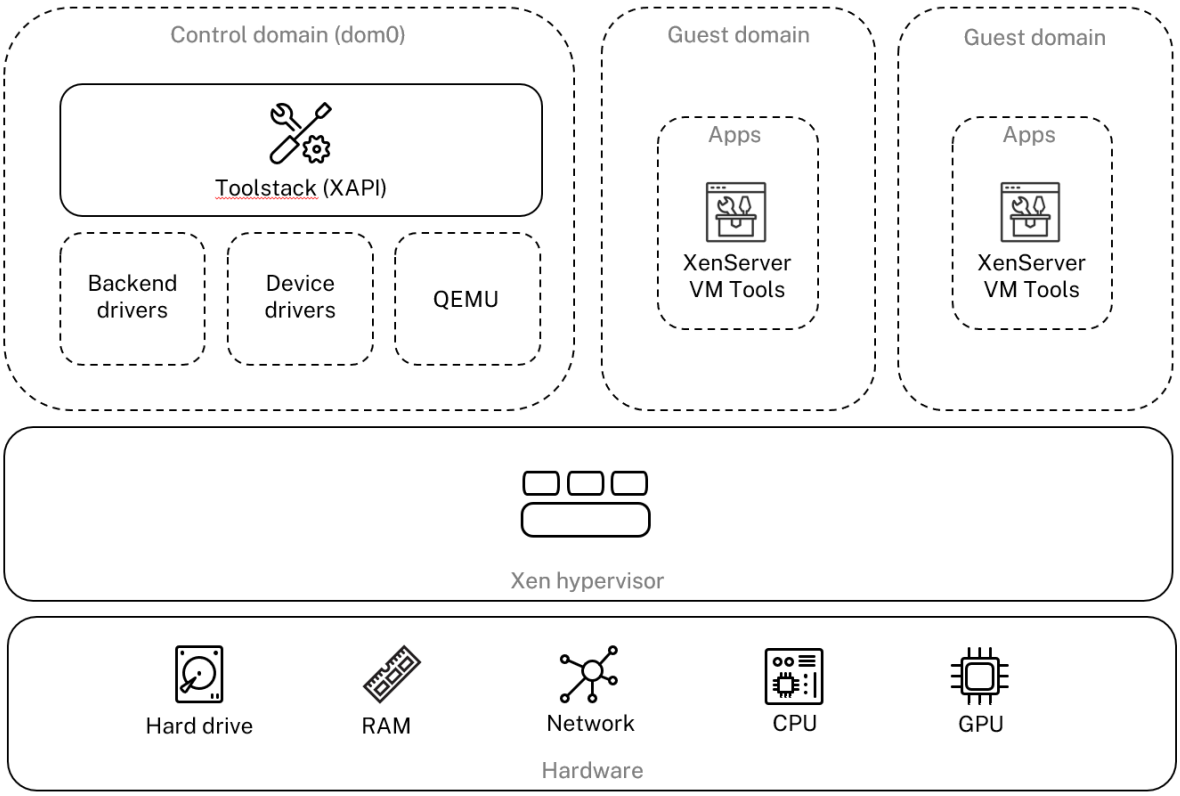
Virtualisierung und Hypervisor

Virtualisierung oder genauer gesagt Hardwarevirtualisierung ist eine Methode zum Ausführen mehrerer unabhängiger VMs auf einem einzigen physischen Computer. Die auf diesen virtuellen Maschinen ausgeführte Software ist von den zugrunde liegenden Hardwareressourcen getrennt. Auf diese Weise können die physischen Ressourcen moderner leistungsfähiger Server vollständig genutzt werden, wodurch die Gesamtbetriebskosten (TCO) für Serverbereitstellungen gesenkt werden.

Ein Hypervisor ist die grundlegende Abstraktionsschicht der Software. Der Hypervisor führt Aufgaben auf niedriger Ebene wie die CPU-Planung aus und ist für die Speicherisolierung von residenten VMs verantwortlich. Der Hypervisor abstrakt die Hardware für die VMs. Der Hypervisor hat keine Kenntnisse über Netzwerke, externe Speichergeräte, Video usw.

Hauptkomponenten

In diesem Abschnitt erhalten Sie ein umfassendes Verständnis der Funktionsweise von XenServer. In der folgenden Abbildung finden Sie die wichtigsten Komponenten von XenServer:



Architecture overview

Hardware

Die Hardwareschicht enthält die physischen Serverkomponenten wie CPU, Speicher, Netzwerk und Datenträgerlaufwerke.

Sie benötigen ein Intel VT oder AMD-V 64-Bit-x86-basiertes System mit einer oder mehreren CPUs, um alle unterstützten Gastbetriebssysteme ausführen zu können. Weitere Informationen zu den Systemanforderungen für XenServer-Hosts finden Sie unter Systemanforderungen.
Eine vollständige Liste der von XenServer zertifizierten Hardware und Systeme finden Sie in der Hardwarekompatibilitätsliste (HCL).

Xen-Hypervisor

Der Xen Project-Hypervisor ist ein Open-Source-Hypervisor vom Typ 1 oder Bare-Metal. Es ermöglicht, dass viele Instanzen eines Betriebssystems oder verschiedener Betriebssysteme parallel auf einem einzigen Computer (oder Host) ausgeführt werden. Der Xen-Hypervisor wird als Grundlage für viele verschiedene kommerzielle und Open-Source-Anwendungen verwendet, z. B.: Servervirtualisierung,

Infrastructure as a Service (IaaS), Desktop-Virtualisierung, Sicherheitsanwendungen, Embedded- und Hardware-Appliances.

XenServer basiert auf dem Xen Project Hypervisor und darüber hinaus bieten wir zusätzliche Funktionen und Support. XenServer verwendet Version 4.13.4 des Xen-Hypervisors.

Domäne steuern

Die **Control Domain**, auch Domain 0 oder dom0 genannt, ist eine sichere, privilegierte Linux-VM, auf der der als XAPI bekannte XenServer-Management-Toolstack ausgeführt wird. Diese Linux-VM basiert auf einer CentOS 7.5-Distribution. Neben der Bereitstellung von XenServer-Verwaltungsfunktionen führt dom0 auch die physikalischen Gerätetreiber für Netzwerk, Speicher usw. aus. Die Steuerdomäne kann mit dem Hypervisor kommunizieren und ihn anweisen, Gast-VMs zu starten oder zu beenden.

Werkzeugstapel Der **Toolstack**oder XAPI ist der Software-Stack, der VM-Lebenszyklusvorgänge, Host- und VM-Netzwerke, VM-Speicher und Benutzerauthentifizierung steuert. Es ermöglicht auch die Verwaltung von XenServer-Ressourcenpools.
XAPI bietet die öffentlich dokumentierte Management-API, die von allen Tools zur Verwaltung von VMs und Ressourcenpools verwendet wird. Weitere Informationen finden Sie unter der XenServer Management API.

Gastdomäne (virtuelle Maschinen)

Gastdomänen sind vom Benutzer erstellte virtuelle Maschinen, die Ressourcen von dom0 anfordern. Eine ausführliche Liste der unterstützten Distributionen finden Sie unter Unterstützte Gäste, virtueller Speicher und Datenträgergrößenbeschränkungen.

Vollständige Virtualisierung Vollständige Virtualisierung oder hardwareunterstützte Virtualisierung nutzt Virtualisierungserweiterungen von der Host-CPU, um Gäste zu virtualisieren. Vollständig virtualisierte Gäste benötigen keine Kernelunterstützung. Der Gast wird als virtuelle Hardware-Maschine (HVM) bezeichnet. HVM erfordert Intel VT- oder AMD-V-Hardwareerweiterungen für Arbeitsspeicher und privilegierten Betrieb. XenServer verwendet Quick Emulator (QEMU), um PC-Hardware zu emulieren, einschließlich BIOS, IDE-Datenträgercontroller, VGA-Grafikadapter, USB-Controller, Netzwerkadapter usw. Um die Leistung hardwaresensitiver Operationen wie Datenträger- oder Netzwerkzugriff zu verbessern, werden HVM-Gäste mit den XenServer-Tools installiert. Weitere Informationen finden Sie unter PV auf HVM.

HVM wird häufig bei der Virtualisierung eines Betriebssystems wie Microsoft Windows verwendet, wo es unmöglich ist, den Kernel zu modifizieren, um ihn auf die Virtualisierung aufmerksam zu machen.

PV auf HVM PV auf HVM ist eine Mischung aus Paravirtualisierung und vollständiger Hardwarevirtualisierung. Das Hauptziel besteht darin, die Leistung von HVM-Gästen durch den Einsatz speziell optimierter paravirtualisierter Treiber zu steigern. In diesem Modus können Sie die virtuellen x86-Container-Technologien in neueren Prozessoren nutzen, um die Leistung zu verbessern. Der Netzwerk- und Speicherzugriff dieser Gäste erfolgt weiterhin im PV-Modus, wobei in die Kernel integrierte Treiber verwendet werden.

Windows- und Linux-Distributionen sind im PV-on-HVM-Modus in XenServer verfügbar. Eine Liste der unterstützten Distributionen mit PV auf HVM finden Sie unter Unterstützung für Gastbetriebssysteme.

XenServer VM-Tools XenServer VM Tools (früher Citrix VM Tools oder XenServer PV Tools) bieten leistungsstarke I/O-Dienste ohne den Aufwand herkömmlicher Geräteemulation.

- XenServer VM Tools für Windows bestehen aus I/O-Treibern (auch bekannt als paravirtualisierte Treiber oder PV-Treiber) und dem Management Agent.

  Die I/O-Treiber enthalten Front-End-Speicher- und Netzwerktreiber sowie Verwaltungsschnittstellen auf niedriger Ebene. Diese Treiber ersetzen die emulierten Geräte und ermöglichen eine schnelle Übertragung zwischen VMs und der Software der XenServer-Produktfamilie.

  Der Management Agent, auch Gastagent genannt, ist für die Verwaltungsfunktionen virtueller Maschinen auf hoher Ebene verantwortlich. Es bietet volle Funktionalität für XenCenter (für Windows-VMs).

  XenServer VM Tools für Windows müssen auf jeder Windows-VM installiert sein, damit die VM eine vollständig unterstützte Konfiguration hat. Eine VM funktioniert ohne die XenServer VM Tools für Windows, aber die Leistung wird erheblich beeinträchtigt, wenn die I/O-Treiber (PV-Treiber) nicht installiert sind.

- Die XenServer VM Tools für Linux enthalten einen Gast-Agent, der dem Host zusätzliche Informationen über die VM zur Verfügung stellt. Installieren Sie den Gastagenten auf jeder Linux-VM, um Dynamic Memory Control (DMC) zu aktivieren.

> **Hinweis:**
>
> Sie können die Funktion Dynamic Memory Control (DMC) nicht auf Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 oder CentOS Stream 9 VMs verwenden,

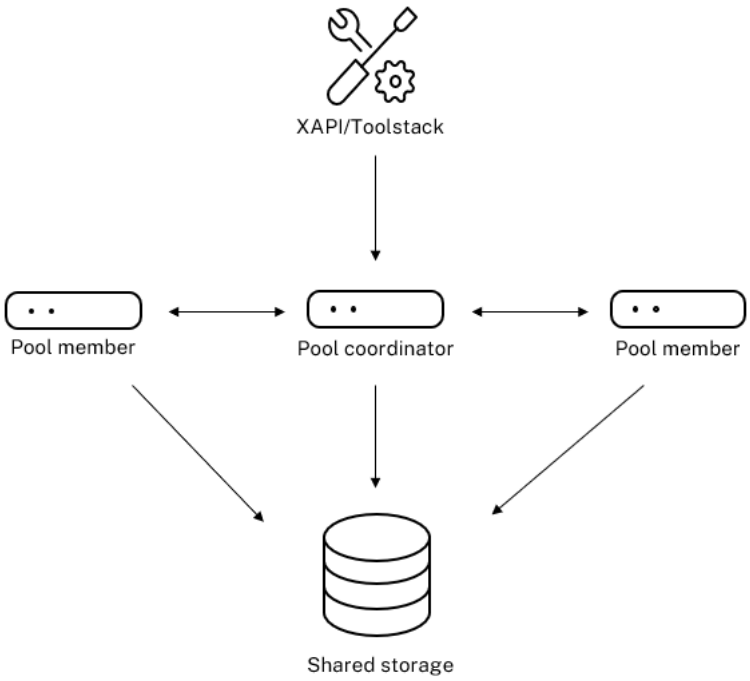
> da diese Betriebssysteme kein Memory Ballooning mit dem Xen-Hypervisor unterstützen.

Weitere Informationen finden Sie unter XenServer VM Tools.

Die wichtigsten Konzepte

Ressourcen-Pool

Mit XenServer können Sie mehrere Hosts und deren verbundenen gemeinsamen Speicher mithilfe von Ressourcenpools als eine Einheit verwalten. Mit Ressourcenpools können Sie virtuelle Maschinen auf verschiedenen XenServer-Hosts verschieben und ausführen. Sie ermöglichen es allen Hosts auch, ein gemeinsames Framework für Netzwerk und Speicher gemeinsam zu nutzen. Ein Pool kann bis zu 64 Hosts enthalten, auf denen dieselbe Version der XenServer-Software auf derselben Patch-Ebene und mit weitgehend kompatibler Hardware ausgeführt wird. Weitere Informationen finden Sie unter Hosts und Ressourcenpools.



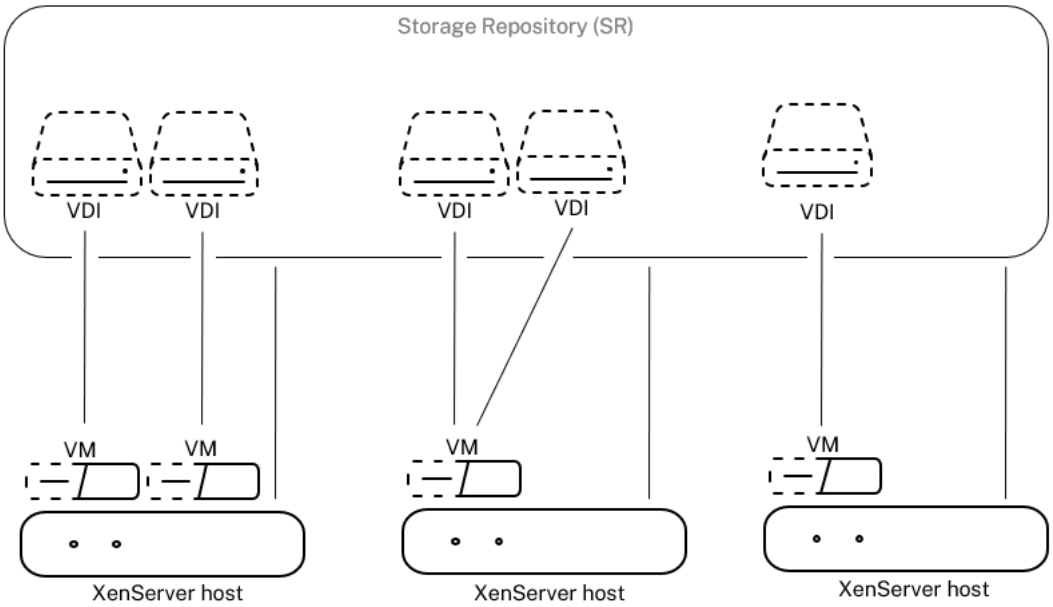
Resource pool overview

Der XenServer-Ressourcenpool verwendet eine primäre/sekundäre Architektur, die von XAPI implementiert wird. XAPI-Aufrufe werden vom Poolkoordinator (dem primären) an die Poolmitglieder (die sekundären) weitergeleitet. Poolmitglieder erstellen DB-RPCs gegen den Poolkoordinator. Der Poolkoordinator ist für die Koordination und Sperrung der Ressourcen innerhalb des Pools verantwortlich und verarbeitet alle Kontrollvorgänge. Poolmitglieder kommunizieren über HTTP

und XMLRPC mit dem Poolkoordinator, aber sie können über Spiegelplatten (Speichermigration) miteinander kommunizieren (über denselben Kanal)

Speicherrepository

XenServer-Speicherziele werden als Speicherrepositorien (SRs) bezeichnet. In einem Speicherrepository werden Virtual Disk Images (VDIs) gespeichert, die den Inhalt einer virtuellen Datenträger enthalten.
SRs sind flexibel, mit integrierter Unterstützung für SATA-, SCSI-, NVMe- und SAS-Laufwerke, die lokal verbunden sind, und iSCSI, NFS, SAS, SMB und Fibre Channel remote verbunden. Die SR- und VDI-Abstraktionen ermöglichen die Bereitstellung erweiterter Speicherfunktionen wie Thin Provisioning, VDI-Snapshots und schnelles Klonen auf Speicherzielen, die sie unterstützen.



Storage overview

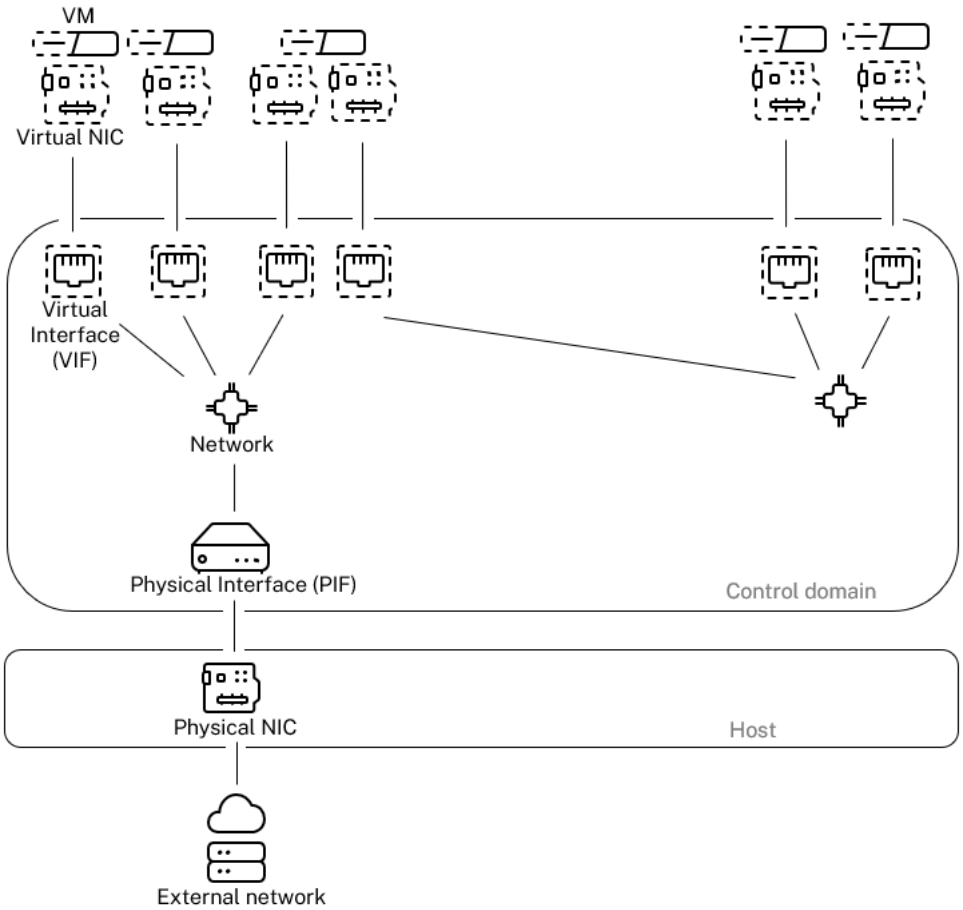
Jeder XenServer-Host kann mehrere SRs und verschiedene SR-Typen gleichzeitig verwenden. Diese SRs können zwischen Hosts geteilt oder für bestimmte Hosts reserviert werden. Gemeinsam genutzter Speicher wird zwischen mehreren Hosts innerhalb eines definierten Ressourcenpools gepoolt. Ein gemeinsam genutztes SR muss für jeden Host im Pool über das Netzwerk zugänglich sein. Alle Hosts in einem einzigen Ressourcenpool müssen über mindestens ein gemeinsam genutztes SR verfügen. Gemeinsam genutzter Speicher kann nicht von mehreren Pools gemeinsam genutzt werden.

Weitere Informationen zum Betrieb mit SRs finden Sie unter Konfigurieren des Speichers.

Netzwerke

Auf Architekturebene gibt es drei Arten von serverseitigen Softwareobjekten, die Netzwerkeinheiten darstellen. Diese Objekte sind:

- Ein **PIF**, ein Softwareobjekt, das in dom0 verwendet wird und eine physische Netzwerkkarte auf einem Server darstellt. PIF-Objekte haben einen Namen und eine Beschreibung, eine UUID, die Parameter der NIC, die sie repräsentieren, sowie das Netzwerk und den Host, mit dem sie verbunden sind.
- Ein **VIF**, bei dem es sich um ein Softwareobjekt handelt, das in dom0 verwendet wird und eine virtuelle Netzwerkkarte auf einer virtuellen Maschine darstellt. VIF-Objekte haben einen Namen und eine Beschreibung, eine UUID sowie das Netzwerk und die VM, mit der sie verbunden sind.
- Ein **Netzwerk**, bei dem es sich um einen virtuellen Ethernet-Switch auf einem Host handelt, mit dem Netzwerkverkehr auf einem Netzwerkhost weitergeleitet wird. Netzwerkobjekte haben einen Namen und eine Beschreibung, eine UUID und die Sammlung von VIFs und PIFs, die mit ihnen verbunden sind.



Networking overview

XenServer-Verwaltungs-APIs ermöglichen die folgenden Operationen:

- Konfiguration der Netzwerkoptionen
- Kontrolle über die Netzwerkkarte, die für Verwaltungsvorgänge verwendet werden soll
- Erstellen erweiterter Netzwerkfunktionen wie VLANs und NIC-Bindungen

Weitere Informationen zum Verwalten von Netzwerken auf XenServer finden Sie unter Networking.

Zugehörige Add-ons und Anwendungen

Xen Hypervisor arbeitet zwar auf der Kernebene, aber es gibt XenServer-spezifische Add-Ons, die sich auf hypervisor-unabhängige Anwendungen und Dienste beziehen, um das Virtualisierungserlebnis zu vervollständigen.

- **XenCenter**

  Ein Windows GUI-Client für die VM-Verwaltung, der basierend auf der Verwaltungs-API implementiert wurde. XenCenter bietet eine umfangreiche Benutzererfahrung für die Verwaltung mehrerer XenServer-Hosts,
  Ressourcenpools und der gesamten damit verbundenen virtuellen Infrastruktur.

- **Workloadausgleich (WLB)**

  Eine Appliance, die Ihren Pool ausgleicht, indem sie virtuelle Maschinen auf die für ihre Workload bestmöglichen Hosts in einem Ressourcenpool verlagert. Weitere Informationen finden Sie unter Workload Balancing (/en-us/xenserver/8/wlb.html).

- **Citrix Lizenzserver**

  Ein Linux-basiertes Gerät, das XenCenter kontaktiert, um eine Lizenz für den angegebenen Server anzufordern.

- **XenServer Conversion Manager**

  Eine virtuelle Appliance, mit der Benutzer vorhandene virtuelle VMware-Maschinen in virtuelle XenServer-Maschinen mit vergleichbarer Netzwerk- und Speicherkonnektivität konvertieren können. Weitere Informationen finden Sie unter Konvertierungsmanager.

- **Citrix Provisioning**

  Provisioning Services, die den PXE-Start von gängigen Images unterstützen. Wird häufig mit Citrix Virtual Desktops und Citrix Virtual Apps verwendet. Weitere Informationen finden Sie unter Provisioning.

- **Citrix Virtual Desktops**

  Ein Virtual Desktop Infrastructure (VDI) -Produkt, das auf Windows-Desktops spezialisiert ist. Citrix Virtual Desktops verwendet XAPI, um XenServer in einer Poolkonfiguration mit mehreren Hosts zu verwalten. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops.

layout: doc
description: Answers to frequently asked questions about XenServer.—

Häufig gestellte technische Fragen

Hardware

Was sind die Mindestsystemanforderungen für die Ausführung von XenServer?

Die Mindestsystemanforderungen für diese Version finden Sie unter Systemanforderungen.

Benötige ich ein System mit einem 64-Bit-x86-Prozessor, um XenServer auszuführen?

Ja. Für die Ausführung aller unterstützten Gastbetriebssystemeist entweder ein Intel VT- oder AMD-V 64-Bit-x86-basiertes System mit einer oder mehreren CPUs erforderlich.

Weitere Informationen zu den Anforderungen des Hostsystems finden Sie unter Systemanforderungen.

Benötige ich ein System mit Unterstützung der Hardwarevirtualisierung?

Sie benötigen ein System mit 64-Bit-x86-Prozessoren, das entweder die Intel VT- oder AMD-V-Hardwarevirtualisierungstechnologie im Prozessor und in der Systemfirmware unterstützt.

Welche Systeme sind für die Ausführung von XenServer zertifiziert?

Eine vollständige Liste der XenServer-zertifizierten Systeme finden Sie in der Hardwarekompatibilitätsliste (HCL).

Unterstützt XenServer AMD Rapid Virtualization Indexing und Intel Extended Page Tables?

Ja. XenServer unterstützt AMD Rapid Virtualization Indexing und Intel Extended Page Tables. Rapid Virtualization Indexing bietet eine Implementierung der Technologie für verschachtelte Tabellen, mit der die Leistung des Xen-Hypervisors weiter verbessert wird. Erweiterte Seitentabellen bieten eine Implementierung von hardwareunterstütztem Paging, mit dem die Leistung des Xen-Hypervisors weiter verbessert wird.

Kann XenServer auf einem Notebook oder Desktop-Systemen ausgeführt werden?

XenServer läuft auf vielen Notebook- oder Desktop-Systemen, die die Mindestanforderungen an die CPU erfüllen. XenServer unterstützt jedoch nur Systeme, die zertifiziert und in der Hardwarekompatibilitätsliste (HCL) aufgeführt wurden.

Sie können zu Demonstrations- und Testzwecken auf nicht unterstützten Systemen arbeiten. Einige Funktionen, wie z. B. Energieverwaltungsfunktionen, funktionieren jedoch nicht.

Kann XenServer auf SD- oder USB-Karten installiert werden?

Nein. XenServer unterstützt die Verwendung von SD-Karten oder USB-Karten für Ihre XenServer-Installation nicht.

Wir unterstützen nur Hardware, die zertifiziert und auf der Hardwarekompatibilitätsliste (HCL) aufgeführt ist.

Grenzwerte für Produkte

> **Hinweis:**
>
> Eine vollständige Liste der von XenServer unterstützten Grenzwerte finden Sie unter Configuration Limits.

Was ist die maximale Speichergröße, die XenServer auf einem Hostsystem verwenden kann?

XenServer-Hostsysteme können bis zu 6 TB physischen Speicher verwenden.

Wie viele Prozessoren kann XenServer verwenden?

XenServer unterstützt bis zu 448 logische Prozessoren pro Host. Die maximale Anzahl unterstützter logischer Prozessoren ist je nach CPU unterschiedlich.

Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste (HCL).

Wie viele virtuelle Maschinen können gleichzeitig auf XenServer ausgeführt werden?

Die maximale Anzahl virtueller Maschinen (VMs), die auf einem XenServer-Host ausgeführt werden können, beträgt 1000. Für Systeme mit mehr als 500 VMs empfehlen wir, dom0 mindestens 16 GB RAM zuzuweisen. Weitere Informationen finden Sie unter Ändern der Speichermenge, die der Steuerdomäne zugewiesenist.

Für jedes bestimmte System hängt die Anzahl der VMs, die gleichzeitig und mit akzeptabler Leistung ausgeführt werden können, von den verfügbaren Ressourcen und der VM-Workload ab. XenServer skaliert automatisch die Speichermenge, die der Steuerdomäne (dom0) zugewiesen ist, basierend auf dem verfügbaren physischen Speicher.

> **Hinweis:**
>
> Wenn mehr als 50 VMs pro Host vorhanden sind und der physische Arbeitsspeicher des Hosts weniger als 48 GB beträgt, ist es möglicherweise ratsam, diese Einstellung zu überschreiben. Weitere Informationen finden Sie unter Speicherauslastung.

Wie viele physische Netzwerkschnittstellen unterstützt XenServer?

XenServer unterstützt bis zu 16 physische NIC-Ports. Diese Netzwerkkarten können verbunden werden, um bis zu 8 logische Netzwerkbindungen zu erstellen. Jede Bindung kann bis zu 4 NICs enthalten.

Wie viele virtuelle Prozessoren (vCPUs) kann XenServer einer VM zuweisen?

XenServer unterstützt bis zu 32 vCPUs pro VM. Die Anzahl der vCPUs, die unterstützt werden können, hängt vom Gastbetriebssystem ab.

> **Hinweis:**
>
> Konsultieren Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten.

Wie viel Speicher kann XenServer einer VM zuweisen?

XenServer unterstützt bis zu 1,5 TB pro Gast. Die Menge an Speicher, die unterstützt werden kann, hängt vom Gastbetriebssystem ab.

> **Hinweis:**
>
> Die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, variiert. Wenn Sie den Speicher auf einen höheren Wert als den vom Betriebssystem unterstützten Grenzwert einstellen, kann dies zu Leistungsproblemen innerhalb Ihres Gastes führen.

Wie viele Virtual Disk Images (VDIs) kann XenServer einer VM zuweisen?

XenServer kann bis zu 255 VDIs einschließlich eines virtuellen DVD-ROM-Geräts pro VM zuweisen.

> **Hinweis:**
>
> Die maximale Anzahl unterstützter VDIs hängt vom Gastbetriebssystem ab. Konsultieren Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten.

Wie viele virtuelle Netzwerkschnittstellen kann XenServer einer VM zuweisen?

XenServer kann bis zu 7 virtuelle NICs pro VM zuweisen. Die Anzahl der virtuellen Netzwerkkarten, die unterstützt werden können, hängt vom Gastbetriebssystem ab.

Teilen von Ressourcen

Wie werden Verarbeitungsressourcen zwischen virtuellen Rechnern aufgeteilt?

XenServer teilt die Verarbeitungsressourcen mithilfe eines Fair-Share-Balancing-Algorithmus zwischen vCPUs auf. Dieser Algorithmus stellt sicher, dass alle VMs ihren Anteil an den Verarbeitungsressourcen des Systems erhalten.

Wie wählt XenServer aus, welche physischen Prozessoren es der VM zuweist?

XenServer weist keiner bestimmten VM statisch physische Prozessoren zu. Stattdessen weist XenServer der VM je nach Last dynamisch alle verfügbaren logischen Prozessoren zu. Diese dynamische Zuweisung stellt sicher, dass die Prozessorzyklen effizient genutzt werden, da die VM überall dort laufen kann, wo freie Kapazität vorhanden ist.

Wie werden Datenträger-E/A-Ressourcen zwischen den VMs aufgeteilt?

XenServer verwendet eine faire Aufteilung der Ressourcen für Datenträger-I/O-Ressourcen zwischen VMs. Sie können einer VM auch Zugriff mit höherer oder niedrigerer Priorität auf Datenträger-E/A-Ressourcen gewähren.

Wie werden Netzwerk-I/O-Ressourcen zwischen den virtuellen Rechnern aufgeteilt?

XenServer verwendet eine faire Aufteilung der Ressourcen für Netzwerk-I/O-Ressourcen zwischen den VMs. Sie können die Rate der ausgehenden Daten auch mit dem Open vSwitch steuern. Weitere Informationen finden Sie unter Rate ausgehender Daten (QoS) steuern.

Gast-Betriebssysteme

Kann XenServer 32-Bit-Betriebssysteme als Gäste ausführen?

Ja. Weitere Informationen finden Sie unter Unterstützte Gastbetriebssysteme.

Kann XenServer 64-Bit-Betriebssysteme als Gäste ausführen?

Ja. Weitere Informationen finden Sie unter Unterstützte Gastbetriebssysteme.

Welche Versionen von Microsoft Windows können als Gäste auf XenServer ausgeführt werden?

Eine Liste der unterstützten Windows-Gastbetriebssysteme finden Sie unter Unterstützte Gastbetriebssysteme.

Welche Versionen von Linux können als Gäste auf XenServer ausgeführt werden?

Eine Liste der unterstützten Linux-Gastbetriebssysteme finden Sie unter Unterstützte Gastbetriebssysteme.

Kann ich verschiedene Versionen der unterstützten Betriebssysteme oder anderer nicht aufgeführter Betriebssysteme ausführen?

Wir unterstützen nur Betriebssysteme (OS) im Rahmen des Betriebssystemanbietersupports. Obwohl nicht unterstützte Betriebssysteme möglicherweise weiterhin funktionieren, bitten wir Sie möglicherweise, ein Upgrade auf ein unterstütztes Betriebssystem-Service Pack durchzuführen, bevor wir Probleme untersuchen können.

Entsprechende Treiber sind möglicherweise nicht für Betriebssystemversionen verfügbar, die nicht unterstützt werden. Ohne die Treiber funktionieren diese Betriebssystemversionen nicht mit optimierter Leistung.

Es ist oft möglich, andere Linux-Distributionen zu installieren. XenServer kann jedoch nur die unter Unterstützte Gastbetriebssysteme aufgeführten Betriebssystemeunterstützen. Möglicherweise bitten wir Sie, zu einem unterstützten Betriebssystem zu wechseln, bevor wir Probleme untersuchen können.

Unterstützt XenServer FreeBSD, NetBSD oder andere BSD-Varianten als Gastbetriebssystem?

XenServer unterstützt keine BSD-basierten Gastbetriebssysteme für allgemeine Virtualisierungsbereitstellungen. FreeBSD-VMs, die auf XenServer laufen, wurden jedoch für die Verwendung in bestimmten NetScaler-Produkten zertifiziert.

Was sind die XenServer VM Tools?

Die XenServer VM Tools sind Softwarepakete für Windows- und Linux-Gastbetriebssysteme. Für Windows-Betriebssysteme enthalten die XenServer VM Tools für Windows Hochleistungs-I/O-Treiber (PV-Treiber) und den Management Agent.

Für Linux-Betriebssysteme enthalten die XenServer VM Tools für Linux einen Gast-Agent, der dem XenServer-Host zusätzliche Informationen über die VM bereitstellt.

Weitere Informationen finden Sie unter XenServer VM Tools.

Docker

Kann ich Docker-Container auf meinen Linux-VMs ausführen?

Ja. Docker wird auf Linux-VMs unterstützt, die auf XenServer gehostet werden.

Kann ich Docker-Container auf meinen Windows-VMs ausführen?

Nein. Sie können Docker-Container nicht auf einer Windows-VM ausführen, die auf XenServer gehostet wird. Diese Einschränkung liegt daran, dass XenServer keine verschachtelte Virtualisierung für Windows-VMs unterstützt.

Bietet XenServer zusätzliche Funktionen für die Arbeit mit Docker?

Nein.

In früheren Versionen von XenServer und Citrix Hypervisor war ein Container Management-Zusatzpaket verfügbar, mit dem Sie Ihre Docker-Container über XenCenter verwalten konnten. Diese Funktion wurde entfernt.

XenCenter

Weitere Informationen finden Sie unter XenCenter.

Muss ich XenCenter auf einem Windows-Computer ausführen?

Ja. Die XenCenter Verwaltungskonsole läuft auf einem Windows-Betriebssystem. Informationen zu den Systemanforderungen finden Sie unter Systemanforderungen

Wenn Sie Windows nicht ausführen möchten, können Sie Ihre XenServer-Hosts und -Pools mithilfe der Xe-CLI oder mithilfe `xsconsole`einer Systemkonfigurationskonsole verwalten.

Kann ich mich mit meinen Active Directory-Benutzerkonten bei XenCenter anmelden?

Ja. Sie können XenCenter-Anmeldeanfragen einrichten, um Active Directory auf allen Editionen von XenServer zu verwenden.

Weitere Informationen finden Sie unter Benutzer verwalten.

Kann ich den Zugriff auf bestimmte Funktionen in XenCenter auf bestimmte Benutzer beschränken?

Ja. Die Funktion “rollenbasierte Zugriffssteuerung”in Kombination mit der Active Directory Authentifizierung kann den Zugriff für Benutzer in XenCenter einschränken.

Weitere Informationen finden Sie unter Benutzer verwalten.

Kann ich eine einzige XenCenter-Konsole verwenden, um eine Verbindung zu mehreren XenServer-Hosts herzustellen?

Ja. Sie können eine einzige XenCenter-Konsole verwenden, um eine Verbindung zu mehreren XenServer-Hostsystemen herzustellen.

Kann ich XenCenter verwenden, um eine Verbindung zu mehreren Hosts herzustellen, auf denen unterschiedliche Versionen von XenServer ausgeführt werden?

Abhängig von der Version von XenServer - ja. XenCenter ist abwärtskompatibel mit Citrix Hypervisor 8.0 und späteren Versionen. Beachten Sie jedoch, dass nur Citrix Hypervisor 8.2 CU 1 volle Unterstützung erhält.

Kann ich XenCenter verwenden, um eine Verbindung zu mehreren Ressourcenpools herzustellen?

Ja. Sie können über eine einzige XenCenter Konsole eine Verbindung zu mehreren Ressourcenpools herstellen.

Wie erhalte ich Zugriff auf die Konsole einer Linux-VM?

Die Registerkarte "**Konsole** "in XenCenter bietet Zugriff auf die textbasierten und grafischen Konsolen von VMs, auf denen Linux-Betriebssysteme ausgeführt werden. Bevor Sie eine Verbindung mit der grafischen Konsole einer Linux-VM herstellen können, müssen Sie einen VNC-Server und einen X-Display-Manager auf der VM installieren und konfigurieren.

XenCenter ermöglicht es Ihnen auch, über SSH eine Verbindung zu Linux-VMs herzustellen, indem **Sie die Option SSH-Konsole öffnen** auf der Registerkarte **Konsole** der VM verwenden.

Wie erhalte ich Zugriff auf die Konsole einer Windows VM?

XenCenter bietet Zugriff auf die emulierte Grafik für eine Windows-VM. Wenn XenCenter Remotedesktopfunktionen auf der VM erkennt, bietet XenCenter eine Schnellverbindungsschaltfläche zum Starten eines integrierten RDP-Clients, der eine Verbindung zur VM herstellt. Oder Sie können sich direkt mit Ihren Gästen verbinden, indem Sie eine externe Remotedesktop-Software verwenden.

Befehlszeilenschnittstelle (CLI)

Weitere Informationen finden Sie unter Befehlszeilenschnittstelle.

Beinhaltet XenServer eine CLI?

Ja. Alle Editionen von XenServer enthalten eine vollständige Befehlszeilenschnittstelle (CLI) — bekannt als `xe`.

Kann ich direkt auf dem Host auf die Xe-CLI zugreifen?

Ja. Sie können auf die CLI zugreifen, indem Sie einen Bildschirm und eine Tastatur direkt an den Host oder über einen Terminalemulator anschließen, der an die serielle Port des Hosts angeschlossen ist.

Kann ich von einem Remote-System aus auf die Xe-CLI zugreifen?

Ja. XenServer liefert die Xe-CLI, die auf Windows- und 64-Bit-Linux-Computern installiert werden kann, um XenServer remote zu steuern. Sie können XenCenter auch verwenden, um über die Registerkarte Konsole auf die Konsole des Hosts zuzugreifen.

Kann ich die Xe-CLI mit meinen Active Directory-Benutzerkonten verwenden?

Ja. Sie können sich mit Active Directory auf allen Editionen von XenServer anmelden.

Kann ich den Zugriff bestimmter CLI-Befehle auf bestimmte Benutzer beschränken?

Ja. Sie können den Benutzerzugriff auf der Xe-CLI einschränken.

VMs

Weitere Informationen finden Sie unter Verwalten virtueller Maschinen.

Können mit VMware oder Hyper-V erstellte VMs auf XenServer ausgeführt werden?

Ja. Sie können VMs mithilfe des OVF-Formats nach Industriestandard exportieren und importieren.

Mit dem XenServer Conversion Manager können Sie VMs auch stapelweise konvertieren. Tools von Drittanbietern sind ebenfalls verfügbar.

Weitere Informationen finden Sie unter Conversion Manager.

Mit welchen Installationsmedien kann ich ein Gastbetriebssystem installieren?

Sie können ein Gastbetriebssystem mithilfe von:

- Eine CD im CD-ROM-Laufwerk des Hosts
- Ein virtuelles CD-ROM-Laufwerk mit Technologie wie DRAC
- Platzieren von ISO-Images auf einem freigegebenen Netzlaufwerk
- Netzwerkinstallation, sofern vom jeweiligen Gast unterstützt.

Weitere Informationen finden Sie unter Verwalten virtueller Maschinen.

Kann ich einen Klon einer vorhandenen VM erstellen?

Ja. Jede auf XenServer erstellte VM kann geklont oder in eine VM-Vorlage konvertiert werden. Eine VM-Vorlage kann dann verwendet werden, um weitere virtuelle Maschinen zu erstellen.

Können VMs aus einer Version von XenServer exportiert und in eine andere verschoben werden?

Ja. Aus älteren Versionen von XenServer exportierte VMs können in eine neuere Version importiert werden.

Kann ich eine VM von der Open-Source-Version von Xen zu XenServer konvertieren?

Nein.

Bietet XenServer Datenträger-Snapshot-Funktionen für VMs?

Ja. XenServer unterstützt die Verwendung von Snapshots in allen Editionen. Weitere Informationen finden Sie unter VM-Snapshots.

Speicher

Weitere Informationen finden Sie unter Speicher.

Welche Arten von lokalem Speicher können mit XenServer verwendet werden?

XenServer unterstützt lokalen Speicher wie SATA, SAS und NVMe.

Welche Art von SAN/NAS-Speicher kann mit XenServer verwendet werden?

XenServer unterstützt Fibre Channel-, FCoE-, hardwarebasierte iSCSI (HBA) -, iSCSI-, NFS- und SMB-Speicherrepositorien.

Weitere Informationen finden Sie unter Speicher und Hardwarekompatibilitätsliste.

Unterstützt XenServer softwarebasiertes iSCSI?

Ja. XenServer enthält einen integrierten softwarebasierten iSCSI-Initiator (Open-iSCSI).

Welche Version von NFS ist für die Verwendung von Remote-Speicher erforderlich?

XenServer benötigt NFSv3 oder NFSv4 über TCP für die Verwendung im Remotespeicher. XenServer unterstützt derzeit kein NFS over User Datagram Protocol (UDP).

Kann ich softwarebasiertes NFS, das auf einem Allzweckserver ausgeführt wird, für gemeinsam genutzten Remote-Speicher verwenden?

Ja. Wir empfehlen jedoch, ein dediziertes NAS-Gerät mit NFSv3 oder NFSv4 mit nichtflüchtigem Hochgeschwindigkeits-Caching zu verwenden, um ein akzeptables I/O-Leistungsniveau zu erreichen.

Kann ich ein XenServer-Hostsystem von einem iSCSI-, Fibre Channel- oder FCoE-SAN starten?

Ja. XenServer unterstützt das Starten vom SAN mithilfe von Fibre Channel-, FCoE- oder iSCSI-HBAs.

Kann ich einen XenServer-Host von UEFI aus booten?

Ja. XenServer unterstützt das Booten von UEFI. UEFI Secure Boot wird jedoch für XenServer-Hosts nicht unterstützt.

Das Booten vom BIOS aus wird derzeit unterstützt, ist aber veraltet und wird in einer zukünftigen Version entfernt.

Weitere Informationen finden Sie unter Netzwerk-Boot-Installationen

Unterstützt XenServer Multipath I/O (MPIO) für Speicherverbindungen?

Ja. Wir empfehlen die Verwendung von Multipath für ausfallsichere Speicherverbindungen.

Unterstützt XenServer eine softwarebasierte RAID-Implementierung?

Nein. XenServer unterstützt kein Software-RAID.

Unterstützt XenServer HostRAID- oder FakeRAID-Lösungen?

Nein. XenServer unterstützt keine proprietären RAID-ähnlichen Lösungen wie HostRAID oder FakeRAID.

Unterstützt XenServer Thin Cloning vorhandener VMs?

Ja. Thin Cloning ist auf lokalen Datenträger verfügbar, die als EXT3/EXT4 formatiert sind, zusätzlich zu NFS- und SMB-Speicherrepositorys.

Unterstützt XenServer DRBD-Speicher (Distributed Replicated Block Device)?

Nein. XenServer unterstützt DRBD nicht.

Unterstützt XenServer ATA über Ethernet?

Nein. XenServer unterstützt keinen ATA-über-Ethernet-basierten Speicher.

Netzwerke

Weitere Informationen finden Sie unter Networking

Kann ich private Netzwerke erstellen, die Gruppen von virtuellen Rechnern isolieren?

Ja. Sie können ein privates Netzwerk auf einem einzigen Host für residenten VMs erstellen.

Unterstützt XenServer mehrere physische Netzwerkverbindungen?

Ja. Sie können eine Verbindung zu mehreren physikalischen Netzwerken herstellen oder diese zuordnen, die an verschiedene Netzwerkschnittstellen auf dem physischen Hostsystem angeschlossen werden.

Können virtuelle Maschinen eine Verbindung zu mehreren Netzwerken herstellen?

Ja. Virtuelle Rechner können sich mit jedem Netzwerk verbinden, das für den Host verfügbar ist.

Unterstützt XenServer IPv6?

Auf XenServer gehostete VMs können eine beliebige Kombination von konfigurierten IPv4- und IPv6-Adressen verwenden.

XenServer unterstützt jedoch nicht die Verwendung von IPv6 in seiner Steuerdomäne (dom0). Sie können IPv6 nicht für das Host-Verwaltungsnetzwerk oder das Speichernetzwerk verwenden. IPv4 muss verfügbar sein, damit der XenServer-Host es verwenden kann.

Unterstützt XenServer VLANs auf einer physischen Netzwerkschnittstelle?

Ja. XenServer unterstützt die Zuweisung von VM-Netzwerken zu bestimmten VLANs.

Übergeben virtuelle XenServer-Netzwerke den gesamten Netzwerkverkehr an alle VMs?

Standardmäßig sind XenServer-Netzwerkschnittstellen nicht promiskuitiv und eine VM kann nur den Datenverkehr für diese VM sehen und den Datenverkehr senden.

Dieses Verhalten kann je nach verwendetem Netzwerkstapel konfiguriert werden.

- Wenn Sie die Linux-Brücke als Netzwerkstapel verwenden, können Ihre virtuellen Netzwerkschnittstellen für den promiskuitiven Modus konfiguriert werden. In diesem Modus können Sie den gesamten Datenverkehr auf einem virtuellen Switch anzeigen. Weitere Informationen zur Konfiguration des promiskuitiven Modus finden Sie in den folgenden Knowledge Center-Artikeln:

  - CTX116493 - So aktivieren Sie den Promiscuous-Modus auf einer physischen Netzwerkkarte
  - CTX121729 —Konfigurieren einer promiscuous virtuellen Maschine in XenServer

  Wenn Sie den Promiscuous-Modus auf einer virtuellen Netzwerkschnittstelle aktivieren, müssen Sie auch den Promiscuous-Modus innerhalb Ihrer VM aktivieren, damit eine VM diese Konfiguration nutzen kann.

- Wenn Sie den Open vSwitch (OVS) als Ihren Netzwerk-Stack verwenden, fungiert er als Layer-2-Switch. Eine VM sieht nur Datenverkehr für diese VM. Außerdem ermöglicht die Switch-Port-Sperre in XenServer ein höheres Maß an Isolation und Sicherheit. OVS kann nicht im Promiscuous-Modus konfiguriert werden.

Unterstützt XenServer die Bündelung oder das Teaming von physischen Netzwerkschnittstellen?

Ja. XenServer unterstützt die Bündelung physischer Netzwerkschnittstellen für Failover und Link-Aggregation mit optionaler LACP-Unterstützung. Weitere Informationen finden Sie unter Netzwerk.

Speicher

Wie viel Speicher wird beim Ausführen von XenServer verbraucht?

Drei Komponenten tragen zum Speicherbedarf eines XenServer-Hosts bei.

1. Der Xen-Hypervisor
2. Die Steuerdomäne auf dem Host (dom0)
3. Der XenServer Crash Kernel

Die zum Ausführen von dom0 erforderliche Speichermenge wird automatisch angepasst. Standardmäßig weist XenServer der Steuerdomäne 1 GiB plus 5% des gesamten physischen Speichers zu, bis zu einem anfänglichen Maximum von 8 GiB.

> **Hinweis:**

> Die Menge an Speicher, die der Steuerdomäne zugewiesen ist, kann über den Standardbetrag hinaus erhöht werden.

In XenCenter gibt das **Xen-Feld** auf der Registerkarte **Speicher den Speicher** an, der von der Control Domain, vom Xen-Hypervisor selbst und vom XenServer Crash Kernel verwendet wird. Der vom Hypervisor verwendete Arbeitsspeicher ist für Hosts mit mehr Arbeitsspeicher größer.

Weitere Informationen finden Sie unter Speicherauslastung

Optimiert XenServer die VM-Speichernutzung?

Ja. XenServer verwendet Dynamic Memory Control (DMC), um den Speicher laufender VMs automatisch anzupassen. Durch diese Anpassungen wird die Menge des jeder VM zugewiesenen Speichers zwischen den angegebenen minimalen und maximalen Speicherwerten gehalten, wodurch die Leistung garantiert und eine höhere VM-Dichte ermöglicht wird.

Weitere Informationen finden Sie unter VM-Speicher.

Ressourcen-Pools

Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

Was ist ein Ressourcenpool?

Ein Ressourcenpool besteht aus einer Reihe von XenServer-Hosts, die als Einheit verwaltet werden. In der Regel teilt sich ein Ressourcenpool eine gewisse Menge an Netzwerkspeicher, damit VMs innerhalb des Pools schnell von einem Host zum anderen migriert werden können.

Benötigt XenServer einen dedizierten Host, um einen Ressourcenpool zu verwalten?

Nein. Ein einzelner Host im Pool muss als Poolkoordinator angegeben werden. Der Poolkoordinator kontrolliert alle für den Pool erforderlichen administrativen Aktivitäten. Diese Konstruktion bedeutet, dass es keinen externen Single Point of Failure gibt. Wenn der Poolkoordinator ausfällt, werden andere Hosts im Pool weiter ausgeführt, und die residenten VMs werden weiterhin wie gewohnt ausgeführt. Wenn der Poolkoordinator nicht wieder online gehen kann, befördert XenServer einen der anderen Hosts im Pool zum Koordinator, um die Kontrolle über den Pool wiederzuerlangen.

Dieser Prozess wird mit der Funktion “Hochverfügbarkeit”automatisiert. Weitere Informationen finden Sie unter Hochverfügbarkeit.

Wo werden die Konfigurationsdaten für einen Ressourcenpool gespeichert?

Eine Kopie der Konfigurationsdaten wird auf jedem Host im Ressourcenpool gespeichert. Wenn der aktuelle Poolkoordinator ausfällt, ermöglichen diese Daten jedem Host im Ressourcenpool, der neue Poolkoordinator zu werden.

Welche Arten von Konfigurationen können auf der Ebene des Ressourcenpools vorgenommen werden?

Gemeinsam genutzte Remote-Speicher- und Netzwerkkonfigurationen können auf der Ebene des Ressourcenpools vorgenommen werden. Wenn eine Konfiguration im Ressourcenpool gemeinsam genutzt wird, leitet das Koordinatorsystem die Konfigurationsänderungen automatisch an alle Mitgliedssysteme weiter.

Werden neue Hostsysteme zu einem Ressourcenpool hinzugefügt und automatisch mit gemeinsamen Einstellungen konfiguriert?

Ja. Alle neuen Hostsysteme, die zu einem Ressourcenpool hinzugefügt werden, erhalten automatisch dieselben Konfigurationen für gemeinsam genutzten Speicher und Netzwerkeinstellungen.

Kann ich verschiedene CPU-Typen im selben XenServer-Ressourcenpool verwenden?

Ja. Wir empfehlen, dass im gesamten Pool derselbe CPU-Typ verwendet wird (homogener Ressourcenpool). Hosts mit unterschiedlichen CPU-Typen können jedoch einem Pool beitreten (heterogen), vorausgesetzt, die CPUs stammen vom selben Anbieter.

Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

Aktuelle Informationen zur Unterstützung der Feature-Maskierung für bestimmte CPU-Typen finden Sie unter Hardwarekompatibilitätsliste.

Livemigration (früher XenMotion)

Weitere Informationen finden Sie unter Migrieren von virtuellen Rechnern.

Kann ich eine laufende VM von einem Host zum anderen verschieben?

Mit der Livemigration können Sie laufende VMs verschieben, wenn Hosts Speicher gemeinsam nutzen (in einem Pool).

Außerdem ermöglicht die Speicher-Livemigration die Migration zwischen Hosts, die keinen Speicher gemeinsam nutzen. Virtuelle Rechner können innerhalb oder über Pools hinweg migriert werden.

Hohe Verfügbarkeit

Weitere Informationen finden Sie unter Hochverfügbarkeit.

Bietet XenServer Hochverfügbarkeitsfunktionen?

Ja. Wenn Hochverfügbarkeit aktiviert ist, überwacht XenServer kontinuierlich den Zustand der Hosts in einem Pool. Wenn Hochverfügbarkeit feststellt, dass ein Host beeinträchtigt ist, wird der Host automatisch heruntergefahren. Mit dieser Aktion können VMs sicher auf einem alternativen fehlerfreien Host neu gestartet werden.

Unterstützt XenServer High Availability lokalen Speicher?

Nein. Wenn Sie Hochverfügbarkeit verwenden möchten, ist gemeinsam genutzter Speicher erforderlich. Mit diesem gemeinsam genutzten Speicher können VMs bei einem Ausfall eines Hosts verlegt werden. Durch die hohe Verfügbarkeit können jedoch VMs, die im lokalen Speicher gespeichert sind, für einen automatischen Neustart gekennzeichnet werden, wenn sich der Host nach einem Neustart erholt.

Kann ich Hochverfügbarkeit verwenden, um den Neustart wiederhergestellter VMs automatisch zu sequenzieren?

Ja. Mit der Konfiguration mit hoher Verfügbarkeit können Sie die Reihenfolge festlegen, in der VMs gestartet werden. Mit dieser Funktion können virtuelle Maschinen, die voneinander abhängig sind, automatisch sequenziert werden.

Leistungskennzahlen

Sammeln die XenServer-Verwaltungstools Leistungsinformationen?

Ja. XenServer bietet eine detaillierte Überwachung der Leistungsmetriken. Zu diesen Metriken gehören CPU-, Arbeitsspeicher-, Datenträger-, Netzwerk-, C-State/P-State-Informationen und Speicher. Gegebenenfalls sind diese Metriken pro Host und pro VM verfügbar. Leistungsmetriken sind direkt verfügbar (als Round-Robin-Datenbanken verfügbar) oder können in XenCenter oder anderen Anwendungen von Drittanbietern abgerufen und grafisch angezeigt werden. Weitere Informationen finden Sie unter Überwachen und Verwalten Ihrer Bereitstellung.

Wie werden XenServer-Leistungsmetriken erfasst?

Daten für die XenServer-Leistungsmetriken werden aus verschiedenen Quellen gesammelt. Zu diesen Quellen gehören der Xen-Hypervisor, Dom0, Standard-Linux-Schnittstellen und Standard-Windows-Schnittstellen wie WMI.

Zeigt XenCenter Leistungsmetriken in Echtzeit an?

Ja. XenCenter zeigt Leistungsmetriken in Echtzeit auf der Registerkarte **Leistung** für jede laufende VM und für den XenServer-Host an. Sie können die angezeigten Metriken anpassen.

Speichert XenCenter historische Leistungsmetriken und zeigt sie an?

Ja. XenServer behält die Leistungsmetriken des letzten Jahres bei (mit abnehmender Granularität). XenCenter bietet eine Visualisierung dieser Metriken in grafischen Echtzeitanzeigen.

Installation

Weitere Informationen finden Sie unter Installation.

Wird XenServer auf Systemen installiert, auf denen bereits ein vorhandenes Betriebssystem ausgeführt wird?

Nein. XenServer wird direkt auf Bare-Metal-Hardware installiert, wodurch die Komplexität, der Overhead und die Leistungsengpässe eines zugrunde liegenden Betriebssystems vermieden werden.

Kann ich eine bestehende XenServer-Installation auf eine neuere Version aktualisieren?

Ja. Wenn Sie eine unterstützte Version von XenServer ausführen, können Sie auf eine neuere Version von XenServer aktualisieren, anstatt eine Neuinstallation durchzuführen. Weitere Informationen finden Sie unter Upgrade.

Kann ich von einer Version von Citrix Hypervisor oder XenServer, die nicht mehr unterstützt wird, auf diese Version aktualisieren?

Wenn Ihre vorhandene Version von Citrix Hypervisor oder XenServer nicht mehr unterstützt wird, können Sie kein Upgrade oder Update auf die neueste Version von XenServer durchführen. Nur Upgrades von Citrix Hypervisor 8.2 Cumulative Update 1 werden unterstützt.

Weitere Informationen finden Sie unter Upgrade.

Wie viel lokalen Speicher benötigt XenServer für die Installation auf dem physischen Hostsystem?

XenServer benötigt mindestens 46 GB lokalen Speicher auf dem physischen Hostsystem.

Kann ich mit PXE eine Netzwerkinstallation von XenServer auf dem Hostsystem durchführen?

Ja. Sie können XenServer mithilfe von PXE auf dem Hostsystem installieren. Sie können XenServer auch automatisch mithilfe von PXE installieren, indem Sie eine vorkonfigurierte Antwortdatei erstellen.

Läuft der Xen-Hypervisor auf Linux?

Nein. Xen ist ein Typ-1-Hypervisor, der direkt auf der Host-Hardware ("Bare Metal") ausgeführt wird. Nachdem der Hypervisor geladen wurde, startet er die privilegierte Verwaltungsdomäne —die Steuerdomäne (dom0), die eine minimale Linux-Umgebung enthält.

Woher bezieht XenServer seine Gerätetreiberunterstützung?

XenServer verwendet die Gerätetreiber, die im Linux-Kernel verfügbar sind. Daher läuft XenServer auf einer Vielzahl von Hardware- und Speichergeräten. Wir empfehlen jedoch, zertifizierte Gerätetreiber zu verwenden.

Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste.

Lizenzierung

Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung.

Technischer Support

Weitere Informationen zum Support finden Sie unter Support.

Bietet XenServer direkten technischen Support für XenServer?

Ja. Weitere Informationen finden Sie auf den XenServer-Supportseiten.

Muss ich gleichzeitig mit dem Kauf von XenServer einen Vertrag für technischen Support für XenServer abschließen?

Nein. Ein Vertrag über technischen Support ist in Ihrem Lizenzkauf enthalten. Informationen zum Umfang des Supports, den wir für Premium- und Standard Edition-Kunden anbieten, finden Sie auf den XenServer-Supportseiten.

Zu welchem Support-Level berechtigt mich meine Lizenz?

Wenn Sie eine XenServer-Lizenz pro Socket erwerben, profitieren Sie auch von unseren technischen Support-Services. Weitere Informationen zu den Unterstützungsstufen finden Sie unter https://xenserver.com/support.

Kann ich Support erhalten, wenn meine Hosts in der Trial Edition laufen?

Wenn Sie ein Benutzer der Trial Edition sind, haben Sie keinen Anspruch auf Support. Wir schätzen jedoch Ihr Feedback: Feedback geben.

Gibt es alternative Kanäle, um Unterstützung für XenServer zu erhalten?

Ja. Es gibt mehrere alternative Kanäle, um technischen Support für XenServer zu erhalten. Sie können auch das Citrix Knowledge Center verwenden oder einen Vertrag mit autorisierten XenServer-Partnern abschließen, die technische Supportdienste anbieten.

Bietet XenServer technischen Support für das Open-Source-Xen-Projekt?

Nein. XenServer bietet keinen technischen Support für das Open-Source-Xen-Projekt. Weitere Informationen finden Sie auf http://www.xen.org/.

Kann ich einen technischen Support-Vorfall mit XenServer eröffnen, wenn ich ein nichttechnisches Problem habe?

Nein. Wenden Sie sich bei nichttechnischen Problemen an den Citrix Customer Service. Zum Beispiel Probleme im Zusammenhang mit Softwarewartung, Lizenzierung, administrativem Support und Auftragsbestätigung.

Lizenzierungsübersicht

April 12, 2024

> **Wichtig:**
>
> Wenn Sie XenServer zum Ausführen Ihrer Citrix Virtual Apps and Desktops-Workloads verwenden, benötigen Sie eine Premium Edition-Lizenz. Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy.
> Diese Anforderung ist eine Verhaltensänderung seit der vorherigen Version von Citrix Hypervisor/XenServer. Weitere Informationen finden Sie in den häufig gestellten Fragen zur Lizenzierung.
>
> Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

XenServer 8 ist in den folgenden Editionen verfügbar:

- Die**Premium Edition** ist unser Premium-Angebot, das für Desktop-, Server- und Cloud-Workloads optimiert ist. Zusätzlich zu den in der Standard Edition verfügbaren Funktionen bietet die Premium Edition folgende Funktionen:
  - Dynamischer Workloadausgleich
  - GPU-Virtualisierung mit NVIDIA vGPU und Intel GvT-G
  - Thin Provisioning für gemeinsam genutzte Blockspeichergeräte
  - Unterstützung für SMB-Speicher
  - Direkte Inspektion von APIs
  - Exportieren von Pool-Ressourcendaten
  - Lese-Zwischenspeicherung im Speicher
  - PVS-Accelerator
  - Aktivierung für Citrix Virtual Desktops im Tabletmodus
  - Geänderte Blockverfolgung
  - IGMP-Snooping
  - USB-Durchgang
  - SR-IOV-Netzwerkunterstützung
  - Überwachen Sie Host- und Dom0-Ressourcen mit NRPE
  - Überwachen Sie Host- und Dom0-Ressourcen mit SNMP
- **Die Standard Edition** ist unser kommerzielles Einstiegsangebot. Es bietet eine Reihe von Funktionen für Kunden, die eine robuste und leistungsstarke Virtualisierungsplattform wünschen, aber nicht die Premium-Funktionen der Premium Edition benötigen. In der Zwischenzeit möchten sie weiterhin von der Gewissheit eines umfassenden Supports und einer

umfassenden Wartung profitieren.

- Die **Trial Edition** bietet derzeit unseren Premium Edition-Funktionsumfang für einen Pool mit begrenzter Größe (maximal drei Hosts), ermöglicht jedoch kein Rolling-Pool-Upgrade über XenCenter.

Weitere Informationen finden Sie unter https://www.xenserver.com/editions.

	Premium Edition	Standard Edition	Test-Ausgabe
Premium-Funktionsumfang	Ja		Ja
Rolling-Pool-Upgrade über XenCenter	Ja	Ja	
Kontinuierliche Funktions- und Sicherheitsupdates	Ja	Ja	Ja
Maximale Poolgröße	64 (16 mit GFS2 SRs)	64 (16 mit GFS2 SRs)	3

XenServer wird *pro Socket* lizenziert. Die Zuteilung von Lizenzen wird zentral verwaltet und von einem eigenständigen Citrix Lizenzserver (physisch oder virtuell) in der Umgebung durchgesetzt. Weitere Informationen zur XenServer-Lizenzierung finden Sie in den häufig gestellten Fragen zur Lizenzierung.

Lizenzierung Ihrer Hosts und Pools

XenServer verwendet den gleichen Lizenzierungsprozess wie einige Citrix-Produkte. Um XenServer Premium Edition oder XenServer Standard Edition verwenden zu können, benötigen Sie eine gültige Lizenz, die auf einem Citrix Lizenzserver installiert und Ihrem XenServer-Host zugewiesen ist. Dieser Vorgang wird im Lizenzierungsleitfaden für XenServerausführlich behandelt.

> **Hinweis:**
>
> XenServer unterstützt derzeit keine Lizenzierung, die auf Citrix Cloud gehostet wird. Ein on-premises Citrix Lizenzserver ist erforderlich.

Um Ihre Hosts zu lizenzieren, benötigen Sie die folgenden Elemente:

- Eine Lizenz
- Ein Citrix Lizenzserver
- Ein XenServer-Host
- XenCenter

1. Installieren Sie den Citrix Lizenzserver

Sie können den Citrix Lizenzserver für Windows von der Downloadseite für die Citrix Lizenzierung herunterladen.

Installieren Sie den Citrix Lizenzserver auf einem Windows-System gemäß den Anweisungen in der Dokumentation zur Citrix Lizenzierung.

Das Windows-System, auf dem Sie Ihren Citrix Lizenzserver installieren, kann eine Windows-VM sein, die in Ihrem XenServer-Pool gehostet wird.

XenServer arbeitet mit einer Grace-Lizenz, bis der Lizenzserver booten kann. Dieses Verhalten bedeutet, dass, nachdem Sie die XenServer-Hosts in Ihrem Pool lizenziert haben, wenn Sie den Host neu starten, auf dem der Citrix Lizenzserver läuft, eine Kulanzzeit gilt, bis der Lizenzserver neu gestartet wird.

2. Lizenzdateien herunterladen

Laden Sie eine Lizenzdatei herunter, die mit dem Hostnamen Ihres Citrix Lizenzservers unter Berücksichtigung der Groß- und Kleinschreibung verknüpft ist und eine ausreichend große Anzahl an Pro-Socket-Lizenzen enthält, um sie auf allen Hosts, die Sie lizenzieren möchten, gemeinsam zu nutzen.

Informationen zum Kauf einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy.

Weitere Informationen zum Abrufen Ihrer Lizenzdateien finden Sie in der Produktdokumentation zur Citrix Lizenzierung.

3. Hinzufügen der Lizenzdatei zum Citrix Lizenzserver

Verwenden Sie den Citrix Licensing Manager, um die Lizenzen auf Ihrem Citrix Lizenzserver zu installieren. Weitere Informationen finden Sie in der Produktdokumentation zur Citrix Lizenzierung.

4. Wenden Sie die Lizenzen auf Hosts in Ihrem Ressourcenpool an

Sie können Ihren XenServer-Hosts und -Pools mithilfe von XenCenter oder der Xe-CLI Lizenzen zuweisen, die auf einem Citrix Lizenzserver gehostet werden.

Wenden Sie eine Lizenz auf alle Hosts an, die XenCenter verwenden A: Gehen Sie wie folgt vor, um eine Lizenz anzuwenden:

1. Klicken Sie im Menü **Extras** auf **Lizenzmanager**.

2. Wählen Sie den Pool oder die Hosts aus, die Sie lizenzieren möchten, und klicken Sie dann auf **Lizenz zuweisen**.
3. Geben **Sie im Dialogfeld Lizenz anwenden** den **Editionstyp** an, der dem Host zugewiesen werden soll.
4. Geben Sie den Hostnamen oder die IP-Adresse des Citrix Lizenzservers ein.
5. Klicken Sie auf **OK**.

Wenden Sie mithilfe der Xe-CLI eine Lizenz auf Hosts oder Pools an Um eine Lizenz auf einen einzelnen Host anzuwenden, führen Sie den `host-apply-edition` folgenden Befehl aus:

```
1     xe host-apply-edition edition=premium-per-socket|standard-per-
          socket  \
2
3          license-server-address=<license_server_address> host-uuid=<
              uuid_of_host>  \
4
5          license-server-port=<license_server_port>
6 <!--NeedCopy-->
```

Um eine Lizenz auf alle Hosts in einem Pool anzuwenden, führen Sie den `pool-apply-edition` folgenden Befehl aus:

```
1     xe pool-apply-edition edition=premium-per-socket|standard-per-
          socket  \
2
3          license-server-address=<license_server_address> pool-uuid=<
              uuid_of_pool>  \
4
5          license-server-port=<license_server_port>
6 <!--NeedCopy-->
```

Häufig gestellte Fragen zur Lizenzierung

April 12, 2024

Dieser Artikel enthält häufig gestellte Fragen zur Lizenzierung Ihrer XenServer-Hosts und -Pools.

- Allgemeine Fragen
- Citrix Virtual Apps and Desktops
- Citrix Lizenzserver
- Lizenzierung eines XenServer-Pools
- Weitere Informationen

Allgemeine Fragen

F: Wo kann ich eine XenServer-Lizenz kaufen?

A: Informationen zum Kauf einer XenServer-Lizenz finden Sie unter http://www.xenserver.com/buy.

F: Wie beantrage ich eine XenServer-Lizenz?

A: XenServer benötigt einen Lizenzserver. Nach der Lizenzierung von XenServer erhalten Sie einen .LIC-Lizenzzugriffscode. Installieren Sie diesen Lizenzzugangscode auf Ihrem Citrix Lizenzserver.

Wenn Sie einem XenServer-Host eine Lizenz zuweisen, kontaktiert XenServer den angegebenen Citrix Lizenzserver und fordert eine Lizenz für die angegebenen Hosts an. Bei Erfolg wird eine Lizenz ausgecheckt und der Lizenzmanager zeigt Informationen über die Lizenz an, unter der die Hosts lizenziert sind.

F: Wie viele Lizenzen benötige ich, um meinen Ressourcenpool zu lizenzieren?

A: XenServer wird *pro CPU-Socket* lizenziert. Damit ein Pool als lizenziert gilt, müssen alle XenServer-Hosts im Pool lizenziert sein. XenServer zählt nur bestückte CPU-Sockets.

Sie können den Citrix Lizenzserver verwenden, um die Anzahl der verfügbaren Lizenzen anzuzeigen, die im *Dashboard der License Administration Console*angezeigt werden.

F: Benötige ich eine Pro-Socket-Lizenz für Sockets, die nicht belegt sind?

A: Nein, nur belegte CPU-Sockel werden für die Anzahl der zu lizenzierenden Sockets gezählt.

F: Verliere ich meine virtuelle Maschine (VM), wenn meine Lizenz abläuft?

A: Nein, Sie verlieren keine virtuellen Maschinen oder deren Daten.

F: Was passiert, wenn ich einen lizenzierten Pool habe und der Lizenzserver nicht mehr verfügbar ist?

Antwort: Wenn Ihre Lizenz nicht abgelaufen und der Lizenzserver nicht verfügbar ist, erhalten Sie eine *Übergangsfrist* von 30 Tagen auf der zuvor geltenden Lizenzstufe.

Wenn Ihre Lizenz nach Ablauf der Übergangszeit immer noch nicht verfügbar ist, wird Ihr Pool in einen Test-Edition-Pool umgewandelt und nur die in der Testversion enthaltenen Funktionen sind verfügbar.

Ihr Pool bleibt gleich groß, aber wenn er drei oder mehr Hosts hat, können Sie ihm keine weiteren Hosts hinzufügen.

F: Wie erhalte ich eine Lizenz zur Evaluierung von XenServer?

A: Mit der Trial Edition können Sie XenServer ohne Lizenz installieren und alle Funktionen der Premium Edition in einem Pool mit reduzierter Größe testen. Weitere Informationen finden Sie unter XenServer-Editionen.

F: Kann ich XenServer 8 ohne Lizenz verwenden?

A: Ja. Mit der XenServer 8 Trial Edition ist XenServer ohne Lizenz verfügbar. Die Edition bietet alle Funktionen der Premium Edition in einem reduzierten Pool von bis zu drei Hosts. Weitere Informationen finden Sie unter XenServer-Editionen.

F: Kann ich Citrix Cloud verwenden, um eine Lizenz auf XenServer anzuwenden?

Nein, XenServer unterstützt derzeit keine Lizenzierung, die auf Citrix Cloud gehostet wird. Um XenServer zu lizenzieren, benötigen Sie einen Lizenzserver. Weitere Informationen finden Sie unter Lizenzieren Ihrer Hosts und Pools.

F: Zu welchem Support-Level berechtigt mich meine Lizenz?

Wenn Sie eine XenServer-Lizenz pro Socket erwerben, profitieren Sie auch von unseren technischen Support-Services. Weitere Informationen zu den Unterstützungsstufen finden Sie unter https://xenserver.com/support.

Wenn Sie ein Benutzer der Trial Edition sind, haben Sie keinen Anspruch auf Support. Wir schätzen jedoch Ihr Feedback: Feedback geben.

Weitere Informationen finden Sie unter Fragen zum technischen Support und Support.

F: Ich aktualisiere von einer früheren Citrix Hypervisor-Version mit einer Pro-Socket-Lizenz auf XenServer 8. Muss ich irgendwas tun?

A: Nein. Sie können Ihre Hosts mit den zuvor gekauften Pro-Socket-Lizenzen auf XenServer 8 aktualisieren, sofern Customer Success Services mindestens bis zum 1. März 2024 gültig ist.

Wenn Sie Ihren Customer Success Services nach dem ursprünglichen Kauf erneuert haben, müssen Sie möglicherweise die Lizenzdatei auf dem Lizenzserver aktualisieren, um sicherzustellen, dass die Berechtigung für Customer Success Services angezeigt wird.

F: Ich aktualisiere von einer früheren Citrix Hypervisor-Version mit einer Citrix Virtual Apps and Desktops-Lizenz auf XenServer 8. Muss ich irgendwas tun?

A: Ja. Bevor Sie versuchen, ein Upgrade auf XenServer 8 durchzuführen, müssen Sie XenServer Premium Edition-Lizenzen erwerben, sie in den Citrix Lizenzserver importieren und sie den XenServer-Hosts zuweisen, die derzeit Citrix Virtual Apps and Desktops-Lizenzen verwenden.

Weitere Informationen finden Sie unter Fragen zu Citrix Virtual Apps and Desktops.

F: Ich wechsle von der Vorschauversion von XenServer 8 zur GA-Version von XenServer 8. Muss ich irgendwas tun?

A: Vielleicht. Das hängt von Ihrer Lizenz ab.

- Wenn Sie eine Premium- oder Standard Edition-Lizenz verwenden oder XenServer 8 Preview ohne Lizenz (Trial Edition) verwenden, benötigen Ihre XenServer-Hosts keine Lizenzänderungen.
- Wenn Sie eine Citrix Virtual Apps and Desktops-Lizenz verwenden, zeigen Ihre XenServer-Hosts diese Lizenz als veraltet an. Sie benötigen eine XenServer Premium Edition-Lizenz, um Ihre Citrix Virtual Apps and Desktops-Workloads weiterhin auf XenServer ausführen zu können.

Weitere Informationen finden Sie unter Fragen zu Citrix Virtual Apps and Desktops.

Citrix Virtual Apps and Desktops

F: Welche Edition von XenServer benötige ich, um Citrix Virtual Apps and Desktops-Workloads auf XenServer auszuführen?

A: Um Ihre Citrix Virtual Apps and Desktops-Workloads auf XenServer auszuführen, benötigen Sie eine Premium Edition-Lizenz pro Socket für XenServer. Die Premium Edition bietet viele erweiterte Funktionen, die XenServer zu einer hochoptimierten Hypervisor-Plattform für Ihre Workload machen. Weitere Informationen finden Sie unter XenServer-Editionen.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy.

Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

F: Ich bin ein Kunde von Citrix Virtual Apps and Desktops oder Citrix DaaS, der von einer früheren Version von Citrix Hypervisor auf XenServer 8 umsteigt. Muss ich irgendwas tun?

A: Ja. Bevor Sie versuchen, ein Upgrade auf XenServer 8 durchzuführen, müssen Sie XenServer Premium Edition-Lizenzen erwerben, sie in den Citrix Lizenzserver importieren und sie den XenServer-Hosts zuweisen, die derzeit Citrix Virtual Apps and Desktops-Lizenzen verwenden.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy. Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Dieses Verhalten unterscheidet sich von dem früherer Versionen von Citrix Hypervisor und XenServer. Citrix Hypervisor 8.2 Cumulative Update 1 und frühere Versionen waren als Anspruch für Citrix Virtual Apps and Desktops-Kunden verfügbar.

F: Ich bin ein Citrix Service Provider, der für Citrix Virtual Apps and Desktops oder Citrix DaaS lizenziert ist. Kann ich diese Lizenz für XenServer verwenden, wenn ich auf XenServer 8 aktualisiere?

A: Nein. Bevor Sie versuchen, ein Upgrade auf XenServer 8 durchzuführen, müssen Sie XenServer Premium Edition-Lizenzen erwerben, sie in den Citrix Lizenzserver importieren und sie den XenServer-Hosts zuweisen, die derzeit Citrix Virtual Apps and Desktops-Lizenzen verwenden.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy. Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Dieses Verhalten unterscheidet sich von dem früherer Versionen von Citrix Hypervisor und XenServer. Citrix Hypervisor 8.2 Cumulative Update 1 und frühere Versionen waren als Anspruch für Citrix Virtual Apps and Desktops-Kunden verfügbar.

F: Ich bin Kunde mit einem Citrix DaaS-Abonnement. Bin ich berechtigt, XenServer 8 zu verwenden?

A: Nein. Sie müssen XenServer Premium Edition-Lizenzen erwerben, sie in den Citrix Lizenzserver importieren und sie Ihren XenServer-Hosts zuweisen.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy. Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Dieses Verhalten unterscheidet sich von dem früherer Versionen von Citrix Hypervisor und XenServer. Citrix Hypervisor 8.2 Cumulative Update 1 und frühere Versionen waren als Anspruch für Citrix DaaS-Kunden verfügbar.

F: Welche Einschränkungen gelten für die Nutzung der erweiterten Virtualisierungsverwaltungsfunktionen von XenServer, die als Teil von Citrix Virtual Apps and Desktops bereitgestellt werden?

A: Um Citrix Virtual Apps and Desktops-Workloads auf XenServer auszuführen, benötigen Sie eine Premium Edition-Lizenz. Die Premium Edition bietet viele erweiterte Funktionen, die XenServer zu einer hochoptimierten Hypervisor-Plattform für Ihre Workload machen.

Informationen zu den erweiterten Funktionen, die XenServer für Citrix Virtual Apps and Desktops bietet, finden Sie unter XenServer mit Citrix-Produkten verwenden.

Weitere Informationen zum Abrufen einer XenServer-Lizenz finden Sie unter https://xenserver.com/buy. Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Citrix Lizenzserver

F: Welche Lizenzserver kann ich mit XenServer verwenden?

A: Sie können die Citrix Lizenzserver-Software Version 11.16 oder höher auf einem Server verwenden, auf dem Microsoft Windows ausgeführt wird.

In früheren Versionen haben wir eine virtuelle Linux-basierte Lizenzserver-Appliance unterstützt. Dieses Produkt wird nicht mehr unterstützt. Wenn Sie die virtuelle License Server-Appliance mit einem vorhandenen Pool verwenden, migrieren Sie zur neuesten Version von Citrix License Server für Windows, bevor Sie auf XenServer 8 aktualisieren.

F: Wie importiere ich meine Lizenz auf den Citrix Lizenzserver?

A: Informationen zum Importieren einer Lizenzdatei finden Sie in der Dokumentation zur Citrix Lizenzierung.

F: Kann ich den Lizenzserver in meinem XenServer-Pool ausführen?

A: Ja. Sie können die Citrix Lizenzserver-Software auf einer Windows-VM installieren.

XenServer arbeitet mit einer Grace-Lizenz, bis der Lizenzserver booten kann. Dieses Verhalten bedeutet, dass, nachdem Sie die XenServer-Hosts in Ihrem Pool lizenziert haben und den Host neu gestartet haben, auf dem der Citrix Lizenzserver ausgeführt wird, eine Kulanzzeit auf diesen Host angewendet wird, bis der Lizenzserver neu gestartet wird.

F: Kann ich die Windows-Version des Citrix Lizenzservers mit XenServer verwenden?

A: Ja.

F: Kann ich Lizenzen für Citrix-Produkte auf der unter Windows installierten Citrix Lizenzserver-Software installieren?

A: Ja, Sie können Citrix-Produkte mit der unter Windows installierten Citrix License Server-Software lizenzieren. Weitere Informationen finden Sie unter Lizenzierung auf der Website der Citrix Produktdokumentation .

Lizenzierung eines XenServer-Pools

F: Wie wende ich eine Lizenz auf alle Hosts an, die XenCenter verwenden?

A: Gehen Sie wie folgt vor, um eine Lizenz anzuwenden:

1. Klicken Sie im Menü **Extras** auf **Lizenzmanager**.
2. Wählen Sie den Pool oder die Hosts, der/die Sie lizenzieren möchten, und klicken Sie auf **Lizenz zuteilen**.
3. Geben Sie im Dialogfeld **Lizenz anwenden** den **Editionstyp** an, der dem Host zugewiesen werden soll, und geben Sie den Hostnamen oder die IP-Adresse des Lizenzservers ein.

F: Kann ich eine Lizenz anwenden, ohne XenCenter zu verwenden?

A: Ja, Sie können die xe CLI verwenden. Führen Sie den Befehl `host-apply-edition` aus. Geben Sie beispielsweise Folgendes ein, um einen Host zu lizenzieren:

```
1     xe host-apply-edition edition=enterprise-per-socket|standard-per-
         socket  \
2
3         license-server-address=<license_server_address> host-uuid=<
             uuid_of_host>  \
4
5         license-server-port=<license_server_port>
6 <!--NeedCopy-->
```

Verwenden Sie den `pool-apply-edition` Befehl, um einen Pool zu lizenzieren. Geben Sie beispielsweise Folgendes ein, um einen Pool zu lizenzieren:

```
1     xe pool-apply-edition edition=enterprise-per-socket|standard-per-
         socket  \
2
```



```
        license-server-address=<license_server_address> host-uuid=<
            uuid_of_host>  \

        license-server-port=<license_server_port>
<!--NeedCopy-->
```

F: Wie kann ich den Lizenzstatus meiner Hosts und Pools ermitteln?

A: XenCenter zeigt den Lizenztyp eines Hosts oder Pools an.

Um den Lizenztyp eines Hosts oder Pools zu sehen, wählen Sie diesen Host oder Pool in der Strukturansicht aus. XenCenter zeigt den Lizenzstatus in der Titelleiste für diesen Host oder Pool nach dem Host- oder Poolnamen an.

Sie können auch zur Registerkarte **Allgemein** des Hosts gehen und den Lizenztyp im Abschnitt **Lizenzdetails** suchen.

Um den Lizenztyp eines Hosts mithilfe der Befehlszeile zu ermitteln, führen Sie den folgenden Befehl in der Konsole eines Hosts in Ihrem Pool aus:

```
xe host-license-view host\_uuid=<UUID> | grep sku\_marketing\_name
```

Weitere Informationen

- Weitere Informationen zur XenServer 8-Version finden Sie unter XenServer 8-Versionshinweise.
- Die XenServer 8-Produktdokumentation finden Sie in der XenServer 8-Produktdokumentation.
- Einen Überblick über das XenServer-Produkt finden Sie unter Technischer Überblick.
- Weitere Informationen zum Support finden Sie unter https://xenserver.com/support.

---

layout: doc
description: Install XenServer directly on a dedicated 64-bit x86 server. Set up XenCenter on a Windows system and connect it to your XenServer hosts.—

Installieren

XenServer wird direkt auf Bare-Metal-Hardware installiert, wodurch Komplexität, Overhead und Leistungsengpässe eines zugrunde liegenden Betriebssystems vermieden werden.

XenServer verwendet die Gerätetreiber, die im Linux-Kernel verfügbar sind. Daher kann XenServer auf einer Vielzahl von Hardware- und Speichergeräten ausgeführt werden. Stellen Sie jedoch sicher, dass Sie zertifizierte Gerätetreiber verwenden. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste (HCL).

> **Wichtig:**
>
> Der XenServer-Host muss auf einem dedizierten 64-Bit-x86-Server installiert sein. Installieren Sie kein anderes Betriebssystem in einer Dual-Boot-Konfiguration mit dem XenServer-Host. Diese Konfiguration wird nicht unterstützt.

Dieser Abschnitt richtet sich in erster Linie an Systemadministratoren, die XenServer-Hosts auf physischen Servern einrichten möchten. Es enthält Verfahren, die Sie durch den Installations- oder Update prozess führen. Es enthält auch Informationen zur Behebung von Problemen, die während der Installation auftreten können, und weist Sie auf zusätzliche Ressourcen hin.

Vorbereitung

Je nach Umgebung unterscheidet sich die Installationsmethode, die Sie verwenden müssen, um Ihre Hosts und Pools auf die neueste Version von XenServer 8 zu bringen.

- Wenn Sie Citrix Hypervisor 8.2 Cumulative Update 1 bereits auf Ihren Hosts und Pools installiert haben, führen Sie ein Upgrade von Citrix Hypervisor 8.2 Cumulative Update 1 durch.
- Wenn Sie XenServer 8 bereits installiert haben (auch während der Vorschauphase), können Sie kein Upgrade oder Update von den Installations-ISOs aus durchführen. Wenden Sie stattdessen die neuesten häufigen Updates über XenCenter an. Weitere Informationen finden Sie unter Updates anwenden.
- Wenn Sie bereits eine andere Version von XenServer oder Citrix Hypervisor auf Ihren Hosts und Pools ausführen, wird ein Upgrade von diesen Versionen nicht unterstützt. Führen Sie eine Neuinstallation von XenServer 8 durch.
- Wenn Sie XenServer zum ersten Mal auf Ihren Hosts und Pools installieren, führen Sie eine Neuinstallation von XenServer 8 durch.

Installationsmethoden

XenServer 8 kann auf eine der folgenden Arten installiert werden:

Neuinstallation Wenn Sie eine Neuinstallation von XenServer 8 erstellen:

- Verwenden Sie die **ISO-Datei für die XenServer 8-Installation** . Sie können diese Datei von der XenServer-Downloadseite herunterladen.

- Lesen Sie die Informationen unter Systemanforderungen, Lizenzierung von XenServerund Installation von XenServer und XenCenter, bevor Sie XenServer installieren.

Upgrade Wenn Sie von Citrix Hypervisor 8.2 Cumulative Update 1 auf XenServer 8 aktualisieren:

- Verwenden Sie die **ISO-Datei für die XenServer 8-Installation** . Sie können diese Datei von der XenServer-Downloadseite herunterladen.
- Lesen Sie die Informationen unter Systemanforderungen, Lizenzierung von XenServer und Upgrade von einer vorhandenen Version, bevor Sie XenServer aktualisieren.

Das Installationsprogramm bietet die Option zum Upgrade, wenn es eine zuvor installierte Version von XenServer erkennt. Der Upgradevorgang folgt dem erstmaligen Installationsprozess, wobei jedoch mehrere Einrichtungsschritte umgangen werden. Die vorhandenen Einstellungen werden beibehalten, einschließlich Netzwerkkonfiguration, Systemzeit usw.

Sie können nicht direkt von Versionen von XenServer oder Citrix Hypervisor, die nicht mehr unterstützt werden, auf XenServer 8 aktualisieren. Führen Sie stattdessen eine Neuinstallation durch.

Aktualisieren Bestehende Installationen von XenServer 8 erhalten die neuesten Updates über den Mechanismus für häufige Updates. Weitere Informationen finden Sie unter Updates anwenden.

Unterstützte Startmodi

XenServer unterstützt das Booten von Hosts im UEFI- oder BIOS-Startmodus. UEFI Secure Boot ist derzeit nicht für XenServer-Hosts verfügbar.

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Sie können Ihre XenServer 8-Hosts weiterhin im BIOS-Startmodus installieren. Dadurch können Sie jedoch verhindern, dass Sie Ihre XenServer 8-Hosts auf eine zukünftige Version von XenServer aktualisieren. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

Der Serverstartmodus ändert die Art und Weise, wie Sie den Installationsvorgang starten. Nach dem Start des Installationsprogramms ist der Installationsvorgang für beide Startmodi derselbe.

Installieren Sie den XenServer-Host

Dieses Verfahren führt Sie durch die manuelle Installation von lokalen Medien. Informationen zu anderen Installationstypen, z. B. Netzwerkinstallation, unbeaufsichtigte Installation oder Start über ein SAN, finden Sie unter Andere Installationsszenarien.

> **Tipp:**
>
> Wechseln Sie während der Installation schnell zum nächsten Bildschirm, indem Sie **F12**drücken. Verwenden Sie die **Tabulatortaste**, um zwischen Elementen zu wechseln, und die ****Leertaste, um sie auszuwählen. Drücken Sie ****F1** für allgemeine Hilfe.

So installieren Sie einen XenServer-Host:

1. Machen Sie ein Backup aller Daten, die Sie behalten möchten. Durch die Installation von XenServer werden Daten auf allen Datenträgern überschrieben, die Sie für die Installation auswählen.
2. Starten Sie den Computer vom Installationsmedium aus:
   - So installieren Sie den XenServer-Host von einem bootfähigen USB-Stick:
     a) Erstellen Sie einen bootfähigen USB-Stick aus der XenServer-Installations-ISO. Stellen Sie sicher, dass das Tool den Inhalt der ISO-Datei nicht ändert.
        - Unter Linux können Sie den Befehl `dd` verwenden, um die ISO auf einen USB-Stick zu schreiben. Beispiel: `dd if=<path_to_source_iso> of=<path_to_destination_usb>`.
        - Unter Windows können Sie Rufus verwenden. Achten Sie darauf, dass Sie **Im DD-Image-Modus schreiben** auswählen. Wenn diese Option nicht ausgewählt ist, kann Rufus den Inhalt der ISO-Datei ändern und dafür sorgen, dass sie nicht bootet.

     b) Stecken Sie das bootfähige USB-Laufwerk in das Zielsystem.

     c) Starten Sie das System neu.

     d) Gehe in das Startmenü.

     e) Ändern Sie die Einstellungen, um das System über USB zu starten.

        (Falls erforderlich, finden Sie Informationen zum Ändern der Startreihenfolge in der Dokumentation Ihres Hardwareanbieters.)

   - So installieren Sie den XenServer-Host von einer CD/DVD:
     a) Brennen Sie die XenServer-Installations-ISO-Datei auf eine CD/DVD.

     b) Legen Sie die bootfähige CD/DVD in das CD/DVD-Laufwerk des Zielsystems ein.

     c) Starten Sie das System neu.

     d) Gehe in das Startmenü.

     e) Ändern Sie die Einstellungen, um das System von der CD/DVD zu starten.

(Falls erforderlich, finden Sie Informationen zum Ändern der Startreihenfolge in der Dokumentation Ihres Hardwareanbieters.)

- So installieren Sie den XenServer-Host von Virtual Media:
  a) Gehen Sie zur virtuellen Konsole Ihres Systems.
  b) Fügen Sie die XenServer-Installations-ISO-Datei als Virtual Media ein.
  c) Starten Sie das System neu.
  d) Gehe in das Startmenü.
  e) Ändern Sie die Einstellungen, um das System von den virtuellen Medien aus zu starten.

  (Falls erforderlich, finden Sie Informationen zum Ändern der Startreihenfolge in der Dokumentation Ihres Hardwareanbieters.)
- Informationen zur Netzwerkinstallation finden Sie unter Andere Installationsszenarien.

3. Wählen Sie nach den ersten Startmeldungen und dem Bildschirm **Willkommen bei XenServer** Ihre Tastenbelegung (Tastaturlayout) für die Installation aus.

> **Hinweis:**
>
> Wenn ein Warnbildschirm für Systemhardware angezeigt wird und Unterstützung für die Hardwarevirtualisierung auf Ihrem System verfügbar ist, wenden Sie sich an den Hardwarehersteller, um BIOS-Upgrades zu erhalten.

4. Auf dem Bildschirm **Willkommen beim XenServer-Setup** bietet XenServer die folgenden Optionen:

   - **Um einen Gerätetreiber zu laden, drücken Sie <F9>**

     XenServer wird mit einem breiten Treibersatz geliefert, der die meisten modernen Serverhardwarekonfigurationen unterstützt. Möglicherweise müssen Sie jedoch Treiberdatenträger (eine Art Zusatzpaket) anwenden, um die XenServer-Installation durchführen zu können. Wenn Sie zusätzliche wichtige Gerätetreiber erhalten haben, drücken Sie F9. Das Installationsprogramm führt Sie durch das Laden der erforderlichen Treiber.

     > **Warnung:**
     >
     > Zu diesem Zeitpunkt des Installationsvorgangs können Sie keine anderen Arten von Zusatzpaketen installieren. Sie können sie gegen Ende des Installationsvorgangs zusammen mit zusätzlichen Treiberdatenträgern installieren.

   - **Um erweiterte Speicherklassen einzurichten, drücken Sie <F10>**

     Wenn Sie die erforderliche Konfiguration in Ihrer Netzwerkinfrastruktur vorgenommen haben, können Sie die XenServer-Installation so konfigurieren, dass sie von der Software

FCoE (veraltet) gestartet wird. Drücken Sie F10 und folgen Sie den Anweisungen auf dem Bildschirm, um die Software FCoE einzurichten. Weitere Informationen finden Sie unter Andere Installationsszenarien.

Nachdem Sie alle erforderlichen Schritte auf dieser Seite abgeschlossen haben, wählen Sie **OK**, um fortzufahren.

5. Scrollen Sie durch und lesen Sie die XenServer-Endbenutzervereinbarung (EUA). Wählen Sie **Accept EUA** aus, um fortzufahren.

   Wenn Sie die EUA nicht akzeptieren, können Sie mit der Installation nicht fortfahren.

6. Wählen Sie die entsprechende Aktion aus der Liste aus. Diese Liste beinhaltet immer:

   - **Neuinstallation durchführen**: Wählen Sie diese Option, um mit einer Neuinstallation fortzufahren.

   Je nach Status Ihres Servers werden Ihnen möglicherweise auch die folgenden Optionen angezeigt:

   - **Upgrade**: Wenn das Installationsprogramm eine zuvor installierte Version von XenServer oder Citrix Hypervisor erkennt, bietet es die Option zum Upgrade. Informationen zum Upgrade Ihres XenServer-Hosts finden Sie unter Upgrade von einer vorhandenen Version.
   - **Wiederherstellen**: Wenn das Installationsprogramm eine zuvor erstellte Backup-Installation erkennt, bietet es die Möglichkeit, XenServer aus einem Backup wiederherzustellen.

   Treffen Sie Ihre Auswahl und wählen Sie **OK**, um fortzufahren.

7. Wenn Sie mehrere lokale Datenträger haben, wählen Sie eine primären Datenträger für die Installation aus. Wählen Sie **OK**.

8. Wählen Sie aus, welche Datenträger Sie für den Speicher virtueller Maschinen verwenden möchten. Zeigen Sie Informationen zu einer bestimmten Datenträger an, indem Sie **F5**drücken. Wählen Sie **OK**.

9. Wenn Sie Datenträger ausgewählt haben, die alle 512-Byte-Blöcke haben, haben Sie die Möglichkeit, Thin Provisioning zu verwenden, um die Nutzung des verfügbaren Speichers zu optimieren. Wählen Sie **Thin Provisioning aktivieren** aus, damit die lokale SR des Hosts für das lokale Caching von VM-VDIs verwendet werden kann. Citrix Virtual Desktops und DaaS-Benutzern wird empfohlen, diese Option auszuwählen, damit das lokale Caching ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Speicher.

   > **Hinweis:**
   >
   > Wenn Sie Datenträger ausgewählt haben, die 4 KB nativ sind, wird der Speicher der

> virtuellen Maschine automatisch für eine große Datenträgerblockgröße konfiguriert.

Wählen Sie **OK**, um fortzufahren.

10. Wählen Sie Ihre Installationsmedienquelle aus.

    - Um von einem USB, einer CD oder einem virtuellen Medium zu installieren, wählen Sie **Lokales Medium**aus.
    - Um über das Netzwerk zu installieren, wählen Sie **HTTP** oder **FTP** oder **NFS**.

    Wählen Sie **OK**, um fortzufahren.

11. Wenn Sie im vorherigen Schritt HTTP, FTP oder NFS ausgewählt haben, richten Sie das Netzwerk so ein, dass das Installationsprogramm eine Verbindung zu den XenServer-Installationsmediendateien herstellen kann:

    a) Wenn der Computer über mehrere Netzwerkkarten verfügt, wählen Sie eine davon aus, die für den Zugriff auf die XenServer-Installationsmediendateien verwendet werden soll. Wählen Sie **OK**, um fortzufahren.

    b) Wählen Sie **Automatische Konfiguration (DHCP)**, um die Netzwerkkarte mit DHCP zu konfigurieren, oder Statische Konfiguration, um die Netzwerkkarte manuell zu konfigurieren. Wenn Sie **Statische Konfiguration** wählen, geben Sie gegebenenfalls Details ein.

    c) Geben Sie die VLAN-ID an, wenn Ihr Installationsmedium in einem VLAN-Netzwerk vorhanden ist.

    d) Wenn Sie **HTTP** oder **FTP**wählen, geben Sie die URL für Ihr HTTP- oder FTP-Repository sowie gegebenenfalls einen Benutzernamen und ein Kennwort an.

    Wenn Sie **NFS** wählen, geben Sie den Server und den Pfad Ihrer NFS-Freigabe an.

    e) Wählen Sie **OK**, um fortzufahren.

    Weitere Informationen zum Einrichten Ihrer Installationsmedien auf NFS, FTP oder HTTP finden Sie unter Andere Installationsszenarien.

12. Geben Sie an, ob Sie die Integrität des Installationsmediums überprüfen möchten. Wenn Sie **Installationsquelle überprüfen**auswählen, wird die SHA256-Prüfsumme der Pakete berechnet und mit dem bekannten Wert verglichen. Die Überprüfung kann einige Zeit dauern. Treffen Sie Ihre Auswahl und wählen Sie **OK**, um fortzufahren.

13. Legen Sie ein Root-Kennwort fest und bestätigen Sie es, mit dem XenCenter eine Verbindung zum XenServer-Host herstellt. Sie verwenden dieses Kennwort (mit dem Benutzernamen “root”) auch, um sich bei **xsconsole, der Systemkonfigurationskonsole**, anzumelden.

> **Hinweis:**
>
> XenServer-Root-Kennwörter dürfen nur ASCII-Zeichen enthalten.

14. Richten Sie die primäre Verwaltungsschnittstelle ein, über die XenCenter eine Verbindung zum Host herstellt und ihn verwaltet.

    Wenn Ihr Computer über mehrere Netzwerkkarten verfügt, wählen Sie die Netzwerkkarte aus, die Sie für die Verwaltung verwenden möchten. Wählen Sie **OK**, um fortzufahren.

15. Konfigurieren Sie die Verwaltungsschnittstelle mit den folgenden Optionen:

    - Wählen Sie **Automatische Konfiguration (DHCP)**, um die Netzwerkkarte mit DHCP zu konfigurieren.
    - Wählen Sie **Statische Konfiguration**, um die Netzwerkkarte manuell zu konfigurieren Geben Sie eine IP-Adresse, eine Subnetzmaske und ein Gateway an.
    - Wählen Sie **VLAN verwenden**, um die Verwaltungsschnittstelle in einem VLAN-Netzwerk zu haben. Geben Sie die VLAN-ID an.

    > **Hinweis:**
    >
    > Um Teil eines Pools zu sein, müssen XenServer-Hosts statische IP-Adressen haben oder über DNS adressierbar sein. Stellen Sie bei der Verwendung von DHCP sicher, dass eine statische DHCP-Reservierungsrichtlinie vorhanden ist.

16. Geben Sie den Hostnamen und die DNS-Konfiguration an.

    a) Wählen Sie im Abschnitt **Hostnamen-Konfiguration** eine der folgenden Optionen aus:

    - Wählen Sie **Automatisch über DHCP einstellen**, damit der DHCP-Server den Hostnamen zusammen mit der IP-Adresse bereitstellt.
    - Wählen Sie **Manuell angeben**, um den Hostnamen selbst zu definieren. Geben Sie den Hostnamen für den Server in das dafür vorgesehene Feld ein.

    > **Hinweis:**
    >
    > Wenn Sie den Hostnamen manuell angeben, geben Sie einen kurzen Hostnamen und *nicht den vollqualifizierten Domänennamen (FQDN)*ein. Die Eingabe eines FQDN kann dazu führen, dass die externe Authentifizierung fehlschlägt oder der XenServer-Host möglicherweise mit einem anderen Namen zu Active Directory hinzugefügt wird.

    a) Wählen Sie im Abschnitt **DNS-Konfiguration** eine der folgenden Optionen aus:

    - Wählen Sie **Automatisch über DHCP einstellen**, um die Namensdienstkonfiguration mithilfe von DHCP abzurufen.

- Wählen Sie **Manuell angeben**, um die DNS-Server selbst zu definieren. Geben Sie die IP-Adressen Ihrer primären (erforderlich), sekundären (optional) und tertiären (optional) DNS-Server in die dafür vorgesehenen Felder ein.

Wählen Sie **OK**, um fortzufahren.

17. Wählen Sie Ihre Zeitzone nach geografischem Gebiet und Stadt. Sie können den ersten Buchstaben des gewünschten Gebietsschemas eingeben, um zum ersten Eintrag zu springen, der mit diesem Buchstaben beginnt. Wählen Sie **OK**, um fortzufahren.
18. Geben Sie an, wie der XenServer-Host die Ortszeit ermitteln soll. XenServer bietet die folgenden Optionen:

    - **NTP verwenden**: Wählen Sie diese Option, um das NTP-Protokoll zur Einstellung Ihrer Serverzeit zu verwenden. Konfigurieren Sie es auf dem nächsten Bildschirm auf eine der folgenden Arten:

      – Wählen Sie **NTP wird von meinem DHCP-Server so konfiguriert**, dass Ihr Netzwerk den Hostnamen oder die IP-Adresse des NTP-Servers bereitstellt.

      – Geben Sie manuell mindestens einen NTP-Servernamen oder eine IP-Adresse ein.

      Wählen Sie **OK**, um fortzufahren.

    - **Manuelle Zeiteingabe**: Wählen Sie diese Option, um Datum und Uhrzeit manuell einzustellen.

      Geben Sie auf dem nächsten Bildschirm die aktuelle Uhrzeit in UTC ein.

      Wählen Sie **OK**, um fortzufahren.

    > **Hinweis:**
    >
    > XenServer geht davon aus, dass die Zeiteinstellung auf dem Server die aktuelle Uhrzeit in UTC ist.

    Wählen Sie **OK**, um fortzufahren.
19. Wählen Sie **XenServer installieren**.

    Der Installationsvorgang beginnt. Dieser Vorgang kann einige Minuten dauern.
20. Auf dem nächsten Bildschirm werden Sie gefragt, ob Sie zusätzliche Pakete (einschließlich Treiberdatenträger) installieren möchten.

    > **Hinweis:**
    >
    > Wenn Sie bei der Erstinstallation bereits einen Treiberdatenträger geladen haben, werden Sie möglicherweise aufgefordert, den Treiberdatenträger erneut einzulegen, damit der Treiber auf der Datenträger installiert werden kann. Legen Sie zu diesem Zeitpunkt

> den Treiberdatenträger erneut ein, um sicherzustellen, dass Ihre XenServer-Instanz den neuen Treiber enthält.

- Wenn Sie zusätzliche Pakete oder Treiberdatenträger installieren möchten, die von Ihrem Hardwarehersteller bereitgestellt werden, wählen Sie **Ja**.
  a) Sie werden aufgefordert, das Zusatzpaket einzulegen. Werfen Sie das XenServer-Installationsmedium aus und legen Sie das Zusatzpackmedium ein.
  b) Wählen Sie **OK**.
  c) Wählen Sie **Medien verwenden** aus, um mit der Installation fortzufahren.
  d) Wiederholen Sie dies für jedes zu installierende Paket.
- Wenn Sie kein zusätzliches Paket installieren möchten, wählen Sie **Nein**.

  Der Installationsvorgang ist abgeschlossen. Dieser Vorgang kann einige Minuten dauern.

21. Wenn Sie auf dem Bildschirm "**Installation abgeschlossen** "dazu aufgefordert werden, werfen Sie das Installationsmedium aus (bei der Installation von USB oder CD).
22. Wählen Sie **OK**, um den Host neu zu starten.

Nach dem Neustart des Hosts zeigt XenServer **xsconsole an, eine Systemkonfigurationskonsole**. Um von **xsconsole**aus auf eine lokale Shell zuzugreifen, drücken Sie **Alt+F3**; um zur **xsconsole**zurückzukehren, drücken Sie **Alt+F1**.

> **Hinweis:**
>
> Notieren Sie sich die angezeigte IP-Adresse. Verwenden Sie diese IP-Adresse, wenn Sie XenCenter mit dem XenServer-Host verbinden.

Installieren Sie XenCenter

XenCenter muss auf einem Windows-Computer installiert sein, der über Ihr Netzwerk eine Verbindung zum XenServer-Host herstellen kann. Stellen Sie sicher, dass .NET Framework Version 4.8 oder höher auf diesem System installiert ist.

Um XenCenter zu installieren:

1. Laden Sie das Installationsprogramm für die neueste Version von XenCenter von der XenServer-Downloadseiteherunter.
2. Starten Sie die Installationsdatei `.msi`.
3. Folgen Sie dem **Setup-Assistenten**, mit dem Sie den Standardzielordner ändern und anschließend XenCenter installieren können.

Weitere Informationen zur Verwendung von XenCenter finden Sie in der XenCenter-Dokumentation.

Verbinden Sie XenCenter mit dem XenServer-Host

So verbinden Sie XenCenter mit dem XenServer-Host:

1. Starten Sie XenCenter. Das Programm öffnet sich auf der Registerkarte **Home** .
2. Klicken Sie auf das Symbol **Neuen Server hinzufügen**.
3. Geben Sie die IP-Adresse des XenServer-Hosts in das Feld **Server** ein. Geben Sie den root-Benutzernamen und das Kennwort ein, die Sie während der XenServer-Installation festgelegt haben. Klicken Sie auf **Hinzufügen**.
4. Wenn Sie zum ersten Mal einen Host hinzufügen, wird das Dialogfeld **Verbindungsstatus speichern und wiederherstellen** angezeigt. In diesem Dialog können Sie Ihre Einstellungen für das Speichern Ihrer Host-Verbindungsinformationen und das automatische Wiederherstellen von Hostverbindungen festlegen.

   Wenn Sie Ihre Einstellungen später ändern möchten, können Sie dies im XenCenter-Hauptmenü tun, indem Sie **Tools** und dann **Options** auswählen. Das Dialogfenster **Optionen** wird geöffnet. Wählen Sie die Registerkarte **Speichern und Wiederherstellen** und legen Sie Ihre Einstellungen fest. Klicken Sie auf **OK**, um die Änderungen zu speichern.

XenServer-Hosts lizenzieren

Ihre neu installierten XenServer-Hosts können in der Trial Edition ohne Lizenz ausgeführt werden. Diese Edition schränkt Ihre Poolgröße ein und ermöglicht kein rollendes Pool-Upgrade über XenCenter. Weitere Informationen finden Sie unter http://www.xenserver.com/editions.

Informationen zur Lizenzierung Ihrer XenServer-Hosts finden Sie unter Lizenzierung von XenServer.

---

layout: doc
h3InToc: true
description: Configure your servers to enable PXE booting of XenServer host installations, boot from SAN, or unattended installation.—

Andere Installationsszenarien

Zusätzlich zu einem manuellen Standardinstallationsprozess bietet XenServer die Möglichkeit, verschiedene andere Arten von Installationen durchzuführen, darunter die folgenden:

- Netzwerkinstallationen mit PXE-Boot

- Unbeaufsichtigte Installationen
- Den Host für das Booten vom SAN aus einrichten
- Host-Multipathing konfigurieren

Unterstützte Startmodi

XenServer unterstützt das Booten von Hosts im UEFI- oder BIOS-Startmodus. UEFI Secure Boot ist derzeit nicht für XenServer-Hosts verfügbar.

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Sie können Ihre XenServer 8-Hosts weiterhin im BIOS-Startmodus installieren. Dadurch können Sie jedoch verhindern, dass Sie Ihre XenServer 8-Hosts auf eine zukünftige Version von XenServer aktualisieren. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

Der Serverstartmodus ändert die Art und Weise, wie Sie den Installationsvorgang starten. Nach dem Start des Installationsprogramms ist der Installationsvorgang für beide Startmodi derselbe.

Stellen Sie beim Upgrade Ihrer XenServer-Hosts sicher, dass das Upgrade denselben Startmodus wie die Erstinstallation verwendet.

Installation im Netzwerk

Wenn der Server, auf dem Sie die Installation durchführen möchten, über eine PXE-Boot-fähige Ethernet-Karte verfügt, können Sie diese Funktion verwenden, um eine Netzwerkinstallation mit PXE-Boot durchzuführen.

Die Verwendung von PXE-Start für die Installation über das Netzwerk umfasst die folgenden Schritte:

- Kopieren Sie die Installationsdateien auf einen TFTP-Server und konfigurieren Sie Ihre TFTP- und DHCP-Server für die PXE-Boot-Installation. Die Methode hierfür hängt von Ihrem Startmodus ab: BIOS oder UEFI.
- Hosten Sie Ihre Installationsmedien auf NFS, FTP oder HTTP. Nur auf die Installationsdateien wird vom TFTP-Server aus zugegriffen. Die XenServer-Dateien, die auf dem Server installiert werden sollen, werden auf einem NFS-, FTP- oder HTTP-Server gehostet. Alternativ können Sie die Installation, nachdem Sie sie über den PXE-Start gestartet haben, über lokale Medien abschließen, die auf dem Zielserver gehostet werden.
- Erstellen Sie eine Antwortdatei für die unbeaufsichtigte Installation. Sie können sich stattdessen für eine beaufsichtigte Installation entscheiden und das Installationsprogramm manuell ausführen.

- Starten Sie den Installationsvorgang.

> **Hinweis:**
>
> Der PXE-Start wird über ein getaggtes VLAN-Netzwerk nicht unterstützt. Stellen Sie sicher, dass das VLAN-Netzwerk, das Sie für den PXE-Start verwenden, nicht gekennzeichnet ist

Konfigurieren Sie Ihre TFTP- und DHCP-Server

Bevor Sie das XenServer-Installationsmedium einrichten, müssen Sie Ihre TFTP- und DHCP-Server konfigurieren. Die folgenden Abschnitte enthalten Informationen zur Konfiguration Ihres TFTP-Servers für den PXE-Start mit BIOS oder UEFI. Konsultieren Sie die Dokumentation Ihres Anbieters für allgemeine Einrichtungsverfahren.

Konfigurieren Sie Ihren TFTP-Server für den PXE-Start mit dem BIOS

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

Hosten Sie die Installationsdateien auf einem TFTP-Server und konfigurieren Sie Ihren TFTP-Server so, dass PXE-Boot im BIOS-Startmodus aktiviert wird. Diese Konfiguration wird verwendet, um den Installationsvorgang zu starten.

1. Erstellen Sie in Ihrem TFTP-Stammverzeichnis (z. B. `/tftpboot`) ein Verzeichnis mit dem Namen `xenserver`.
2. Kopieren Sie vom XenServer-Installationsmedium die `pxelinux.0` Dateien `mboot.c32` und aus dem `/boot/pxelinux` Verzeichnis Ihres Installationsmediums in das TFTP-Stammverzeichnis.

   > **Hinweis:**
   >
   > Wir empfehlen dringend, `pxelinux.0` Dateien aus derselben Quelle zu verwenden `mboot.c32` (z. B. von derselben XenServer-Installations-ISO).

3. Kopieren Sie die Dateien vom XenServer-Installationsmedium in das neue `xenserver` Verzeichnis auf dem TFTP-Server:

   - `install.img` aus dem Stammverzeichnis
   - `vmlinuz` aus dem `/boot` Verzeichnis
   - `xen.gz` aus dem `/boot` Verzeichnis

4. Erstellen Sie im TFTP-Stammverzeichnis (z. B. `/tftpboot`) ein Verzeichnis mit dem Namen `pxelinux.cfg`.

5. Erstellen Sie im Verzeichnis `pxelinux.cfg` Ihre Konfigurationsdatei mit dem Namen **`default`**.

   Der Inhalt dieser Datei hängt davon ab, wie Sie Ihre PXE-Boot-Umgebung konfigurieren möchten und welche Werte für Ihre Server geeignet sind.

   - **Beispiel: Unbeaufsichtigte Installation** Diese Beispielkonfiguration führt eine unbeaufsichtigte Installation mithilfe der Antwortdatei unter der angegebenen URL durch:

     ```
     default xenserver-auto
     label xenserver-auto
         kernel mboot.c32
         append xenserver/xen.gz dom0_max_vcpus=1-16 \
             dom0_mem=max:8192M com1=115200,8n1 \
             console=com1,vga ---  xenserver/vmlinuz \
             console=hvc0 console=tty0 \
             answerfile=<http://pxehost.example.com/
                answer_file> \
             answerfile_device=<device> \
             install ---  xenserver/install.img
     <!--NeedCopy-->
     ```

     > **Hinweis:**
     >
     > Um anzugeben, welcher Netzwerkadapter zum Abrufen der Antwortdatei verwendet werden soll, geben Sie den Parameter `answerfile_device=ethX` oder `answerfile_device=MAC` ein und geben Sie entweder die Ethernet-Gerätenummer oder die MAC-Adresse des Geräts an.

     Weitere Informationen zur Verwendung einer Antwortdatei finden Sie unter Erstellen einer Antwortdatei für die unbeaufsichtigte Installation.

   - **Beispiel: Manuelle Installation** Diese Beispielkonfiguration startet eine Installation, die vom TFTP-Server bootet und manuelle Antworten erfordert:

     ```
     default xenserver
     label xenserver
         kernel mboot.c32
         append xenserver/xen.gz dom0_max_vcpus=1-16 \
         dom0_mem=max:8192M com1=115200,8n1 \
         console=com1,vga ---  xenserver/vmlinuz \
         console=hvc0 console=tty0 \
         ---  xenserver/install.img
     <!--NeedCopy-->
     ```

   Weitere Informationen zum Inhalt der PXE-Konfigurationsdatei finden Sie auf der SYSLINUX-Website .

Nächster Schritt: Hosten Sie Ihr Installationsmedium auf NFS, FTP oder HTTP. Zusätzlich zu den

TFTP- und DHCP-Servern benötigen Sie einen NFS-, FTP- oder HTTP-Server, um die auf Ihrem Server installierten XenServer-Dateien zu speichern.

Konfigurieren Sie Ihren TFTP-Server für den PXE-Boot mit UEFI Hosten Sie die Installationsdateien auf einem TFTP-Server und konfigurieren Sie Ihre DHCP- und TFTP-Server so, dass PXE-Boot im UEFI-Startmodus aktiviert wird. Diese Konfiguration wird verwendet, um den Installationsvorgang zu starten.

1. Erstellen Sie im TFTP-Stammverzeichnis (z. B. `/tftpboot`) ein Verzeichnis mit dem Namen `EFI/xenserver`.
2. Kopieren Sie die folgenden Dateien vom XenServer-Installationsmedium in das neue Verzeichnis `EFI/xenserver` auf dem TFTP-Server:
   - `grubx64.efi` aus dem `/EFI/xenserver` Verzeichnis
   - `install.img` aus dem Stammverzeichnis
   - `vmlinuz` aus dem `/boot` Verzeichnis
   - `xen.gz` aus dem `/boot` Verzeichnis
3. Konfigurieren Sie Ihren DHCP-Server so, dass `/EFI/xenserver/grubx64.efi` als Startdatei bereitgestellt wird.
4. Erstellen Sie die `grub.cfg` Datei im `EFI/xenserver` Verzeichnis auf dem TFTP-Server.

   Der Inhalt dieser Datei hängt davon ab, wie Sie Ihre PXE-Boot-Umgebung konfigurieren möchten und welche Werte für Ihre Server geeignet sind.

   - **Beispiel: Unbeaufsichtigte Installation** Diese Beispielkonfiguration führt eine unbeaufsichtigte Installation mithilfe der Antwortdatei unter der angegebenen URL durch:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16
       dom0_mem=max:8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address
       >/<path_to_answer_file> install
    module2 /EFI/xenserver/install.img
 }

<!--NeedCopy-->
```

> **Hinweis:**
>
> Um anzugeben, welcher Netzwerkadapter zum Abrufen der Antwortdatei verwendet werden soll, geben Sie den Parameter `answerfile_device=ethX` oder `answerfile_device=MAC` ein und geben Sie entweder die Ethernet-

> Gerätenummer oder die MAC-Adresse des Geräts an.

Weitere Informationen zur Verwendung einer Antwortdatei finden Sie unter Erstellen einer Antwortdatei für die unbeaufsichtigte Installation.

- **Beispiel: Manuelle Installation** Diese Beispielkonfiguration startet eine Installation, die vom TFTP-Server bootet und manuelle Antworten erfordert:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16
       dom0_mem=max:8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
    module2 /EFI/xenserver/install.img
 }

<!--NeedCopy-->
```

Nächster Schritt: Hosten Sie Ihr Installationsmedium auf NFS, FTP oder HTTP. Zusätzlich zu den TFTP- und DHCP-Servern benötigen Sie einen NFS-, FTP- oder HTTP-Server, um die auf Ihrem Server installierten XenServer-Dateien zu speichern.

Hosten Sie Ihre Installationsmedien auf NFS, FTP oder HTTP

Der TFTP-Server hostet die Dateien, die zum Starten des Installationsprogramms benötigt werden, aber die zu installierenden Dateien werden auf einem NFS-, FTP- oder HTTP-Server gehostet.

Sie können auch Dateien verwenden, die auf NFS, FTP oder HTTP gehostet werden, um eine Installation abzuschließen, die von lokalen Medien auf Ihrem Server gestartet wurde.

1. Erstellen Sie auf dem HTTP-, FTP- oder NFS-Server ein Verzeichnis, aus dem das XenServer-Installationsmedium über HTTP, FTP oder NFS exportiert werden kann.
2. Kopieren Sie den gesamten Inhalt des XenServer-Installationsmediums in das neu erstellte Verzeichnis auf dem HTTP-, FTP- oder NFS-Server. Dieses Verzeichnis ist Ihr Installationsrepository.

   > **Hinweis:**
   >
   > Achten Sie beim Kopieren des XenServer-Installationsmediums darauf, dass Sie die Datei `.treeinfo` in das neu erstellte Verzeichnis kopieren.
   >
   > Wenn Sie IIS zum Hosten des Installationsmediums verwenden, stellen Sie sicher, dass das doppelte Escaping auf IIS aktiviert ist, bevor Sie das Installations-ISO-Image darauf extrahieren.

Der nächste Schritt:

- Wenn Sie eine unbeaufsichtigte Installation abschließen: Erstellen Sie eine Antwortdatei für die unbeaufsichtigteInstallation.
- Wenn Sie PXE-Boot verwenden, um eine manuelle Installation zu starten: Starten Sie die Netzwerkinstallation.

Erstellen Sie eine Antwortdatei für die unbeaufsichtigte Installation

Um Installationen unbeaufsichtigt durchzuführen, erstellen Sie eine XML-Antwortdatei.

Enthalten alle Knoten innerhalb eines Stammknotens mit dem Namen *installation*. Beachten Sie beim Erstellen Ihrer Antwortdatei die Referenz zur Antwortdatei.

Hier ist ein Beispiel für eine Antwortdatei:

```
<?xml version="1.0"?>
    <installation srtype="ext">
        <primary-disk>sda</primary-disk>
        <guest-disk>sdb</guest-disk>
        <guest-disk>sdc</guest-disk>
        <keymap>us</keymap>
        <root-password>mypassword</root-password>
        <source type="url">http://pxehost.example.com/xenserver/</
           source>
        <script stage="filesystem-populated" type="url">
          http://pxehost.example.com/myscripts/post-install-script
        </script>
        <admin-interface name="eth0" proto="dhcp" />
        <timezone>Europe/London</timezone>
    </installation>
<!--NeedCopy-->
```

Nächster Schritt: Starten Sie die Netzwerkinstallation.

Automatisierte Upgrades mit einer Antwortdatei Sie können auch automatische Upgrades durchführen, indem Sie die Antwortdatei entsprechend ändern.

1. Stellen Sie das Attribut `mode` des Elements `installation` auf `upgrade` ein.
2. Geben Sie den Datenträger an, auf der die vorhandene Installation mit dem Element `existing-installation` ist.
3. Lassen Sie die `primary-disk`- und `guest-disk`-Elemente nicht spezifiziert.

Beispiel:

```
<?xml version="1.0"?>
<installation mode="upgrade">
    <existing-installation>sda</existing-installation>
    <source type="url">http://pxehost.example.com/xenserver/</source>
    <script stage="filesystem-populated" type="url">
```



```
6           http://pxehost.example.com/myscripts/post-install-script
7       </script>
8   </installation>
9   <!--NeedCopy-->
```

Referenz zur Antwortdatei Im Folgenden finden Sie eine Zusammenfassung der Elemente. Alle Knotenwerte sind Text, sofern nicht anders angegeben. Erforderliche Elemente sind angegeben.

`<installation>` **Erforderlich?** Ja

Beschreibung: Das Stammelement, das alle anderen Elemente enthält.

Eigenschaften:

`srtype`

Das Attribut `srtype` kann einen der folgenden Werte haben: `lvm`, `ext` oder `xfs`:

- `lvm` - Lokalen Speichertyp auf LVM setzen.
- `ext` - Lokalen Speichertyp auf EXT4 setzen. Dadurch kann das lokale Caching für Citrix Virtual Desktops ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter Speicher.
- `xfs` - Lokalen Speichertyp auf XFS setzen. Mit dieser Option können Sie auch lokale Speichergeräte mit physischen Blöcken von 4 KB erstellen, ohne dass eine logische Blockgröße von 512 Byte erforderlich ist.

Um Thin Provisioning zu aktivieren, können Sie das Attribut `srtype` als `ext` oder `xfs` angeben. Wenn Sie das Attribut `srtype` nicht angeben, lautet der Standardwert für `srtype` `lvm`. Wenn Sie das Attribut `srtype` nicht angeben, aber in Ihrer Antwortdatei einen nativen 4-KB-Datenträger für den lokalen Speicher konfigurieren, lautet der Standardwert `xfs`.

> **Hinweis:**
>
> Sie können die Speichertypen Local LVM oder Local EXT3/EXT4 nicht mit physischen Blöcken von 4 KB verwenden. Wenn Sie versuchen, bei der Konfiguration physischer Blöcke mit 4 KB `lvm` oder `ext` für das `srtype` Attribut anzugeben, wird Ihre Antwortdateikonfiguration als inkompatibel zurückgewiesen.

`mode`

Um den Installationstyp für das Upgrade zu ändern, geben Sie Attribut `mode` mit dem Wert `upgrade` an. Wenn dieses Attribut nicht angegeben ist, führt das Installationsprogramm eine Neuinstallation durch und überschreibt alle vorhandenen Daten auf dem Server.

<driver-source> **Erforderlich?** Ja

Beschreibung: Die Quelle eines Zusatzpakets mit Gerätetreibern, die vom Installationsprogramm geladen und nach der Installation des Haupt-Repositorys hinzugefügt werden.

Attribute: Keine

<primary-disk> **Erforderlich?** Ja

> **Hinweis:**
>
> Für Upgrade-Szenarien veraltet.

Beschreibung: Der Name des Speichergeräts, auf dem die Steuerdomäne installiert ist. Dieses Element entspricht der Auswahl, die im Schritt *Primären Datenträger auswählen* des manuellen Installationsvorgangs getroffen wurde.

Attribute: Sie können ein Attribut `guest-storage` mit möglichen Werten `yes` und `no` angeben. Zum Beispiel: `<primary-disk guest-storage="no">sda</primary-disk>`

Der Standardwert ist `yes`. Wenn Sie angeben `no`, können Sie ein Installationsszenario automatisieren, in dem kein Speicherrepository erstellt wird. In diesem Fall geben Sie keine Guest-Disk-Schlüssel an.

<guest-disk> **Erforderlich?** Nein

Beschreibung: Der Name eines Speichergeräts, das zum Speichern von Gästen verwendet werden soll. Verwenden Sie eines dieser Elemente für jeden zusätzlichen Datenträger.

Attribute: Keine

<ntp> **Erforderlich?** Ja

Beschreibung: Gibt die Quelle für NTP-Server an. Wenn das Element `<ntp>` nicht angegeben ist, ist die Standardeinstellung `manual`, wenn `<ntp-server>` angegeben ist, `dhcp` wenn DHCP verwendet wird, andernfalls **`default`**.

Eigenschaften:

Das Attribut `source` kann einen der folgenden Werte haben: `dhcp`, **`default`**, `manual` oder `none` .

- `dhcp` - NTP-Server von DHCP verwenden
- **`default`** - Standard-NTP-Server verwenden
- `manual` - bereitgestellte NTP-Server verwenden, in diesem Fall muss mindestens ein `<ntp-server>` Eintrag angegeben werden

- none - NTP ist deaktiviert

Wenn source = dhcp, **default** oder none, geben Sie nicht <ntp-server> an.

<ntp-server> Erforderlich? Nein

Beschreibung: Gibt einen oder mehrere NTP-Server an. Nur mit dem Element ntp und dem Attribut manual zu verwenden.

Attribute: Keine

<keymap> Erforderlich? Nein

Beschreibung: Der Name der Tastenzuordnung, die während der Installation verwendet werden soll. <keymap>us</keymap> Der Standardwert, us, wird berücksichtigt, wenn Sie keinen Wert für dieses Element angeben.

Attribute: Keine

<root-password> Erforderlich: Nein

Beschreibung: Das gewünschte Root-Kennwort für den XenServer-Host. Wenn kein Kennwort angegeben wird, wird beim ersten Booten des Hosts eine Eingabeaufforderung angezeigt.

Attribute: Sie können einen type angeben, entweder hash oder plaintext

Beispiel:

```
<root-password type="hash">hashedpassword</root-password>
<!--NeedCopy-->
```

Der Hashwert kann jeden Hashtyp verwenden, der von crypt(3) in glibc unterstützt wird. Der Standard-Hash-Typ ist SHA-512.

Sie können den folgenden Python-Code verwenden, um eine Hash-Kennwort-Zeichenfolge zu generieren, die in die Antwortdatei aufgenommen werden soll:

```
python -c 'import crypt; print(crypt.crypt("mypasswordhere", crypt.
    mksalt(crypt.METHOD_SHA512)))'
<!--NeedCopy-->
```

<source> Erforderlich: Ja

Beschreibung: Der Speicherort des hochgeladenen XenServer-Installationsmediums oder eines Supplemental Packs. Dieses Element kann mehrfach vorkommen.

Attribute: Das Attribut type kann einen der folgenden Werte haben: url, nfs oder local.

Wenn der Wert ist `local`, lassen Sie das Element leer. Beispiel:

```
<source type="url">http://server/packages</source>
<source type="local" />
<source type="nfs">server:/packages</source>
<!--NeedCopy-->
```

`<script>` Erforderlich: Nein

Beschreibung: Wo sich das Post-Install-Skript befindet.

Eigenschaften:

Das Attribut `stage` kann einen der folgenden Werte haben: `filesystem-populated`, `installation-start` oder `installation-complete`.

- Wenn der Wert `filesystem-populated` verwendet wird, wird das Skript ausgeführt, kurz bevor die Bereitstellung des Root-Dateisystems aufgehoben wird (z. B. nach der Installation/-dem Upgrade, wenn initrds bereits erstellt wurden usw.). Das Skript erhält ein Argument, das den Bereitstellungspunkt des Root-Dateisystems darstellt.
- Wenn der Wert `installation-start` verwendet wird, wird das Skript vor dem Start der Hauptinstallationssequenz ausgeführt, aber nachdem das Installationsprogramm initialisiert, alle Treiber geladen und die Antwortdatei verarbeitet hat. Das Skript erhält keine Argumente.
- Wenn der Wert `installation-complete` verwendet wird, wird das Skript ausgeführt, nachdem das Installationsprogramm alle Vorgänge abgeschlossen hat (und daher das Root-Dateisystem nicht eingehängt wurde). Das Skript erhält ein Argument mit dem Wert Null, wenn die Installation erfolgreich abgeschlossen wurde, und ist ungleich Null, falls die Installation aus irgendeinem Grund fehlgeschlagen ist.

Das Attribut `type` kann einen der folgenden Werte haben: `url`, `nfs` oder `local`.

Wenn der Wert `url` oder `nfs` ist, geben Sie die URL oder den NFS-Pfad in die PCDATA ein. Wenn der Wert ist `local`, lassen Sie PCDATA leer. Beispiel:

```
<script stage="filesystem-populated" type="url">
    http://prehost.example.com/post-install-script
</script>
<script stage="installation-start" type="local">
    file:///scripts/run.sh
</script>
<script stage="installation-complete" type="nfs">
    server:/scripts/installation-pass-fail-script
</script>
<!--NeedCopy-->
```


> **Hinweis:**
>
> Wenn eine lokale Datei verwendet wird, stellen Sie sicher, dass der Pfad absolut ist. Das bedeutet im Allgemeinen, dass auf das Präfix `file://` ein weiterer Schrägstrich folgt und dann der vollständige Pfad zum Skript.

`<admin-interface>` **Erforderlich:** Manchmal

> **Hinweis:**
>
> Erforderlich während der Installation/Neuinstallation, aber nicht während des Upgrades oder der Wiederherstellung.

Beschreibung: Die einzige Netzwerkschnittstelle, die als Host-Administrationsschnittstelle verwendet werden soll.

Eigenschaften:

Geben Sie eines der folgenden Attribute an:

- `name` - Zum Beispiel den Namen Ihrer Netzwerkschnittstelle `eth0`.
- `hwaddr` - Zum Beispiel die MAC-Adresse Ihrer Netzwerkschnittstelle `00:00:11:aa:bb:cc`.

Das Attribut `proto` kann einen der folgenden Werte haben: `dhcp` oder **`static`**.

Wenn Sie angeben `proto="static"`, müssen Sie auch alle diese untergeordneten Elemente angeben:

Untergeordnete Elemente

- `<ipaddr>`: Die IP-Adresse
- `<subnet>`: Die Subnetzmaske
- `<gateway>`: Das Gateway

`<timezone>` **Erforderlich:** Nein

Beschreibung: Die Zeitzone im Format, das von der Variablen TZ verwendet wird, zum Beispiel Europe/London oder Amerika/Los_Angeles. Der Standardwert ist `Etc/UTC`.

`<name-server>` **Erforderlich:** Nein

Beschreibung: Die IP-Adresse eines Nameservers. Verwenden Sie eines dieser Elemente für jeden Nameserver, den Sie verwenden möchten.

`<hostname>` **Erforderlich:** Nein

Beschreibung: Geben Sie dieses Element an, wenn Sie manuell einen Hostnamen festlegen möchten.

`<ntp-server>` **Erforderlich:** Nein

Beschreibung: Geben Sie einen oder mehrere NTP-Server an.

Starten Sie die Netzwerkinstallation

Nachdem Sie die für eine PXE-Startinstallation erforderlichen Netzwerkserver eingerichtet haben, führen Sie die folgenden Schritte auf dem Server durch, auf dem Sie die Installation durchführen:

1. Starten Sie das System und rufen Sie das Startmenü auf (**F12** in den meisten BIOS-Programmen).
2. Wählen Sie aus, ob Sie von Ihrer Ethernet-Karte starten
3. Das System startet dann mit PXE von der Installationsquelle, die Sie eingerichtet haben, und das Installationsskript wird gestartet.
    - Wenn Sie eine Antwortdatei eingerichtet haben, wird die Installation unbeaufsichtigt fortgesetzt.
    - Wenn Sie sich für eine manuelle Installation entschieden haben, geben Sie Informationen an, wenn Sie dazu aufgefordert werden. Weitere Informationen finden Sie unter Installation.

Booten von SAN

Boot-from-SAN-Umgebungen bieten mehrere Vorteile, darunter hohe Leistung, Redundanz und Speicherplatzkonsolidierung. In diesen Umgebungen ist der Startdatenträger auf einem Remote-SAN und nicht auf dem lokalen Host.

Die folgenden Arten der Boot-from-SAN-Konfiguration werden unterstützt:

- HBA und Hardware Fibre Channel
- Software-FCoE (veraltet)
- Software-Start von iSCSI

Für eine vollständig redundante Boot-from-SAN-Umgebung müssen Sie mehrere Pfade für den I/O-Zugriff konfigurieren. Weitere Informationen finden Sie unter Multipathing aktivieren.

HBA und Hardware Fibre Channel

Diese Art der Boot-from-SAN-Bereitstellung hängt von SAN-basierten Datenträger-Arrays ab, die entweder Hardware-Fibre-Channel- oder HBA-iSCSI-Adapter auf dem Host unterstützen. Der Host kommuniziert mit dem SAN über einen Hostbusadapter (HBA). Das BIOS des HBA enthält die Anweisungen, die es dem Host ermöglichen, den Startdatenträger zu finden.

Die gesamte Konfiguration für den Start vom SAN über Hardware-Fibre Channel oder einen HBA-Adapter erfolgt in Ihrer Netzwerkinfrastruktur, bevor Sie XenServer auf Ihren Servern installieren. Informationen zum Abschließen dieser Einrichtung finden Sie in der vom Anbieter bereitgestellten Dokumentation.

Nachdem Ihre Netzwerkinfrastruktur korrekt eingerichtet ist, aktivieren Sie Multipathing auf Ihren Servern während der XenServer-Installation. Weitere Informationen finden Sie unter Multipathing aktivieren. Fahren Sie mit der Installation wie gewohnt fort.

Software-FCoE (veraltet)

Sie können einen XenServer-Host von einem FCoE-SAN aus starten, indem Sie einen Software-FCoE-Stack verwenden.

Für diese Art der Boot-from-SAN-Bereitstellung müssen Sie vor der Installation Ihres XenServer-Hosts die Konfiguration manuell abschließen, die erforderlich ist, um eine LUN für den Host verfügbar zu machen. Diese manuelle Konfiguration umfasst die Konfiguration der Storage-Fabric und die Zuweisung von LUNs zum Public Worldwide Name (PWWN) Ihres SAN. Nachdem Sie diese Konfiguration abgeschlossen haben, wird die verfügbare LUN als SCSI-Gerät in den CNA des Hosts eingebunden. Das SCSI-Gerät kann dann für den Zugriff auf die LUN verwendet werden, als wäre es ein lokal angeschlossenes SCSI-Gerät. Verwenden Sie beim Konfigurieren der FCoE-Fabric kein VLAN 0. Der XenServer-Host kann keinen Verkehr finden, der sich auf VLAN 0 befindet.

Informationen zum Konfigurieren des physischen Switches und des Arrays zur Unterstützung von FCoE finden Sie in der Dokumentation des Herstellers.

Nachdem Ihre Netzwerkinfrastruktur korrekt eingerichtet ist, aktivieren Sie Multipathing auf Ihren Servern während der XenServer-Installation. Weitere Informationen finden Sie unter Multipathing aktivieren. Fahren Sie mit der Installation wie gewohnt fort.

Bei einer manuellen Installation von XenServer haben Sie auf dem Bildschirm **Willkommen beim XenServer-Setup** die Möglichkeit, erweiterte Speicherklassen einzurichten. Drücken Sie **F10** und folgen Sie den Anweisungen auf dem Bildschirm, um die Software FCoE einzurichten.

Software-Start von iSCSI

Die Software-Boot-from-iSCSI-Funktion ermöglicht es Kunden, XenServer mithilfe von iSCSI vom SAN aus zu installieren und zu starten. Mit dieser Funktion kann XenServer auf einer LUN, die von einem iSCSI-Ziel bereitgestellt wird, installiert, gebootet und von dieser ausgeführt werden. Das iSCSI-Ziel ist in der iSCSI-Boot-Firmware-Tabelle angegeben. Mit dieser Funktion kann die Rootdatenträger über iSCSI angeschlossen werden. Dieser Startdatenträger kann sich auf demselben Ziel befinden, das eine SR bereitstellt.

Um diese Funktion nutzen zu können, stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

- Die Netzwerkschnittstelle oder Schnittstellen, die für den iSCSI-Boot vorgesehen sind, müssen von den Verwaltungsschnittstellen und Schnittstellen getrennt sein, die für den VM-Verkehr verwendet werden.
- Der Speicher (iSCSI-Ziele) muss sich in einem separaten Layer 3 (IP) -Netzwerk zu allen anderen Netzwerkschnittstellen mit IP-Adressen auf dem Host befinden.
- Verwenden Sie kein markiertes VLAN für die Netzwerkschnittstellen, die den iSCSI-Boot-Zielen zugewiesen sind.
- Wir empfehlen Ihnen, Multipathing auf Ihren Servern zu aktivieren.

Um die Software-Boot-from-iSCSI-Funktion zu konfigurieren, müssen Sie den `use_ibft` Parameter zu Ihren Boot-Parametern hinzufügen. Wie Sie diesen Parameter hinzufügen, hängt von Ihrem Startmodus und der Art der Installation ab, die Sie durchführen.

Aktivieren Sie die Software-Boot-from-iSCSI-Funktion auf einem UEFI-Boot-Server während einer Installation von lokalen Medien

1. Starten Sie den Computer vom Installationsmedium aus. Weitere Informationen finden Sie unter Installieren des XenServer-Hosts.

   Nach den ersten Startmeldungen sehen Sie ein GRUB-Menü. Dieses Menü wird für 5 Sekunden angezeigt.

2. Wählen Sie mit den Cursortasten eine Installationsoption aus:

   - Wählen Sie für eine LUN mit einem Pfad die Option **Installieren**aus.
   - Wählen Sie für eine LUN mit mehreren Pfaden die Option **Multipath** (empfohlen) aus.

3. Drücken Sie die e Taste, um die Befehle vor dem Booten zu bearbeiten.

4. Bearbeiten Sie die Zeile, beginnend mit dem Folgenden:

   ```
   module2 /EFI/xenserver/vmlinuz ...
   <!--NeedCopy-->
   ```

   Bearbeiten Sie diese Zeile mit den Cursortasten so, dass sie `use_ibft` am Ende Folgendes enthält:

   ```
   module2 /EFI/xenserver/vmlinuz ... use_ibft
   <!--NeedCopy-->
   ```

5. Drücken Sie die **Eingabetaste**.

6. Setzen Sie den XenServer-Host-Installationsvorgang wie gewohnt fort.

Aktivieren Sie die Software-Boot-from-iSCSI-Funktion auf einem BIOS-Boot-Server während einer Installation von einem lokalen Medium

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

1. Starten Sie den Computer vom Installationsmedium aus. Weitere Informationen finden Sie unter Installieren des XenServer-Hosts.

   Nach den ersten Startmeldungen wird der Bildschirm **Willkommen bei XenServer** angezeigt.

2. Geben Sie an der Startaufforderung ein `menu.c32`.

3. Wählen Sie mit den Cursortasten eine Installationsoption aus:

   - Wählen Sie für eine LUN mit einem Pfad die Option **Installieren**aus.
   - Wählen Sie für eine LUN mit mehreren Pfaden die Option **Multipath** aus.

4. Drücken Sie die Tabulatortaste.

5. Bearbeiten Sie die Zeile, die mit folgendem endet:

   ```
   ---  /install.img
   <!--NeedCopy-->
   ```

   Bearbeiten Sie diese Zeile mit den Cursortasten, um zu lesen:

   ```
   use_ibft ---  /install.img
   <!--NeedCopy-->
   ```

6. Drücken Sie die **Eingabetaste**.

7. Setzen Sie den XenServer-Host-Installationsvorgang wie gewohnt fort.

Aktivieren Sie die Software-Boot-from-iSCSI-Funktion auf einem UEFI-Boot-Server während einer PXE-Startinstallation Stellen Sie bei der Installation mit PXE sicher, dass Sie das Schlüsselwort **use_ibft** in den Kernelparametern hinzufügen. Wenn Multipathing erforderlich ist, müssen Sie **device_mapper_multipath=enabled**hinzufügen.

Beispiel:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16 dom0_mem=max
       :8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address>/<
       path_to_answer_file> install use_ibft device_mapper_multipath=
       enabled
    module2 /EFI/xenserver/install.img
     }
```



```
7
8 <!--NeedCopy-->
```

Weitere Informationen zum Einrichten von PXE-Start finden Sie unter Konfigurieren Ihres TFTP-Servers für PXE-Startmit UEFI.

Aktivieren Sie die Funktion Software-Boot-from-iSCSI auf einem BIOS-Boot-Server während einer PXE-Startinstallation

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

Stellen Sie bei der Installation mit PXE sicher, dass Sie das Schlüsselwort **use_ibft** in den Kernelparametern hinzufügen. Wenn Sie Multipathing verwenden (empfohlen), müssen Sie **device_mapper_multipath=enabled** hinzufügen.

Beispiel:

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
    append xenserver/xen.gz dom0_max_vcpus=1-16 \
    dom0_mem=max:8192M com1=115200,8n1 \
    console=com1,vga ---  xenserver/vmlinuz \
    console=hvc0 console=tty0 \
    answerfile=<http://pxehost.example.com/answer_file> \
    answerfile_device=<device> \
    use_ibft device_mapper_multipath=enabled ---  xenserver/install.img
<!--NeedCopy-->
```

Weitere Informationen zum Einrichten von PXE-Start finden Sie unter Konfigurieren Ihres TFTP-Servers für PXE-Startmit BIOS.

Multipathing aktivieren

Für eine vollständig redundante Boot-from-SAN-Umgebung müssen Sie mehrere Pfade für den I/O-Zugriff konfigurieren. Stellen Sie dazu sicher, dass auf dem Root-Gerät Multipath-Unterstützung aktiviert ist.

Wenden Sie sich an Ihren Speicheranbieter oder Administrator, um Informationen darüber zu erhalten, ob Multipath für Ihre SAN-Umgebung verfügbar ist.

> **Warnung:**
>
> Multipath-Einstellungen werden während des Upgrade-Vorgangs *nicht* vererbt. Folgen Sie bei der Aktualisierung mithilfe von ISO oder Netzwerkstart denselben Anweisungen wie im folgen-

> den Installationsvorgang, um sicherzustellen, dass die Konfiguration korrekt `multipath` ist.

Wenn mehrere Pfade verfügbar sind, aktivieren Sie Multipathing in Ihrer XenServer-Bereitstellung, während Sie den Installationsvorgang initialisieren. Wie Sie Multipathing aktivieren, hängt von Ihrem Startmodus und der Art der Installation ab, die Sie durchführen.

Multipathing auf einem UEFI-Boot-Server während einer manuellen Installation aktivieren

1. Starten Sie den Computer vom Installationsmedium aus. Weitere Informationen finden Sie unter Installieren des XenServer-Hosts.

   Nach den ersten Startmeldungen sehen Sie ein GRUB-Menü. Dieses Menü wird für 5 Sekunden angezeigt.

2. Wählen Sie im GRUB-Menü `multipath` und drücken Sie die **Eingabetaste**.

Der XenServer-Installationsprozess konfiguriert den XenServer-Host, der von einem Remote-SAN mit aktiviertem Multipathing bootet.

Multipathing auf einem BIOS-Boot-Server während einer manuellen Installation aktivieren

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

1. Starten Sie den Computer vom Installationsmedium aus. Weitere Informationen finden Sie unter Installieren des XenServer-Hosts.

   Nach den ersten Startmeldungen wird der Bildschirm **Willkommen bei XenServer** angezeigt.

2. Drücken Sie auf dem Willkommensbildschirm **F2**, um **Erweiterte** Installation auszuwählen.

3. Geben Sie an der Startaufforderung ein `multipath`.

Der XenServer-Installationsprozess konfiguriert den XenServer-Host, der von einem Remote-SAN mit aktiviertem Multipathing bootet.

Multipathing auf einem UEFI-Boot-Server während einer unbeaufsichtigten Installation aktivieren Um Dateisystem-Multipathing während der PXE-Installation zu aktivieren, fügen Sie es `device_mapper_multipath=enabled` zu Ihrer Konfigurationsdatei hinzu.

Beispiel:

```
menuentry "XenServer Install (serial)" {

    multiboot2 /EFI/xenserver/xen.gz dom0_max_vcpus=1-16 dom0_mem=max
       :8192M com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
       answerfile_device=eth0 answerfile=http://<ip_address>/<
       path_to_answer_file> install use_ibft device_mapper_multipath=
       enabled
    module2 /EFI/xenserver/install.img
     }

<!--NeedCopy-->
```

Weitere Informationen zum Einrichten von PXE-Start finden Sie unter Konfigurieren Ihres TFTP-Servers für PXE-Startmit UEFI.

Multipathing auf einem BIOS-Boot-Server während einer unbeaufsichtigten Installation aktivieren

> **Hinweis:**
>
> Das Booten von XenServer-Hosts im BIOS-Modus ist jetzt veraltet. Wir empfehlen, dass Sie Ihre XenServer 8-Hosts im UEFI-Startmodus installieren.

Um Dateisystem-Multipathing während der PXE-Installation zu aktivieren, fügen Sie es `device_mapper_multi` `=enabled` zu Ihrer Konfigurationsdatei hinzu.

Beispiel:

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
```



```
    append xenserver/xen.gz dom0_max_vcpus=1-16 \
    dom0_mem=max:8192M com1=115200,8n1 \
    console=com1,vga ---  xenserver/vmlinuz \
    console=hvc0 console=tty0 \
    answerfile=<http://pxehost.example.com/answer_file> \
    answerfile_device=<device> \
    device_mapper_multipath=enabled \
    install ---  xenserver/install.img
<!--NeedCopy-->
```

Weitere Informationen zum Einrichten von PXE-Start finden Sie unter Konfigurieren Ihres TFTP-Servers für PXE-Startmit BIOS.

Zusätzliche Pakete installieren

Zusätzliche Pakete werden verwendet, um die Funktionen von XenServer zu ändern und zu erweitern, indem Software in der Steuerdomäne (dom0) installiert wird. Ein OEM-Partner könnte beispielsweise XenServer mit einer Reihe von Verwaltungstools ausliefern, für die SNMP-Agenten installiert werden müssen. Sie können ein zusätzliches Paket entweder während der ersten XenServerinstallation oder jederzeit danach auf einer laufenden XenServer-Instanz installieren.

Wenn Sie Zusatzpakete während der XenServer-Installation installieren, entpacken Sie jedes Zusatzpaket in ein separates Verzeichnis auf einem Webserver.

Sie können das Zusatzpaket auf eine der folgenden Arten installieren:

- Wenn Sie während einer interaktiven Installation aufgefordert werden, zusätzliche Pakete zu installieren, geben Sie die URL zu den Zusatzpaketmedien an.
- Wenn Sie eine Antwortdatei für Ihre Installation verwenden, fügen Sie ein zusätzliches `<source>` Element hinzu, um den Speicherort des Zusatzpakets anzugeben.

Treiberdatenträger installieren

Sie können einen Treiberdatenträger mit einer der folgenden Methoden installieren:

- Mit XenCenter (empfohlen)
- Während einer sauberen XenServer-Installation
- Mit der Xe-CLI

Informationen zum Installieren eines Treiberdatenträgers mithilfe von XenCenter finden Sie unter Treiberdatenträger installieren. Informationen zur Installation eines Treiberdatenträgers während einer XenServer-Neuinstallation finden Sie unter Installieren des XenServer-Hosts.

Starten Sie nach der Installation des Treibers Ihren Server neu, damit die neue Version des Treibers wirksam wird. Wie bei jedem Softwareupdate empfehlen wir Ihnen, Ihre Daten zu sichern, bevor Sie einen Treiberdatenträger installieren.

Treiberdatenträger mithilfe der xe-CLI installieren

Führen Sie die folgenden Schritte aus, um den Treiberdatenträger mithilfe der Xe-CLI remote zu installieren:

1. Laden Sie den Treiberdatenträger an einen bekannten Ort auf einem Computer herunter, auf dem die Remote-XE-CLI installiert ist.
2. Extrahieren Sie den Inhalt der Zip-Datei.

   Stellen Sie für den nächsten Schritt sicher, dass Sie das Treiber-ISO verwenden und nicht das ISO, das die Quelldateien enthält.
3. Laden Sie den Treiberdatenträger hoch:

   ```
   xe [connection_parameters] update-upload file-name=
   <!--NeedCopy-->
   ```

   Die UUID des Treiberdatenträgers wird zurückgegeben, wenn der Upload abgeschlossen ist.
4. Wenden Sie den Treiberdatenträger an:

   ```
   xe [connection_parameters] update-apply uuid=
   <!--NeedCopy-->
   ```
5. Starten Sie den Host neu, um die Installation abzuschließen. Der Treiber wird erst wirksam, nachdem der Host neu gestartet wurde.

---

layout: doc
description: Upgrade from older versions of XenServer. You can complete the update manually or automatically.—

Upgrade von Citrix Hypervisor 8.2 Kumulatives Update 1

Durch ein Upgrade von einer vorhandenen Installation von Citrix Hypervisor 8.2 Cumulative Update 1 auf XenServer 8 können Sie Ihre vorhandenen VMs, SRs und Konfiguration beibehalten.

Führen Sie ein rollendes Pool-Upgrade durch, um alle vom Pool angebotenen Dienste und Ressourcen verfügbar zu halten und gleichzeitig alle Hosts im Pool zu aktualisieren. Bei dieser Upgrade-Methode

wird jeweils nur ein XenServer-Host offline geschaltet. Kritische VMs werden während des Vorgangs am Laufen gehalten, indem die VMs live auf andere Hosts im Pool migriert werden.

Sie können ein Rolling-Pool-Upgrade auf eine der folgenden Arten abschließen:

- Wenn Sie über eine Premium Edition-Lizenz verfügen, können Sie den XenCenter **Rolling Pool Upgrade-Assistenten** verwenden. Dieser Assistent organisiert den Upgrade-Pfad automatisch und führt Sie durch das Upgrade-Verfahren.

  Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.

- Sie können die Xe-CLI verwenden, um ein Rolling-Pool-Upgrade manuell durchzuführen, indem Sie laufende VMs zwischen XenServer-Hosts entsprechend live migrieren.

  Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe der Xe-CLI.

Kann ich ein Upgrade durchführen?

Stellen Sie sicher, dass Sie auf XenServer 8 aktualisieren können:

- Führen Ihre Hosts derzeit Citrix Hypervisor 8.2 Cumulative Update 1 aus?

  Wenn nicht, können Sie nicht direkt auf XenServer 8 aktualisieren. Führen Sie stattdessen eine Neuinstallation durch. Weitere Informationen finden Sie unter Installation.

  Wenn Sie XenServer 8 bereits verwenden, versuchen Sie nicht, das Update mit der Installations-ISO durchzuführen. Wenden Sie stattdessen Updates an, um Ihren XenServer 8-Pool auf den neuesten Stand zu bringen. Weitere Informationen finden Sie unter Updates anwenden.

- Verwenden Sie ein unterstütztes Partitionslayout?

  Das Legacy-Partitionslayout wird nicht mehr unterstützt. Wenn Sie es verwenden, können Sie möglicherweise nicht auf XenServer 8 aktualisieren. Weitere Informationen finden Sie unter Legacy-Partitionslayout.

- Verwenden Sie die virtuelle Appliance des Citrix Licensing Servers?

  In früheren Versionen haben wir die virtuelle Linux-basierte License Server-Appliance unterstützt. Dieses Produkt wird nicht mehr unterstützt. Wenn Sie die virtuelle License Server-Appliance mit einem vorhandenen Pool verwenden, migrieren Sie zur neuesten Version von Citrix License Server für Windows, bevor Sie auf XenServer 8 aktualisieren. Weitere Informationen finden Sie unter Lizenzierung.

- Ist die Schlüsselgröße des Identitätszertifikats des Servers kleiner als 2048 Byte?

  Wenn Ihr Pool zuerst mit XenServer 7.6 oder früher installiert wurde, verfügt er möglicherweise noch über Zertifikate mit einer kleineren Schlüsselgröße als 2048 Byte. In diesem Fall zeigt der

Upgrade-Assistent beim Versuch, ein Upgrade auf XenServer 8 durchzuführen, bei den Vorprüfungen einen Fehler an. Um mit dem Upgrade fortzufahren, müssen Sie das selbstsignierte Zertifikat auf jedem betroffenen Server zurücksetzen, indem Sie den folgenden Befehl ausführen:

```
1  xe host-emergency-reset-server-certificate
```

Dieser Befehl kann den laufenden Betrieb im Pool unterbrechen.

- Ist Ihre Hardware mit XenServer 8 kompatibel?

  Stellen Sie sicher, dass die Hardware, auf der Ihr Pool installiert ist, mit der Version von XenServer kompatibel ist, auf die Sie aktualisieren möchten. Weitere Informationen finden Sie in der Hardwarekompatibilitätsliste (HCL).

- Werden Ihre VM-Betriebssysteme von XenServer 8 unterstützt?

  Überprüfen Sie, ob die Betriebssysteme Ihrer VMs von XenServer 8 unterstützt werden. Wenn Ihr VM-Betriebssystem nicht unterstützt wird, aktualisieren Sie Ihr VM-Betriebssystem auf eine unterstützte Version, bevor Sie XenServer aktualisieren. Weitere Informationen finden Sie unter Unterstützung für Gastbetriebssysteme.

- Verwenden Sie XenServer, um Ihre Citrix Virtual Apps and Desktops-Workloads zu hosten?

  Wenn Sie Ihre Citrix Virtual Apps and Desktops-Lizenz verwenden, um Ihr Citrix Hypervisor 8.2 Cumulative Update 1 zu lizenzieren, gilt diese Lizenz nicht mehr für XenServer 8. Sie müssen stattdessen eine Xenserver Premium Edition-Lizenz erwerben. Weitere Informationen finden Sie unter https://xenserver.com/buy.

  Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

  Wenden Sie Ihre neuen Lizenzen auf Ihren Pool an, bevor Sie mit dem Upgrade beginnen.

  Sie können ein Upgrade auf XenServer 8 durchführen, indem Sie die in diesem Artikel beschriebenen Methoden verwenden. Abhängig von Ihrer XenServer-Umgebung und Ihrer Citrix Virtual Apps and Desktops-Workload müssen jedoch möglicherweise bestimmte Verhaltensweisen und Anforderungen berücksichtigt werden, die Ihren XenServer-Upgrade-Prozess optimieren können. Weitere Informationen finden Sie unter Upgrade-Szenarien für Citrix Virtual Apps and Desktops.

Vorbereitung

Lesen Sie die folgenden Informationen, bevor Sie mit dem Upgrade beginnen. Ergreifen Sie die erforderlichen Schritte, um sicherzustellen, dass Ihr Upgradevorgang erfolgreich ist.

Plan für das Upgrade

1. Ordnen Sie Ihren Verbesserungspfad sorgfältig zu Das Upgrade von XenServer-Hosts, insbesondere eines Pools von XenServer-Hosts, erfordert sorgfältige Planung und Aufmerksamkeit, um den Verlust vorhandener Daten zu vermeiden.

   Beachten Sie bei der Planung Ihres Upgrades die folgenden Informationen:

   - Sie können eine VM nicht von einer neueren Version von XenServer auf eine ältere migrieren.
   - Betreiben Sie Ihren Pool nicht länger als nötig im gemischten Modus (mit mehreren Versionen von XenServer). Der Pool arbeitet während des Upgrades in einem heruntergestuften Zustand.
   - Schlüsselsteuerungsvorgänge sind während des Upgradevorgangs nicht verfügbar. Versuchen Sie nicht, Steuervorgänge durchzuführen.
   - Kopieren, fahren oder exportieren Sie keine virtuellen Maschinen während des Upgrade-Vorgangs.
   - Führen Sie während des Upgrade-Vorgangs keine speicherbezogenen Vorgänge wie das Hinzufügen, Entfernen oder Ändern der Größe virtueller Laufwerke aus.
   - Während des Upgrades des Poolkoordinators wechseln die anderen Hosts im Pool in den *Notfallmodus*.

2. Stellen Sie sicher, dass Ihre Server nicht übermäßig bereitgestellt werden: Überprüfen Sie, ob die Server über ausreichend Arbeitsspeicher verfügen, um das Upgrade durchzuführen.

   Wenn N der Gesamtzahl der Server in einem Pool entspricht, muss im Allgemeinen genügend Arbeitsspeicher auf den N-1-Servern vorhanden sein, um alle Live-VMs im Pool auszuführen. Es empfiehlt sich, alle nicht kritischen VMs während des Upgradevorgangs auszusetzen.

3. Stellen Sie sicher, dass Ihr Pool über gemeinsam genutzten Speicher verfügt, damit Ihre VMs während eines Rolling-Pool-Upgrades am Laufen bleiben. Wenn Ihr Pool keinen gemeinsam genutzten Speicher hat, müssen Sie Ihre VMs vor dem Upgrade anhalten, da die VMs nicht live migriert werden können.

   Die Speicher-Livemigration wird bei Rollpool-Upgrades nicht unterstützt.

4. Wenn Sie Ihre Citrix Virtual Apps and Desktops-Lizenz verwenden, um Ihr Citrix Hypervisor 8.2 Cumulative Update 1 zu lizenzieren, wenden Sie stattdessen eine Xenserver Premium Edition-Lizenz auf alle Hosts im Pool an. Weitere Informationen finden Sie unter https://xenserver.com/buy.

5. Wenn Sie ein Rolling-Pool-Upgrade von Citrix Hypervisor 8.2 CU1 auf XenServer 8 durchführen, können Sie Workload Balancing 8.2.2 und früher nicht mit Ihren XenServer 8-Pools verwenden. Aktualisieren Sie Ihre virtuelle Workload Balancing-Appliance auf Version 8.3.0, bevor Sie das

Rolling Pool-Upgrade durchführen. Sie können die neueste Version der virtuellen Workload Balancing-Appliance von der XenServer-Downloadseite herunterladen.

6. Beachten Sie die folgenden Verhaltensweisen:

   - Das Upgrade muss denselben Startmodus wie die Erstinstallation verwenden.
   - Boot-from-SAN-Einstellungen werden während des manuellen Upgrade-Vorgangs *nicht* vererbt. Wenn Sie ein Upgrade mit dem ISO- oder PXE-Prozess durchführen, müssen Sie sicherstellen, dass `multipathd` es korrekt konfiguriert ist. Weitere Informationen finden Sie unter Booten von SAN.
   - Wenn Sie XenServer aktualisieren, werden zuvor angewendete Zusatzpakete entfernt und müssen daher während oder nach dem Upgrade erneut angewendet werden. Das PVS-Accelerator Supplemental Pack muss jedoch nicht mehr auf XenServer 8 installiert werden. Seine Funktionen sind jetzt in der Hauptinstallation des Produkts enthalten.

Bereite deinen Pool vor

1. Erstellen Sie mit dem xe-Befehl CLI eine Backup des Status Ihres vorhandenen Pools `xe pool-dump-database`.

   Durch das Erstellen eines Backups des Status wird sichergestellt, dass Sie ein teilweise vollständiges fortlaufendes Upgrade in den ursprünglichen Zustand zurücksetzen können, ohne VM-Daten zu verlieren.

2. Deaktivieren Sie die Hochverfügbarkeit.

Bereiten Sie Ihre VMs vor

1. Wenn in Ihrem Pool Windows-VMs ausgeführt werden, führen Sie für jede VM die folgenden Schritte aus:

   - Stellen Sie sicher, dass die neueste Version der XenServer VM Tools für Windows installiert ist.
   - Erstellen Sie einen Snapshot der VM.

2. Wenn in Ihrem Pool Linux-VMs ausgeführt werden, stellen Sie sicher, dass die neueste Version der XenServer VM Tools für Linux installiert ist.
3. Wenn in Ihrem Pool NVIDIA-vGPU-fähige VMs ausgeführt werden, führen Sie die folgenden Schritte aus, um den Pool zu migrieren, während diese VMs laufen:

   a) Stellen Sie sicher, dass die von Ihnen verwendete GPU von der Version unterstützt wird, auf die Sie ein Upgrade planen.

b) Identifizieren Sie eine Version der NVIDIA GRID-Treiber, die sowohl für Ihre aktuelle Version von Citrix Hypervisor oder XenServer als auch für die Version von XenServer verfügbar ist, auf die Sie aktualisieren. Wenn möglich, wählen Sie die neuesten verfügbaren Treiber.
c) Installieren Sie die neuen GRID-Treiber auf Ihren XenServer-Hosts und die passenden Gasttreiber auf einer Ihrer vGPU-fähigen VMs.
d) Stellen Sie sicher, dass Sie auch über die Version des GRID-Treibers verfügen, die der XenServer-Version entspricht, auf die Sie aktualisieren. Sie werden aufgefordert, diese Treiber als zusätzliches Paket im Rahmen des Rolling Pool-Upgrade-Prozesses zu installieren.

4. Leeren Sie die CD/DVD-Laufwerke aller VMs im Pool.

Holen Sie sich die erforderlichen Dateien

1. Wenn Sie XenCenter zum Upgrade Ihrer Hosts verwenden, laden Sie die neueste Version von XenCenter von der XenServer-Downloadseite herunter und installieren Sie sie.

   Weitere Informationen finden Sie unter Installieren von XenCenter.

2. Laden Sie die XenServer 8-Installations-ISO von der XenServer-Downloadseite herunter.
3. Bereiten Sie das Installationsmedium vor:

   - Um Ihre Hosts von einem bootfähigen USB aus zu aktualisieren, verwenden Sie ein Tool wie `rufus` oder erstellen `diskpart` Sie ein bootfähiges USB mithilfe der XenServer 8-Installations-ISO. Stellen Sie sicher, dass das Tool den Inhalt der ISO-Datei nicht ändert.
   - Um Ihre Hosts von einer CD zu aktualisieren, brennen Sie die XenServer 8-Installations-ISO-Datei auf eine CD.
   - Um Ihre Hosts von Virtual Media zu aktualisieren, rufen Sie die virtuelle Konsole Ihres Systems auf und mounten Sie die XenServer-Installations-ISO-Datei als Virtual Media.
   - So führen Sie ein Upgrade von einem Netzwerkstandort aus durch:

     a) Richten Sie einen über das Netzwerk zugänglichen TFTP-Server ein, von dem aus das Installationsprogramm gestartet werden kann.

     b) Richten Sie einen Netzwerkpfad ein, über den Sie über HTTP, FTP oder NFS auf das Installations-ISO zugreifen können.

     c) Entpacken Sie das Installations-ISO in den Netzwerkordner.

        Wenn Sie IIS zum Hosten des Installationsmediums verwenden, stellen Sie sicher, dass das doppelte Escaping auf IIS aktiviert ist, bevor Sie das Installations-ISO-Image darauf extrahieren.

d) Notieren Sie sich die Informationen, die Sie während des Upgrades benötigen:

- Notieren Sie sich für HTTP oder FTP die URL für Ihr HTTP- oder FTP-Repository und gegebenenfalls einen Benutzernamen und ein Kennwort.
- Notieren Sie sich für NFS den Server und den Pfad Ihres NFS-Shares.

Weitere Informationen finden Sie unter Netzwerkstart.

Nachdem diese erforderlichen Schritte abgeschlossen sind, können Sie ein Rolling-Pool-Upgrade mit einer der folgenden Methoden durchführen:

- Rolling-Pool-Upgrade mit XenCenter
- Rolling-Pool-Upgrade mit der Xe-CLI

Rolling-Pool-Upgrade mit XenCenter

Der **Rolling Pool-Upgrade-Assistent** führt Sie durch den Upgradevorgang und organisiert den Upgrade-Pfad automatisch. Bei Pools wird jeder der Server im Pool nacheinander aktualisiert, beginnend mit dem
Poolkoordinator. Bevor Sie ein Upgrade starten, führt der Assistent eine Reihe von Vorprüfungen durch. Diese Vorabprüfungen stellen sicher, dass bestimmte poolweite Funktionen, wie z. B. Hochverfügbarkeit, vorübergehend deaktiviert sind und dass jeder Server im Pool für das Upgrade vorbereitet
ist. Es ist jeweils nur ein Server offline. Alle laufenden VMs werden automatisch von jedem Server migriert, bevor das Upgrade auf diesem Server installiert wird.

> **Hinweis:**
>
> Der XenCenter **Rolling Pool Upgrade-Assistent** ist nur verfügbar, wenn Sie über eine Premium Edition-Lizenz verfügen.

Wenn Sie XenCenter noch nicht installiert haben, laden Sie die neueste Version von der XenServer-Downloadseite herunter und führen Sie die Schritte unter XenCenter installieren aus.

Der Assistent kann im manuellen oder automatischen Modus arbeiten:

- Im manuellen Modus müssen Sie das XenServer-Installationsprogramm nacheinander auf jedem Server manuell ausführen und den Anweisungen auf dem Bildschirm auf der seriellen Konsole des Servers folgen. Wenn das Upgrade beginnt, fordert XenCenter Sie auf, das Installationsmedium einzulegen oder für jeden Server, den Sie aktualisieren, einen Netzwerk-Boot-Server anzugeben.
- Im automatischen Modus verwendet der Assistent Netzwerkinstallationsdateien auf einem HTTP-, NFS- oder FTP-Server, um die einzelnen Server nacheinander zu aktualisieren. In

diesem Modus müssen Sie kein Installationsmedium einlegen, manuell neu starten oder das Installationsprogramm auf jedem Server schrittweise durchlaufen. Wenn Sie auf diese Weise ein Rolling-Pool-Upgrade durchführen, müssen Sie das Installationsmedium auf Ihrem HTTP-, NFS- oder FTP-Server entpacken, bevor Sie mit dem Upgrade beginnen.

Aktualisieren von XenServer-Hosts mithilfe des XenCenter Rolling Pool-Upgradeassistenten:

1. Wählen Sie im Menü XenCenter **Tools** die Option **Rolling Pool Upgrade**aus.
2. Lesen Sie die Informationen **Bevor Sie beginnen** . Klicken Sie zum Fortfahren auf **Weiter**.
3. Wählen Sie die Pools und alle einzelnen Hosts aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie einen der folgenden Modi:

   - **Automatischer Modus** für ein automatisiertes Upgrade von Netzwerkinstallationsdateien auf einem HTTP-, NFS- oder FTP-Server.

     Wenn Sie den **automatischen Modus** wählen und IIS zum Hosten des Installationsmediums verwenden, stellen Sie sicher, dass das doppelte Escaping auf IIS aktiviert ist, bevor Sie das Installations-ISO-Image darauf extrahieren.

   - **Manueller Modus** für ein manuelles Upgrade entweder von einem USB/CD/DVD oder mithilfe des Netzwerkstarts (unter Verwendung der vorhandenen Infrastruktur).

     Wenn Sie den **manuellen Modus**wählen, müssen Sie das XenServer-Installationsprogramm nacheinander auf jedem Host ausführen. Befolgen Sie die Anweisungen auf dem Bildschirm auf der seriellen Konsole des Hosts. Wenn das Upgrade beginnt, fordert XenCenter Sie auf, das XenServer-Installationsmedium einzulegen oder für jeden Host, den Sie aktualisieren, einen Netzwerkbootserver anzugeben.

5. Nachdem Sie den Upgrade-Modus ausgewählt haben, klicken Sie auf **Vorabprüfungen ausführen**.
6. Befolgen Sie die Empfehlungen, um fehlgeschlagene Upgrade-Vorprüfungen zu beheben. Wenn XenCenter alle fehlgeschlagenen Vorprüfungen automatisch auflösen soll, klicken Sie auf **Alle auflösen**.

   > **Hinweis:**
   >
   > Einige Prechecks können nicht automatisch aufgelöst werden. Wenn Ihre Hosts beispielsweise eine Citrix Virtual Apps and Desktops-Lizenz verwenden, zeigt XenCenter an, dass diese Lizenz nicht für XenServer 8-Hosts gilt. Sie können kein Upgrade durchführen, bis Sie eine XenServer Premium Edition-Lizenz erhalten haben. Weitere Informationen finden Sie unter https://xenserver.com/buy.

7. Wenn alle Vorprüfungen gelöst wurden, klicken Sie auf **Weiter**, um fortzufahren.

8. Bereiten Sie das XenServer-Installationsmedium vor.

   - Wenn Sie den **automatischen Modus**gewählt haben, geben Sie die Details zum Installationsmedium ein. Wählen Sie **HTTP**, **NFS**oder **FTP** und geben Sie dann je nach Bedarf die URL, den Benutzernamen und das Kennwort an.

     > **Hinweise:**
     >
     > ```
     > - Wenn Sie FTP wählen, achten Sie darauf, dass Sie alle führenden Schrägstriche im Dateipfadabschnitt der URL umgehen.
     >
     > - Geben Sie den Benutzernamen und das Kennwort für Ihren HTTP- oder FTP-Server ein, falls Sie Sicherheitsanmeldeinformationen konfiguriert haben. Geben Sie nicht den Benutzernamen und das Kennwort für Ihren XenServer-Pool ein.
     >
     > - XenServer unterstützt FTP nur im passiven Modus.
     > ```

   - Wenn Sie den **manuellen Modus**gewählt haben, notieren Sie sich den Upgrade-Plan und folgen Sie den Anweisungen.

9. Klicken Sie auf **Upgrade starten**.
10. Wenn das Upgrade beginnt, führt Sie der **Rolling Pool Upgrade-Assistent** durch alle Aktionen, die Sie für das Upgrade der einzelnen Hosts ergreifen müssen. Befolgen Sie die Anweisungen, bis Sie alle Hosts in den Pools aktualisiert und aktualisiert haben.
11. Wenn Sie über vGPU-fähige VMs verfügen und den Schritt erreicht haben, der Ihnen die Option bietet, ein zusätzliches Paket bereitzustellen, laden Sie den NVIDIA-Treiber hoch, der mit dem Treiber auf Ihren vGPU-fähigen VMs übereinstimmt. Stellen Sie sicher, dass Sie die Version des Treibers für die XenServer-Version hochladen, auf die Sie aktualisieren.
12. Der **Rolling Pool-Upgrade-Assistent** gibt eine Zusammenfassung aus, wenn das Upgrade abgeschlossen ist. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

> **Hinweis:**
>
> Wenn das Upgrade oder des Updatessvorgang aus irgendeinem Grund fehlschlägt, stoppt der **Rolling Pool Upgrade-Assistent** den Vorgang. Auf diese Weise können Sie das Problem beheben und den Upgrade- odes Updatessvorgang fortsetzen, indem Sie auf die Schaltfläche **Wiederholen** klicken.

Nach dem Upgrade

Nach dem Upgrade Ihres Pools empfehlen wir Ihnen, die folgenden Aufgaben auszuführen:

- Aktivieren Sie die Funktion zur Zertifikatsüberprüfung. Weitere Informationen finden Sie unter Zertifikatsverifizierung.
- Konfigurieren Sie Updates und wenden Sie das neueste Set an. Weitere Informationen finden Sie unter XenServer-Hosts aktualisieren.

Nach Abschluss eines Rolling-Pool-Upgrades befindet sich eine VM möglicherweise nicht auf ihrem Home-Host. Um die VM zu verlagern, können Sie eine der folgenden Aktionen ausführen:

- Migrieren Sie die VM live auf ihren Home-Host
- Fahren Sie die VM herunter und starten Sie sie dann auf ihrem Home-Host

Rolling-Pool-Upgrade mit der Xe-CLI

Bevor Sie ein Rolling Pool-Upgrade über die xe-CLI durchführen, stellen Sie sicher, dass Sie alle erforderlichen Schritte unter Bevor Sie beginnen ausgeführt haben.

> **Wichtig:**
>
> Stellen Sie sicher, dass Sie alle Server in Ihrem Pool aktualisieren. Wir raten dringend davon ab, einen Pool im gemischten Modus (einen mit mehreren XenServer-Versionen) länger als nötig auszuführen, da der Pool während des Upgrades in einem heruntergestuften Zustand betrieben wird.
>
> Schlüsselsteuerungsvorgänge sind während des Upgradevorgangs nicht verfügbar. Versuchen Sie nicht, Steuervorgänge durchzuführen. Obwohl VMs weiterhin wie gewohnt funktionieren, sind andere VM-Aktionen als die Migration nicht verfügbar (z. B. Herunterfahren, Kopieren und Exportieren). Insbesondere ist es nicht sicher, speicherbezogene Vorgänge wie das Hinzufügen, Entfernen oder Ändern der Größe virtueller Laufwerke auszuführen.

So führen Sie ein Rolling-Pool-Upgrade mit der Xe-CLI durch:

Beginnen Sie mit dem Poolkoordinator:

1. Deaktivieren Sie den Poolkoordinator. Dadurch wird verhindert, dass neue VMs auf dem angegebenen Host gestartet oder auf diesen migriert werden.

   ```
   xe host-disable host-selector=<host_selector_value>
   ```

2. Stellen Sie sicher, dass keine VMs auf dem Poolkoordinator ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:

     ```
     xe vm-shutdown
     ```

   - Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:


```
xe vm-suspend
```

- Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

```
xe vm-migrate
```

Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

- Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

```
xe host-evacuate
```

Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

3. Fahren Sie den Poolkoordinator herunter.

```
xe host-shutdown
```

> **Wichtig:**
>
> Sie können den Poolkoordinator erst kontaktieren, wenn das Upgrade des Poolkoordinators abgeschlossen ist. Durch das Herunterfahren des Poolkoordinators wechseln die anderen Hosts im Pool in den *Notfallmodus*. Hosts können in den Notfallmodus wechseln, wenn sie sich in einem Pool befinden, dessen Poolkoordinator aus dem Netzwerk verschwunden ist und nach mehreren Versuchen nicht kontaktiert werden kann. Virtuelle Rechner werden im Notfallmodus weiterhin auf Hosts ausgeführt, Steuervorgänge sind jedoch nicht verfügbar.

4. Starten Sie den Poolkoordinator mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).
5. Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.

   Wenn Ihr Poolkoordinator neu gestartet wird, verlassen die anderen Hosts im Pool den Notfallmodus und der normale Dienst wird nach einigen Minuten wiederhergestellt.
6. Starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.
7. Migrieren Sie alle gewünschten VMs zurück zum Poolkoordinator.

Wenn das Upgrade des Poolkoordinators durch irgendetwas unterbrochen wird oder das Upgrade aus irgendeinem Grund fehlschlägt, versuchen Sie nicht, mit dem Upgrade fortzufahren. Starten Sie den Poolkoordinator neu und stellen Sie eine funktionierende Version wieder her.

Wiederholen Sie diese Schritte für alle anderen Hosts im Pool:

1. Wählen Sie den nächsten XenServer-Host in Ihrem Upgrade-Pfad aus. Deaktivieren Sie den Host.

```
xe host-disable host-selector=<host_selector_value>
```

2. Stellen Sie sicher, dass keine virtuellen Maschinen auf dem Host ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:

```
xe vm-shutdown
```

   - Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:

```
xe vm-suspend
```

   - Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

```
xe vm-migrate
```

     Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

```
xe host-evacuate
```

     Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

3. Fahren Sie den Host herunter.

```
xe host-shutdown
```

4. Starten Sie den Host mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).
5. Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.
6. Nachdem das Host-Upgrade abgeschlossen ist, starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.
7. Migrieren Sie alle virtuellen Maschinen, die Sie möchten, zurück zum Host.

Wenn das Upgrade eines untergeordneten Hosts fehlschlägt oder unterbrochen wird, müssen Sie es nicht rückgängig machen. Führen Sie den Befehl `xe host-forget` im Pool aus, um diesen Host zu vergessen. Installieren Sie XenServer erneut auf dem Host und fügen Sie ihn dann mit dem Befehl `xe pool-join`als neuen Host dem Pool hinzu.

Nach dem Upgrade

Nach dem Upgrade Ihres Pools empfehlen wir Ihnen, die folgenden Aufgaben auszuführen:

- Aktivieren Sie die Funktion zur Zertifikatsüberprüfung. Weitere Informationen finden Sie unter Zertifikatsverifizierung.
- Konfigurieren Sie Updates und wenden Sie das neueste Set an. Weitere Informationen finden Sie unter XenServer-Hosts aktualisieren.

Nach Abschluss eines Rolling-Pool-Upgrades befindet sich eine VM möglicherweise nicht auf ihrem Home-Host. Um die VM zu verlagern, können Sie eine der folgenden Aktionen ausführen:

- Migrieren Sie die VM live auf ihren Home-Host
- Fahren Sie die VM herunter und starten Sie sie dann auf ihrem Home-Host

Andere Szenarios

Legacy Partitionslayout

Das Legacy-Partitionslayout wird nicht mehr unterstützt. Wenn Sie es verwenden, können Sie möglicherweise kein Upgrade auf XenServer 8 durchführen und müssen stattdessen eine Neuinstallation durchführen.

XenServer 6.5 und früher verwendet eine 4 GB Control Domain (dom0) -Partition für alle dom0-Funktionen, einschließlich Swap und Protokollierung. Diese Partitionskonfiguration wird als Legacy-Partitionslayout bezeichnet. In späteren Versionen von XenServer und Citrix Hypervisor wurde ein Partitionslayout eingeführt, das die Steuerdomänenpartition auf 18 GB erhöhte und eine separate Protokollierungspartition enthielt. In XenServer 8 wird nur das neuere Partitionslayout unterstützt.

Woher weiß ich, welches Partitionslayout mein Server verwendet? In den folgenden Fällen haben Sie möglicherweise das Legacy-Partitionslayout auf Ihren XenServer-Hosts:

- Sie haben Ihren XenServer-Host ursprünglich mit XenServer 5.6 Service Pack 2 oder früher installiert und seitdem auf spätere unterstützte Versionen aktualisiert.
- Sie verwenden alte Hardware mit weniger als 46 GB primärem Speicherplatz.
- Ihre Hardware erfordert, dass eine Utility-Partition vorhanden ist.

Um herauszufinden, wie viele Partitionen Ihr XenServer-Host hat, führen Sie den folgenden Befehl in der
Serverkonsole aus:


```
fdisk -l
```

- Wenn der Befehl 6 Partitionen auflistet, verwenden Sie das neue Partitionslayout und können ein Upgrade auf XenServer 8 durchführen.
- Wenn der Befehl 3 oder 4 Partitionen auflistet, verwenden Sie das Legacy-Partitionslayout.

Was kann ich als Nächstes tun? Wenn Sie das neue Partitionslayout verwenden, können Sie auf XenServer 8 aktualisieren.

Wenn Sie das Legacy-Partitionslayout verwenden:

- Wenn Sie weniger als 46 GB primären Speicherplatz haben oder für Ihre Hardware eine Dienstprogrammpartition erforderlich ist, können Sie XenServer 8 nicht installieren oder auf XenServer 8 aktualisieren.
- Wenn Ihr Datenträger GPT ist und das lokale Speicherrepository leer ist und mindestens 38 GB frei sind, können Sie während des Upgrades vom Legacy-Partitionslayout zum neuen Partitionslayout wechseln. Sie müssen XenCenter verwenden, um das Upgrade auf einem Server mit dem älteren Partitionslayout zu versuchen. Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.
- Für andere Hardware können Sie eine Neuinstallation von XenServer 8 abschließen. Weitere Informationen finden Sie unter Installation.

Citrix Virtual Apps and Desktops-Umgebungen

Wenn Sie XenServer zum Hosten Ihrer Citrix Virtual Apps and Desktops-Workloads verwenden, finden Sie weitere Informationen unter Upgrade-Szenarien für Citrix Virtual Apps andDesktops.

XenServer-Hosts aktualisieren

April 12, 2024

Mit XenServer 8 werden neue Funktionen und Bugfixes häufig als verfügbare Updates für Ihre XenServer-Hosts und -Pools an das Content Delivery Network (CDN) übertragen, sodass Sie von einem effizienteren Release-Prozess profitieren können, der Ihnen neue Inhalte schneller als bisher zur Verfügung stellt.

Um sicherzustellen, dass Sie immer über das neueste und beste Update verfügen, gibt es kein Aussuchen. Wenn Sie Updates auf Ihren Pool anwenden, wird er auf den neuesten, vollständig getesteten

Zustand aktualisiert. Konfigurieren Sie Ihren Pool so, dass er automatisch mit einem Updatekanal synchronisiert wird. Diese Aktion lädt alle verfügbaren Updates auf den Poolkoordinator herunter. Sie können dann alle heruntergeladenen Updates mithilfe von XenCenter oder der xe-CLI anwenden.

> **Hinweis:**
>
> Wenn Sie XenServer 8 während der Vorschauphase verwendet haben, müssen Sie Ihre Hosts nicht neu installieren oder aktualisieren, um auf die GA-Version umzusteigen. Wenden Sie die neuesten Updates über XenCenter an, um in der Produktion unterstützt zu werden.

Lebenszyklus

Während seines Lebenszyklus bietet XenServer 8 einen Strom häufiger und einfach anzuwendender Updates, mit denen Sie neue Funktionen und Bugfixes zum frühestmöglichen Zeitpunkt nutzen können. Sie müssen alle verfügbaren Updates regelmäßig anwenden. Infolgedessen können sich das Verhalten und der Funktionsumfang in XenServer 8 ändern.

Weitere Informationen finden Sie unter XenServer-Lebenszyklus.

Updatevorgang

Der XenServer 8-Release-Stream und das Content Delivery Network (CDN) arbeiten zusammen, sodass Sie häufige Updates von XenCenter aus auf Ihre XenServer-Hosts und -Pools anwenden können.

1. Wir stellen regelmäßige Updates für XenServer 8 in unserem sicheren CDN zur Verfügung.
2. Sehen Sie in XenCenter, wann Updates für Ihren Pool verfügbar sind.
3. Initiieren Sie mit XenCenter den Prozess der Installation von Updates auf Ihren XenServer-Pool.

Updatekanäle

Der XenServer 8-Release-Stream besteht aus zwei Phasen, die auch als Update-Kanäle bezeichnet werden:

- Früherer Zugang
- Normal

Um häufige Updates zu erhalten, konfigurieren Sie Ihren XenServer-Pool so, dass er einen dieser Update-Kanäle abonniert.

1. Wenn Updates zum ersten Mal an unser CDN gesendet werden, gelangen sie in den Early-Access-Updatekanal.

   Early Access eignet sich perfekt für Testumgebungen, sodass Sie die neuesten Updates erhalten, sobald sie der Öffentlichkeit zugänglich sind. Wenn Sie sich dafür entscheiden, Updates frühzeitig zu erhalten, haben Sie die Möglichkeit, sie zu testen, bevor sie dem normalen Updatekanal zur Verfügung gestellt werden.

   > **Hinweis:**
   >
   > Early Access wird für den Produktionseinsatz unterstützt. Wir empfehlen es jedoch nicht für kritische Produktionsumgebungen.

2. Diese Updates fließen dann sequentiell in Normal, den nächsten Updatekanal.

   Sofern wir diesen Fortschritt nicht verzögert haben, könnt ihr davon ausgehen, dass Early-Access-Updates in regelmäßigen Abständen im Normalmodus verfügbar werden. Normal wird für Produktionsumgebungen empfohlen.

Gelegentlich stellen Sie möglicherweise fest, dass Updates gleichzeitig für Ihren Early-Access-Pool und Ihren Normal-Pool verfügbar sind. Diese Updates ermöglichen es uns, Sicherheitspatches und kritische Fixes sofort für alle Update-Kanäle bereitzustellen.

Erste Schritte mit Updates

Informationen zum Konfigurieren und Anwenden von Updates für Ihre XenServer-Hosts mithilfe von XenCenter finden Sie unter Anwenden von Updates mit XenCenter. Alternativ können Sie die xe CLI verwenden, um Updates auf Ihre XenServer-Hosts anzuwenden. Weitere Informationen finden Sie unter Updates mit der xe-CLI anwenden.

> **Wichtig:**
>
> Wir unterstützen nicht die direkte Verwendung oder Änderung der zugrunde liegenden Update-Komponenten in dom0. Sie können nur XenCenter oder die xe CLI verwenden, um Updates zu konfigurieren und anzuwenden.

Wenden Sie Updates mithilfe von XenCenter an

April 12, 2024

Wenden Sie Updates auf Ihre XenServer 8-Hosts und -Pools an, indem Sie die neueste Version von XenCenter verwenden. Die neueste Version von XenCenter finden Sie auf der XenServer-Produktdownloadseite.

Um Update-Benachrichtigungen bereitzustellen, benötigt XenCenter Internetzugang. Wenn sich Ihr XenCenter hinter einer Firewall befindet, stellen Sie sicher, dass es Zugriff auf die Domäne `updates.ops.xenserver.com` hat. Um die Updates zu erhalten, benötigen Ihre XenServer-Hosts Internetzugang. Wenn sich Ihre Hosts hinter einer Firewall befinden, stellen Sie sicher, dass sie Zugriff auf Subdomains von `ops.xenserver.com` haben. Weitere Informationen finden Sie unter Konnektivitätsanforderungen.

Gehen Sie wie folgt vor, um Ihre XenServer-Pools aktualisieren zu können:

1. Installieren Sie die neueste Version von XenCenter.
2. Installieren oder führen Sie ein Upgrade auf XenServer 8 durch.
3. Konfigurieren Sie Updates für Ihren Pool.
4. Sehen Sie sich die verfügbaren Updates für Ihren Pool an.
5. Wenden Sie Updates auf Ihren Pool an.
6. Führen Sie die Updateaufgaben aus.

Updates für Ihren Pool konfigurieren

Bevor Sie Updates auf Ihre XenServer-Hosts und -Pools anwenden können, müssen Sie Hostupdates konfigurieren, indem Sie Ihren Pool oder Host für einen Update-Channel abonnieren. Diese Kanäle steuern, wie schnell Sie auf Updates zugreifen können, die im Content Delivery Network (CDN) verfügbar sind.

Die beiden Updatekanäle sind:

- Early Access —perfekt für Testumgebungen
- Normal —empfohlen für Produktionsumgebungen

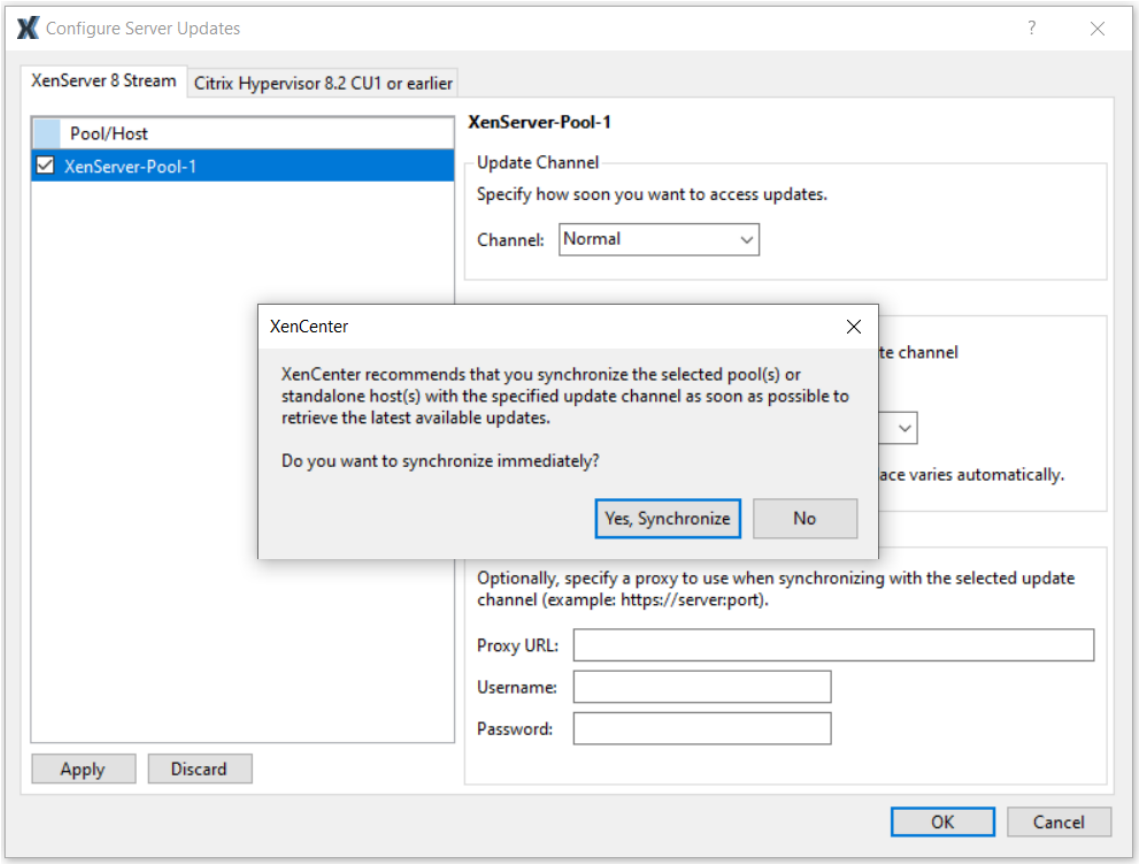
Nachdem Sie Ihren Pool bei einem des Updatesskanäle abonniert haben, synchronisiert sich Ihr Pool regelmäßig und automatisch mit dem Updatekanal. Diese Aktion lädt alle verfügbaren Updates auf den Poolkoordinator herunter. Sie können dann alle heruntergeladenen Updates mithilfe von XenCenter anwenden.

1. Wählen Sie in XenCenter im Menü **Tools** die Option Updates **konfigurieren**aus. Gehen Sie alternativ zum Abschnitt **Updates** auf der Registerkarte **Allgemein** Ihres Pools und wählen Sie **Updates konfigurieren** aus oder klicken Sie mit der rechten Maustaste auf Ihren Pool und wählen Sie **Updates** > **Updates konfigurieren**. Das Fenster **Serverupdates konfigurieren** wird geöffnet.

2. Wählen Sie auf der Registerkarte **XenServer 8** die Pools oder Hosts aus, die Sie konfigurieren möchten.
3. Geben Sie unter **Updatekanal**an, wie schnell Sie auf Updates zugreifen möchten. Ihr Pool oder Host kann einen der folgenden Update-Kanäle abonnieren:
   - **Früherer Zugang**
   - **Normal**
4. Wählen Sie unter **Synchronisierungszeitplan**aus, wie oft Ihr XenServer-Pool mit dem Updatekanal synchronisiert werden soll. Dies kann täglich oder wöchentlich an einem bestimmten Wochentag sein.

   > **Hinweis:**
   >
   > Wenden Sie die Updates nach der Synchronisierung so schnell wie möglich auf Ihren Pool an, um von den neuesten Updates zu profitieren.
   >
   > Wenn Sie nach der Synchronisierung, aber bevor Sie Updates auf die Hosts im Pool anwenden, einen neuen Poolkoordinator benennen, müssen Sie erneut mit dem neuen Poolkoordinator synchronisieren, bevor Sie den Pool aktualisieren können.
   >
   > Synchronisieren Sie Ihren XenServer-Pool nicht, während der Pool gerade aktualisiert wird.

5. (Optional) Geben Sie unter **Proxyserver**einen Proxy an, der bei der Synchronisierung mit dem Updatekanal verwendet werden soll. Dieser Proxyserver wird für die Kommunikation zwischen dem Host und dem öffentlichen CDN verwendet.
6. Klicken Sie auf **Anwenden**, um die Konfigurationsänderungen auf Ihren XenServer-Pool anzuwenden, und wiederholen Sie dann die obigen Schritte, um Updates für den Rest Ihrer XenServer-Pools zu konfigurieren.
7. Wenn Sie mit den Konfigurationsänderungen an Ihren Pools zufrieden sind, klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Fenster **Serverupdates konfigurieren** zu schließen. Wenn Sie Ihren Host oder Pool zum ersten Mal mit einem Updatekanal einrichten (oder wenn Sie später Ihren Host oder Pool ändern, um ihn mit einem anderen Updatekanal zu synchronisieren), werden Sie gefragt, ob Sie Ihren Host oder Pool sofort mit dem Updatekanal synchronisieren möchten. Wählen Sie in dem sich öffnenden Dialogfeld **Ja, Synchronisieren** aus, wenn Sie Ihren Host oder Pool sofort mit dem Update-Channel synchronisieren möchten.

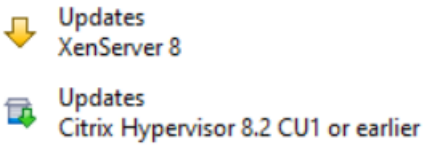


8. Sobald Ihr Pool mit dem Updatekanal synchronisiert ist, wenden Sie die heruntergeladenen Updates mithilfe des Assistenten zum **Installieren von Updates** auf Ihren Pool an. Weitere Informationen finden Sie unter Updates auf Ihren Pool anwenden.

Nach der Konfiguration Ihres XenServer-Pools finden Sie Informationen zu dem Updatekanal, den Ihr Pool abonniert hat, und zum letzten Mal, als Ihr Pool mit dem Updatekanal synchronisiert wurde, im Abschnitt **Updates** auf der Registerkarte **Allgemein** Ihres Pools in XenCenter. Informationen darüber, wann der Host das letzte Mal aktualisiert wurde, finden Sie auch im Bereich **Updates** auf dem Tab **Allgemein** des Hosts.

Verfügbare Updates für Ihren Pool anzeigen

XenCenter gibt Benachrichtigungen über verfügbare Updates für Ihre Hosts und Pools auf den Registerkarten **Updates** in der **Benachrichtigungsansicht** aus. Die Registerkarten **Updates** sind in XenServer 8-Updates und Citrix Hypervisor-Updates unterteilt.



Die Registerkarte XenServer **8-Updates** wird aktualisiert, wenn Ihre XenServer 8-Hosts und -Pools mit dem Updatekanal synchronisiert werden. Die Häufigkeit dieser Aktualisierung hängt von dem Synchronisierungszeitplan ab, den Sie für Ihren Pool eingerichtet haben (entweder täglich oder wöchentlich an einem bestimmten Wochentag).

Um die neuesten verfügbaren Updates für Ihren Pool anzuzeigen, synchronisieren Sie Ihren XenServer-Pool mit dem Update-Channel. Sie können dies von den folgenden Stellen aus tun:

- In der Ansicht **Nach Server** auf der Registerkarte **Updates** können Sie **Alle synchronisieren** wählen, um alle von XenCenter verwalteten Pools zu synchronisieren, oder **Ausgewählte synchronisieren**, um die ausgewählten Pools zu synchronisieren.
- Gehen Sie alternativ zum Abschnitt **Updates** auf der Registerkarte **Allgemein** Ihres Pools und wählen Sie **Jetzt synchronisieren** aus oder klicken Sie mit der rechten Maustaste auf Ihren Pool und wählen Sie **Updates** > **Jetzt synchronisieren**.

Anschließend können Sie alle für Ihre XenServer 8-Pools verfügbaren Updates überprüfen. Es gibt folgende Arten von Updates:

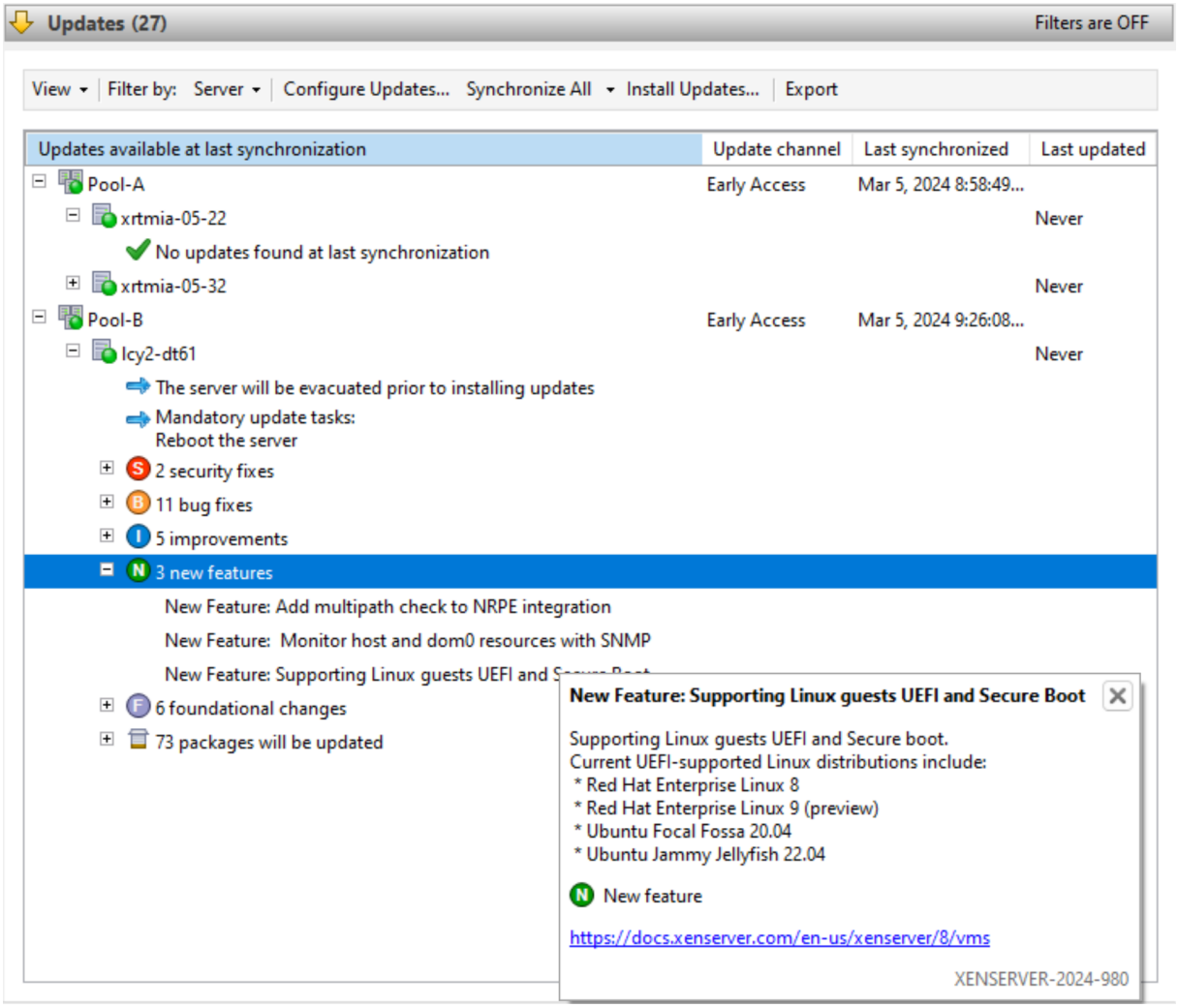
- **Sicherheitsupdates**
- **Bugfixes**
- **Verbesserungen**
- **Neue Features**
- **Preview-Features**
- **Grundlegende Änderungen**

  > **Hinweis:**
  >
  > Grundlegende Änderungen sind nicht für den Kunden sichtbare grundlegende Änderungen zur Wartung und Verbesserung des Produkts.

Wählen Sie im Hauptbereich mit der Option **Ansicht** aus, ob die Updates **nach Server** oder **nach Update** angezeigt werden.

Nach Server

Updates sind nach Host und Art des Updates gruppiert.



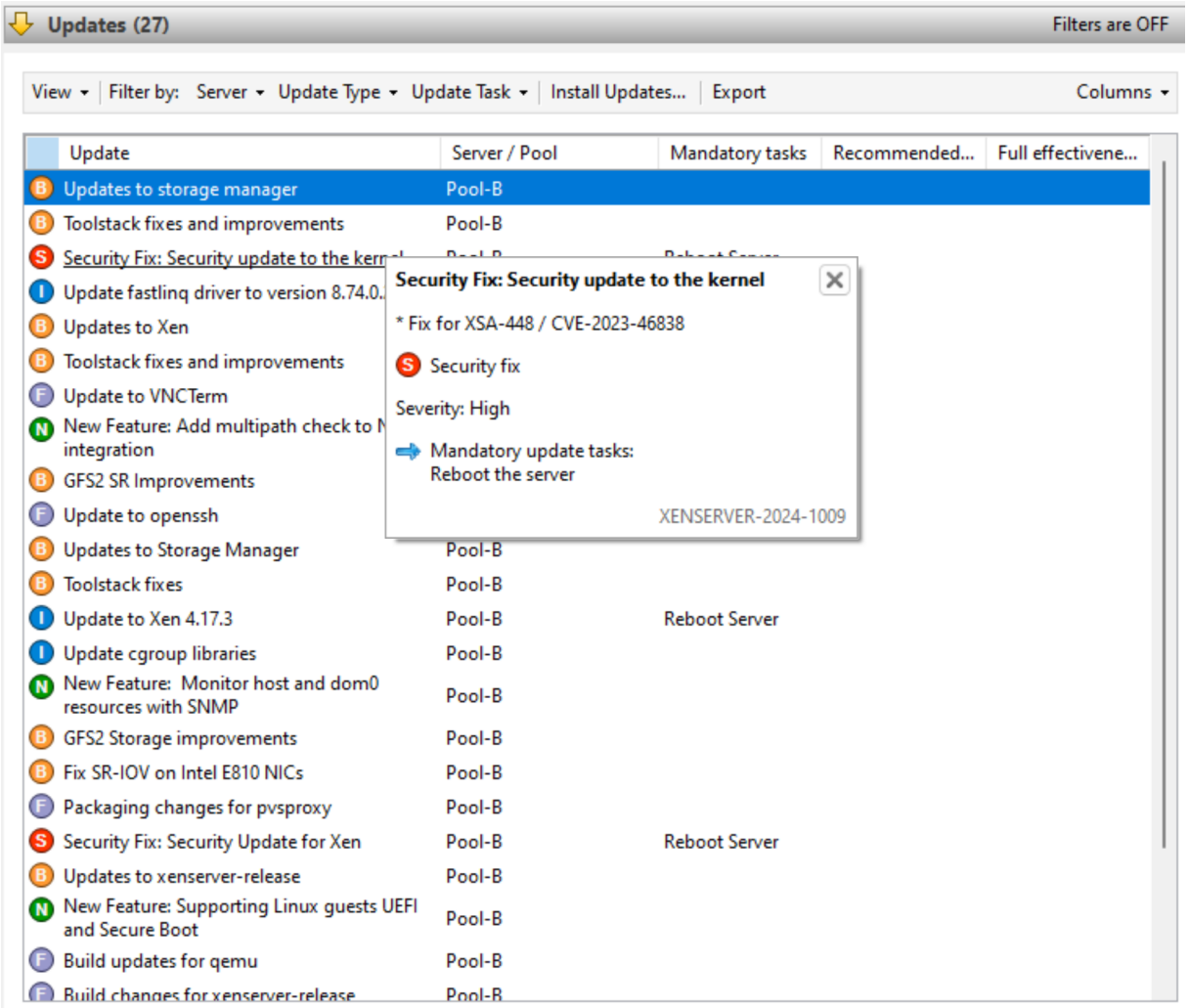
Sie können die Updateinformationen nach Server filtern. Wählen Sie ein Update aus und bewegen Sie den Mauszeiger darüber, um detaillierte Informationen zum Update anzuzeigen.

Um diese Informationen zu Ihren verfügbaren Updates offline anzuzeigen, wählen Sie **Alle exportieren** aus, um die Informationen als `.md`-Datei zu exportieren. Der Inhalt der `.md`-Datei wird nach Pool und dann nach Host gruppiert. Für jeden Host enthält die Datei die folgenden Informationen:

- Alle Updateaufgaben für diesen Host oder seine VMs. Weitere Informationen zu obligatorischen, empfohlenen und voll wirksamen Aufgaben finden Sie unter Updateaufgaben.
- Updates gruppiert nach Updatetyp
  - Updatename
  - Eine Beschreibung des Updates
- Eine Liste der RPMs, die auf dem Host aktualisiert werden sollen

Nach Update

Alle Updates sind chronologisch in der Reihenfolge ihrer Veröffentlichung aufgeführt.



Sie können die Updateinformationen nach dem Server filtern, auf den sie angewendet werden können, nach dem Updatetyp und nach allen Updateaufgaben, die darauf zutreffen. Wählen Sie ein Update aus und bewegen Sie den Mauszeiger darüber, um detaillierte Informationen zum Update anzuzeigen.

Um diese Informationen zu Ihren verfügbaren Updates offline anzuzeigen, wählen Sie **Alle exportieren** aus, um die Informationen als `.csv`-Datei zu exportieren. Die `.csv` Datei enthält die folgenden Informationen:

- Updatetyp
- Updatename
- Die Server, auf die dieses Update angewendet werden kann
- Die obligatorischen, empfohlenen und voll wirksamen Aufgaben

Weitere Informationen zu obligatorischen, empfohlenen und voll wirksamen Aufgaben finden Sie unter Updateaufgaben.

- Um die Updates auf Ihre Hosts oder Pools anzuwenden, wählen Sie **Updates installieren** aus, um den Assistenten zum **Installieren von Updates** zu öffnen. Weitere Informationen finden Sie im folgenden Abschnitt Updates auf Ihren Pool anwenden.

Wenden Sie Updates auf Ihren Pool an

Der Updateinstallationsmechanismus in XenCenter wendet die Updates mithilfe des Assistenten zum **Installieren** von Updates auf Ihre Hosts und Pools an. Während des Vorgangs ermittelt XenCenter automatisch die Aktion mit der geringsten Auswirkung, die nach der Installation aller verfügbaren Updates erforderlich ist. Der Assistent zum **Installieren von Updates** führt automatisch die folgenden Schritte aus:

1. Bei Bedarf migriert es VMs von jedem Host.
2. Falls erforderlich, versetzt es den Host in den Wartungsmodus.
3. Es wendet die Updates an.
4. Bei Bedarf führt es alle erforderlichen Updateaufgaben aus, z. B. das Neustarten des Hosts, das Neustarten des Toolstacks oder das Neustarten der VMs.
5. Es migriert die VMs zurück auf den aktualisierten Host.

Alle Aktionen, die in der Phase vor der Prüfung ergriffen wurden, um die Installation der Updates zu ermöglichen, wie z. B. das Ausschalten der Hochverfügbarkeit, werden rückgängig gemacht.

Vorbereitung

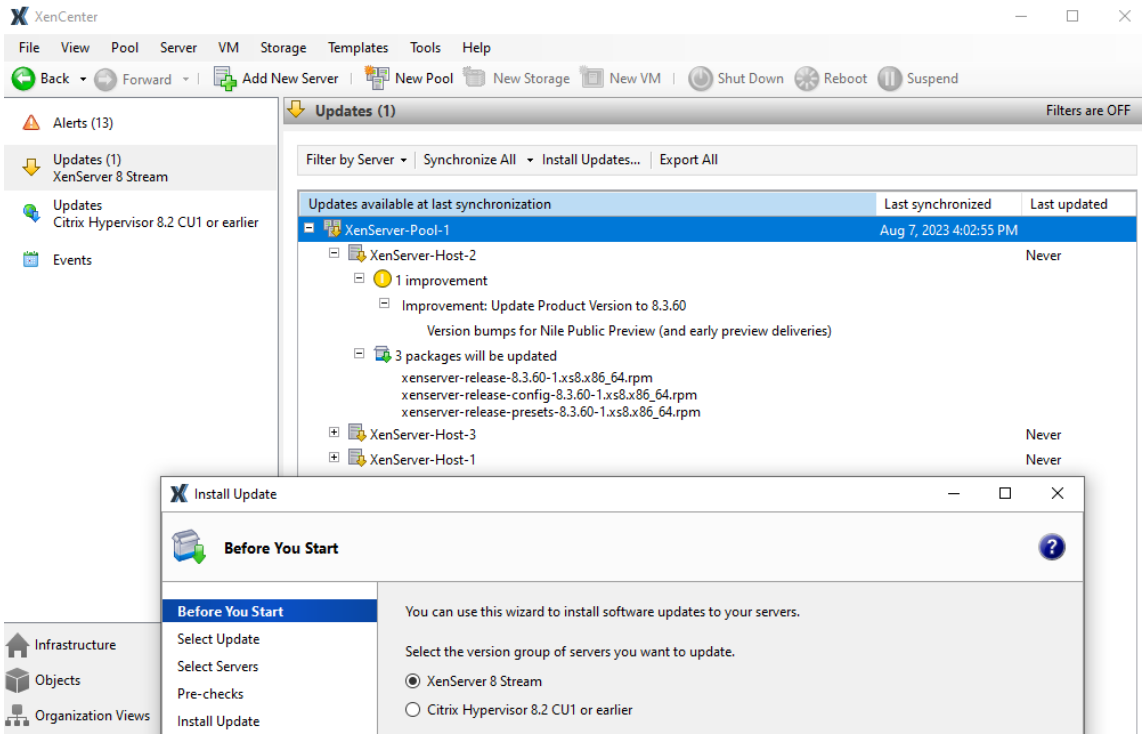
Bevor Sie ein Update auf Ihre Server anwenden, sollten Sie Folgendes beachten:

- Sichern Sie alle Ihre Server
- Stellen Sie sicher, dass High Availability (HA) in keinem Pool aktiviert ist, auf den Sie Updates anwenden möchten.
- Stellen Sie sicher, dass Sie als Pooladministrator oder Pool-Operator oder mit einem lokalen Root-Konto bei XenCenter angemeldet sind.

Updates installieren

Der folgende Abschnitt enthält schrittweise Anweisungen zum Anwenden von Updates mithilfe des Assistenten zum **Installieren von Updates** :

1. Wählen Sie im XenCenter-Menü **Tools** und dann Updates **installieren**aus.



2. Wählen **Sie im Assistenten zum Installieren von UpdatesXenServer 8**aus und überprüfen Sie die Informationen auf der Seite**Bevor Sie beginnen**. Klicken Sie zum Fortfahren auf**Weiter**.
3. Wählen Sie **Automatisierte Updates**aus. Klicken Sie auf **Weiter**.
4. Wählen Sie Ihre XenServer-Pools oder Hosts aus, die Sie aktualisieren möchten. Klicken Sie auf **Weiter, um zur nächsten** Assistentenseite zu gelangen und mit den Vorabprüfungen zu beginnen.
5. Der Assistent führt mehrere Vorabprüfungen durch, um sicherzustellen, dass die Updates auf Ihrem Host oder Pool angewendet werden können. Beispielsweise müssen Sie Ihren Host oder Pool innerhalb der letzten Woche mit dem Update-Channel synchronisiert haben.

   Folgen Sie den Empfehlungen auf dem Bildschirm, um alle fehlgeschlagenen Vorprüfungen zu beheben. Wenn Sie es vorziehen, dass XenCenter alle fehlgeschlagenen Vorprüfungen automatisch löst, wählen Sie **Alle auflösen**. Wenn die Vorprüfungen gelöst wurden, wählen Sie **Weiter** aus, um fortzufahren.

   > **Hinweise:**
   >
   > - Wenn des Updatessvorgang aus irgendeinem Grund nicht abgeschlossen werden kann, stoppt XenCenter den Vorgang. Mit dieser Einstellung können Sie das Problem beheben und den Updatevorgang fortsetzen, indem Sie auf die Schaltfläche **Wiederholen** klicken.

> • Wenn Sie zu diesem Zeitpunkt **Abbrechen** auswählen, macht der Assistent zum **Installieren von Updates** alle Änderungen rückgängig.

6. Nach der Installation der Updates sind möglicherweise einige Updateaufgaben (z. B. der Neustart Ihrer Hosts) erforderlich. Wählen Sie auf der Seite **Updatemodus** die Ebene der Updateaufgaben aus, die XenCenter nach dem Anwenden von Updates auf Ihren Pool automatisch ausführen soll (z. B. den Neustart Ihrer Hosts). Standardmäßig wählt XenCenter die empfohlene Anzahl von Updateaufgaben aus. Obligatorische Aufgaben können nicht abgewählt werden und XenCenter führt diese Aufgaben automatisch aus.

   Die obligatorischen, empfohlenen und vollständigen Updateaufgaben sind unter **Aufgaben** aufgeführt. Wenn kein Updateaufgaben erforderlich sind, wird auf der Seite ein Hinweis angezeigt, der besagt, dass **keine Aktion erforderlich ist**. Weitere Informationen zu den verschiedenen Arten von Updateaufgaben und den von XenCenter bereitgestellten Leitfäden finden Sie unter Updateaufgaben.

7. Klicken Sie auf **Updates für XenCenter installieren**, um mit der Installation von Updates für Ihren Host oder Pool zu beginnen.

8. Der Assistent zum **Installieren von Updates** zeigt den Fortschritt des Updates an und zeigt die wichtigsten Vorgänge an, die XenCenter bei des Updates der einzelnen Hosts im Pool ausführt. Klicken Sie auf **Fertigstellen**, um die Updates abzuschließen und den Assistenten zum **Installieren von Updates zu** schließen.

Aufgaben für das Update

Einige Aufgaben (wie das Evakuieren oder Neustarten Ihrer Hosts) sind möglicherweise vor und nach der Installation von Updates für Ihren Pool erforderlich. Manchmal sind kein Updateaufgaben erforderlich.

Kategorien von Leitlinien

XenServer versucht, die Störung Ihrer virtuellen Maschinen, die durch diese Updateaufgaben verursacht werden könnten, zu minimieren, indem die Aufgaben in ****Erforderlich, **Empfohlen**, **Voll wirksam** und **Live-Patch** unterteilt werden. Anhand dieser Kategorisierungen können Sie beurteilen, ob ein Updateaufgabe, die zu Ausfallzeiten oder geringfügigen Unterbrechungen für Ihre Hosts oder VMs führen könnte, für Ihre Umgebung und Ihr Risikoprofil erforderlich ist.

Bei Updates können Aufgaben in mehr als einer dieser Kategorien aufgeführt sein. Für ein Update kann es beispielsweise erforderlich sein, dass Sie den Host neu starten, um die volle Wirksamkeit der aktualisierten Features zu nutzen. Es wird jedoch empfohlen, den Toolstack neu zu starten, um die Vorteile des Updates optimal nutzen zu können und den Pool weniger zu stören.

Während des Updatevorgangs können Sie wählen, ob Sie eine der folgenden drei Aufgabenstufen ausführen möchten:

1. Erforderlich
2. Obligatorisch + Empfohlen
3. Erforderlich + Empfohlen + Volle Wirksamkeit

Erforderlich Obligatorische Aufgaben *müssen* nach einem Update ausgeführt werden, da das System sonst zur Laufzeit ausfallen kann. Diese Maßnahmen sind erforderlich, um wichtige Korrekturen zu ermöglichen und sicherzustellen, dass Ihre Umgebung sicher und stabil ist. Wenn Sie Updates anwenden, führt XenCenter diese Aufgaben aus. Sie können erforderliche Aufgaben nicht überspringen.

Empfohlen Empfohlene Aufgaben sind die Aufgaben, die Sie ausführen sollten, um die meisten Funktionen und Fehlerbehebungen der Updates nutzen zu können. Wenn Sie Updates anwenden, werden diese Aufgaben standardmäßig in XenCenter ausgewählt, Sie können sie jedoch deaktivieren. Wenn Sie diese Aufgaben jetzt nicht ausführen möchten, werden sie in den ausstehenden Aufgaben für den entsprechenden Pool, Host oder die virtuelle Maschine aufgeführt.

Warum die empfohlenen Aufgaben ausgeführt werden sollten:

- Diese Aufgaben gewährleisten eine sichere, stabile XenServer-Umgebung.

Warum empfohlene Aufgaben übersprungen werden können:

- Nachdem Sie die detaillierten Informationen für die Updates überprüft haben, sind Sie der Meinung, dass das Risiko, dass diese Updates jetzt nicht vollständig angewendet werden, akzeptabel ist.
- Die empfohlenen Aufgaben führen jetzt zu unerwünschten Unterbrechungen Ihrer VMs.

Volle Wirksamkeit Um die Vorteile der entsprechenden Updates nutzen zu können, sind Aufgaben im vollen Umfang erforderlich. Die Updates, denen Aufgaben zur vollen Wirksamkeit zugeordnet sind, sind in der Regel nur für Benutzer relevant, die bestimmte Geräte verwenden oder bestimmte Funktionen verwenden.

Lesen Sie die Updateinformationen, um zu erfahren, ob diese Aufgaben für Ihre Umgebung erforderlich sind. Wenn Sie Updates anwenden, werden diese Aufgaben in XenCenter nicht standardmäßig ausgewählt. Sie können sie jedoch während des Updates ausführen, wenn Sie der Meinung sind, dass das Update für Ihre Umgebung oder Konfiguration gilt. Wenn Sie diese Aufgaben jetzt nicht ausführen möchten, werden sie in den ausstehenden Aufgaben für den entsprechenden Pool, Host oder die virtuelle Maschine aufgeführt.

Warum die Aufgaben mit voller Wirksamkeit ausgeführt werden sollten:

- Die Updates mit Aufgaben zur vollen Wirksamkeit sind für Ihre Hardware, Umgebung oder Konfiguration relevant.

Warum sollten Sie sich nicht für die Aufgaben mit voller Wirksamkeit entscheiden:

- Die Updates mit einer Anleitung zur vollen Wirksamkeit sind für Ihre Hardware, Umgebung oder Konfiguration nicht relevant.
- Die Aufgaben mit voller Wirksamkeit führen jetzt zu unerwünschten Unterbrechungen Ihrer virtuellen Maschinen.
- Sie benötigen die Vorteile dieser Updates derzeit nicht.

Wenn die Aufgaben mit voller Wirksamkeit für Ihre Umgebung gelten, Sie sich aber dafür entschieden haben, sie zu verschieben, planen Sie, diese Aufgaben während eines geeigneten Wartungsfensters abzuschließen, um die Stabilität Ihrer Umgebung aufrechtzuerhalten.

Live-Patches Updates für bestimmte Komponenten können einen Live-Patch beinhalten. Ob ein Live-Patch auf Ihre Hosts angewendet werden kann, hängt von der Version der Komponente ab, die beim letzten Neustart der Hosts installiert wurde. Wenn ein Update als Live-Patch auf Ihre Hosts angewendet werden kann, ersetzt die Live-Patch-Anleitung die empfohlene Anleitung.

> **Beispiel:**
>
> Sie haben zwei Pools. Pool A wurde auf ein aktuelles Niveau aktualisiert. Pool B wurde seit einiger Zeit nicht aktualisiert. Wir veröffentlichen ein Update, die die empfohlene Updateaufgabe “Host neu starten”und die Live-Patch-Updateaufgabe “Toolstack neu starten”enthält.
>
> In Pool A kann der Live-Patch auf diese aktuelleren Hosts angewendet werden. Die von XenCenter empfohlene Anleitung zeigt “Toolstack neu starten”. Die weniger störende Aufgabe aus der Live-Patch-Anleitung hat Vorrang vor den empfohlenen Empfehlungen.
>
> In Pool B kann der Live-Patch nicht auf die Hosts angewendet werden, da sie sich auf einem älteren Level befinden. In der von XenCenter empfohlenen Anleitung wird “Host neu starten” angezeigt. Die empfohlenen Leitlinien gelten weiterhin. Die Live-Patch-Anleitung ist in diesem Fall irrelevant.

Manchmal werden nur einige der Fixes in einem Update aktiviert, wenn das Update als Live-Patch angewendet wird. Sehen Sie sich die Details zum Update an, um herauszufinden, ob Sie alle Fixes des Updates benötigen oder nur die Fixes, die durch den Live-Patch aktiviert wurden. Anhand dieser Informationen können Sie dann entscheiden, ob Sie die empfohlenen Aufgaben ausführen möchten. Weitere Informationen finden Sie unter Verfügbare Updates für Ihren Pool anzeigen.

Aufgaben für das Update

Bei der Installation einer Aktualisierung ist möglicherweise mindestens eine der folgenden Aufgaben erforderlich. Jede Art von Updateaufgabe kann in jeder Leitfadenkategorie aufgeführt werden.

Updateaufgaben für Ihren Host Sie führen diese Aufgabe immer nur aus, *bevor* Sie Updates installieren, und manchmal führen Sie sie im Rahmen der Aufgabe "Host neu starten"aus:

- **Server evakuieren**: Alle VMs müssen vom XenServer-Host migriert oder heruntergefahren werden, bevor das Update angewendet wird. Um diese Aufgabe abzuschließen, migriert XenCenter alle VMs vom Host. Während dieser Aufgabe wird der XenServer-Pool mit reduzierter Kapazität betrieben, da ein Host vorübergehend nicht für die Ausführung von VMs verfügbar ist.

Die folgenden Aufgaben erfordern Aktionen auf dem aktualisierten Host:

- **Server neu starten**: Der XenServer-Host muss neu gestartet werden. Um diese Aufgabe abzuschließen, migriert XenCenter alle VMs vom Host und startet den Host neu. Während dieser Aufgabe wird der XenServer-Pool mit reduzierter Kapazität betrieben, da ein Host vorübergehend nicht für die Ausführung von VMs verfügbar ist.
- **Toolstack neu starten**: Der Toolstack auf dem Host muss neu gestartet werden. Wenn XenCenter den Toolstack auf dem Poolkoordinator neu startet, verliert XenCenter die Verbindung zum Pool und versucht automatisch, die Verbindung erneut herzustellen. Bei anderen Poolmitgliedern gibt es keinen sichtbaren Effekt.

Updateaufgaben für Ihre VM Einige Updates bieten neue Features für Ihre VMs. Für diese Updates sind möglicherweise die folgenden Aufgaben auf Ihren VMs erforderlich:

- **VM neu starten**: Die VM muss neu gestartet werden. In XenCenter wird beim Neustart der VM das rote Stoppsymbol (Quadrat auf Rot) angezeigt. Wenn die Aufgabe abgeschlossen ist, wird das grüne Startsymbol angezeigt. Während dieser Zeit ist die VM für den Endbenutzer nicht verfügbar.
- **Gerätemodell neu starten**: Das Gerätemodell für VMs auf dem aktualisierten Host muss neu gestartet werden. In XenCenter zeigt die VM beim Neustart des Gerätemodells ein gelbes Warndreieck an. Wenn die Aufgabe abgeschlossen ist, wird das grüne Startsymbol angezeigt. Während dieser Zeit können Sie die VM nicht stoppen, starten oder migrieren. Der Endbenutzer der VM sieht möglicherweise eine kurze Pause und setzt seine Sitzung fort.

  Damit die Aktion "Gerätemodell neu starten"auf einer Windows-VM unterstützt wird, müssen auf der VM die XenServer VM Tools für Windows installiert sein.

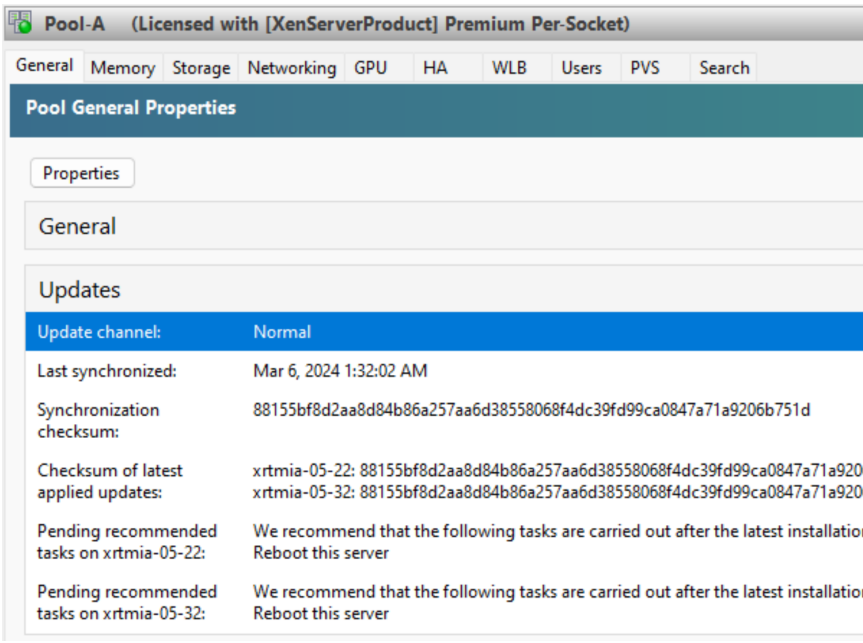
Updateaufgaben überprüfen, bevor Sie Updates anwenden

Diese Aufgaben sind auf der Registerkarte XenServer 8-**Updates** in der Ansicht **Benachrichtigungen** aufgeführt. Weitere Informationen finden Sie unter Verfügbare Updates für Ihren Pool anzeigen.

Ausstehende Aufgaben anzeigen

Wenn Sie während einer Aktualisierung nicht alle Aufgaben ausführen möchten, werden die ausstehenden Aufgaben für jeden Pool, Host oder jede VM in der XenCenter-Ansicht **Infrastruktur** angezeigt.

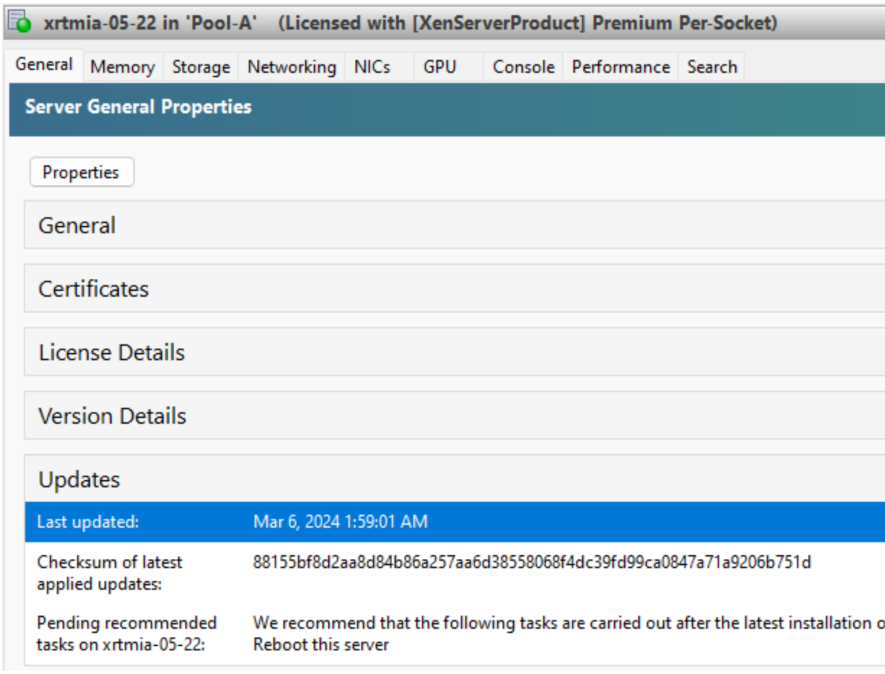
Weitere Informationen finden Sie auf der Registerkarte **Allgemein** für den Pool, den Host oder die VM im Abschnitt **Updates**.



Ausstehende Aufgaben für einen Pool

In diesem Abschnitt werden die ausstehenden Aufgaben für alle Hosts im Pool angezeigt.

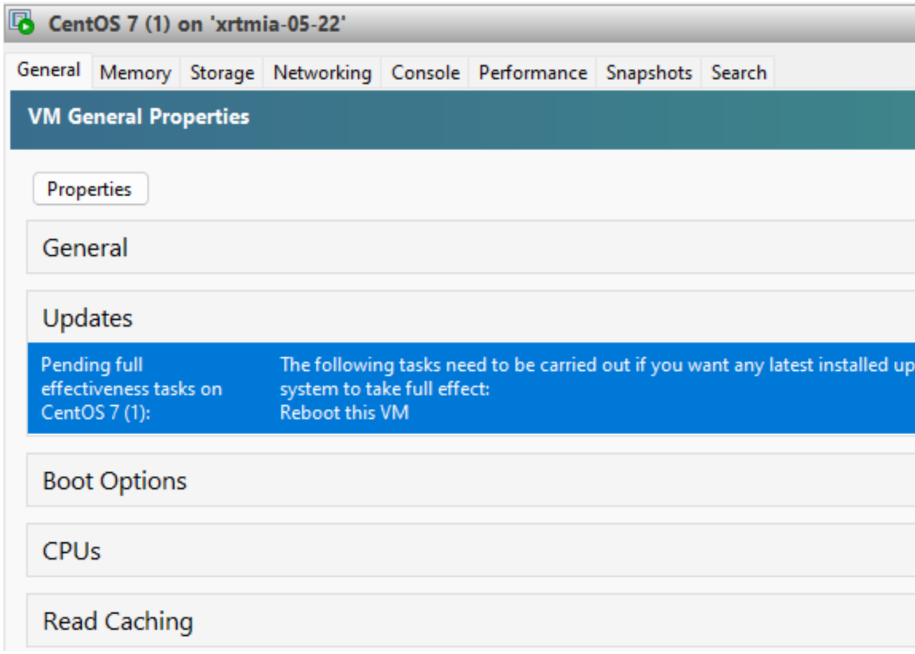
Gezeigt werden auch eine Prüfsumme, die die Ebene angibt, auf die der aktuelle Poolkoordinator synchronisiert hat, und Prüfsummen für jeden Host, die die Ebene der installierten Updates angeben. Diese Prüfsummen können nützliche Informationen liefern, wenn Sie den technischen Support kontaktieren müssen.



Ausstehende Aufgaben für den Host

In diesem Abschnitt werden die ausstehenden Aufgaben für den XenServer-Host angezeigt.

Außerdem wird eine Prüfsumme angezeigt, die den Stand der installierten Updates angibt. Diese Prüfsumme kann nützliche Informationen liefern, wenn Sie den technischen Support kontaktieren müssen.



Ausstehende Aufgaben für die VM

In diesem Abschnitt werden die ausstehenden Aufgaben für eine VM angezeigt.

Aktuelle Version von XenCenter

April 12, 2024

Verwenden Sie XenCenter yyyy.x.x, um Ihre XenServer 8-Umgebung zu verwalten und virtuelle Maschinen von Ihrem Windows-Desktopcomputer aus bereitzustellen, zu verwalten und zu überwachen.

> **Hinweis:**
>
> XenCenter yyyy.x.x wird noch nicht für die Verwendung mit Citrix Hypervisor 8.2 CU1 in Produktionsumgebungen unterstützt. Verwenden Sie XenCenter 8.2.7, um Ihre Citrix Hypervisor 8.2 CU1-Produktionsumgebung zu verwalten. Weitere Informationen finden Sie in der XenCenter 8.2.7-Dokumentation.
>
> Sie können XenCenter 8.2.7 und XenCenter yyyy.x.x auf demselben System installieren. Die Installation von XenCenter yyyy.x.x überschreibt Ihre XenCenter 8.2.7-Installation nicht.

Sie können das Installationsprogramm für die neueste Version von XenCenter von der XenServer-Downloadseiteherunterladen.

XenServer mit Citrix-Produkten verwenden

April 12, 2024

XenServer bietet Funktionen, die die Interoperabilität mit Citrix Virtual Apps and Desktops, Citrix DaaS und Citrix Provisioning verbessern.

Weitere Informationen zu diesen Produkten finden Sie unter:

- Produktdokumentation zu Citrix Virtual Apps and Desktops
- Produktdokumentation zu Citrix DaaS
- Produktdokumentation für Citrix Provisioning

Unterstützte Versionen

Die Versionen dieser Produkte, mit denen XenServer 8 zusammenarbeitet, finden Sie auf der Citrix-Website: Unterstützte Hypervisors für Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS).

Lizenzierung

Um XenServer für Ihre Citrix Virtual Apps and Desktops- oder Citrix DaaS-Workloads verwenden zu können, benötigen Sie eine XenServer Premium Edition-Lizenz. Weitere Informationen finden Sie unter Lizenzierung.

Wenn Sie XenServer oder Citrix Hypervisor bereits zum Hosten Ihrer Citrix Virtual Apps and Desktops-Workloads verwenden, können Sie die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Sie können XenServer-Lizenzen von https://xenserver.com/buy abrufen.

XenServer-Funktionen für Citrix Virtual Apps and Desktops

Die folgenden XenServer-Funktionen sind für die Verwendung mit Citrix Virtual Apps and Desktops, Citrix DaaS und Citrix Provisioning konzipiert:

- **Intellicache**: Die Verwendung von XenServer mit IntelliCache macht gehostete Citrix Virtual Desktop-Bereitstellungen kostengünstiger, da Sie eine Kombination aus gemeinsam genutztem Speicher und lokalem Speicher verwenden können. Dies ist von besonderem Vorteil, wenn viele VMs alle ein gemeinsames Betriebssystemimage verwenden. Die Belastung des Speicher-Arrays wird reduziert und die Leistung wird verbessert. Darüber hinaus wird der Netzwerkverkehr zu und von gemeinsam genutztem Speicher reduziert, da der lokale Speicher das primäre Image aus dem gemeinsam genutzten Speicher zwischenspeichert.
- **Lese-Caching**: Das Lese-Caching verbessert die Datenträgerleistung einer VM, indem Daten im freien Speicher des Hosts zwischengespeichert werden. Es verbessert die Leistung in einer Citrix Virtual Desktops Machine Creation Services-Umgebung (MCS), in der viele VMs von einer einzelnen Basis-VM geklont werden, da dadurch die Anzahl der von der Datenträger gelesenen Blöcke drastisch reduziert wird.
- **PVS-Accelerator**: Die XenServer PVS-Accelerator-Funktion bietet erweiterte Funktionen für Kunden, die XenServer mit Citrix Provisioning verwenden. PVS-Accelerator bietet viele Vorteile, darunter Datenlokalität, verbesserte Endbenutzererfahrung, beschleunigte VM-Boots und Boot-Storms, vereinfachtes Scale-Out durch Hinzufügen weiterer Hypervisor-Hosts sowie geringere Gesamtbetriebskosten und vereinfachte Infrastrukturanforderungen.
- **Reibungslose Roaming-Unterstützung für den Virtual Desktop Tablet-Modus**: XenServer ermöglicht Ihnen in Verbindung mit Citrix Virtual Apps and Desktops, die Windows 10 Continuum-Benutzeroberfläche in einer virtualisierten Umgebung zu erleben.
- **Grafikvirtualisierung**: XenServer bietet die virtuelle Bereitstellung professioneller 3D-Grafikanwendungen und Workstations in XenServer über GPU-Passthrough (für NVIDIA-, AMD- und Intel-GPUs) und hardwarebasiertes GPU-Sharing mit NVIDIA vGPU™ und Intel GVT-G™.

Bewährte Methoden

Bei der Konfiguration und Verwaltung Ihrer XenServer-Umgebung können Sie Maßnahmen ergreifen, um die Funktionsweise mit Citrix-Produkten zu optimieren.

Installation und Aktualisierung

- Bei der ersten Installation von XenServer-Hosts können Sie Intellicache aktivieren, um VM-Daten lokal zwischenzuspeichern und die Leistung zu verbessern. Weitere Informationen finden Sie unter Intellicache.
- Wenn Sie ein Upgrade von einer früheren Version von Citrix Hypervisor oder XenServer durchführen, kann die Methode, die Sie für dieses Upgrade verwenden, von Ihrer Citrix Virtual Apps and Desktops-Workload abhängen. Weitere Informationen finden Sie unter Upgrade-Szenarien für Citrix Virtual Apps and Desktops.

Konfigurieren der Umgebung

- Der XenServer-Host wird mit einem Standard-TLS-Zertifikat installiert. Um jedoch HTTPS zur Sicherung der Kommunikation zwischen XenServer und Citrix Virtual Apps and Desktops zu verwenden, installieren Sie ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle bereitgestellt wird. Weitere Informationen finden Sie unter Installieren eines TLS-Zertifikats auf Ihrem Host.

Speichernutzung

- Wenn XenServer zum ersten Mal installiert wird, weist er der Steuerdomäne eine bestimmte Menge an Speicher zu. In vielen Citrix Virtual Apps and Desktops-Umgebungen ist es ratsam, den der Steuerdomäne zugewiesenen Arbeitsspeicher über diesen Standardwert hinaus zu erhöhen.

  Erhöhen Sie den Steuerdomänenspeicher in den folgenden Fällen:

  - Sie führen viele virtuelle Maschinen auf dem Server aus
  - Sie verwenden den PVS-Accelerator
  - Sie verwenden Lesecaching

  Hinweise zum Ändern der Größe des Steuerdomänenspeichers und zum Überwachen des Speicherverhaltens finden Sie unter Speicherauslastung.

layout: doc
description: Upgrade scenarios and recommendations for Citrix Virtual Apps and Desktops environments.—

Upgrade-Szenarien für XenServer und Citrix Virtual Apps and Desktops

XenServer enthält Funktionen und Optimierungen, die ihn zu einem idealen Hypervisor für die Verwendung in Ihrer Citrix Virtual Apps and Desktops-Umgebung machen.

Wenn Sie XenServer mit Citrix Virtual Apps and Desktops verwenden, gibt es bei der Durchführung Ihres Upgrades einige Überlegungen, die im Hauptartikel zum Upgrade nicht behandelt werden: Upgrade von einer vorhandenen Version. Lesen Sie sowohl diesen Artikel als auch den Haupt-Upgrade-Artikel, bevor Sie mit dem Upgrade von Citrix Hypervisor 8.2 auf XenServer 8 beginnen.

> **Wichtig:**
>
> Wenn Sie Ihre Citrix Virtual Apps and Desktops-Lizenz verwenden, um Ihre Citrix Hypervisor 8.2 Cumulative Update 1-Hosts zu lizenzieren, gilt diese Lizenz nicht mehr für XenServer 8. Sie müssen stattdessen XenServer Premium Edition-Lizenzen erwerben, um jeden CPU-Sockel in Ihrem Pool abzudecken. Weitere Informationen finden Sie unter https://xenserver.com/buy.
>
> Bestandskunden können die Teilnahme an unserer Aktion beantragen und bis zu 10.000 XenServer Premium Edition-Socket-Lizenzen kostenlos erhalten. Weitere Informationen

Überlegungen beim Upgrade von XenServer in einer Citrix Virtual Apps and Desktops-Umgebung:

- XenServer-Hosts werden im Rahmen eines Upgrades zweimal neu gestartet. Zu Beginn des Upgrades müssen Sie Ihren Server auf dem Installationsmedium starten. Am Ende des Vorgangs startet das Installationsprogramm den Server neu, um das Upgrade abzuschließen. VMs auf diesen Hosts müssen während dieser Zeit entweder migriert oder gestoppt werden.
- Der für das Upgrade von XenServer zu verwendende Ansatz hängt von Ihrer XenServer-Umgebung, Ihrer Citrix Virtual Apps and Desktops-Umgebung und den Typen der Maschinen und Anwendungen ab, die von XenServer gehostet werden.
- Möglicherweise müssen Sie in Ihrer Citrix Virtual Apps and Desktops-Umgebung einige Vorbereitungen treffen, bevor Sie mit dem XenServer-Upgrade beginnen.
- Dieser Artikel behandelt nur Anwendungsfälle, in denen die Citrix Virtual Apps and Desktops-Workload im XenServer-Pool gehostet wird. Fälle, in denen Sie auch Teile Ihrer Citrix Virtual Apps and Desktops-Infrastruktur auf VMs im XenServer-Pool hosten, werden in diesem Artikel nicht behandelt. Berücksichtigen Sie diese Komponenten bei der Upgrade-Planung.
- Stellen Sie sicher, dass die Version von Citrix Virtual Apps and Desktops, die Sie verwenden, sowohl für die Version von XenServer, von der Sie ein Upgrade durchführen, als auch für die Version, auf die Sie das Upgrade durchführen, unterstützt wird. Weitere Informationen finden

Sie unter Unterstützte Hypervisors für Citrix Virtual Apps and Desktops (MCS) und Citrix Provisioning (PVS).

- Die Zeit, die für das Upgrade benötigt wird, und die Wahrscheinlichkeit eines Serviceausfalls hängen von Ihrem Upgrade-Ansatz ab. Das vollständige Upgrade eines gesamten Pools kann mehrere Stunden in Anspruch nehmen.
- In diesem Artikel wird davon ausgegangen, dass die Zeit für das vollständige Upgrade eines einzelnen XenServer-Hosts 35 Minuten beträgt. Diese Host-Upgrade-Zeit beinhaltet den Upgrade-Vorgang und alle erforderlichen Neustarts.

Die in diesem Artikel beschriebenen Lösungsansätze sollen Sie zu einer Upgrade-Methode führen, die die Wahrscheinlichkeit von Serviceausfällen reduziert und dafür sorgt, dass der Upgrade-Prozess in Ihr Wartungsfenster passt. In einigen Fällen sind Serviceausfälle jedoch unvermeidlich. Wenn der XenServer-Upgrade-Vorgang nicht in Ihr Wartungsfenster passt, können Sie Ihren Pool zwischen den Wartungsfenstern für kurze Zeit im gemischten Modus ausführen. Dies wird jedoch nicht empfohlen. Weitere Informationen finden Sie unter Pools im gemischten Modus.

Beachten Sie während des geplanten Wartungsfensters für das XenServer-Upgrade die folgenden Einschränkungen:

- Versuchen Sie nicht, die Infrastruktur des Pools, der aktualisiert wird, neu zu konfigurieren. Fügen Sie beispielsweise keine Hosts zum Pool hinzu oder werfen Sie sie aus dem Pool aus.
- Fügen Sie dem Pool, der aktualisiert wird, keine virtuellen Maschinen hinzu, starten oder beenden Sie sie nicht.
- Führen Sie während des Fensters keine Katalogupdates durch.

Upgrade des rollenden Pools

Rolling Pool Upgrade ist eine XenServer-Funktion, die entwickelt wurde, um den Upgrade-Prozess zu vereinfachen und Ausfallzeiten zu minimieren.

Der **Rolling Pool Upgrade-Assistent** in XenCenter führt Sie durch den Upgrade-Vorgang und organisiert den Upgrade-Pfad automatisch. Bei Pools wird jeder Server im Pool nacheinander aktualisiert, beginnend mit dem Poolkoordinator. Bevor Sie ein Upgrade starten, führt der Assistent eine Reihe von Vorprüfungen durch. Diese Vorabprüfungen stellen sicher, dass bestimmte poolweite Funktionen, wie z. B. Hochverfügbarkeit, vorübergehend deaktiviert werden und dass jeder Server im Pool für das Upgrade vorbereitet ist. Es ist jeweils nur ein Server offline. Alle laufenden VMs werden automatisch von jedem Server migriert, bevor das Upgrade auf diesem Server installiert wird.

Sie können Rolling Pool Upgrade für viele der in diesem Artikel beschriebenen Anwendungsfälle von Citrix Virtual Apps and Desktops verwenden. Für jeden ist die Upgrade-Zeit dieselbe: Die Anzahl der Hosts im Pool multipliziert mit der Upgrade-Zeit für einen einzelnen Host. (**N x 35 Minuten**). Das Potenzial eines VM-Ausfalls hängt von Ihrer Citrix Virtual Apps and Desktops-Workload und der Konfiguration des XenServer-Pools ab.

Auch wenn Sie Rolling Pool Upgrade verwenden möchten, um Ihren XenServer-Pool zu aktualisieren, überprüfen Sie die Informationen für Ihre spezifische Umgebung, um sicherzustellen, dass Sie die erforderlichen Aktionen für Citrix Virtual Apps and Desktops, alle besonderen Überlegungen und das zu erwartende Verhalten verstehen.

Anwendungsfälle

Dieser Artikel identifiziert mehrere breite Anwendungsfälle. Für jeden dieser Anwendungsfälle gehen wir davon aus, dass der XenServer-Pool nur einen Typ von Citrix Virtual Apps and Desktops-Workload hostet. Wenn Ihr Pool eine Mischung aus verschiedenen Arten von Workloads enthält, überprüfen Sie alle Fälle, die auf Ihren Pool zutreffen, um zu entscheiden, was Ihr bevorzugter Upgrade-Ansatz ist.

Überlegen Sie sich zunächst, wie Ihre XenServer-Umgebung konfiguriert ist:

- XenServer-Pool mit gemeinsam genutztem Speicher

  In einem XenServer-Pool mit einem oder mehreren gemeinsam genutzten Speicher-Repositorys (SRs) können die VM-Datenträger auf diesem gemeinsam genutzten Speicher gehostet werden, sodass die VMs während des Upgrades zwischen Hosts migrieren können. Diese Konfiguration kann die Notwendigkeit von VM-Ausfallzeiten reduzieren oder ganz vermeiden.

- XenServer-Pool ohne gemeinsamen Speicher oder eigenständigen Host

  In einem XenServer-Pool ohne gemeinsam genutzten Speicher oder auf einem eigenständigen XenServer-Host können die VMs während des Upgrade-Vorgangs nicht migrieren. Wenn der Host im Rahmen des Upgrades neu gestartet wird, müssen Sie die VMs herunterfahren.

XenServer-Pool mit gemeinsam genutztem Speicher

Wenn Sie einen Pool aktualisieren, in dem sich die VM-Datenträger auf gemeinsam genutztem Speicher befinden, können Sie während des Upgrades VMs von jedem XenServer-Host im Pool evakuieren.

Die meisten Anwendungsfälle für diesen Pooltyp können mithilfe von Rolling Pool Upgrade aktualisiert werden. Die erforderlichen Aktionen in Citrix Virtual Apps and Desktops und das Ausfallverhalten sind jedoch je nach Workload unterschiedlich.

Überlegen Sie, welche Art von Citrix Virtual Apps and Desktops-Workload in Ihrem Pool gehostet wird:

- Nicht zugewiesene Einzelsitzungs-Desktops
- Andere Workloads

XenServer-Pool ohne gemeinsamen Speicher oder eigenständigen Host

Wenn Sie einen Pool aktualisieren, in dem sich die VM-Datenträger im lokalen Speicher befinden, oder wenn Sie einen einzelnen Host in Ihrem Pool haben, können die VMs während des Upgrades nicht von den XenServer-Hosts migriert werden. In diesen Fällen müssen die VMs für die Dauer des Host- oder Pool-Upgrades heruntergefahren werden. Ein gewisser Ausfall Ihrer virtuellen Apps und Desktops ist in diesen Fällen unvermeidlich.

Überlegen Sie, welche Art von Citrix Virtual Apps and Desktops-Workload in Ihrem Pool gehostet wird:

- Zugewiesene Desktops
- Andere Workloads

Fall 1: Einzelsitzungs-Desktops, die in einem Pool mit gemeinsam genutztem Speicher ausgeführt werden

Dieser Anwendungsfall deckt XenServer-Pools mit gemeinsam genutztem Speicher ab, deren primärer Workload virtuelle Einzelsitzungs-Desktops mit zufälliger Maschinenzuweisung sind. Maschinen dieses Typs müssen entweder von Citrix Provisioning oder von Machine Creation Services verwaltet werden.

Für alle Workloads, die von Citrix Virtual Apps and Desktops verwaltet werden, einschließlich solcher, die von Citrix Provisioning und Machine Creation Services mit Energieverwaltung verwaltet werden, können Sie während des Upgrades keine vollständige Workload aufrechterhalten. Die Energieverwaltung von Maschinen kann während des Upgrade-Vorgangs problematisch sein. Sie können die Energieverwaltung nicht deaktivieren, ohne auch die Erstellung neuer Sitzungen zu deaktivieren.

Empfohlene Optionen für das Upgrade:

- Upgrade des rollenden Pools
  - Geschätzte Upgrade-Zeit: Die Anzahl der Hosts im Pool multipliziert mit der Upgrade-Zeit für einen einzelnen Host. (**N x 35 Minuten**)
  - Ausfallverhalten: Alle Maschinen befinden sich während der gesamten Upgrade-Zeit im Wartungsmodus von Citrix Virtual Apps and Desktops.

Wenn möglich, stellen Sie die Workload während des Upgrades dieses Pools von anderen XenServer-Pools mit Kapazität zur Verfügung. Dieser Ansatz kann während des Upgrades zu einer verringerten Kapazität führen. Wenn Sie keine Kapazität für die Workload auf Ihren anderen XenServer-Hosts und -Pools haben, empfehlen wir Ihnen, einen Ausfall für alle Maschinen in Ihrem Workload zu melden.

Rolling Pool Upgrade (1)

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Versetzen Sie alle Maschinen im Pool in den Wartungsmodus. Wenn alle Maschinen dieselbe Verbindung verwenden, können Sie den gesamten Maschinenkatalog in den Wartungsmodus versetzen.
2. Informieren Sie alle betroffenen Benutzer über den bevorstehenden Ausfall.
   - Wenn auf den Computern in diesem Pool immer noch Sitzungen ausgeführt werden, bitten Sie die Benutzer, sich abzumelden, oder erzwingen Sie das Ende ihrer Sitzungen.
   - Informieren Sie die Benutzer darüber, dass sie sich nach dem Abmelden erst wieder anmelden können, wenn der volle Service wieder aufgenommen wird.
3. Starten Sie in XenCenter den Rolling Pool Upgrade-Assistenten und wählen Sie den automatischen Modus. Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.

   Wenn das Upgrade abgeschlossen ist, werden alle VMs, die im Rahmen des Rolling Pool-Upgrades gesperrt wurden, neu gestartet.
4. Schalten Sie die Maschinen aus dem Wartungsmodus.

   Neue Sitzungen können jetzt gestartet und der volle Service wieder aufgenommen werden.

Fall 2: Andere Workloads, die in einem Pool mit gemeinsam genutztem Speicher ausgeführt werden

Dieser Anwendungsfall deckt XenServer-Pools mit gemeinsam genutztem Speicher ab, deren primäre Workload entweder virtuelle Desktops mit einer Sitzung mit dem zugewiesenen Maschinenzuordnungstyp oder virtuelle Anwendungen mit mehreren Sitzungen mit dem zufälligen Maschinenzuordnungstyp sind.

Empfohlene Optionen für das Upgrade:

- Upgrade des rollenden Pools
  - Geschätzte Upgrade-Zeit: Die Anzahl der Hosts im Pool multipliziert mit der Upgrade-Zeit für einen einzelnen Host. (**N x 35 Minuten**)
  - Ausfallverhalten: Kein Serviceausfall

Rolling Pool Upgrade (2)

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Stellen Sie sicher, dass der Pool über genügend Kapazität verfügt, um Ihre Arbeitslast mit einem Host weniger im Pool auszuführen. Während des Upgrade-Vorgangs wird jeder Host einzeln entfernt. Die verbleibenden Hosts müssen in der Lage sein, alle erforderlichen VMs auszuführen.

   Wenn im Pool nicht genügend Kapazität vorhanden ist, sind einige Maschinen während des Upgrade-Vorgangs möglicherweise nicht verfügbar. Wenn möglich, können Sie alle unkritischen VMs während des Upgrade-Vorgangs aussetzen.

2. Stellen Sie sicher, dass alle vom XenServer-Pool bereitgestellten Maschinen eingeschaltet und bei Citrix Virtual Apps and Desktops in den entsprechenden Bereitstellungsgruppen registriert sind.

   - Für nicht verwaltete Maschinen:
     - Verwenden Sie XenCenter, um zu bestätigen, dass alle VMs eingeschaltet sind.
     - Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
   - Für Maschinen mit Energieverwaltung:
     - Stellen Sie sicher, dass alle Maschinen eingeschaltet sind (mithilfe von XenCenter, Citrix Studio oder Web Studio).
     - **Gehen Sie wie folgt vor, um den Start neuer Sitzungen während des Upgrade-Vorgangs zu ermöglichen:**
       * Versetzen Sie die Maschinen nicht in den Wartungsmodus.
       * Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
       * Deaktivieren Sie alle Energieverwaltungsschemata, die Maschinen aussetzen könnten.
       * Stellen Sie sicher, dass keine anderen Prozesse die Maschinen ausschalten oder aussetzen könnten.
     - **Wenn es akzeptabel ist, dass neue Sitzungen während des Upgrades nicht gestartet werden können:**
       * Versetzen Sie die Hosting-Verbindung in den Wartungsmodus. Weitere Informationen finden Sie unter Wartungsmodus für eine Verbindung ein- oder ausschalten.
       * Informieren Sie die Endbenutzer darüber, dass sie sich während des Upgrades nicht erneut verbinden können, wenn sie sich abmelden.

     Weitere Informationen finden Sie unter Maschinen mit Energieverwaltung in einer Bereitstellungsgruppe.

   - Für Maschinen, die von Machine Creation Services verwaltet werden
     - Folgen Sie den gleichen Anweisungen wie für Maschinen mit Energieverwaltung im vorherigen Listenpunkt.

  - Versuchen Sie außerdem nicht, während des gesamten Upgrade-Zeitraums neue Maschinen zu erstellen.

3. Starten Sie in XenCenter den Rolling Pool Upgrade-Assistenten und wählen Sie den automatischen Modus. Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.
4. Stellen Sie den Betrieb Ihrer Umgebung auf die gewohnte Konfiguration wieder her.
   - Entfernen Sie alle Wartungsmodus-Flags, die in früheren Schritten gesetzt wurden.
   - Machen Sie alle in den vorherigen Schritten vorgenommenen Anpassungen des Energieverwaltungsschemas rückgängig.

Fall 3: Zugewiesene Desktops, die in einem Pool mit lokalem Speicher oder auf einem eigenständigen Host ausgeführt werden

Dieser Anwendungsfall deckt eigenständige XenServer-Hosts oder Pools ab, die keinen gemeinsamen Speicher haben und deren primäre Workload entweder virtuelle Einzelsitzungs-Desktops mit dem zugewiesenen Maschinenzuordnungstyp sind.

Empfohlene Optionen für das Upgrade:

- Rolling Pool Upgrade Verwenden Sie RPU im automatischen Modus in einem einzigen Wartungsfenster. Dies setzt voraus, dass alle Benutzer während des gesamten Upgrades einen Ausfall haben, was jedoch einen geringeren Verwaltungsaufwand für einen Pool mit sich bringt.
  - Geschätzte Upgrade-Zeit: Die Anzahl der Hosts im Pool multipliziert mit der Upgrade-Zeit für einen einzelnen Host. (**N x 35 Minuten**)
  - Ausfallverhalten: Alle Maschinen befinden sich während der gesamten Upgrade-Zeit im Wartungsmodus von Citrix Virtual Apps and Desktops.
- Manuelles Upgrade Dieser Modus bietet den geringsten Ausfall für jeden Benutzer während des Upgrades, ist jedoch für den Administrator aufwändiger
  - Geschätzte Upgrade-Zeit: Das Doppelte der Upgrade-Zeit für einen einzelnen Host. (**Ungefähr 70 Minuten**)
  - Ausfallverhalten: Jeder Desktop ist während der Upgrade-Zeit für seinen individuellen Host nicht verfügbar. Diese Zeit beträgt in der Regel 35 Minuten.

Rolling Pool Upgrade (3)

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Versetzen Sie alle Bereitstellungsgruppen oder Kataloge, die Maschinen aus dem Pool bereitstellen, in den Wartungsmodus.

   Während sich die Maschinen im Wartungsmodus befinden, können keine neuen Sitzungen auf Maschinen im Pool gestartet werden. Bestehende Sitzungen werden beibehalten, bis die Maschinen heruntergefahren oder angehalten werden.

   Weitere Informationen finden Sie unter Verhindern, dass Benutzer eine Verbindung zu einer Maschine in einer Bereitstellungsgruppeherstellen.

2. Informieren Sie alle betroffenen Benutzer über den bevorstehenden Ausfall. Geben Sie eine Zeit an, bis zu der sie ihre Sitzungen beenden müssen, und geben Sie an, wann der Dienst wiederhergestellt wird.

3. Suchen Sie nach verbleibenden Sitzungen auf betroffenen Computern und ergreifen Sie die entsprechenden Maßnahmen für diese Sitzungen.

4. Starten Sie in XenCenter den Rolling Pool Upgrade-Assistenten und wählen Sie den automatischen Modus. Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.

   Wenn das Upgrade abgeschlossen ist, werden alle VMs, die im Rahmen des Rolling Pool-Upgrades gesperrt wurden, neu gestartet.

5. Schalten Sie die Maschinen aus dem Wartungsmodus.

   Neue Sitzungen können jetzt gestartet und der volle Service wieder aufgenommen werden.

Manuelles Upgrade (3)

Sie können diesen manuellen Vorgang verwenden, um zuerst den Poolkoordinator und dann alle anderen Hosts parallel zu aktualisieren, um die Gesamtausfallzeit erheblich zu reduzieren.

> **Hinweis:**
>
> Mit dem parallelen Upgrade-Ansatz ändert sich das Risikoprofil. Wenn während des Upgrades ein Problem auftritt, wird es möglicherweise erst erkannt, nachdem alle Hosts aktualisiert wurden und das Problem auftritt. Wenn Sie dagegen Ihre Hosts sequentiell aktualisieren, können Sie überprüfen, ob das Upgrade auf jedem Host erfolgreich war, bevor Sie mit dem nächsten fortfahren.

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Stellen Sie sicher, dass alle vom XenServer-Pool oder Host bereitgestellten Maschinen eingeschaltet und bei Citrix Virtual Apps and Desktops in den entsprechenden Bereitstellungsgruppen registriert sind.

- Für nicht verwaltete Maschinen:
  - Verwenden Sie XenCenter, um zu bestätigen, dass alle VMs eingeschaltet sind.
  - Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
- Für Maschinen mit Energieverwaltung:
  - Stellen Sie sicher, dass alle Maschinen eingeschaltet sind (mit XenCenter oder Studio).
  - **Gehen Sie wie folgt vor, um den Start neuer Sitzungen während des Upgrade-Vorgangs zu ermöglichen:**
    * Versetzen Sie die Maschinen nicht in den Wartungsmodus.
    * Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
    * Deaktivieren Sie alle Energieverwaltungsschemata, die Maschinen aussetzen könnten.
    * Stellen Sie sicher, dass keine anderen Prozesse die Maschinen ausschalten oder aussetzen könnten.
  - **Wenn es akzeptabel ist, dass neue Sitzungen während des Upgrades nicht gestartet werden können:**
    * Versetzen Sie die Hosting-Verbindung in den Wartungsmodus. Weitere Informationen finden Sie unter Wartungsmodus für eine Verbindung ein- oder ausschalten.
    * Informieren Sie die Endbenutzer darüber, dass sie sich während des Upgrades nicht erneut verbinden können, wenn sie sich abmelden.

  Weitere Informationen finden Sie unter Maschinen mit Energieverwaltung in einer Bereitstellungsgruppe.
- Für Maschinen, die von Machine Creation Services verwaltet werden
  - Folgen Sie den gleichen Anweisungen wie für Maschinen mit Energieverwaltung im vorherigen Listenpunkt.
  - Versuchen Sie außerdem nicht, während des gesamten Upgrade-Zeitraums Maschinen zu erstellen.

2. Identifizieren Sie den Poolkoordinator und die zugehörigen VMs.
3. Versetzen Sie die Maschinen im Katalog auf dem Poolkoordinator-Host in den Wartungsmodus.
4. Verwenden Sie Director, Citrix Studio oder Web Studio, um Nachrichten an Benutzer zu senden, die noch mit aktiven Sitzungen verbunden sind, und warnen Sie sie, dass ihr Desktop für einen bestimmten Zeitraum offline ist. Dieser Zeitraum ist die Upgrade-Zeit für diesen einzelnen Host (ungefähr 35 Minuten).
5. Aktualisieren Sie den Pool-Koordinator mithilfe der xe-CLI:

a) Deaktivieren Sie den Pool-Koordinator. Dadurch wird verhindert, dass neue VMs auf dem angegebenen Host gestartet oder auf diesen migriert werden.

```
xe host-disable host=<uuid_or_name_label>
```

b) Stellen Sie sicher, dass keine VMs auf dem Poolkoordinator ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

- Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:

  ```
  xe vm-shutdown
  ```

- Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:

  ```
  xe vm-suspend
  ```

- Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

  ```
  xe vm-migrate
  ```

  Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

- Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

  ```
  xe host-evacuate
  ```

  Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

c) Fahren Sie den Poolkoordinator herunter.

```
xe host-shutdown
```

> **Wichtig:**
>
> Sie können den Poolkoordinator erst kontaktieren, wenn das Upgrade des Poolkoordinators abgeschlossen ist. Durch das Herunterfahren des Poolkoordinators wechseln die anderen Hosts im Pool in den *Notfallmodus*. Hosts können in den Notfallmodus wechseln, wenn sie sich in einem Pool befinden, dessen Pool-Koordinator aus dem Netzwerk verschwunden ist und nach mehreren Versuchen nicht kontaktiert werden kann. Virtuelle Rechner werden im Notfallmodus weiterhin auf Hosts ausgeführt, Steuervorgänge sind jedoch nicht verfügbar.

d) Starten Sie den Poolkoordinator mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).

e) Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.

Wenn Ihr Pool-Koordinator neu gestartet wird, verlassen die anderen Hosts im Pool den Notfallmodus und der normale Dienst wird nach einigen Minuten wiederhergestellt.

f) Starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.

g) Migrieren Sie alle gewünschten VMs zurück zum Poolkoordinator.

Wenn das Upgrade des Poolkoordinators durch irgendetwas unterbrochen wird oder das Upgrade aus irgendeinem Grund fehlschlägt, versuchen Sie nicht, mit dem Upgrade fortzufahren. Starten Sie den Pool-Koordinator neu und stellen Sie eine funktionierende Version wieder her.

6. Nachdem der Pool-Koordinator aktualisiert wurde, beenden Sie den Wartungsmodus für die Maschinen auf dem Pool-Koordinator in Citrix Studio oder Web Studio.
7. Führen Sie die folgenden Schritte parallel für alle verbleibenden Hosts im Pool aus:

   a) Versetzen Sie die Maschinen im Katalog auf dem Host in den Wartungsmodus.

   b) Verwenden Sie Director, Citrix Studio oder Web Studio, um Nachrichten an Benutzer zu senden, die noch mit aktiven Sitzungen verbunden sind, und warnen Sie sie, dass ihr Desktop für einen bestimmten Zeitraum offline ist. Dieser Zeitraum ist die Upgrade-Zeit für diesen einzelnen Host (ungefähr 35 Minuten).

   c) Deaktivieren Sie den Host mithilfe der xe-CLI.

   ```
   xe host-disable host-selector=<host_selector_value>
   ```

   d) Stellen Sie sicher, dass keine virtuellen Maschinen auf dem Host ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:

     ```
     xe vm-shutdown
     ```

   - Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:

     ```
     xe vm-suspend
     ```

   - Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

     ```
     xe vm-migrate
     ```

     Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

     ```
     xe host-evacuate
     ```


Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

e) Fahren Sie den Host herunter.

```
1 xe host-shutdown
```

f) Starten Sie den Host mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).

g) Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.

h) Nachdem das Host-Upgrade abgeschlossen ist, starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.

i) Migrieren Sie alle virtuellen Maschinen, die Sie möchten, zurück zum Host.

Wenn das Upgrade eines untergeordneten Hosts fehlschlägt oder unterbrochen wird, müssen Sie es nicht rückgängig machen. Führen Sie den Befehl `xe host-forget` im Pool aus, um diesen Host zu vergessen. Installieren Sie XenServer erneut auf dem Host und fügen Sie ihn dann mit dem Befehl `xe pool-join`als neuen Host dem Pool hinzu.

8. Nachdem die XenServer-Hosts aktualisiert wurden, beenden Sie die Maschinen in Citrix Studio oder Web Studio aus dem Wartungsmodus.

Fall 4: Andere Workloads, die in einem Pool mit lokalem Speicher oder auf einem eigenständigen Host ausgeführt werden

Dieser Anwendungsfall deckt XenServer-Pools mit gemeinsam genutztem Speicher ab, deren primäre Workload virtuelle Desktops mit einer Sitzung oder virtuelle Anwendungen mit mehreren Sitzungen mit dem Zuordnungstyp zufällige Maschinenzuweisung sind.

Für alle Workloads, die von Citrix Virtual Apps and Desktops verwaltet werden, einschließlich solcher, die von Citrix Provisioning und Machine Creation Services mit Energieverwaltung verwaltet werden, können Sie während des Upgrades keine vollständige Workload aufrechterhalten. Die Energieverwaltung von Maschinen kann während des Upgrade-Vorgangs problematisch sein. Sie können die Energieverwaltung nicht deaktivieren, ohne auch die Erstellung neuer Sitzungen zu deaktivieren.

Empfohlene Optionen für das Upgrade:

- Upgrade des rollenden Pools
  - Geschätzte Upgrade-Zeit: Die Anzahl der Hosts im Pool multipliziert mit der Upgrade-Zeit für einen einzelnen Host. (**N x 35 Minuten**)
  - Ausfallverhalten: Alle Maschinen befinden sich während der gesamten Upgrade-Zeit im Wartungsmodus von Citrix Virtual Apps and Desktops.

- Manuelles Upgrade
  - Geschätzte Upgrade-Zeit: Das Doppelte der Upgrade-Zeit für einen einzelnen Host. (**Ungefähr 70 Minuten**)
  - Ausfallverhalten: Alle Maschinen befinden sich während der gesamten Upgrade-Zeit im Wartungsmodus von Citrix Virtual Apps and Desktops.

Wenn möglich, stellen Sie die Workload während des Upgrades dieses Pools von anderen XenServer-Pools mit Kapazität zur Verfügung. Dieser Ansatz kann während des Upgrades zu einer verringerten Kapazität führen. Wenn Sie keine Kapazität für die Workload auf Ihren anderen XenServer-Hosts und -Pools haben, empfehlen wir Ihnen, einen Ausfall für alle Maschinen in Ihrem Workload zu melden.

Rolling Pool Upgrade (4)

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Versetzen Sie alle Maschinen im Pool in den Wartungsmodus. Wenn alle Maschinen dieselbe Verbindung verwenden, können Sie den gesamten Maschinenkatalog in den Wartungsmodus versetzen.
2. Informieren Sie alle betroffenen Benutzer über den bevorstehenden Ausfall.
   - Wenn auf den Computern in diesem Pool immer noch Sitzungen ausgeführt werden, bitten Sie die Benutzer, sich abzumelden, oder erzwingen Sie das Ende ihrer Sitzungen.
   - Informieren Sie die Benutzer darüber, dass sie sich nach dem Abmelden erst wieder anmelden können, wenn der volle Service wieder aufgenommen wird.
3. Starten Sie in XenCenter den Rolling Pool Upgrade-Assistenten und wählen Sie den automatischen Modus. Weitere Informationen finden Sie unter Rolling Pool-Upgrade mithilfe von XenCenter.

   Wenn das Upgrade abgeschlossen ist, werden alle VMs, die im Rahmen des Rolling Pool-Upgrades gesperrt wurden, neu gestartet.
4. Schalten Sie die Maschinen aus dem Wartungsmodus.

   Neue Sitzungen können jetzt gestartet und der volle Service wieder aufgenommen werden.

Manuelles Upgrade (4)

Sie können diesen manuellen Vorgang verwenden, um zuerst den Poolkoordinator und dann alle anderen Hosts parallel zu aktualisieren, um die Gesamtausfallzeit erheblich zu reduzieren.

> **Hinweis:**
>
> Mit dem parallelen Upgrade-Ansatz ändert sich das Risikoprofil. Wenn während des Upgrades ein Problem auftritt, wird es möglicherweise erst erkannt, nachdem alle Hosts aktualisiert wurden und das Problem auftritt. Wenn Sie dagegen Ihre Hosts sequentiell aktualisieren, können Sie überprüfen, ob das Upgrade auf jedem Host erfolgreich war, bevor Sie mit dem nächsten fortfahren.

Lesen Sie die Schritte und Anleitungen unter Bevor Sie beginnen.

1. Stellen Sie sicher, dass alle vom XenServer-Pool oder Host bereitgestellten Maschinen eingeschaltet und bei Citrix Virtual Apps and Desktops in den entsprechenden Bereitstellungsgruppen registriert sind.

   - Für nicht verwaltete Maschinen:
     - Verwenden Sie XenCenter, um zu bestätigen, dass alle VMs eingeschaltet sind.
     - Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
   - Für Maschinen mit Energieverwaltung:
     - Stellen Sie sicher, dass alle Maschinen eingeschaltet sind (mit XenCenter oder Studio).
     - **Gehen Sie wie folgt vor, um den Start neuer Sitzungen während des Upgrade-Vorgangs zu ermöglichen:**
       * Versetzen Sie die Maschinen nicht in den Wartungsmodus.
       * Führen Sie während des Upgrade-Vorgangs keine manuellen Maßnahmen zur Stromversorgung durch.
       * Deaktivieren Sie alle Energieverwaltungsschemata, die Maschinen aussetzen könnten.
       * Stellen Sie sicher, dass keine anderen Prozesse die Maschinen ausschalten oder aussetzen könnten.
     - **Wenn es akzeptabel ist, dass neue Sitzungen während des Upgrades nicht gestartet werden können:**
       * Versetzen Sie die Hosting-Verbindung in den Wartungsmodus. Weitere Informationen finden Sie unter Wartungsmodus für eine Verbindung ein- oder ausschalten.
       * Informieren Sie die Endbenutzer darüber, dass sie sich während des Upgrades nicht erneut verbinden können, wenn sie sich abmelden.

   Weitere Informationen finden Sie unter Maschinen mit Energieverwaltung in einer Bereitstellungsgruppe.

   - Für Maschinen, die von Machine Creation Services verwaltet werden

- Folgen Sie den gleichen Anweisungen wie für Maschinen mit Energieverwaltung im vorherigen Listenpunkt.
- Versuchen Sie außerdem nicht, während des gesamten Upgrade-Zeitraums Maschinen zu erstellen.

2. Identifizieren Sie den Poolkoordinator und die zugehörigen VMs.
3. Versetzen Sie die Maschinen im Katalog auf dem Poolkoordinator-Host in den Wartungsmodus.
4. Verwenden Sie Director, Citrix Studio oder Web Studio, um Nachrichten an Benutzer zu senden, die noch mit aktiven Sitzungen verbunden sind, und warnen Sie sie, dass ihr Desktop für einen bestimmten Zeitraum offline ist. Dieser Zeitraum ist die Upgrade-Zeit für diesen einzelnen Host (ungefähr 35 Minuten).
5. Aktualisieren Sie den Pool-Koordinator mithilfe der xe-CLI:

   a) Deaktivieren Sie den Pool-Koordinator. Dadurch wird verhindert, dass neue VMs auf dem angegebenen Host gestartet oder auf diesen migriert werden.

   ```
   xe host-disable host=<uuid_or_name_label>
   ```

   b) Stellen Sie sicher, dass keine VMs auf dem Poolkoordinator ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:

     ```
     xe vm-shutdown
     ```

   - Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:

     ```
     xe vm-suspend
     ```

   - Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

     ```
     xe vm-migrate
     ```

     Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

   - Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

     ```
     xe host-evacuate
     ```

     Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

   c) Fahren Sie den Poolkoordinator herunter.

   ```
   xe host-shutdown
   ```


> **Wichtig:**
>
> Sie können den Poolkoordinator erst kontaktieren, wenn das Upgrade des Poolkoordinators abgeschlossen ist. Durch das Herunterfahren des Poolkoordinators wechseln die anderen Hosts im Pool in den *Notfallmodus*. Hosts können in den Notfallmodus wechseln, wenn sie sich in einem Pool befinden, dessen Pool-Koordinator aus dem Netzwerk verschwunden ist und nach mehreren Versuchen nicht kontaktiert werden kann. Virtuelle Rechner werden im Notfallmodus weiterhin auf Hosts ausgeführt, Steuervorgänge sind jedoch nicht verfügbar.

d) Starten Sie den Poolkoordinator mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).

e) Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.

Wenn Ihr Pool-Koordinator neu gestartet wird, verlassen die anderen Hosts im Pool den Notfallmodus und der normale Dienst wird nach einigen Minuten wiederhergestellt.

f) Starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.

g) Migrieren Sie alle gewünschten VMs zurück zum Poolkoordinator.

Wenn das Upgrade des Poolkoordinators durch irgendetwas unterbrochen wird oder das Upgrade aus irgendeinem Grund fehlschlägt, versuchen Sie nicht, mit dem Upgrade fortzufahren. Starten Sie den Pool-Koordinator neu und stellen Sie eine funktionierende Version wieder her.

6. Nachdem der Pool-Koordinator aktualisiert wurde, beenden Sie den Wartungsmodus für die Maschinen auf dem Pool-Koordinator in Citrix Studio oder Web Studio.

7. Führen Sie die folgenden Schritte parallel für alle verbleibenden Hosts im Pool aus:

a) Versetzen Sie die Maschinen im Katalog auf dem Host in den Wartungsmodus.

b) Verwenden Sie Director, Citrix Studio oder Web Studio, um Nachrichten an Benutzer zu senden, die noch mit aktiven Sitzungen verbunden sind, und warnen Sie sie, dass ihr Desktop für einen bestimmten Zeitraum offline ist. Dieser Zeitraum ist die Upgrade-Zeit für diesen einzelnen Host (ungefähr 35 Minuten).

c) Deaktivieren Sie den Host mithilfe der xe-CLI.

```
xe host-disable host-selector=<host_selector_value>
```

d) Stellen Sie sicher, dass keine virtuellen Maschinen auf dem Host ausgeführt werden. Fahren Sie VMs herunter, setzen Sie sie aus oder migrieren Sie sie auf andere Hosts im Pool.

- Verwenden Sie den folgenden Befehl, um eine VM herunterzufahren:


```
xe vm-shutdown
```

- Verwenden Sie den folgenden Befehl, um eine VM anzuhalten:

```
xe vm-suspend
```

- Verwenden Sie den folgenden Befehl, um eine bestimmte VM zu migrieren:

```
xe vm-migrate
```

Durch die Migration bestimmter VMs auf bestimmte Hosts haben Sie die volle Kontrolle über die Verteilung der migrierten VMs auf andere Hosts im Pool.

- Verwenden Sie den folgenden Befehl, um den Host zu evakuieren:

```
xe host-evacuate
```

Beim Evakuieren aller VMs von einem Host verbleibt die Verteilung der migrierten VMs an XenServer.

e) Fahren Sie den Host herunter.

```
xe host-shutdown
```

f) Starten Sie den Host mit dem XenServer-Installationsmedium und der Methode Ihrer Wahl (z. B. USB oder Netzwerk).

g) Befolgen Sie das XenServer-Installationsverfahren, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. Wählen Sie Upgrade.

h) Nachdem das Host-Upgrade abgeschlossen ist, starten oder setzen Sie alle heruntergefahrenen oder angehaltenen VMs fort.

i) Migrieren Sie alle virtuellen Maschinen, die Sie möchten, zurück zum Host.

Wenn das Upgrade eines untergeordneten Hosts fehlschlägt oder unterbrochen wird, müssen Sie es nicht rückgängig machen. Führen Sie den Befehl `xe host-forget` im Pool aus, um diesen Host zu vergessen. Installieren Sie XenServer erneut auf dem Host und fügen Sie ihn dann mit dem Befehl `xe pool-join`als neuen Host dem Pool hinzu.

8. Nachdem die XenServer-Hosts aktualisiert wurden, beenden Sie die Maschinen in Citrix Studio oder Web Studio aus dem Wartungsmodus.

Pools im gemischten Modus

Ein Pool im gemischten Modus ist ein Pool, bei dem Hosts im Pool verschiedene Versionen von XenServer verwenden. Betreiben Sie Ihren Pool nicht länger als nötig im gemischten Modus (mit

mehreren Versionen von XenServer), da der Pool während des Upgrades in einem herabgesetzten Zustand arbeitet. In diesem heruntergestuften Zustand sind bestimmte VM-, SR-, VDI- und Host-Operationen blockiert. VMs, die auf einem Host in der höheren Version von XenServer ausgeführt wurden, können nicht auf einen Host in der niedrigeren Version von XenServer migriert oder auf diesem gestartet werden.

Pools im gemischten Modus werden für die Standardnutzung nicht unterstützt und werden nur als Übergangsstatus während des Upgrades eines Pools unterstützt. Wenn bei der Ausführung im gemischten Modus ein Problem auftritt, werden Sie vom technischen Support aufgefordert, Ihr Pool-Upgrade abzuschließen und das Problem dann in einem nicht gemischten Pool zu reproduzieren.

Nachdem Sie die Upgrade-Optionen für Ihre Citrix Virtual Apps and Desktops-Umgebung überprüft haben, dauert Ihr geplanter XenServer-Upgrade-Pfad möglicherweise länger als das verfügbare Wartungsfenster. Wenn möglich, verlängern Sie das Wartungsfenster, damit Ihr XenServer-Upgrade darin abgeschlossen werden kann. Wenn dies nicht möglich ist, können Sie den Pool bis zu Ihrem nächsten Wartungsfenster im gemischten Modus ausführen. Wenn Sie Ihren Pool jedoch im gemischten Modus ausführen, erhöht sich die Wahrscheinlichkeit unerwarteter Verhaltensweisen oder Probleme, die dazu führen könnten, dass Sie stattdessen ein Notfallwartungsfenster benötigen. Planen Sie ein, die Zeit, die Ihr Pool im gemischten Modus verbringt, so gering wie möglich zu halten.

Wenn Ihre Citrix Virtual Apps and Desktops-Umgebung vorübergehend auf einem XenServer-Pool im gemischten Modus ausgeführt wird, beachten Sie das folgende Verhalten:

- Bei gepoolten Desktop-Workloads, bei denen die VMs vor ihrer Wiederverwendung neu gestartet werden müssen, werden die VMs nur auf den Hosts neu gestartet, auf denen die neuere Version von XenServer ausgeführt wird. Die effektive Kapazität des Pools ist begrenzt. Je nachdem, wie viele Hosts in Ihrem Pool aktualisiert wurden, reicht die Kapazität möglicherweise nicht aus, um alle erforderlichen VMs neu zu starten. Dieses Verhalten kann zu Fehlern führen und einige Benutzer von Citrix Virtual Apps and Desktops können möglicherweise nicht auf ihre erforderlichen Sitzungen zugreifen.
- Wenn Sie dedizierte Maschinen haben, die lokalen Speicher verwenden und sich auf Hosts befinden, auf denen die ältere Version von XenServer ausgeführt wird, können diese VMs gestoppt werden, aber sie können erst neu gestartet werden, wenn das Upgrade abgeschlossen ist und sich der Pool nicht mehr im gemischten Modus befindet.

IntelliCache

April 12, 2024

> **Hinweis:**
>
> Diese Funktion wird nur unterstützt, wenn XenServer Premium Edition mit Citrix Virtual Desktops verwendet wird.
>
> Intellicache wird nicht für VMs unterstützt, die eine GFS2- oder XFS-SR verwenden.

Durch die Verwendung von XenServer mit *IntelliCache* werden gehostete Virtual Desktop Infrastructure-Bereitstellungen kostengünstiger, da Sie eine Kombination aus gemeinsam genutztem Speicher und lokalem Speicher verwenden können. Dies ist von besonderem Vorteil, wenn viele virtuelle Maschinen (VMs) alle ein gemeinsames Betriebssystemimage teilen. Die Belastung des Speicher-Arrays wird reduziert und die Leistung wird verbessert. Darüber hinaus wird der Netzwerkverkehr zu und von gemeinsam genutztem Speicher reduziert, da der lokale Speicher das primäre Image aus dem gemeinsam genutzten Speicher zwischenspeichert.

IntelliCache speichert Daten von einem übergeordneten VDI einer virtuellen Maschine im lokalen Speicher auf dem VM-Host. Dieser lokale Cache wird dann gefüllt, während Daten vom übergeordneten VDI gelesen werden. Wenn viele VMs einen gemeinsamen übergeordneten VDI gemeinsam nutzen, kann eine VM die von einer anderen VM in den Cache gelesenen Daten verwenden. Weiterer Zugriff auf das primäre Image auf Shared Storage ist nicht erforderlich.

Für IntelliCache ist eine lokale SR mit Thin-Provisioning erforderlich. Thin Provisioning ist eine Möglichkeit, die Nutzung des verfügbaren Speichers zu optimieren. Mit diesem Ansatz können Sie den lokalen Speicher anstelle des gemeinsam genutzten Speichers stärker nutzen. Es stützt sich auf die On-Demand-Zuweisung von Datenblöcken. Bei anderen Ansätzen werden alle Blöcke im Voraus zugewiesen.

> **Wichtig:**
>
> Thin Provisioning ändert den standardmäßigen lokalen Speichertyp des Hosts von LVM zu EXT4. Thin Provisioning **muss aktiviert sein**, damit das lokale Caching von Citrix Virtual Desktops ordnungsgemäß funktioniert.

Thin Provisioning ermöglicht es dem Administrator, den VMs, die sich mit dem Speicherrepository (SR) verbinden, mehr Speicherplatz zu präsentieren, als in dem SR verfügbar ist. Es gibt keine Speichergarantien, und die Zuweisung einer LUN beansprucht keine Datenblöcke, bis die VM Daten schreibt.

> **Warnung:**
>
> Für SRs mit Thin Provisioning kann der physische Speicherplatz knapp werden, da die darin enthaltenen VMs wachsen und bei Bedarf Datenträgerkapazität verbrauchen können. IntelliCache-VMs behandeln diese Bedingung, indem sie automatisch auf den gemeinsam genutzten Speicher zurückgreifen, wenn der lokale SR-Cache voll ist. Mischen Sie keine herkömmlichen

> virtuellen Maschinen und IntelliCache-VMs auf demselben SR, da IntelliCache-VMs schnell an Größe zunehmen können.

IntelliCache-Bereitstellung

IntelliCache muss entweder während der Host-Installation aktiviert werden oder manuell auf einem laufenden Host über die CLI aktiviert werden.

Wir empfehlen die Verwendung eines lokalen Hochleistungsspeichergeräts, um eine schnellstmögliche Datenübertragung zu gewährleisten. Verwenden Sie beispielsweise eine Solid State Disk oder ein Hochleistungs-RAID-Array. Berücksichtigen Sie bei der Dimensionierung lokaler Datenträger sowohl Datendurchsatz als auch Speicherkapazität. Der freigegebene Speichertyp, der zum Hosten des Virtual Disk Image (VDI) verwendet wird, muss NFS- oder EXT3/EXT4-basiert sein.

Auf Host-Installation aktivieren

Um IntelliCache während der Hostinstallation zu aktivieren, wählen Sie im Bildschirm **Virtual Machine Storage** die Option **Thin Provisioning aktivieren**aus. Diese Option wählt das lokale SR des Hosts aus, das für das lokale Zwischenspeichern von VM-VDIs verwendet werden soll.

Konvertieren eines vorhandenen Hosts zur Verwendung von Thin Provisioning

Um eine bestehende lokale LVM-SR zu löschen und sie durch eine EXT3/EXT4-SR mit Thin-Provisioning zu ersetzen, geben Sie die folgenden Befehle ein.

> **Warnung:**
>
> Mit diesen Befehlen wird Ihr vorhandenes lokales SR entfernt, und die VMs auf dem SR werden

> dauerhaft gelöscht.

```
    localsr=`xe sr-list type=lvm host=hostname params=uuid --minimal`
        echo localsr=$localsr
        pbd=`xe pbd-list sr-uuid=$localsr params=uuid --minimal`
        echo pbd=$pbd
        xe pbd-unplug uuid=$pbd
        xe pbd-destroy uuid=$pbd
        xe sr-forget uuid=$localsr
        sed -i "s/'lvm'/'ext'/" /etc/firstboot.d/data/default-storage.
            conf
        rm -f /var/lib/misc/ran-storage-init
        systemctl restart storage-init.service
        xe sr-list type=ext
<!--NeedCopy-->
```

Um das lokale Caching zu aktivieren, geben Sie die folgenden Befehle ein:

```
    xe host-disable host=hostname
        localsr=`xe sr-list type=ext host=hostname params=uuid --
            minimal`
        xe host-enable-local-storage-caching host=hostname sr-uuid=
            $localsr
        xe host-enable host=hostname
<!--NeedCopy-->
```

VM-Verhalten mit Intellicache

Das VDI-Flag `on-boot` bestimmt das Verhalten eines VM-VDI beim Booten der VM, und das VDI-Flag `allow-caching` bestimmt das Caching-Verhalten.

Die für diese Parameter zu verwendenden Werte hängen vom Typ der VM ab, die Sie erstellen, und von ihrem Verwendungszweck:

- **Für gemeinsam genutzte oder zufällig zugewiesene Maschinen:**
  - Setzen Sie den Parameter `on-boot` auf `reset`.
  - Setzen Sie den Parameter `allow-caching` auf **`true`**

  Beispiel:

  ```
  xe vdi-param-set uuid=vdi_uuid on-boot=reset allow-caching=true
  <!--NeedCopy-->
  ```

  Beim Start der VM wird der VDI in den Zustand zurückgesetzt, in dem er sich beim vorherigen Start befand. Alle Änderungen während der Ausführung der VM gehen verloren, wenn die VM das nächste Mal gestartet wird. Neue VM-Daten werden nur in den lokalen Speicher geschrieben. Es gibt keine Schreibvorgänge in den gemeinsam genutzten Speicher. Dieser Ansatz bedeutet,

dass die Belastung des gemeinsam genutzten Speichers reduziert wird. Die VM kann jedoch nicht zwischen Hosts migriert werden.

Wählen Sie diese Option, wenn Sie standardisierte Desktops bereitstellen möchten, an denen Benutzer keine dauerhaften Änderungen vornehmen können.

- **Für statische oder dedizierte Maschinen:**
  - Setzen Sie den Parameter `on-boot` auf `persist`.
  - Setzen Sie den Parameter `allow-caching` auf **`true`**

  Beispiel:

```
1  xe vdi-param-set uuid=vdi_uuid on-boot=persist allow-caching=true
2  <!--NeedCopy-->
```

  Beim Start der VM befindet sich der VDI in dem Zustand, in dem er beim letzten Herunterfahren belassen wurde. Neue VM-Daten werden sowohl in den lokalen als auch in den gemeinsamen Speicher geschrieben. Das Lesen von zwischengespeicherten Daten erfordert keinen E/A-Verkehr zum freigegebenen Speicher, sodass die Belastung des gemeinsam genutzten Speichers reduziert wird. Eine VM-Migration auf einen anderen Host ist zulässig und der lokale Cache auf dem neuen Host wird beim Lesen der Daten gefüllt.

  Wählen Sie diese Option aus, wenn Sie Benutzern erlauben möchten, dauerhafte Änderungen an ihren Desktops vorzunehmen.

> **Hinweis:**
>
> Für VMs, deren VDIs sich auf einer GFS2-SR befinden, unterscheidet sich das Verhalten der VM beim Booten von VMs mit VDIs auf anderen Arten von SRs. Für VDIs auf einem GFS2 SR wird die On-Boot-Option beim Herunterfahren der VM angewendet, nicht beim VM-Start.

Einzelheiten zur Implementierung und Fehlerbehebung

F: Ist IntelliCache mit Livemigration und Hochverfügbarkeit kompatibel?

A: Sie können Livemigration und Hochverfügbarkeit mit IntelliCache verwenden, wenn sich virtuelle Desktops im privaten Modus befinden, d. h. wenn `on-boot=persist`

> **Warnung:**
>
> Eine VM kann nicht migriert werden, wenn für eines der VDIs Cacheverhaltensflags auf `on-boot=reset` und `allow-caching=true` festgelegt sind. Migrationsversuche für virtuelle Rechner mit diesen Eigenschaften schlagen fehl.

F: Wo ist der lokale Cache auf dem lokalen Datenträger?

A: Der Cache ist in einem Speicherrepository (SR). Jeder Host hat einen Konfigurationsparameter (local-cache-sr), der angibt, welches (lokale) SR für die Cachedateien verwendet werden soll. In der Regel ist dieses SR ein SR vom Typ EXT3/EXT4. Wenn Sie VMs mit IntelliCache ausführen, sehen Sie innerhalb des SRs Dateien mit Namen `uuid.vhdcache`. Diese Datei ist die Cachedatei für den VDI mit der angegebenen UUID. Diese Dateien werden in XenCenter nicht angezeigt. Sie können sie nur anzeigen, indem Sie sich bei dom0 anmelden und den Inhalt von `/var/run/sr-mount/sr-uuid`

F: Wie gebe ich ein bestimmtes SR für die Verwendung als Cache an?

A: Das Host-Objektfeld `local-cache-sr` verweist auf ein lokales SR. Sie können seinen Wert anzeigen, indem Sie den folgenden Befehl ausführen:

```
1 xe sr-list params=local-cache-sr,uuid,name-label
2 <!--NeedCopy-->
```

Dieses Feld ist entweder gesetzt:

- Wenn Sie nach der Hostinstallation die Option “Thin Provisioning aktivieren”im Host-Installationsprogramm ausgewählt haben, oder
- Durch Ausführen von `xe host-enable-local-storage-caching host=host sr-uuid=sr`. Für den Befehl muss der angegebene Host deaktiviert sein. Fahren Sie die virtuellen Maschinen herunter, wenn Sie diesen Befehl verwenden.

Die erste Option verwendet das lokale SR vom Typ EXT3/EXT4 und wird während der Host-Installation erstellt. Die zweite Option verwendet das SR, das in der Befehlszeile angegeben ist.

> **Warnung:**
>
> Diese Schritte sind nur für Benutzer erforderlich, die mehr als ein lokales SR konfiguriert haben.

F: Wann wird der lokale Cache gelöscht?

A: Eine VDI-Cachedatei wird nur gelöscht, wenn der VDI selbst gelöscht wird. Der Cache wird zurückgesetzt, wenn ein VDI an eine VM angeschlossen wird (z. B. beim Start der VM). Wenn der Host beim Löschen des VDI offline ist, führt die SR-Synchronisierung beim Start eine Bereinigung der Cachedatei durch.

> **Hinweis:**
>
> Die Cachedatei wird nicht vom Host gelöscht, wenn eine VM auf einen anderen Host migriert oder heruntergefahren wird.

---

layout: doc
description: If you use Citrix Provisioning for image management and hosting for Citrix Virtual Apps

and Desktops or Citrix DaaS, PVS-Accelerator dramatically improves the already excellent combination of XenServer and Citrix Provisioning.—

PVS-Accelerator

Die XenServer PVS-Accelerator-Funktion bietet erweiterte Funktionen für Kunden, die XenServer mit Citrix Provisioning verwenden. Citrix Provisioning ist eine beliebte Wahl für die Image-Verwaltung und das Hosting für Citrix Virtual Apps and Desktops oder Citrix DaaS. PVS-Accelerator verbessert die bereits hervorragende Kombination von XenServer und Citrix Provisioning erheblich. Zu den Vorteilen, die diese neue Funktion bietet, gehören:

- **Datenlokalität:** Nutzen Sie die Leistung und Lokalität von Speicher-, SSD- und NVM-Geräten für Leseanfragen und reduzieren Sie gleichzeitig die Netzwerkauslastung erheblich.
- **Verbesserte Endbenutzererfahrung:** Die Datenlokalität ermöglicht eine Reduzierung der Lese-I/O-Latenz für zwischengespeicherte Zielgeräte (VMs), wodurch Endbenutzeranwendungen weiter beschleunigt werden.
- **Beschleunigte VM-Boots und Boot-Storms:** Eine reduzierte I/O-Latenz für das Lesen und eine verbesserte Effizienz können die VM-Startzeiten beschleunigen und eine schnellere Leistung ermöglichen, wenn viele Geräte innerhalb eines engen Zeitrahmens hochfahren.
- **Vereinfachtes Skalieren durch Hinzufügen weiterer Hypervisor-Hosts:** Möglicherweise werden weniger Citrix Provisioning-Server benötigt, da die Speicherlast effizient auf alle XenServer-Hosts verteilt wird. Spitzenlasten werden mithilfe des Cache innerhalb der ursprünglichen Hosts behandelt.
- **Geringere Gesamtbetriebskosten und vereinfachte Infrastrukturanforderungen:** Weniger Citrix Provisioning-Server bedeuten eine Reduzierung der Hardware- und Lizenzanforderungen sowie einen geringeren Verwaltungsaufwand. Freigesetzte Kapazität ist für Workloaden verfügbar.

> **Hinweise:**
>
> PVS-Accelerator ist für Kunden der XenServer Premium Edition verfügbar. Um die PVS-Accelerator-Funktion zu verwenden, aktualisieren Sie den Citrix Lizenzserver auf Version 11.14 oder höher.
>
> Um den PVS-Accelerator mit UEFI-fähigen VMs zu verwenden, stellen Sie sicher, dass Sie Citrix Provisioning 1906 oder höher verwenden.

Wie funktioniert der PVS-Beschleuniger

PVS-Accelerator verwendet einen Proxy-Mechanismus, der sich in der Control Domain (dom0) von XenServer befindet. Wenn diese Funktion aktiviert ist, werden Leseanforderungen für Citrix Provisioning-Zielgeräte (VM) direkt auf der XenServer-Hostmaschine zwischengespeichert. Diese Anforderungen werden im physikalischen Speicher oder in einem Speicherrepository zwischengespeichert. Wenn nachfolgende VMs auf diesem XenServer-Host dieselbe Leseanforderung stellen, wird das virtuelle Laufwerk direkt aus dem Cache gestreamt, nicht vom Citrix Provisioning-Server. Die Notwendigkeit, vom Citrix Provisioning Server zu streamen, reduziert die Netzwerkauslastung und -verarbeitung auf dem Server erheblich. Dieser Ansatz führt zu einer erheblichen Verbesserung der VM-Leistung.

Überlegungen

Beachten Sie bei der Verwendung der PVS-Accelerator-Funktion Folgendes:

- Citrix Provisioning-Zielgeräte sind sich ihres Proxy-Status bewusst. Nach der Installation der Funktion ist keine zusätzliche Konfiguration erforderlich.
- In Umgebungen, in denen mehrere Citrix Provisioning-Server mit derselben VHD bereitgestellt werden, aber unterschiedliche Zeitstempel des Dateisystems haben, werden Daten möglicherweise mehrmals zwischengespeichert. Aufgrund dieser Einschränkung empfehlen wir die Verwendung des VHDX-Formats anstelle von VHD für virtuelle Datenträger.
- Verwenden Sie keinen großen Portbereich für die PVS-Serverkommunikation. Das Einstellen eines Bereichs von mehr als 20 Ports auf dem PVS-Server ist selten erforderlich. Ein großer Portbereich kann die Paketverarbeitung verlangsamen und die Startzeit der XenServer-Steuerdomäne verlängern, wenn PVS-Accelerator verwendet wird.
- Nachdem Sie eine VM mit aktiviertem PVS-Beschleuniger gestartet haben, wird der Cache-Status für die VM in XenCenter angezeigt:
  - Auf der Registerkarte **PVS** des Pools oder des Hosts
  - Auf der Registerkarte **Allgemein** für die VM
- Sie können nicht mehr als 200 PVS-Accelerator-fähige VMs auf einem XenServer-Host ausführen.
- Kunden können den korrekten Betrieb des PVS-Accelerators mithilfe von RRD-Metriken auf der Registerkarte **Performance** des Hosts in XenCenter bestätigen. Weitere Informationen finden Sie unter Überwachen und Verwalten Ihrer Bereitstellung.
- Für PVS-Accelerator ist Citrix Provisioning 7.13 oder höher erforderlich.
- Um den PVS-Accelerator mit UEFI-fähigen VMs zu verwenden, stellen Sie sicher, dass Sie Citrix Provisioning 1906 oder höher verwenden.

- PVS-Accelerator ist für Kunden der XenServer Premium Edition verfügbar.
- Für PVS-Accelerator ist Lizenzserver 11.14 oder höher erforderlich.
- Der PVS-Accelerator verwendet Funktionen von OVS und ist daher nicht auf Hosts verfügbar, die Linux Bridge als Netzwerk-Backend verwenden.
- PVS-Accelerator arbeitet an der ersten virtuellen Netzwerkschnittstelle (VIF) einer zwischengespeicherten VM. Verbinden Sie daher das erste VIF mit dem Citrix Provisioning-Speichernetzwerk, damit das Caching funktioniert.
- Der PVS-Beschleuniger kann derzeit nicht an Netzwerk-Ports verwendet werden, die erzwingen, dass IPs an bestimmte MAC-Adressen gebunden sind. Diese Switch-Funktionalität kann als "IP Source Guard"oder ähnlich bezeichnet werden. In solchen Umgebungen starten PVS-Ziele nicht mit dem Fehler "Zeitüberschreitung bei Anmeldeanforderung!"nach der Aktivierung des PVS-Beschleunigers.

PVS-Beschleuniger aktivieren

Kunden müssen die folgenden Konfigurationseinstellungen in XenServer und in Citrix Provisioning vornehmen, um die PVS-Accelerator-Funktion zu aktivieren:

1. Konfigurieren Sie PVS-Accelerator in XenServer mithilfe von XenCenter oder der xe CLI. Diese Konfiguration umfasst das Hinzufügen einer Citrix Provisioning-Site und das Angeben des Speicherorts für den Citrix Provisioning-Cachespeicher.
    - Anweisungen zur CLI finden Sie im *folgenden Abschnitt unter Konfiguration von PVS-Accelerator in XenServer mithilfe der CLI* .
    - Informationen zum Konfigurieren von PVS-Accelerator mit XenCenter finden Sie unter PVS-Accelerator in der XenCenter-Dokumentation.
2. Nachdem Sie PVS-Accelerator in XenServer konfiguriert haben, schließen Sie die Cache-Konfiguration für die PVS-Site mithilfe der PVS-Benutzeroberfläche ab. Ausführliche Anweisungen finden Sie unter Abschließen der Cache-Konfiguration in Citrix Provisioning.

Konfigurieren von Ports

Citrix Provisioning Services verwendet die folgenden Ports:

- 6901, 6902, 6905: Wird für die Bereitstellung der ausgehenden Serverkommunikation verwendet (Pakete, die für das Zielgerät bestimmt sind)
- 6910: Wird für die Zielgerätanmeldung mit Citrix Provisioning Services verwendet
- Konfigurierbarer Zielgerät-Anschluss. Der Standardport ist 6901.
- Konfigurierbarer Serverportbereich. Der Standardbereich ist 6910-6930.

Informationen zu den von Citrix Provisioning Services verwendeten Ports finden Sie unter Von XenServer verwendete Kommunikationsports.

Der konfigurierte Portbereich in XenServer muss alle verwendeten Ports enthalten. Verwenden Sie beispielsweise 6901-6930 für die Standardkonfiguration.

> **Hinweis:**
>
> Verwenden Sie keinen großen Portbereich für die PVS-Serverkommunikation. Das Einstellen eines Bereichs von mehr als 20 Ports auf dem PVS-Server ist selten erforderlich. Ein großer Portbereich kann die Paketverarbeitung verlangsamen und die Startzeit der XenServer-Steuerdomäne verlängern, wenn PVS-Accelerator verwendet wird.

Konfigurieren Sie PVS-Accelerator in XenServer mithilfe der CLI

1. Führen Sie den folgenden Befehl aus, um eine Citrix Provisioning-Site-Konfiguration auf XenServer zu erstellen:

```
PVS_SITE_UUID=$(xe pvs-site-introduce name-label=My PVS Site)
```

2. Geben Sie für jeden Host im Pool an, welcher Cache verwendet werden soll. Sie können den Cache in einem Speicherrepository (SR) oder im Control Domain Memory speichern.

Konfigurieren des Cachespeichers in einem Speicherrepository Beachten Sie die folgenden Merkmale, wenn Sie ein Speicherrepository (SR) als Cachespeicher auswählen:

Vorteile:

- Die zuletzt gelesenen Daten werden bestmöglich im Speicher zwischengespeichert. Der Zugriff auf die Daten kann so schnell erfolgen wie die Verwendung des Control Domain-Speichers.
- Der Cache kann viel größer sein, wenn er sich auf einem SR befindet. Die Kosten für den SR-Speicherplatz betragen typischerweise einen Bruchteil der Kosten des Speicherplatzes. Das Zwischenspeichern auf einem SR kann den Citrix Provisioning-Server stärker entlasten.
- Sie müssen die Speichereinstellung der Control Domain nicht ändern. Der Cache verwendet automatisch den in der Steuerdomäne verfügbaren Speicher und führt niemals dazu, dass der Control Domain der Speicher ausgeht.
- Die Cache-VDIs können im gemeinsam genutzten Speicher gespeichert werden. Diese Wahl des Speichers ist jedoch selten sinnvoll. Dieser Ansatz ist nur sinnvoll, wenn der gemeinsam genutzte Speicher erheblich schneller ist als der Citrix Provisioning-Server.
- Sie können entweder ein dateibasiertes oder ein blockbasiertes SR für den Cachespeicher verwenden.

Nachteile:

- Wenn das SR langsam ist und sich die angeforderten Daten nicht in der Speicherebene befinden, kann der Cachingvorgang langsamer sein als bei einem Citrix Provisioning-Remoteserver.
- Gecachte VDIs, die auf freigegebenem Speicher gespeichert sind, können nicht zwischen Hosts freigegeben werden. Ein zwischengespeicherter VDI ist spezifisch für einen Host.

Führen Sie die folgenden Schritte aus, um den Cachespeicher in einem Speicherrepository zu konfigurieren:

1. Führen Sie den folgenden Befehl aus, um die UUID des SRs zu finden, die für das Zwischenspeichern verwendet werden soll:

```
xe sr-list name-label=Local storage host=host-name-label --minimal
   )
<!--NeedCopy-->
```

2. Erstellen Sie den Cachespeicher.

```
xe pvs-cache-storage-create host=host-name-label pvs-site-uuid=
   PVS_SITE_UUID \
         sr-uuid=SR_UUID size=10GiB
<!--NeedCopy-->
```

> **Hinweis:**
>
> Bei der Auswahl eines Speicherrepository (SR) verwendet die Funktion bis zur angegebenen Cachegröße auf der SR. Es verwendet auch implizit den verfügbaren Control Domain-Speicher als Cache-Stufe nach bestem Aufwand.

Konfigurieren des Cachespeichers im Speicher der Steuerdomäne Beachten Sie bei der Auswahl des Control Domain-Speichers für die Cachespeicherung die folgenden Merkmale:

Vorteile:

Die Verwendung von Speicher bedeutet eine konstant schnelle Lese-/Schreibleistung beim Zugriff auf oder beim Füllen des Caches.

Nachteile:

- Die Hardware muss entsprechend dimensioniert sein, da das für den Cachespeicher verwendete RAM für VMs nicht verfügbar ist.
- Steuerdomänenspeicher muss **vor** der Konfiguration des Cachespeichers erweitert werden

> **Hinweis:**
>
> Wenn Sie den Cache im Speicher der Steuerdomäne speichern möchten, verwendet die Funktion bis zur angegebenen Cachegröße im Speicher der Steuerdomäne. Diese Option ist nur verfügbar, nachdem der Steuerdomäne zusätzlicher Speicher zugewiesen wurde.

> Hinweise zum Erhöhen des Speichers der Steuerdomäne finden Sie unter Ändern der Speichermenge, die der Steuerdomäne zugewiesenist.

Nachdem Sie die Speichermenge erhöht haben, die der Steuerdomäne des Hosts zugewiesen ist, kann der zusätzliche Speicher explizit für den PVS-Beschleuniger zugewiesen werden.

Führen Sie die folgenden Schritte aus, um den Cachespeicher im Speicher der Control Domain zu konfigurieren:

1. Führen Sie den folgenden Befehl aus, um die UUID des Hosts zu finden, der für das Caching konfiguriert werden soll:

```
xe host-list name-label=host-name-label --minimal
<!--NeedCopy-->
```

2. Erstellen Sie ein SR des speziellen Typs `tmpfs`:

```
xe sr-create type=tmpfs name-label=MemorySR host-uuid=
   HOST_UUID device-config:uri=""
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für SRs des speziellen Typs `tmpfs` wird der Wert des erforderlichen Parameters `name-label` ignoriert und stattdessen wird ein fester Name verwendet.

3. Führen Sie den folgenden Befehl aus, um den Cachespeicher zu erstellen:

```
xe pvs-cache-storage-create host-uuid=HOST_UUID
pvs-site-uuid=PVS_SITE_UUID sr-uuid=SR_UUID size=1GiB
<!--NeedCopy-->
```

Wobei `SR_UUID` die UUID des in Schritt b erstellten SRs ist

Schließen Sie die Cache-Konfiguration in Citrix Provisioning ab

Führen Sie nach der Konfiguration von PVS-Accelerator in XenServer die folgenden Schritte aus, um die Cache-Konfiguration für die Citrix Provisioning-Site abzuschließen.

Verwenden Sie in der Citrix Provisioning Administrator Console den Citrix Virtual Desktops Setup-Assistenten oder den Streaming-VM-Assistenten (je nach Bereitstellungstyp), um auf die Proxy-Funktion zuzugreifen. Obwohl beide Assistenten ähnlich sind und sich viele der gleichen Bildschirme teilen, bestehen die folgenden Unterschiede:

- Der **Citrix Virtual Desktops-Setupassistent** wird verwendet, um VMs zu konfigurieren, die auf dem XenServer-Hypervisor ausgeführt werden, der mit Citrix Virtual Desktops gesteuert wird.

- Der **Streaming-VM-Assistent** wird verwendet, um VMs auf einem Host zu erstellen. Citrix Virtual Desktops sind nicht beteiligt.

Starten Sie die Citrix Provisioning Administratorkonsole:

1. Navigieren Sie zur Citrix Provisioning-Site.
2. Wählen Sie die Citrix Provisioning-Site aus und klicken Sie mit der rechten Maustaste, um ein Kontextmenü anzuzeigen
3. Wählen Sie den entsprechenden Assistenten basierend auf der Bereitstellung aus. Wählen Sie die Option **PVS-Beschleuniger für alle virtuellen Maschinen** aktivieren, um den PVS-Beschleuniger zu aktivieren.
4. Wenn Sie das Zwischenspeichern virtueller Datenträger zum ersten Mal aktivieren, wird der **XenServer-Bildschirm** im Setupassistenten für gestreamte virtuelle Maschinen angezeigt. Es wird eine Liste aller Citrix Provisioning-Sites angezeigt, die auf XenServer konfiguriert sind und noch keiner Citrix Provisioning-Site zugeordnet wurden. Wählen Sie aus der Liste eine Citrix Provisioning-Site aus, um PVS-Accelerator anzuwenden. Dieser Bildschirm wird nicht angezeigt, wenn Sie den Assistenten für dieselbe Citrix Provisioning-Site mit demselben XenServer-Host ausführen.
5. Klicken Sie auf **Weiter**, um die Konfiguration des Zwischenspeichers abzuschließen.
6. Klicken Sie auf **Fertigstellen**, um Citrix Virtual Desktops oder gestreamte VMs bereitzustellen und die ausgewählte Citrix Provisioning-Site mit dem PVS Accelerator in XenServer zu verknüpfen. Wenn dieser Schritt abgeschlossen ist, ist die Schaltfläche **PVS-Server anzeigen** im Konfigurationsfenster des **PVS-Accelerator-Konfigurationsfensters** in XenCenter aktiviert. Wenn Sie auf die Schaltfläche **PVS-Server anzeigen** klicken, werden die IP-Adressen aller PVS-Server angezeigt, die mit der Citrix Provisioning-Site verknüpft sind.

Caching-Vorgang

Der PVS-Accelerator cacht:

- **Liest** von virtuellen Datenträger, aber schreibt oder liest nicht aus einem Schreibcache
- **Basiert auf Imageversionen**. Mehrere virtuelle Rechner teilen sich zwischengespeicherte Blöcke, wenn sie dieselbe Image-Version verwenden
- Geräte mit einem beliebigen **nicht persistenten** Schreibcachetyp
- Virtuelle Datenträger mit dem **Zugriffsmodus Standardimage**. Es funktioniert nicht für virtuelle Datenträger mit dem Zugriffsmodus Privatimage
- Geräte, die als **Typ Production oder Test** gekennzeichnet sind. Geräte, die als Typ Wartung gekennzeichnet sind, werden nicht zwischengespeichert

PVS-Accelerator-CLI-Operationen

Im folgenden Abschnitt werden die Vorgänge beschrieben, die Kunden ausführen können, wenn sie den PVS-Beschleuniger mit der CLI verwenden. Kunden können diese Vorgänge auch mit XenCenter ausführen. Weitere Informationen finden Sie unter PVS-Accelerator in der XenCenter-Dokumentation.

Citrix Provisioning Serveradressen und Ports anzeigen, die von Citrix Provisioning konfiguriert wurden

PVS-Accelerator optimiert den Netzwerkverkehr zwischen einer VM und dem Citrix Provisioning-Server. Nach Abschluss der Konfiguration auf dem Citrix Provisioning-Server füllt der Citrix Provisioning-Server die `pvs-server` Objekte auf XenServer mit ihren IPs und Ports. PVS-Accelerator verwendet diese Informationen später, um speziell den Datenverkehr zwischen einer VM und ihren Citrix Provisioning-Servern zu optimieren. Die konfigurierten Citrix Provisioning-Server können mit dem folgenden Befehl aufgelistet werden:

```
xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
<!--NeedCopy-->
```

Konfigurieren einer VM für das Zwischenspeichern

Der PVS-Accelerator kann mit einem der folgenden Tools für die VM aktiviert werden:

- Citrix Provisioning CLI
- Citrix Virtual Desktops Setup-Assistent
- Setupassistent für gestreamte VMs
- XenCenter
- Die xe-CLI

Die xe CLI konfiguriert den PVS-Beschleuniger mithilfe der VIF einer VM. Es erstellt einen Citrix Provisioning-Proxy, der die VIF der VM mit einer Citrix Provisioning-Site verknüpft.

So konfigurieren Sie eine VM:

1. Suchen Sie das erste VIF der VM, um das Zwischenspeichern zu ermöglichen:

   ```
   VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
       minimal)
   <!--NeedCopy-->
   ```

2. Erstellen des Citrix Provisioning-Proxy


```
xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
<!--NeedCopy-->
```

Deaktivieren Sie das Zwischenspeichern für eine VM

Der PVS-Accelerator kann für eine VM deaktiviert werden, indem der Citrix Provisioning-Proxy zerstört wird, der die VIF der VM mit einem verknüpft `pvs-site`.

1. Suchen Sie das erste VIF der VM:

```
VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
   minimal)
<!--NeedCopy-->
```

2. Suchen Sie den Citrix Provisioning-Proxy der VM:

```
PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
<!--NeedCopy-->
```

3. Zerstören des Citrix Provisioning-Proxy:

```
xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
<!--NeedCopy-->
```

Entfernen des PVS-Accelerator-Speichers für einen Host oder eine Site

So entfernen Sie den PVS-Accelerator-Speicher für einen Host oder eine Site:

1. Suchen Sie den Host, für den Sie den Speicher löschen möchten:

```
HOST_UUID=$(xe host-list name-label=HOST_NAME --minimal)
<!--NeedCopy-->
```

2. Finde die UUID des Objekts:

```
PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=
   $HOST_UUID --minimal)
<!--NeedCopy-->
```

3. Zerstöre das Objekt:

```
xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
<!--NeedCopy-->
```

Vergessen Sie die PVS-Accelerator-Konfiguration für eine Site

Um die PVS-Accelerator-Konfiguration für eine Site zu vergessen:

1. Suchen Sie die Citrix Provisioning-Site:

```
PVS_SITE_UUID=$(xe pvs-site-list name-label=My PVS Site)
<!--NeedCopy-->
```

2. Führen Sie den folgenden Befehl aus, um die Citrix Provisioning Site zu vergessen:

```
xe pvs-site-forget uuid=$PVS_SITE_UUID
<!--NeedCopy-->
```

---

layout: doc
description: Create resource pools to group your XenServer hosts and shared storage into a single managed entity.—

Hosts und Ressourcenpools

In diesem Abschnitt wird beschrieben, wie Ressourcenpools anhand einer Reihe von Beispielen mithilfe der xe-Befehlszeilenschnittstelle (CLI) erstellt werden können. Eine einfache NFS-basierte Konfiguration für gemeinsam genutzten Speicher wird vorgestellt, und es werden mehrere einfache Beispiele für die VM-Verwaltung erörtert. Es enthält auch Verfahren zum Umgang mit Ausfällen physischer Knoten.

Übersicht über XenServer-Hosts und Ressourcenpools

Ein *Ressourcenpool* besteht aus mehreren XenServer-Hostinstallationen, die zu einer einzigen verwalteten Einheit zusammengefasst sind, die virtuelle Maschinen hosten kann. In Kombination mit gemeinsam genutztem Speicher ermöglicht ein Ressourcenpool den Start von VMs auf *jedem* XenServer-Host, der über ausreichend Arbeitsspeicher verfügt. Die VMs können dann dynamisch zwischen XenServer-Hosts verschoben werden, während sie mit minimalen Ausfallzeiten ausgeführt werden (Live-Migration). Wenn ein einzelner XenServer-Host einen Hardwarefehler erleidet, kann der Administrator ausgefallene VMs auf einem anderen XenServer-Host im selben Ressourcenpool neu starten. Wenn Hochverfügbarkeit im Ressourcenpool aktiviert ist, wechseln VMs automatisch zu einem anderen Host, wenn ihr Host ausfällt. Pro Ressourcenpool werden bis zu 64 Hosts unterstützt, obwohl diese Einschränkung nicht durchgesetzt wird.

Ein Pool hat immer mindestens einen physischen Knoten, den sogenannten *Poolkoordinator* (früher "Pool-Master"). Der Koordinatorknoten stellt eine Verwaltungsschnittstelle zur Verfügung (die von XenCenter und der XenServer-Befehlszeilenschnittstelle verwendet wird, die als Xe-CLI bezeichnet wird). Der Koordinator leitet bei Bedarf Befehle an einzelne Mitglieder weiter.

> **Hinweis:**
>
> Wenn der Poolkoordinator ausfällt, findet die Wiederwahl des Koordinators nur statt, wenn Hochverfügbarkeit aktiviert ist.

Anforderungen für das Erstellen von Ressourcenpools

Ein Ressourcenpool ist ein homogenes (oder heterogenes mit Einschränkungen) Aggregat aus einem oder mehreren XenServer-Hosts, bis zu einem Maximum von 64. Die Definition von "homogen" lautet:

- Die CPUs auf dem Host, der dem Pool beitritt, sind dieselben (in Bezug auf den Anbieter, das Modell und die Funktionen) wie die CPUs auf Hosts, die sich bereits im Pool befinden.
- Auf dem Host, der dem Pool beitritt, wird dieselbe Version der XenServer-Software auf derselben Patch-Ebene ausgeführt wie auf den Hosts, die sich bereits im Pool befinden.

Die Software erzwingt zusätzliche Einschränkungen, wenn ein Host zu einem Pool hinzugefügt wird. Insbesondere überprüft XenServer, ob die folgenden Bedingungen für den Host zutreffen, der dem Pool beitritt:

- Der Host ist kein Mitglied eines vorhandenen Ressourcenpools.
- Für den Host ist kein gemeinsam genutzter Speicher konfiguriert.
- Der Host hostet keine laufenden oder angehaltenen VMs.
- Auf den VMs auf dem Host werden keine aktiven Vorgänge ausgeführt, z. B. das Herunterfahren einer VM.
- Die Uhr auf dem Host wird mit derselben Uhrzeit wie der Poolkoordinator synchronisiert (z. B. mithilfe von NTP).
- Die Verwaltungsschnittstelle des Hosts ist nicht gebunden. Sie können die Verwaltungsschnittstelle konfigurieren, wenn der Host dem Pool erfolgreich beitritt.
- Die Management-IP-Adresse ist statisch und wird entweder auf dem Host selbst oder mithilfe einer entsprechenden Konfiguration auf Ihrem DHCP-Server konfiguriert.

XenServer-Hosts in Ressourcenpools können eine unterschiedliche Anzahl von physischen Netzwerkschnittstellen enthalten und über lokale Speicherrepositorys unterschiedlicher Größe verfügen. In der Praxis ist es oft schwierig, mehrere Hosts mit exakt denselben CPUs zu erhalten, weshalb geringfügige Abweichungen zulässig sind. Wenn es akzeptabel ist, Hosts mit unterschiedlichen CPUs als Teil desselben Pools zu haben, können Sie den Pool-Beitritt erzwingen, indem Sie den Parameter `--force` übergeben.

Alle Hosts im Pool müssen sich am selben Standort befinden und über ein Netzwerk mit geringer Latenz verbunden sein.

> **Hinweis:**
>
> Server, die gemeinsam genutzten NFS- oder iSCSI-Speicher für den Pool bereitstellen, müssen über eine statische IP-Adresse verfügen.

Ein Pool muss gemeinsam genutzte Speicher-Repositorys enthalten, um auszuwählen, auf welchem XenServer-Host eine VM ausgeführt werden soll, und um eine VM dynamisch zwischen XenServer-Hosts zu verschieben. Wenn möglich, erstellen Sie einen Pool, nachdem gemeinsam genutzter Speicher verfügbar ist. Es wird empfohlen, vorhandene VMs mit Datenträgern im lokalen Speicher in den freigegebenen Speicher zu verschieben, nachdem Sie gemeinsam genutzten Speicher hinzugefügt haben. Sie können den Befehl `xe vm-copy` oder XenCenter verwenden, um VMs zu verschieben.

Erstellen eines Ressourcenpools

Ressourcenpools können mit XenCenter oder der CLI erstellt werden. Wenn ein neuer Host einem Ressourcenpool beitritt, synchronisiert der beitretende Host seine lokale Datenbank mit der poolweiten Datenbank und erbt einige Einstellungen vom Pool:

- VM-, lokale und Remote-Speicherkonfiguration wird der poolweiten Datenbank hinzugefügt. Diese Konfiguration wird auf den beitretenden Host im Pool angewendet, sofern Sie die Ressourcen nicht explizit freigeben, nachdem der Host dem Pool beigetreten ist.
- Der beitretende Host erbt vorhandene freigegebene Speicherrepositories im Pool. Entsprechende PBD-Datensätze werden erstellt, damit der neue Host automatisch auf vorhandenen freigegebenen Speicher zugreifen kann.
- Netzwerkinformationen werden teilweise an den beitretenden Host vererbt: Die *strukturellen* Details von NICs, VLANs und gebundenen Schnittstellen werden alle vererbt, *Richtlinieninformationen* jedoch nicht. Zu diesen Richtlinieninformationen, die neu konfiguriert werden müssen, gehören:
  - Die IP-Adressen der Verwaltungs-NICs, die von der ursprünglichen Konfiguration beibehalten werden.
  - Der Speicherort der Verwaltungsschnittstelle, der der ursprünglichen Konfiguration entspricht. Wenn die anderen Pool-Hosts beispielsweise Verwaltungsschnittstellen auf einer gebundenen Schnittstelle haben, muss der beitretende Host nach dem Beitritt zur Bindung migriert werden.
  - Dedizierte Speicher-NICs, die dem beitretenden Host von XenCenter oder der CLI neu zugewiesen werden müssen, und die PBDs müssen neu angeschlossen werden, um

den Datenverkehr entsprechend weiterzuleiten. Dies liegt daran, dass IP-Adressen nicht im Rahmen des Pool-Join-Vorgangs zugewiesen werden und die Speicher-NIC nur funktioniert, wenn dies korrekt konfiguriert ist. Weitere Informationen zum Dedizieren einer Speicher-NIC über die CLI finden Sie unter Verwalten von Netzwerken.

> **Hinweis:**
>
> Sie können einen neuen Host nur mit einem Ressourcenpool verbinden, wenn sich die Verwaltungsschnittstelle des Hosts im selben markierten VLAN wie das des Ressourcenpools befindet.

Host zu einem Pool mit der xe-CLI hinzufügen

> **Hinweis:**
>
> Wir empfehlen, Ihren Pool und den beitretenden Host auf die gleiche Stufe zu aktualisieren, bevor Sie versuchen, eine Verbindung herzustellen.

1. Öffnen Sie eine Konsole auf dem XenServer-Host, den Sie einem Pool hinzufügen möchten.
2. Verbinden Sie den XenServer-Host mit dem Pool, indem Sie den folgenden Befehl eingeben:

```
xe pool-join master-address=<address of pool coordinator> master-
    username=<administrator username> master-password=<password>
<!--NeedCopy-->
```

   Die `master-address` muss auf den vollqualifizierten Domänennamen des Poolkoordinators gesetzt werden. Das `password` muss das Administratorkennwort sein, das bei der Installation des Poolkoordinators festgelegt wurde.

> **Hinweis:**
>
> Wenn Sie einen Host zu einem Pool hinzufügen, wird das Administratorkennwort für den beitretenden Host automatisch so geändert, dass es dem Administratorkennwort des Poolkoordinators entspricht.

XenServer-Hosts gehören standardmäßig zu einem unbenannten Pool. Um Ihren ersten Ressourcenpool zu erstellen, benennen Sie den vorhandenen namenlosen Pool um. Verwenden Sie tab-complete, um Folgendes zu finden `pool_uuid`:

```
xe pool-param-set name-label="New Pool" uuid=pool_uuid
<!--NeedCopy-->
```

Erstellen heterogener Ressourcenpools

XenServer vereinfacht die Erweiterung von Bereitstellungen im Laufe der Zeit, indem unterschiedliche Host-Hardware zu einem Ressourcenpool zusammengefasst werden kann, der als

heterogene Ressourcenpools bezeichnet wird. Heterogene Ressourcenpools werden durch den Einsatz von Technologien in Intel (FlexMigration) und AMD (Extended Migration) CPUs ermöglicht, die eine "Maskierung"oder "Leveling"der CPU ermöglichen. Mit CPU-Maskierung und -Leveling kann eine CPU so konfiguriert werden, dass sie eine andere Marke, ein anderes Modell oder eine andere Funktionalität *vorgibt* als sie tatsächlich ist. Mit dieser Funktion können Sie Pools von Hosts mit unterschiedlichen CPUs erstellen und dennoch die Livemigration sicher unterstützen.

> **Hinweis:**
>
> Die CPUs von XenServer-Hosts, die heterogenen Pools beitreten, müssen vom gleichen Hersteller (d. h. AMD, Intel) sein wie die CPUs der Hosts, die sich bereits im Pool befinden. Es ist jedoch nicht erforderlich, dass die Hosts auf der Ebene der Familie, des Modells oder der Schrittnummer vom gleichen Typ sind.

XenServer vereinfacht die Unterstützung heterogener Pools. Hosts können jetzt zu vorhandenen Ressourcenpools hinzugefügt werden, unabhängig vom zugrunde liegenden CPU-Typ (sofern die CPU aus derselben Herstellerfamilie stammt). Das Pool-Feature-Set wird jedes Mal dynamisch berechnet:

- Ein neuer Host tritt dem Pool bei
- Ein Poolmitglied verlässt den Pool
- Ein Poolmitglied stellt nach einem Neustart eine Verbindung wieder her

Jede Änderung des Pool-Feature-Sets wirkt sich nicht auf VMs aus, die derzeit im Pool ausgeführt werden. Eine laufende VM verwendet weiterhin den Funktionssatz, der beim Start angewendet wurde. Dieser Funktionsumfang wird beim Booten behoben und bleibt bei Migrations-, Aussetzungs- und Fortsetzungsvorgängen bestehen Wenn die Poolebene abfällt, wenn ein Host mit weniger Funktionen dem Pool beitritt, kann eine laufende VM auf jeden Host im Pool migriert werden, mit Ausnahme des neu hinzugefügten Hosts. Wenn Sie eine VM auf einen anderen Host innerhalb oder zwischen Pools verschieben oder migrieren, vergleicht XenServer den Funktionsumfang der VM mit dem Funktionsumfang des Zielhosts. Wenn sich herausstellt, dass die Feature-Sets kompatibel sind, kann die VM migriert werden. Auf diese Weise kann sich die VM frei innerhalb und zwischen Pools bewegen, unabhängig von den CPU-Funktionen, die die VM verwendet. Wenn Sie den Workload Balancing verwenden, um einen optimalen Zielhost für die Migration Ihrer VM auszuwählen, wird ein Host mit einem inkompatiblen Funktionsumfang nicht als Zielhost empfohlen.

Shared Storage hinzufügen

Eine vollständige Liste der unterstützten freigegebenen Speichertypen finden Sie unter Speicherrepository-Formate. In diesem Abschnitt wird gezeigt, wie gemeinsam genutzter Speicher (dargestellt als Speicherrepository) auf einem vorhandenen NFS-Server erstellt werden kann.

So fügen Sie gemeinsam genutzten NFS-Speicher über die CLI zu einem Ressourcenpool hinzu

1. Öffnen Sie eine Konsole auf einem beliebigen XenServer-Host im Pool.
2. Erstellen Sie das Speicherrepository auf server:/path, indem Sie den folgenden Befehl ausführen:

```
xe sr-create content-type=user type=nfs name-label="Example SR"
    shared=true \
     device-config:server=server \
     device-config:serverpath=path
<!--NeedCopy-->
```

   `device-config:server` ist der Hostname des NFS-Servers und `device-config:serverpath` der Pfad auf dem NFS-Server. Wenn `shared` auf true gesetzt, wird Shared Storage automatisch mit jedem XenServer-Host im Pool verbunden. Alle XenServer-Hosts, die später beitreten, sind ebenfalls mit dem Speicher verbunden. Der Universally Unique Identifier (UUID) des Speicherrepositorys wird auf dem Bildschirm gedruckt.

3. Suchen Sie die UUID des Pools, indem Sie den folgenden Befehl ausführen:

```
xe pool-list
<!--NeedCopy-->
```

4. Legen Sie den gemeinsam genutzten Speicher mit dem folgenden Befehl als Pool-weiten Standard fest:

```
xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
<!--NeedCopy-->
```

   Da der freigegebene Speicher als poolweiter Standard festgelegt wurde, werden die Datenträger aller zukünftigen VMs standardmäßig auf freigegebenem Speicher erstellt. Informationen zum Erstellen anderer Arten von freigegebenem Speicher finden Sie unter Speicherrepository-Formate.

Entfernen Sie XenServer-Hosts aus einem Ressourcenpool

> **Hinweis:**
>
> Bevor Sie einen XenServer-Host aus einem Pool entfernen, stellen Sie sicher, dass Sie alle auf diesem Host laufenden VMs herunterfahren. Andernfalls wird eine Warnung angezeigt, dass der Host nicht entfernt werden kann.

Wenn Sie einen Host aus einem Pool entfernen (*auswerfen*), wird der Computer neu gestartet, neu initialisiert und in einem Zustand belassen, der einer Neuinstallation ähnelt. Werfen Sie XenServer-Hosts nicht aus einem Pool aus, wenn sich wichtige Daten auf den lokalen Datenträgern befinden.

So entfernen Sie einen Host über die CLI aus einem Ressourcenpool

1. Öffnen Sie eine Konsole auf einem beliebigen Host im Pool.
2. Suchen Sie die UUID des Hosts, indem Sie den folgenden Befehl ausführen:

```
xe host-list
<!--NeedCopy-->
```

3. Werfen Sie den erforderlichen Host aus dem Pool aus:

```
xe pool-eject host-uuid=host_uuid
<!--NeedCopy-->
```

   Der XenServer-Host wird ausgeworfen und befindet sich in einem neu installierten Zustand.

   > **Warnung:**
   >
   > Werfen Sie *keinen* Host aus einem Ressourcenpool aus, wenn er wichtige Daten enthält, die auf seinen lokalen Datenträgern gespeichert sind. Alle Daten werden gelöscht, wenn ein Host aus dem Pool ausgeworfen wird. Wenn Sie diese Daten beibehalten möchten, kopieren Sie die VM mit XenCenter oder dem CLI-Befehl `xe vm-copy` in den freigegebenen Speicher im Pool.

Wenn XenServer-Hosts mit lokal gespeicherten VMs aus einem Pool ausgeworfen werden, sind die VMs in der Pooldatenbank vorhanden. Die lokal gespeicherten VMs sind auch für die anderen XenServer-Hosts sichtbar. Die VMs werden erst gestartet, wenn die ihnen zugewiesenen virtuellen Datenträger so geändert wurden, dass sie auf gemeinsam genutzten Speicher verweisen, der von anderen XenServer-Hosts im Pool gesehen wird, oder entfernt wurden. Daher empfehlen wir, dass Sie jeden lokalen Speicher in den freigegebenen Speicher verschieben, wenn Sie einem Pool beitreten. Durch die Umstellung auf gemeinsam genutzten Speicher können einzelne XenServer-Hosts ohne Datenverlust ausgeworfen werden (oder physisch ausfallen).

> **Hinweis:**
>
> Wenn ein Host aus einem Pool entfernt wird, dessen Verwaltungsschnittstelle sich in einem markierten VLAN-Netzwerk befindet, wird der Computer neu gestartet und seine Verwaltungsschnittstelle ist im selben Netzwerk verfügbar.

Bereiten Sie einen Pool von XenServer-Hosts für die Wartung vor

Bevor Sie Wartungsvorgänge auf einem Host ausführen, der Teil eines Ressourcenpools ist, müssen Sie ihn deaktivieren. Durch das Deaktivieren des Hosts wird verhindert, dass VMs darauf gestartet werden. Anschließend müssen Sie die VMs auf einen anderen XenServer-Host im Pool migrieren. Sie können dies tun, indem Sie den XenServer-Host mit XenCenter in den Wartungsmodus versetzen. Weitere Informationen finden Sie unter Im Wartungsmodus ausführen in der XenCenter-Dokumentation.

Die Backupsynchronisierung erfolgt alle 24 Stunden. Wenn der Poolkoordinator in den Wartungsmodus versetzt wird, gehen die RRD-Updates der letzten 24 Stunden für Offline-VMs verloren.

> **Warnung:**
>
> Wir empfehlen dringend, alle XenServer-Hosts neu zu starten, bevor Sie ein Update installieren und anschließend deren Konfiguration überprüfen. Einige Konfigurationsänderungen werden erst wirksam, wenn der XenServer-Host neu gestartet wird, sodass beim Neustart möglicherweise Konfigurationsprobleme aufgedeckt werden, die dazu führen können, dass das Update fehlschlägt.

So bereiten Sie einen Host in einem Pool über die CLI für Wartungsvorgänge vor

1. Führen Sie den folgenden Befehl aus:

   ```
   xe host-disable uuid=XenServer_host_uuid
   xe host-evacuate uuid=XenServer_host_uuid
   <!--NeedCopy-->
   ```

   Dieser Befehl deaktiviert den XenServer-Host und migriert dann alle laufenden VMs auf andere XenServer-Hosts im Pool.

2. Führen Sie den gewünschten Wartungsvorgang durch.

3. Aktivieren Sie den XenServer-Host, wenn der Wartungsvorgang abgeschlossen ist:

   ```
   xe host-enable
   <!--NeedCopy-->
   ```

4. Starten Sie alle angehaltenen VMs neu und setzen Sie alle gesperrten VMs fort.

Exportieren von Ressourcenpool-Daten

Mit der Option Ressourcendaten exportieren können Sie einen Ressourcendatenbericht für Ihren Pool erstellen und den Bericht in eine .xls- oder .csv-Datei exportieren. Dieser Bericht enthält detaillierte Informationen zu verschiedenen Ressourcen im Pool wie Hosts, Netzwerken, Speicher, virtuellen Maschinen, VDIs und GPUs. Diese Funktion ermöglicht es Administratoren, Ressourcen auf der Grundlage verschiedener Workloads wie CPU, Speicher und Netzwerk zu verfolgen, zu planen und zuzuweisen.

> **Hinweis:**
>
> Export Resource Pool Data ist für Kunden der XenServer Premium Edition verfügbar.

Die Liste der Ressourcen und verschiedene Arten von Ressourcendaten, die im Bericht enthalten sind:

Server:

- Name
- Poolkoordinator
- UUID
- Adresse
- CPU-Nutzung
- Netzwerk (avg/max kBs)
- Benutzter Speicher
- Speicher
- Betriebszeit
- Beschreibung

Netzwerke:

- Name
- Status verknüpfen
- MAC
- MTU
- VLAN
- Typ
- Ort

VDI:

- Name
- Typ
- UUID
- Größe
- Speicher
- Beschreibung

Speicher:

- Name
- Typ
- UUID
- Größe
- Ort
- Beschreibung

Virtuelle Maschinen:

- Name

- Energiestatus
- Ausgeführt auf
- Adresse
- MAC
- Netzwerkkarte
- Betriebssystem
- Speicher
- Benutzter Speicher
- CPU-Nutzung
- UUID
- Betriebszeit
- Vorlage
- Beschreibung

GPU:

- Name
- Server
- PCI-Buspfad
- UUID
- Stromverbrauch
- Temperatur
- Benutzter Speicher
- Computernutzung

> **Hinweis:**
>
> Informationen zu GPUs sind nur verfügbar, wenn GPUs an Ihren XenServer-Host angeschlossen sind.

So exportieren Sie Ressourcendaten

1. Wählen Sie im XenCenter Navigationsbereich **Infrastructure** und dann den Pool aus.
2. Wählen Sie das Menü **Pool** und dann **Ressourcendaten exportieren**.
3. Navigieren Sie zu einem Speicherort, an dem Sie den Bericht speichern möchten, und klicken Sie dann auf **Speichern**.

Host-Einschalten

Hosts remote einschalten

Sie können die XenServer-Host-Power-On-Funktion verwenden, um einen Host remote ein- und auszuschalten, entweder über XenCenter oder über die CLI.

Um die Host-Energie zu aktivieren, muss der Host über eine der folgenden Stromsteuerungslösungen verfügen:

- **Wake on LAN-fähige Netzwerkkarte**.
- **Dell Remote-Zugriffskarten (DRAC)**. Um XenServer mit DRAC zu verwenden, müssen Sie das Dell Supplemental Pack installieren, um DRAC-Unterstützung zu erhalten. Die DRAC-Unterstützung erfordert die Installation des RACADM-Befehlszeilenprogramms auf dem Host mit dem Remote Access Controller und die Aktivierung von DRAC und seiner Schnittstelle. RACADM ist oft in der DRAC-Management-Software enthalten. Weitere Informationen finden Sie in der DRAC-Dokumentation von Dell.
- Ein benutzerdefiniertes Skript, das auf der Management-API basiert und es Ihnen ermöglicht, das Gerät über XenServer ein- und auszuschalten. Weitere Informationen finden Sie im folgenden Abschnitt unter *Konfigurieren eines benutzerdefinierten Skripts für die Host-Einschaltfunktion* .

Für die Verwendung der Host-Power-On-Funktion sind zwei Aufgaben erforderlich:

1. Stellen Sie sicher, dass die Hosts im Pool die Fernsteuerung der Stromversorgung unterstützen. Sie verfügen beispielsweise über Wake-on-LAN-Funktionalität oder eine DRAC-Karte, oder Sie haben ein benutzerdefiniertes Skript erstellt.
2. Aktivieren Sie die Host-Einschaltfunktion über die CLI oder XenCenter.

Verwenden Sie die CLI, um das Einschalten des Hosts zu verwalten

Sie können das Host-Einschaltfeature entweder mit der CLI oder XenCenter verwalten. Dieser Abschnitt enthält Informationen zur Verwaltung mit der CLI.

Host Power On ist auf Host-Ebene aktiviert (d. h. auf jedem XenServer).

Nachdem Sie Host Power On aktiviert haben, können Sie Hosts entweder mit der CLI oder XenCenter einschalten.

So aktivieren Sie das Host-Einschalten über die CLI Führen Sie den Befehl aus:


```
xe host-set-power-on-mode host=<host uuid> \
    power-on-mode=("" , "wake-on-lan", "DRAC","custom") \
    power-on-config=key:value
<!--NeedCopy-->
```

Für DRAC müssen die Schlüssel `power_on_ip` das Kennwort angeben, wenn Sie die Secret-Funktion verwenden. Weitere Informationen finden Sie unter Secrets.

So schalten Sie Hosts über die CLI remote ein Führen Sie den Befehl aus:

```
xe host-power-on host=<host uuid>
<!--NeedCopy-->
```

Konfigurieren Sie ein benutzerdefiniertes Skript für die Host-Einschaltfunktion

Wenn die Remote-Power-Lösung Ihres Hosts ein Protokoll verwendet, das standardmäßig nicht unterstützt wird (z. B. Wake-On-Ring oder Intel Active Management Technology), können Sie ein benutzerdefiniertes Linux-Python-Skript erstellen, um Ihre XenServer-Computer remote einzuschalten. Sie können jedoch auch benutzerdefinierte Skripte für DRAC- und Wake-on-LAN-Remote-Stromversorgungslösungen erstellen.

Dieser Abschnitt enthält Informationen zur Konfiguration eines benutzerdefinierten Skripts für Host Power On mithilfe der Schlüssel/Wert-Paare, die dem XenServer-API-Aufruf zugeordnet sind `host.power_on`.

Wenn Sie ein benutzerdefiniertes Skript erstellen, führen Sie es jedes Mal über die Befehlszeile aus, wenn Sie die Stromversorgung auf einem XenServer-Host fernsteuern möchten. Alternativ können Sie es in XenCenter angeben und die XenCenter UI-Funktionen verwenden, um damit zu interagieren.

Die XenServer-API ist in der XenServer ManagementAPI dokumentiert.

> **Warnung:**
>
> Ändern Sie nicht die standardmäßig im Verzeichnis `/etc/xapi.d/plugins/` bereitgestellten Skripts. Sie können neue Skripte in dieses Verzeichnis aufnehmen, aber Sie dürfen die in diesem Verzeichnis enthaltenen Skripte nach der Installation niemals ändern.

Schlüssel/Wert-Paare Um Host Power On zu verwenden, konfigurieren Sie die Schlüssel `host.power_on_mode` und `host.power_on_config`. Im folgenden Abschnitt finden Sie Informationen zu den Werten.

Es gibt auch einen API-Aufruf, mit dem Sie diese Felder gleichzeitig festlegen können:


```
void host.set_host_power_on_mode(string mode, Dictionary<string,string>
    config)
<!--NeedCopy-->
```

host.power_on_mode

- **Definition**: Enthält Schlüssel/Wert-Paare zur Angabe des Typs der Remote-Stromversorgungslösung (z. B. Dell DRAC).
- **Mögliche Werte**:
  - Eine leere Zeichenfolge, die für deaktivierte Energiesteuerung steht.
  - "DRAC": Ermöglicht die Angabe von Dell DRAC. Um DRAC verwenden zu können, müssen Sie das Dell Zusatzpaket bereits installiert haben.
  - "wake-on-lan": Ermöglicht die Angabe von Wake-on-LAN.
  - Jeder andere Name (wird verwendet, um ein benutzerdefiniertes Einschaltskript anzugeben). Diese Option wird verwendet, um ein benutzerdefiniertes Skript für die Energieverwaltung anzugeben.
- **Typ**: string

host.power_on_config

- **Definition**: Enthält Schlüssel/Wert-Paare für die Moduskonfiguration. Stellt zusätzliche Informationen für DRAC bereit.
- **Mögliche Werte:**
  - Wenn Sie DRAC als Typ der Remote-Stromversorgungslösung konfiguriert haben, müssen Sie auch einen der folgenden Schlüssel angeben:
    - "power_on_ip": Die IP-Adresse, die Sie für die Kommunikation mit der Stromsteuerungskarte konfiguriert haben. Alternativ können Sie den Domänennamen für die Netzwerkschnittstelle eingeben, auf der DRAC konfiguriert ist.
    - "power_on_user": Der mit dem Verwaltungsprozessor verknüpfte DRAC-Benutzername, den Sie möglicherweise gegenüber den werkseitigen Standardeinstellungen geändert haben.
    - "power_on_password_secret": Gibt die Verwendung der Secrets Funktion an, um Ihr Kennwort zu sichern.
  - Um das Secrets Feature zum Speichern Ihres Kennworts zu verwenden, geben Sie den Schlüssel "power_on_password_secret"an. Weitere Informationen finden Sie unter Secrets.

- **Typ**: Map (Zeichenfolge, Zeichenfolge)

Beispiel eines Skripts Das Beispielskript importiert die XenServer-API, definiert sich selbst als benutzerdefiniertes Skript und übergibt dann spezifische Parameter für den Host, den Sie remote steuern möchten. Sie müssen die Parameter `session` in allen benutzerdefinierten Scripts definieren.

Das Ergebnis wird angezeigt, wenn das Script nicht erfolgreich ist.

```
import XenAPI
def custom(session,remote_host,
power_on_config):
result="Power On Not Successful"
for key in power_on_config.keys():
result=result+''
key=''+key+''
value=''+power_on_config[key]
return result
<!--NeedCopy-->
```

> **Hinweis:**
>
> Nachdem Sie das Skript erstellt haben, speichern Sie es in /etc/xapi.d/plugins mit der Erweiterung .py.

Kommunizieren Sie mit XenServer-Hosts und Ressourcenpools

TLS

XenServer verwendet das TLS 1.2-Protokoll, um den Verwaltungs-API-Verkehr zu verschlüsseln. Jegliche Kommunikation zwischen XenServer und Management-API-Clients (oder Appliances) verwendet das TLS 1.2-Protokoll.

> **Wichtig:**
>
> Wir unterstützen keine Kundenänderungen an der kryptographischen Funktionalität des Produkts.

XenServer verwendet die folgende Verschlüsselungssuite:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Darüber hinaus werden die folgenden Verschlüsselungssammlungen für die Abwärtskompatibilität mit einigen Versionen von Citrix Virtual Apps and Desktops unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

SSH

Wenn Sie einen SSH-Client verwenden, um eine direkte Verbindung zum XenServer-Host herzustellen, können die folgenden Algorithmen verwendet werden:

Chiffren:

- aes128-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

MACs:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1

KexAlgorithms:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1

HostKeyAlgorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519
- ssh-rsa

Wenn Sie den SSH-Zugriff auf Ihren XenServer-Host deaktivieren möchten, können Sie dies in tun. `xsconsole`

1. Öffnen Sie in XenCenter die Hostkonsole und melden Sie sich als `root` an.
2. Geben Sie `xsconsole` ein.

3. Gehen Sie in `xsconsole` zu **Remote Service Configuration** > **Remoteshell aktivieren/deaktivieren**.

   Die Konsole zeigt an, ob Remoteshell aktiviert ist.

4. Um zu ändern, ob die Remoteshell aktiviert oder deaktiviert ist, drücken Sie die **EINGABETASTE**.

> **Wichtig:**
>
> Wir unterstützen keine Kundenänderungen an der kryptographischen Funktionalität des Produkts.

Installieren Sie ein TLS-Zertifikat auf Ihrem Host

Der XenServer-Host wird mit einem Standard-TLS-Zertifikat installiert. Um jedoch HTTPS zur Sicherung der Kommunikation zwischen XenServer und Citrix Virtual Apps and Desktops zu verwenden, installieren Sie ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle bereitgestellt wird.

In diesem Abschnitt wird beschrieben, wie Sie über die xe-CLI Zertifikate installieren. Informationen zum Arbeiten mit Zertifikaten über XenCenter finden Sie in der XenCenter-Dokumentation.

Stellen Sie sicher, dass Ihr TLS-Zertifikat und sein Schlüssel die folgenden Anforderungen erfüllen:

- Das Zertifikat und das Schlüsselpaar sind ein RSA-Schlüssel.
- Der Schlüssel stimmt mit dem Zertifikat überein.
- Der Schlüssel wird in einer separaten Datei für das Zertifikat bereitgestellt.
- Das Zertifikat wird in einer separaten Datei zu allen Zwischenzertifikaten bereitgestellt.
- Die Schlüsseldatei muss einen der folgenden Typen haben: `.pem` oder `.key`.
- Alle Zertifikatsdateien müssen einen der folgenden Typen haben: `.pem`, `.cer`, oder `.crt`.
- Der Schlüssel ist größer oder gleich 2048 Bit und kleiner oder gleich 4096 Bit lang.
- Der Schlüssel ist ein unverschlüsselter PKCS #8 -Schlüssel und hat keinen Hauptschlüssel.
- Der Schlüssel und das Zertifikat liegen im Base-64-kodierten PEM-Format vor.
- Das Zertifikat ist gültig und nicht abgelaufen.
- Der Signaturalgorithmus ist SHA-2 (SHA256).

Die xe CLI warnt Sie, wenn das Zertifikat und der Schlüssel, die Sie wählen, diese Anforderungen nicht erfüllen.

Wo erhalte ich ein TLS-Zertifikat?

- Möglicherweise haben Sie bereits ein vertrauenswürdiges Zertifikat, das Sie auf Ihrem XenServer-Host installieren möchten.

- Alternativ können Sie ein Zertifikat auf Ihrem Server erstellen und es zur Signierung an Ihre bevorzugte Zertifizierungsstelle senden. Diese Methode ist sicherer, da der private Schlüssel auf dem XenServer-Host verbleiben und nicht zwischen Systemen kopiert werden kann.

  Das Erstellen eines TLS-Zertifikats umfasst die folgenden Schritte:

  1. Generieren Sie eine Anfrage zum Signieren eines Zertifikats
  2. Senden Sie die Zertifikatssignieranforderung an eine Zertifizierungsstelle
  3. Installieren Sie das signierte Zertifikat auf Ihrem XenServer-Host

1. Generieren Sie eine Anfrage zum Signieren eines Zertifikats Generieren Sie zunächst einen privaten Schlüssel und eine Zertifikatssignieranforderung. Führen Sie auf dem XenServer-Host die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl aus, um eine private Schlüsseldatei zu erstellen:

   ```
   openssl genrsa -des3 -out privatekey.pem 2048
   <!--NeedCopy-->
   ```

   Sie werden zur Eingabe einer Passphrase aufgefordert. Diese Passphrase wird in einem folgenden Schritt entfernt.

2. Entferne die Passphrase aus dem Schlüssel:

   ```
   openssl rsa -in privatekey.pem -out privatekey.nop.pem
   <!--NeedCopy-->
   ```

3. Erstellen Sie die Zertifikatssignierungsanforderung mithilfe des privaten Schlüssels:

   ```
   openssl req -new -key privatekey.nop.pem -out csr
   <!--NeedCopy-->
   ```

4. Befolgen Sie die Anweisungen, um die zum Generieren der Zertifikatssignierungsanforderung erforderlichen Informationen anzugeben.

   - **Name des Landes**. Geben Sie die Ländercodes des TLS-Zertifikats für Ihr Land ein. Zum Beispiel CA für Kanada oder JM für Jamaika. Eine Liste der Ländercodes für TLS-Zertifikate finden Sie im Internet.
   - **Name des Bundesstaates oder der Provinz (vollständiger Name)**. Geben Sie den Bundesstaat oder die Provinz an, in der sich der Pool befindet. Zum Beispiel Massachusetts oder Alberta.
   - **Name der Lokalität**. Der Name der Stadt, in der sich der Pool befindet.
   - **Name der Organisation**. Der Name Ihres Unternehmens oder Ihrer Organisation.
   - **Name der Organisationseinheit**. Geben Sie den Namen der Abteilung ein. Das Feld ist optional.

- **Common Name**: Geben Sie den FQDN Ihres XenServer-Hosts ein. Wir empfehlen, entweder einen FQDN oder eine IP-Adresse anzugeben, die nicht abläuft.
- **E-Mail-Adresse**: Diese E-Mail-Adresse ist im Zertifikat enthalten, wenn Sie es generieren.

Die Anforderung zum Signieren des Zertifikats wird im aktuellen Verzeichnis gespeichert und hat den Namen `csr`.

5. Zeigen Sie die Zertifikatssignierungsanforderung im Konsolenfenster an, indem Sie den folgenden Befehl ausführen:

```
cat csr
<!--NeedCopy-->
```

6. Kopieren Sie die gesamte Zertifikatssignierungsanforderung und verwenden Sie diese Informationen, um das Zertifikat von der Zertifizierungsstelle anzufordern.

   Beispiel für eine Zertifikatsignieranforderung:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDBDCCAewCAQAwgYsxCzAJBgNVBAYTAlVLMRcwFQYDVQQIDA5DYW1icmlkZ2Vz
aGlyZTESMBAGA1UEBwwJQ2FtYnJpZGdlMRIwEAYDVQQKDAlYZW5TZXJ2ZXIxFTAT
...
SdYCkFdo+85z8hBULFzSH6jgSP0UGQU0PcfIy7KPKyI4jnFQqeCDvLdWyhtAx9gq
Fu40qMSm1dNCFfnACRwYQkQgqCt/RHeUtl8srxyZC+odbunnV+ZyQdmLwLuQySUk
ZL8naumG3yU=
-----END CERTIFICATE REQUEST-----
<!--NeedCopy-->
```

2. Senden Sie die Zertifikatssignieranforderung an eine Zertifizierungsstelle Nachdem Sie die Zertifikatsignieranforderung generiert haben, können Sie die Anfrage an die bevorzugte Zertifizierungsstelle Ihrer Organisation senden.

Eine Zertifizierungsstelle ist ein vertrauenswürdiger Drittanbieter, der digitale Zertifikate bereitstellt. Einige Zertifizierungsstellen verlangen, dass die Zertifikate auf einem System gehostet werden, auf das über das Internet zugegriffen werden kann. Wir empfehlen, für diese Anforderung keine Zertifizierungsstelle zu verwenden.

Die Zertifizierungsstelle beantwortet Ihre Signaturanfrage und stellt die folgenden Dateien zur Verfügung:

- das signierte Zertifikat
- ein Stammzertifikat
- falls zutreffend, ein Zwischenzertifikat

Sie können jetzt all diese Dateien auf Ihrem XenServer-Host installieren.

3. Installieren Sie das signierte Zertifikat auf Ihrem XenServer-Host Nachdem die Zertifizierungsstelle auf die Zertifikatsignieranforderung geantwortet hat, führen Sie die folgenden Schritte aus, um das Zertifikat auf Ihrem XenServer-Host zu installieren:

1. Holen Sie sich das signierte Zertifikat, das Stammzertifikat und, falls die Zertifizierungsstelle eines hat, das Zwischenzertifikat von der Zertifizierungsstelle.
2. Kopieren Sie den Schlüssel und die Zertifikate auf den XenServer-Host.
3. Führen Sie den folgenden Befehl auf dem Host aus:

   ```
   xe host-server-certificate-install certificate=<
       path_to_certificate_file> private-key=<path_to_private_key>
       certificate-chain=<path_to_chain_file>
   ```

   Der Parameter `certificate-chain` ist optional.

Für zusätzliche Sicherheit können Sie die private Schlüsseldatei löschen, nachdem das Zertifikat installiert wurde.

Administratorkennwort verwalten

Wenn Sie einen XenServer-Host zum ersten Mal installieren, legen Sie ein Administrator- oder *Root-Kennwort* fest. Sie verwenden dieses Kennwort, um XenCenter mit Ihrem Host zu verbinden oder (mit Benutzername `root`), um sich bei **xsconsole, der Systemkonfigurationskonsole**, anzumelden.

Wenn Sie einen Host zu einem Pool hinzufügen, wird das Administratorkennwort für den Host automatisch so geändert, dass es dem Administratorkennwort des Poolkoordinators entspricht.

> **Hinweis:**
>
> XenServer-Administratorkennwörter dürfen nur ASCII-Zeichen enthalten.

Das Kennwort ändern

Sie können XenCenter, die xe CLI oder **xsconsole** verwenden, um das Administratorkennwort zu ändern.

XenCenter Gehen Sie wie folgt vor, um das Administratorkennwort für einen Pool oder einen eigenständigen Host mithilfe von XenCenter zu ändern:

1. Wählen Sie im Bereich **Ressourcen** den Pool oder einen beliebigen Host im Pool aus.
2. Wählen Sie im Menü **Pool** oder im Menü **Server** die Option **Serverkennwort ändern**aus.

Um das Root-Kennwort eines eigenständigen Hosts zu ändern, wählen Sie den Host im Bereich **Ressourcen** aus und klicken Sie im Menü **Server** auf **Kennwort** und dann auf **Ändern** .

Wenn XenCenter so konfiguriert ist, dass Ihre Host-Anmeldeinformationen zwischen den Sitzungen gespeichert werden, wird das neue Kennwort gespeichert. Weitere Informationen finden Sie unter Speichern des Verbindungsstatus Ihres Hosts.

Nachdem Sie das Administratorkennwort geändert haben, rotieren Sie das Poolgeheimnis. Weitere Informationen finden Sie unter Rotation des Poolgeheimnisses.

xe CLI Um das Administratorkennwort mithilfe der Xe-CLI zu ändern, führen Sie den folgenden Befehl auf einem Host im Pool aus:

```
1   xe user-password-change new=<new_password>
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie dem Befehl ein Leerzeichen voranstellen, um zu vermeiden, dass das Klartextkennwort im Befehlsverlauf gespeichert wird.

Nachdem Sie das Administratorkennwort geändert haben, rotieren Sie das Poolgeheimnis. Weitere Informationen finden Sie unter Rotation des Poolgeheimnisses.

xsconsole Gehen Sie wie folgt vor, um das Administratorkennwort für einen Pool oder einen eigenständigen Host mithilfe von **xsconsole**zu ändern:

1. Gehen Sie im Poolkoordinator zur Konsole.
2. Logge dich ein als `root`.
3. Geben Sie `xsconsole` ein. Drücken Sie die **Eingabetaste**. Die **xsconsole** wird angezeigt.
4. Navigieren Sie in **xsconsole**mit den Pfeiltasten zur Option **Authentifizierung** . Drücken Sie die **Eingabetaste**.
5. Navigieren Sie zu **Kennwort ändern**. Drücken Sie **die Eingabetaste**.
6. Authentifizieren Sie sich mit dem Administratorkennwort.
7. Gehen **Sie im Dialog Kennwort ändern** wie folgt vor

   a) Geben Sie Ihr aktuelles Kennwort ein.
   b) Geben Sie ein neues Kennwort ein.
   c) Geben Sie das neue Kennwort noch einmal ein, um es zu bestätigen.

   Der Bildschirm "**Kennwortänderung erfolgreich** "wird angezeigt. Drücken **Sie zum Schließen die Eingabetaste** .

Wenn der Host Poolkoordinator ist, wird dieses aktualisierte Kennwort jetzt an die anderen Hosts im Pool weitergegeben.

Nachdem Sie das Administratorkennwort geändert haben, rotieren Sie das Poolgeheimnis. Weitere Informationen finden Sie unter Rotation des Poolgeheimnisses.

Ein verlorenes Root-Kennwort zurücksetzen

Wenn Sie das Administratorkennwort (Root) für Ihren XenServer-Host verlieren, können Sie das Kennwort zurücksetzen, indem Sie direkt auf den Host zugreifen.

1. Starten Sie den XenServer-Host neu.
2. Wenn das GRUB-Menü angezeigt wird, drücken Sie **e**, um den Startmenüeintrag zu bearbeiten.
3. Fügen Sie `init=/sysroot/bin/sh` zu der Zeile hinzu, die mit `module2` beginnt.
4. Drücken Sie **Strg-X**, um in eine Root-Shell zu booten.
5. Führen Sie in der Befehlsshell die folgenden Befehle aus:

```
chroot /sysroot
passwd

(type the new password twice)

sync
/sbin/reboot -f
<!--NeedCopy-->
```

Wenn der Host Poolkoordinator ist, wird dieses aktualisierte Kennwort jetzt an die anderen Hosts im Pool weitergegeben.

Nachdem Sie das Administratorkennwort geändert haben, rotieren Sie das Poolgeheimnis.

Poolgeheimnis rotieren

Das Pool-Geheimnis ist ein Geheimnis, das von den Hosts in einem Pool gemeinsam genutzt wird und es dem Host ermöglicht, seine Mitgliedschaft in einem Pool nachzuweisen.

Da Benutzer mit der Pool-Admin-Rolle dieses Geheimnis herausfinden können, empfiehlt es sich, das Pool-Geheimnis zu rotieren, wenn einer dieser Benutzer Ihre Organisation verlässt oder seine Pool-Admin-Rolle verliert.

Sie können das Poolgeheimnis über XenCenter oder die xe-CLI rotieren.

XenCenter

Führen Sie die folgenden Schritte aus, um das Poolgeheimnis für einen Pool mit XenCenter zu rotieren:

1. Wählen Sie im Bereich **Ressourcen** den Pool oder einen beliebigen Host im Pool aus.
2. Wählen Sie im Menü **Pool** die Option **Poolgeheimnis rotieren** aus.

Wenn Sie das Poolgeheimnis rotieren, werden Sie auch aufgefordert, das root-Kennwort zu ändern. Wenn Sie das Poolgeheimnis rotiert haben, weil Sie glauben, dass Ihre Umgebung kompromittiert wurde, stellen Sie sicher, dass Sie auch das Root-Kennwort ändern. Weitere Informationen finden Sie unter Ändern des Kennworts.

xe CLI

Um das Pool-Geheimnis mithilfe der Xe-CLI zu rotieren, führen Sie den folgenden Befehl auf einem Host im Pool aus:

```
xe pool-secret-rotate
<!--NeedCopy-->
```

Wenn Sie das Poolgeheimnis rotiert haben, weil Sie glauben, dass Ihre Umgebung kompromittiert wurde, stellen Sie sicher, dass Sie auch das Root-Kennwort ändern. Weitere Informationen finden Sie unter Ändern des Kennworts.

Aktivieren Sie IGMP-Snooping in Ihrem XenServer-Pool

XenServer sendet Multicast-Verkehr an alle Gast-VMs, was zu einer unnötigen Belastung der Hostgeräte führt, da sie Pakete verarbeiten müssen, die sie nicht angefordert haben. Durch die Aktivierung des IGMP-Snoopings wird verhindert, dass Hosts in einem lokalen Netzwerk Datenverkehr für eine Multicastgruppe empfangen, denen sie nicht explizit beigetreten sind, und verbessert die Leistung von Multicast. IGMP-Snooping ist besonders nützlich für bandbreitenintensive IP-Multicast-Anwendungen wie IPTV.

> **Hinweise:**
>
> - IGMP-Snooping ist nur verfügbar, wenn das Netzwerk-Backend Open vSwitch verwendet.
> - Wenn Sie diese Funktion in einem Pool aktivieren, kann es auch erforderlich sein, den IGMP-Abfrager auf einem der physischen Switches zu aktivieren. Andernfalls fällt Multicast im Subnetzwerk auf Broadcast zurück und kann die XenServer-Leistung beeinträchtigen.
> - Wenn Sie diese Funktion in einem Pool aktivieren, auf dem IGMP v3 ausgeführt wird, führt

> VM-Migration oder Netzwerkbindung-Failover dazu, dass IGMP-Version auf v2 umgeschaltet wird.
>
> - Um diese Funktion mit einem GRE-Netzwerk zu aktivieren, müssen Benutzer einen IGMP-Querier im GRE-Netzwerk einrichten. Alternativ können Sie die IGMP-Abfragenachricht vom physischen Netzwerk in das GRE-Netzwerk weiterleiten. Oder der Multicast-Verkehr im GRE-Netzwerk kann blockiert werden.

Sie können IGMP-Snooping in einem Pool über XenCenter oder der xe-CLI aktivieren.

XenCenter

1. Navigieren Sie zu **Pool Properties**.
2. Wählen Sie **Netzwerkoptionen** aus. Hier können Sie IGMP-Snooping aktivieren oder deaktivieren.

xe CLI

1. Holen Sie sich die Pool-UUID:

   ```
   xe pool-list
   ```

2. Aktivieren/deaktivieren Sie IGMP-Snooping für den Pool:

   ```
   xe pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|
   false]
   ```

Nachdem Sie IGMP-Snooping aktiviert haben, können Sie die IGMP-Snooping-Tabelle mit der xe-CLI einsehen.

Sehen Sie sich die IGMP-Snooping-Tabelle an

Verwenden Sie den folgenden Befehl, um die IGMP-Snooping-Tabelle anzuzeigen:

```
ovs-appctl mdb/show [bridge name]
```

> **Hinweis:**
>
> Sie können den Namen der Brücke mit `xe network-list` abrufen. Diese Brückennamen können `xenbr0`, `xenbr1`, `xenapi` oder `xapi0` lauten.

Dadurch wird eine Tabelle mit vier Spalten ausgegeben:

- Port: Der Port des Switches (OVS).

- VLAN: Die VLAN-ID des Datenverkehrs.
- GRUPPE: Die Multicast-Gruppe, die der Port angefordert hat.
- Alter: Das Alter dieses Datensatzes in Sekunden.

Wenn die **GROUP** eine Multicast-Gruppenadresse ist, bedeutet dies, dass eine IGMP-Berichtsmeldung auf dem zugehörigen Switch-Port empfangen wurde. Dies bedeutet, dass ein Empfänger (Mitglied) der Multicast-Gruppe diesen Port abhört.

Nehmen wir das folgende Beispiel, das zwei Datensätze enthält:

Port	VLAN	GRUPPE	Alter
14	0	227.0.0.1	15
1	0	Abfrager	24

Der erste Datensatz zeigt, dass an Port 14 ein Empfänger die Multicast-Gruppe 227.0.0.1 abhört. Der Open vSwitch leitet Datenverkehr, der für die 227.0.0.1-Multicast-Gruppe bestimmt ist, nur an Listening-Ports für diese Gruppe weiter (in diesem Beispiel Port 14), anstatt ihn an alle Ports zu übertragen. Der Datensatz, der Port 14 und Gruppe 227.0.0.1 verbindet, wurde vor 15 Sekunden erstellt. Standardmäßig beträgt das Timeout-Intervall 300 Sekunden. Das heißt, wenn der Switch nach dem Hinzufügen des Datensatzes 300 Sekunden lang keine weiteren IGMP-Report-Meldungen auf Port 14 empfängt, läuft der Datensatz ab und wird aus der Tabelle entfernt.

Im zweiten Datensatz ist die **GROUPabfragender**, was bedeutet, dass IGMP-Abfragenachrichten auf dem zugehörigen Port empfangen wurden. Ein Querier sendet regelmäßig IGMP-Abfragenachrichten, die an alle Switch-Ports gesendet werden, um festzustellen, welche Netzwerkknoten eine Multicast-Gruppe abhören. Auf den Empfang einer IGMP-Abfragenachricht antwortet der Empfänger mit einer IGMP-Berichtsnachricht, wodurch der Multicast-Datensatz des Empfängers aktualisiert wird und ein Ablauf vermieden wird.

Die **VLAN-Spalte zeigt dem VLAN** an, dass ein Receiver/Querier aktiv ist. ‘0’bedeutet systemeigenes VLAN. Wenn Sie Multicast auf einem markierten VLAN ausführen möchten, stellen Sie sicher, dass das VLAN Datensätze enthält.

> **Hinweis:**
>
> Für das VLAN-Szenario sollten Sie einen Abfragedatensatz mit einem VLAN-Spaltenwert haben, der der VLAN-ID des Netzwerks entspricht, da Multicast sonst im VLAN-Netzwerk nicht funktioniert.

Aktivieren Sie die Migrationsstreamkomprimierung in Ihrem XenServer-Pool

Während der Live-Migration einer VM wird ihr Speicher als Datenstrom zwischen zwei Hosts über das Netzwerk übertragen. Die Komprimierungsfunktion für Migrationsströme komprimiert diesen Datenstrom und beschleunigt so die Speicherübertragung in langsamen Netzwerken. Diese Funktion ist standardmäßig deaktiviert, kann jedoch mithilfe von XenCenter oder der Xe-CLI geändert werden. Weitere Informationen finden Sie unter Pooleigenschaften —Erweitert und Poolparameter. Alternativ können Sie die Komprimierung bei der Migration einer VM über die Befehlszeile aktivieren. Weitere Informationen finden Sie unter dem `vm-migrate` Befehl unter VM-Befehle.

Zertifikatüberprüfung

September 19, 2023

Wenn die Zertifikatüberprüfung für einen Pool aktiviert ist, verwenden alle TLS-Kommunikationsendpunkte in ihrem Verwaltungsnetzwerk Zertifikate, um die Identität ihrer Peers zu überprüfen, bevor vertrauliche Informationen übertragen werden.

Ergebnis

Verbindungen, die von einem XenServer-Host im Verwaltungsnetzwerk initiiert wurden, erfordern, dass der Zielendpunkt ein TLS-Zertifikat zur Überprüfung seiner Identität bereitstellt. Diese Anforderung wirkt sich auf die folgenden Elemente aus, die Teil des Pools sind oder mit dem Pool interagieren:

- Gastgeber im Pool
- XenCenter
- Drittanbieter-Clients, die die API verwenden

Die Zertifikatsüberprüfung ist sowohl mit den von XenServer bereitgestellten selbstsignierten Zertifikaten als auch mit vom Benutzer installierten Zertifikaten kompatibel, die von einer vertrauenswürdigen Stelle signiert wurden. Weitere Informationen finden Sie unter Installieren eines TLS-Zertifikats auf Ihrem Host.

Jeder XenServer-Host in einem Pool hat zwei Zertifikate, die ihn identifizieren:

- *Poolinterne Identitätszertifikate* werden verwendet, um die Kommunikation zwischen Hosts innerhalb des Pools zu sichern. Für die Kommunikation innerhalb des Pools verwendet XenServer immer selbstsignierte Zertifikate.

- *Serveridentitätszertifikate* werden verwendet, um die Identität eines XenServer-Hosts für alle Clientanwendungen zu überprüfen, die mit dem Pool im Verwaltungsnetzwerk kommunizieren. Für die Kommunikation zwischen dem Host und einer Client-Anwendung können Sie selbstsignierte Zertifikate verwenden oder Sie können Ihre eigenen TLS-Zertifikate auf Ihren Hosts installieren.

Wenn ein Host dem Pool zum ersten Mal beitritt oder ein Client zum ersten Mal eine Verbindung zum Pool herstellt, vertraut der Pool der Verbindung. Während dieser ersten Verbindung werden Zertifikate zwischen dem Pool und dem beitretenden Host oder dem verbindenden Client ausgetauscht. Für alle nachfolgenden Kommunikationen dieses Hosts oder Clients im Verwaltungsnetzwerk werden die Zertifikate verwendet, um die Identität der an der Kommunikation beteiligten Parteien zu überprüfen.

Wir empfehlen Ihnen, die Zertifikatsüberprüfung für alle Ihre Hosts und Pools zu aktivieren. Damit ein XenServer-Host erfolgreich einem Pool beitreten kann, muss sowohl für den Host als auch für den Pool die Zertifikatsüberprüfung aktiviert oder deaktiviert sein. Wenn die Zertifikatsüberprüfung auf dem einen aktiviert ist und auf dem anderen nicht, ist der Verbindungsvorgang nicht erfolgreich. XenCenter zeigt eine Warnmeldung an, in der Sie aufgefordert werden, die Zertifikatsüberprüfung im Pool oder auf dem beitretenden Host zu aktivieren.

Wenn ein Host einen Pool mit aktivierter Zertifikatsüberprüfung verlässt, löschen sowohl der Host als auch der Pool die Zertifikate, die sich auf den anderen Host beziehen.

Die virtuelle Workload Balancing Balancing-Appliance kann mit der Zertifikatsüberprüfung verwendet werden. Sie müssen sicherstellen, dass die selbstsignierten Workload Balancing Balancing-Zertifikate auf Ihrem XenServer-Host installiert sind.

Die virtuelle XenServer Conversion Manager Manager-Appliance stellt keine Verbindung zu XenServer-Hosts her und ist daher von der Zertifizierungsprüfungspflicht ausgenommen, wenn sie als TLS-Client-Endpunkt fungiert.

Zertifikatsüberprüfung für Ihren Pool aktivieren

Die Zertifikatsüberprüfung ist bei Neuinstallationen von XenServer 8 und höher standardmäßig aktiviert. Wenn Sie ein Upgrade von einer früheren Version von XenServer oder Citrix Hypervisor durchführen, wird die Zertifikatsüberprüfung nicht automatisch aktiviert und Sie müssen sie aktivieren. XenCenter fordert Sie auf, die Zertifikatsüberprüfung zu aktivieren, wenn Sie das nächste Mal eine Verbindung zum aktualisierten Pool herstellen.

Bevor Sie die Zertifikatüberprüfung für einen Pool aktivieren, stellen Sie sicher, dass keine Vorgänge im Pool ausgeführt werden.

Mithilfe von XenCenter aktivieren

XenCenter bietet verschiedene Möglichkeiten, die Zertifikatsüberprüfung zu aktivieren.

- Wenn Sie XenCenter zum ersten Mal mit einem Pool ohne aktivierte Zertifikatsüberprüfung verbinden, werden Sie aufgefordert, ihn zu aktivieren. Klicken Sie auf **Ja, Zertifikatsüberprüfung aktivieren**.
- Wählen Sie im Menü **Pool** die Option **Zertifikatüberprüfung aktivieren**aus.
- Klicken Sie auf der Registerkarte **Allgemein** des Pools mit der rechten Maustaste auf den Eintrag **Zertifikatüberprüfung**, und wählen Sie im Menü die Option **Zertifikatüberprüfung aktivieren** .

Aktivieren mit der xe-CLI

Um die Zertifikatsüberprüfung für einen Pool zu aktivieren, führen Sie den folgenden Befehl in der Konsole eines Hosts im Pool aus:

```
1 xe pool-enable-tls-verification
```

Verwaltung von Zertifikaten

Sie können die Zertifikate, die zur Überprüfung der Identität eines Hosts verwendet werden, installieren, Informationen darüber anzeigen und sie zurücksetzen.

Installieren von Zertifikaten

Sie können Ihr eigenes TLS-Zertifikat installieren, das der Host als Identitätszertifikat verwendet, wenn er Verbindungen von Client-Anwendungen im Verwaltungsnetzwerk empfängt.

Weitere Informationen finden Sie unter Installieren eines TLS-Zertifikats auf Ihrem Host.

Zertifikatsinformationen anzeigen

So ermitteln Sie, ob für einen Pool die Zertifikatsprüfung aktiviert ist:

- Suchen Sie in XenCenter auf der Registerkarte **Allgemein** nach dem Pool. Der Abschnitt **Allgemein** enthält einen Eintrag für die **Zertifikatsüberprüfung**, der anzeigt, ob die Zertifikatsüberprüfung aktiviert oder deaktiviert ist. Diese Registerkarte enthält auch einen Abschnitt **Zertifikate**, in dem der Name, die Gültigkeit und der Fingerabdruck der CA-Zertifikate aufgeführt sind.

- Mit der xe-CLI können Sie den folgenden Befehl ausführen:

```
xe pool-param-get uuid=<pool_uuid> param-name=tls-verification-
    enabled
```

  Wenn die Zertifikatüberprüfung aktiviert ist, wird die Zeile `tls-verification-enabled ( RO): true` in der Befehlsausgabe angezeigt.

So zeigen Sie Informationen zu den Zertifikaten auf einem XenServer-Host an:

- Gehen Sie in XenCenter zur Registerkarte **Allgemein** für diesen Host. Im Abschnitt **Zertifikate** werden der Fingerabdruck und die Gültigkeitsdaten für das Serveridentitätszertifikat und das poolinterne Identitätszertifikat angezeigt.
- Mit der xe-CLI können Sie den folgenden Befehl ausführen:

```
xe certificate-list
```

Aktualisierung der Pool-internen Identitätszertifikate

Sie können das poolinterne Identitätszertifikat über die xe-CLI aktualisieren:

1. Suchen Sie die UUID des Hosts, dessen Zertifikat Sie zurücksetzen möchten, indem Sie den folgenden Befehl ausführen:

```
xs host-list
```

2. Führen Sie den folgenden Befehl aus, um das Zertifikat zurückzusetzen:

```
xe host-refresh-server-certificate host=<host_uuid>
```

> **Hinweis:**
>
> Jeder Hostauswahlparameter kann mit diesem Befehl verwendet werden, um den Host anzugeben, auf dem das Zertifikat zurückgesetzt werden soll.

Zurücksetzen von Serveridentitätszertifikaten

Sie können das Serveridentitätszertifikat über XenCenter oder die Xe-CLI zurücksetzen. Durch das Zurücksetzen eines Zertifikats wird das Zertifikat vom Host gelöscht und stattdessen ein neues selbstsigniertes Zertifikat installiert.

So setzen Sie ein Zertifikat in XenCenter zurück:

1. Gehen Sie zur Registerkarte **Allgemein** für den Host.

2. Klicken Sie im Abschnitt **Zertifikate** mit der rechten Maustaste auf das Zertifikat, das Sie zurücksetzen möchten.
3. Wählen Sie im Menü **Zertifikat zurücksetzen**aus.
4. Klicken Sie im daraufhin angezeigten Dialogfeld auf **Ja**, um das Zurücksetzen des Zertifikats zu bestätigen.

Alternativ können Sie im Menü **Server** zu **Zertifikate > Zertifikat zurücksetzen**gehen.

Wenn Sie ein Zertifikat zurücksetzen, werden alle vorhandenen Verbindungen zum XenServer-Host getrennt —einschließlich der Verbindung zwischen XenCenter und dem Host. XenCenter stellt nach einem Zurücksetzen des Zertifikats automatisch wieder eine Verbindung zum Host her.

So setzen Sie ein Zertifikat über die xe-CLI zurück:

1. Suchen Sie die UUID des Hosts, dessen Zertifikat Sie zurücksetzen möchten, indem Sie den folgenden Befehl ausführen:

```
xs host-list
```

2. Führen Sie den folgenden Befehl aus, um das Zertifikat zurückzusetzen:

```
xe host-reset-server-certificate host=<host_uuid>
```

> **Hinweis:**
>
> Jeder Hostauswahlparameter kann mit diesem Befehl verwendet werden, um den XenServer-Host anzugeben, auf dem das Zertifikat zurückgesetzt werden soll.

Wenn Sie ein Zertifikat zurücksetzen, werden alle vorhandenen Verbindungen zum XenServer-Host getrennt —einschließlich der Verbindung zwischen XenCenter und dem Host. XenCenter stellt nach einem Zurücksetzen des Zertifikats automatisch wieder eine Verbindung zum Host her.

Ablaufwarnungen

XenCenter zeigt Warnungen in der **Benachrichtigungsansicht** an, wenn Ihre Serveridentitätszertifikate, poolinternen Identitätszertifikate oder Pool-CA-Zertifikate kurz vor ihrem Ablaufdatum stehen.

Die Zertifikatsprüfung vorübergehend deaktivieren

Es wird nicht empfohlen, die Zertifikatsüberprüfung zu deaktivieren, nachdem sie auf einem Host oder Pool aktiviert wurde. XenServer stellt jedoch Befehle bereit, mit denen die Zertifikatsüberprüfung pro Host deaktiviert werden kann, wenn Probleme mit Zertifikaten behoben werden.

Um die Zertifikatsverifizierung vorübergehend zu deaktivieren, führen Sie den folgenden Befehl auf der Hostkonsole aus:

```
xe host-emergency-disable-tls-verification
```

XenCenter zeigt in der Ansicht **Benachrichtigungen** eine Warnung an, wenn die Zertifikatsüberprüfung auf einem Host in einem Pool deaktiviert ist, in dem die Funktion aktiviert ist.

Nachdem Sie alle Probleme mit Zertifikaten auf dem Host behoben haben, stellen Sie sicher, dass Sie die Zertifikatsüberprüfung auf dem Host erneut aktivieren. Um die Zertifikatsüberprüfung erneut zu aktivieren, führen Sie den folgenden Befehl auf der Hostkonsole aus:

```
xe host-emergency-reenable-tls-verification
```

---

layout: doc
description: Create, manage, or destroy a clustered pool of XenServer hosts. Understand the constraints and requirements associated with setting up a clustered pool.—

Clusterpools

Clustering bietet zusätzliche Funktionen, die für Ressourcenpools erforderlich sind, die GFS2-SRs verwenden. Weitere Informationen zu GFS2 finden Sie unter Konfigurieren des Speichers.

Ein Cluster ist ein Pool von bis zu 16 XenServer-Hosts, die enger miteinander verbunden und koordiniert sind als Hosts in nicht geclusterten Pools. Die Hosts im Cluster kommunizieren ständig miteinander in einem ausgewählten Netzwerk. Alle Hosts im Cluster kennen den Status jedes Hosts im Cluster. Diese Host-Koordination ermöglicht es dem Cluster, den Zugriff auf den Inhalt des GFS2-SRs zu steuern.

> **Hinweis:**
>
> Die Clustering-Funktion kommt nur Pools zugute, die eine GFS2-SR enthalten. Wenn Ihr Pool keine GFS2-SR enthält, aktivieren Sie das Clustering in Ihrem Pool nicht.

Quorum

Jeder Host in einem Cluster muss immer mit der Mehrheit der Hosts im Cluster kommunizieren (einschließlich sich selbst). Dieser Zustand ist als Host mit Quorum bekannt. Wenn ein Host kein Quorum hat, grenzt dieser Host sich selbst ein.

Die Anzahl der Hosts, die miteinander kommunizieren müssen, um das Quorum zu erreichen, kann sich von der Anzahl der Hosts unterscheiden, die ein Cluster benötigt, um das Quorum aufrechtzuerhalten.

Die folgende Tabelle fasst dieses Verhalten zusammen. Der Wert von n ist die Gesamtzahl der Hosts im Clusterpool.

	Anzahl der Hosts, die zum Erreichen des Quorums erforderlich sind	Anzahl der Hosts, die erforderlich sind, um quoriert zu bleiben
Ungerade Anzahl von Hosts im Pool	(n+1)/2	(n+1)/2
Gerade Anzahl der Hosts im Pool	(n/2)+1	n/2

Pools mit ungerader Nummerierung

Um den Quorumwert für einen Pool mit ungerader Nummer zu erreichen, benötigen Sie die Hälfte von eins mehr als die Gesamtzahl der Hosts im Cluster: (n+1) /2. Dies ist auch die Mindestanzahl von Hosts, die erreichbar bleiben müssen, damit der Pool quorat bleibt.

In einem Clusterpool mit 5 Hosts müssen beispielsweise 3 Hosts erreichbar sein, damit der Cluster sowohl aktiv wird als auch quorat bleibt [(5+1) /2 = 3].

Wenn möglich, wird empfohlen, eine ungerade Anzahl von Hosts in einem Clusterpool zu verwenden, da dies sicherstellt, dass Hosts immer feststellen können, ob sie über einen Quoratssatz verfügen.

Pools mit geraden Nummern

Wenn ein Pool mit gerader Anzahl von einem Kaltstart hochgefahren wird, müssen (n/2) +1 Hosts verfügbar sein, bevor die Hosts über ein Quorum verfügen. Nachdem die Hosts das Quorum haben, wird der Cluster aktiv.

Ein aktiver Pool mit gerader Nummer kann jedoch quorat bleiben, wenn die Anzahl der kontaktierbaren Hosts mindestens n/2 beträgt. Daher ist es möglich, dass ein laufender Cluster mit einer geraden Anzahl von Hosts exakt in zwei Hälften aufgeteilt wird. Der laufende Cluster entscheidet, welche Hälfte der Cluster-Selbstzäune und welche Hälfte des Clusters über ein Quorum verfügt. Die Hälfte des Clusters, die den Knoten mit der niedrigsten ID enthält, der vor der Clusteraufteilung als aktiv angesehen wurde, bleibt aktiv, und die andere Hälfte des Clusters grenzt sich selbst ab.

In einem Clusterpool mit 4 Hosts müssen beispielsweise 3 Hosts erreichbar sein, damit der Cluster aktiv wird [4/2 + 1 = 3]. Nachdem der Cluster aktiv ist, müssen nur 2 Hosts kontaktiert werden können,

um quorat zu bleiben [4/2 = 2], und diese Gruppe von Hosts muss den Host mit der niedrigsten Knoten-ID enthalten, von der bekannt ist, dass sie aktiv ist.

Fechten

Wenn ein Host feststellt, dass er kein Quorum hat, zäunt er sich innerhalb weniger Sekunden selbst ein. Wenn ein Host sich selbst zäunt, wird er sofort neu gestartet. Alle virtuellen Maschinen, die auf dem Host ausgeführt werden, werden sofort angehalten, da der Host einen Hard-Shutdown durchführt. In einem Clusterpool, der Hochverfügbarkeit verwendet, startet XenServer die VMs entsprechend ihrer Neustartkonfiguration auf anderen Poolmitgliedern neu. Der Host, der sich selbst eingezäunt hat, wird neu gestartet und versucht, dem Cluster erneut beizutreten.

Wenn die Anzahl der Live-Hosts im Cluster unter dem Quorumwert liegt, verlieren alle verbleibenden Hosts das Quorum.

Im Idealfall hat Ihr Clusterpool immer mehr Live-Hosts, als für das Quorum erforderlich sind, und XenServer grenzt nie ab. Um dieses Szenario wahrscheinlicher zu machen, sollten Sie beim Einrichten Ihres Clusterpools die folgenden Empfehlungen berücksichtigen:

- Stellen Sie eine gute Hardwareredundanz sicher.
- Verwenden Sie ein dediziertes Bonded Network für das Cluster-Netzwerk. Stellen Sie sicher, dass sich die gebundenen NICs auf demselben L2-Segment befinden. Weitere Informationen finden Sie unter Netzwerk.
- Konfigurieren Sie das Speicher-Multipathing zwischen dem Pool und dem GFS2-SR. Weitere Informationen finden Sie unter Speicher-Multipathing.

Erstellen eines Clusterpools

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Alle XenServer-Hosts im Clusterpool müssen über mindestens 2 GiB Steuerdomänenspeicher verfügen.

  Abhängig von Ihrer Umgebung benötigen Ihre Hosts möglicherweise mehr Steuerdomänenspeicher als diesen. Wenn Sie auf Ihren Hosts nicht genügend Steuerdomänenspeicher haben, kann es in Ihrem Pool zu Netzwerkinstabilität kommen. Netzwerkinstabilität kann bei einem Clusterpool mit GFS2-SRs zu Problemen führen. Hinweise zum Ändern der Größe des Steuerdomänenspeichers und zum Überwachen des Speicherverhaltens finden Sie unter Speicherauslastung.
- Alle Hosts im Cluster müssen statische IP-Adressen für das Cluster-Netzwerk verwenden.

- Es wird empfohlen, Clustering nur in Pools mit mindestens drei Hosts zu verwenden, da Pools von zwei Hosts empfindlich auf das Selbst-Fencing des gesamten Pools reagieren.
- Clusterpools unterstützen nur bis zu 16 Hosts pro Pool.
- Wenn Sie eine Firewall zwischen den Hosts in Ihrem Pool haben, stellen Sie sicher, dass Hosts über die folgenden Ports im Cluster-Netzwerk kommunizieren können:
  - TCP: 8892, 8896, 21064
  - UDP: 5404, 5405

  Weitere Informationen finden Sie unter Von XenServer verwendete Kommunikationsports.
- Wenn Sie einen vorhandenen Pool clustern, stellen Sie sicher, dass die Hochverfügbarkeit deaktiviert ist. Sie können die Hochverfügbarkeit erneut aktivieren, nachdem das Clustering aktiviert wurde.
- Wir empfehlen dringend, dass Sie für Ihren Clusterpool ein gebundenes Netzwerk verwenden, das nicht für anderen Datenverkehr verwendet wird.

Wenn Sie möchten, können Sie mit XenCenter Clustering in Ihrem Pool einrichten. Weitere Informationen finden Sie in der XenCenter-Produktdokumentation.

So verwenden Sie die xe CLI zum Erstellen eines Clusterpool:

1. Erstellen Sie ein gebundenes Netzwerk, das als Clusternetzwerk verwendet werden kann.

   > **Hinweis:**
   >
   > Wir empfehlen dringend, ein dediziertes gebundenes Netzwerk für Ihren Clusterpool zu verwenden. Verwenden Sie dieses Netzwerk nicht für anderen Datenverkehr.

   Führen Sie auf dem XenServer-Host, den Sie als Poolkoordinator verwenden möchten, die folgenden Schritte aus:

   a) Öffnen Sie eine Konsole auf dem XenServer-Host.

   b) Erstellen Sie ein Netzwerk zur Verwendung mit der gebundenen NIC, indem Sie den folgenden Befehl verwenden:

   ```
   xe network-create name-label=bond0
   <!--NeedCopy-->
   ```

   Die UUID des neuen Netzwerks wird zurückgegeben.

   c) Suchen Sie die UUIDs der PIFs, die in der Bindung verwendet werden sollen, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```


d) Erstellen Sie Ihr gebundenes Netzwerk entweder im aktiv-aktiven Modus, im aktiv-passiven Modus oder im LACP-Bond-Modus. Führen Sie je nach dem Bond-Modus, den Sie verwenden möchten, eine der folgenden Aktionen aus:

- Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den Befehl `bond-create`, um die Bindung zu erstellen. Trennen Sie die Parameter durch Kommas und geben Sie die neu erstellte Netzwerk-UUID und die UUIDs der zu verbindenden PIFs an:

```
xe bond-create network-uuid=<network_uuid> /
     pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4>
<!--NeedCopy-->
```

  Geben Sie zwei UUIDs ein, wenn Sie zwei NICs und vier UUIDs verbinden, wenn Sie vier Netzwerkkarten verbinden. Die UUID für die Bindung wird nach Ausführung des Befehls zurückgegeben.

- Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie dieselbe Syntax, fügen Sie den optionalen Parameter `mode` hinzu und geben Sie `lacp` oder `active-backup` an:

```
xe bond-create network-uuid=<network_uuid> pif-uuids=<
   pif_uuid_1>, /
     <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /
     mode=balance-slb | active-backup | lacp
<!--NeedCopy-->
```

Nachdem Sie Ihr gebundenes Netzwerk auf dem Poolkoordinator erstellt haben und andere XenServer-Hosts mit dem Pool verbinden, werden die Netzwerk- und Bindungsinformationen automatisch auf den beitretenden Server repliziert.

Weitere Informationen finden Sie unter Netzwerk.

2. Erstellen Sie einen Ressourcenpool mit mindestens drei XenServer-Hosts.

   Wiederholen Sie die folgenden Schritte auf jedem XenServer-Host, der ein Poolmitglied (kein Master) ist:

   a) Öffnen Sie eine Konsole auf dem XenServer-Host.

   b) Verbinden Sie den XenServer-Host mit dem Pool auf dem Poolkoordinator, indem Sie den folgenden Befehl verwenden:

```
xe pool-join master-address=master_address master-username=
   administrators_username master-password=password
<!--NeedCopy-->
```


Der Wert des `master-address` Parameters muss auf den vollqualifizierten Domänennamen des XenServer-Hosts gesetzt werden, der der Poolkoordinator ist. Das `password` muss das Administratorkennwort sein, das bei der Installation des Poolkoordinators festgelegt wurde.

Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

3. Stellen Sie für jedes PIF, das zu diesem Netzwerk gehört, ein `disallow-unplug=true`.

   a) Suchen Sie die UUIDs der PIFs, die zum Netzwerk gehören, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

   b) Führen Sie den folgenden Befehl auf einem XenServer-Host in Ihrem Ressourcenpool aus:

   ```
   xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
   <!--NeedCopy-->
   ```

4. Aktivieren Sie das Clustering in Ihrem Pool. Führen Sie den folgenden Befehl auf einem XenServer-Host in Ihrem Ressourcenpool aus:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   <!--NeedCopy-->
   ```

   Geben Sie die UUID des gebundenen Netzwerks an, das Sie in einem früheren Schritt erstellt haben.

Zerstören eines Clusterpool

Sie können einen Clusterpool löschen. Nachdem Sie einen Clusterpool gelöscht haben, besteht der Pool weiterhin, ist jedoch nicht mehr geclustert und kann keine GFS2-SRs mehr verwenden.

Um einen Clusterpool zu löschen, führen Sie den folgenden Befehl aus:

```
xe cluster-pool-destroy cluster-uuid=<uuid>
```

Verwalten Sie Ihren Clusterpool

Bei der Verwaltung Ihres geclusterten Pools können die folgenden Vorgehensweisen das Risiko verringern, dass der Pool das Quorum verliert.

Einen Host in einem Clusterpool hinzufügen oder entfernen

Stellen Sie beim Hinzufügen oder Entfernen eines Hosts in einem Clusterpool sicher, dass alle Hosts im Cluster online sind.

Sie können einen Host in einem Clusterpool mit XenCenter hinzufügen oder entfernen. Weitere Informationen finden Sie unter Server zu einem Pool hinzufügen und Server aus einem Pool entfernen.

Sie können einen Host in einem Clusterpool auch mit der xe-CLI hinzufügen oder entfernen. Weitere Informationen finden Sie unter Host zu einem Pool mit der XE-CLI hinzufgen und XenServer-Hosts aus einem Ressourcenpool entfernen.

Stellen Sie sicher, dass Hosts sauber heruntergefahren werden

Wenn ein Host sauber heruntergefahren wird, wird er vorübergehend aus dem Cluster entfernt, bis er neu gestartet wird. Während der Host heruntergefahren wird, wird er nicht auf den Quorumwert des Clusters angerechnet. Die Abwesenheit des Hosts führt nicht dazu, dass andere Hosts das Quorum verlieren.

Wenn ein Host jedoch zwangsweise oder unerwartet heruntergefahren wird, wird er nicht aus dem Cluster entfernt, bevor er offline geht. Dieser Host wird auf den Quorumwert des Clusters angerechnet. Sein Herunterfahren kann dazu führen, dass andere Hosts das Quorum verlieren.

Wenn ein Host zwangsweise heruntergefahren werden muss, überprüfen Sie zunächst, wie viele Live-Hosts sich im Cluster befinden. Sie können dies mit dem Befehl tun `corosync-quorumtool`. In der Befehlsausgabe ist die Anzahl der Live-Hosts der Wert `Total votes:` und die Anzahl der Live-Hosts, die zur Aufrechterhaltung des Quorums erforderlich sind, ist der Wert `Quorum:`.

- Wenn die Anzahl der Live-Hosts der Anzahl der Hosts entspricht, die benötigt werden, um die Quoration aufrechtzuerhalten, sollten Sie den Host nicht zwangsweise herunterfahren. Dadurch wird der gesamte Cluster eingezäunt.

  Versuchen Sie stattdessen, andere Hosts wiederherzustellen und die Anzahl der Live-Hosts zu erhöhen, bevor Sie den Host zwangsweise herunterfahren.

- Wenn die Anzahl der Live-Hosts in etwa der Anzahl der Hosts entspricht, die benötigt werden, um die Quoration aufrechtzuerhalten, können Sie den Host zwangsweise herunterfahren. Dadurch ist der Cluster jedoch anfälliger für ein vollständiges Fencing, wenn andere Hosts im Pool Probleme haben.

Versuchen Sie immer, den heruntergefahrenen Host so schnell wie möglich neu zu starten, um die Resilienz Ihres Clusters zu erhöhen.

Wartungsmodus verwenden

Bevor Sie etwas auf einem Host tun, das dazu führen könnte, dass dieser Host das Quorum verliert, versetzen Sie den Host in den Wartungsmodus. Wenn sich ein Host im Wartungsmodus befindet, werden laufende VMs von ihm auf einen anderen Host im Pool migriert. Wenn dieser Host der Poolkoordinator war, wird diese Rolle auch an einen anderen Host im Pool übergeben. Wenn Ihre Aktionen dazu führen, dass sich ein Host im Wartungsmodus selbst abgrenzt, verlieren Sie keine VMs und verlieren keine XenCenter-Verbindung zum Pool.

Hosts im Wartungsmodus werden immer noch auf den Quorumwert für den Cluster angerechnet.

Sie können die IP-Adresse eines Hosts, der Teil eines Clusterpools ist, nur ändern, wenn sich dieser Host im Wartungsmodus befindet. Durch das Ändern der IP-Adresse eines Hosts verlässt der Host den Cluster. Wenn die IP-Adresse erfolgreich geändert wurde, tritt der Host dem Cluster wieder bei. Nachdem der Host dem Cluster wieder beigetreten ist, können Sie ihn aus dem Wartungsmodus entfernen.

Stellen Sie Hosts wieder her, die selbst eingezäunt sind oder offline sind

Es ist wichtig, Hosts wiederherzustellen, die sich selbst eingezäunt haben. Während diese Cluster-Mitglieder offline sind, werden sie auf die Quorumnummer für den Cluster angerechnet und verringern die Anzahl der Cluster-Mitglieder, die kontaktiert werden können. Diese Situation erhöht das Risiko eines nachfolgenden Hostausfalls, der dazu führt, dass der Cluster das Quorum verliert und vollständig heruntergefahren wird.

Wenn Sie Offline-Hosts in Ihrem Cluster haben, können Sie auch bestimmte Aktionen ausführen. In einem Clusterpool muss jedes Mitglied des Pools jeder Änderung der Poolmitgliedschaft zustimmen, bevor die Änderung erfolgreich sein kann. Wenn ein Clustermitglied nicht erreichbar ist, verhindert XenServer Operationen, die die Clustermitgliedschaft ändern (z. B. Host hinzufügen oder Host entfernen).

Hosts als nicht wiederherstellbar markieren

Wenn ein oder mehrere Offline-Hosts nicht wiederhergestellt werden können, können Sie den Clusterpool anweisen, sie zu vergessen. Diese Hosts werden dauerhaft aus dem Pool entfernt. Nachdem Hosts aus dem Clusterpool entfernt wurden, werden sie nicht mehr auf den Quorumwert angerechnet.

Verwenden Sie den folgenden Befehl, um einen Host als nicht wiederherstellbar zu markieren:

```
1 xe host-forget uuid=<host_uuid>
```


Stellen Sie einen vergessenen Host wieder her

Nachdem ein Clusterpool angewiesen wurde, einen Host zu vergessen, kann der Host nicht wieder zum Pool hinzugefügt werden.

Um dem Clusterpool wieder beizutreten, müssen Sie XenServer auf dem Host neu installieren, damit er als neuer Host im Pool angezeigt wird. Sie können den Host dann wie gewohnt mit dem Clusterpool verbinden.

Problembehandlung bei Ihrem Clusterpool

Wenn Probleme mit Ihrem Clusterpool auftreten, finden Sie weitere Informationen unter Problembehandlung bei Clusterpools.

Einschränkungen

- Clusterpools unterstützen nur bis zu 16 Hosts pro Pool.
- Um HA in Ihrem Clusterpool zu aktivieren, muss der Heartbeat-SR ein GFS2-SR sein.
- Für Clusterverkehr empfehlen wir dringend, ein gebundenes Netzwerk zu verwenden, das mindestens zwei verschiedene Netzwerk-Switches verwendet. Verwenden Sie dieses Netzwerk nicht für andere Zwecke.
- Um die IP-Adresse des Cluster-Netzwerks mithilfe von XenCenter zu ändern, müssen Clustering und GFS2 vorübergehend deaktiviert werden.
- Ändern Sie nicht die Bindung Ihres Clusternetzwerks, während der Cluster aktiv ist und über laufende VMs verfügt. Diese Aktion kann dazu führen, dass Hosts im Cluster neu gestartet werden (Fencing).
- Wenn Sie in Ihrem Clusternetzwerk einen IP-Adresskonflikt haben (mehrere Hosts mit derselben IP-Adresse), an dem mindestens ein Host mit aktiviertem Clustering beteiligt ist, wird der Cluster nicht korrekt gebildet und die Hosts können bei Bedarf kein Fencing durchführen. Um dieses Problem zu beheben, lösen Sie den IP-Adresskonflikt.

Problembehandlung bei Cluster-Pools

January 19, 2024

XenServer-Pools, die GFS2 für die Thin Provisioning ihres gemeinsam genutzten Blockspeichers verwenden, sind geclustert. Diese Pools verhalten sich anders als Pools, die gemeinsam genutzten dateibasierten Speicher oder LVM mit gemeinsam genutztem Blockspeicher verwenden. Daher können in XenServer-Clusterpools und GFS2-Umgebungen einige spezifische Probleme auftreten.

Verwenden Sie die folgenden Informationen, um kleinere Probleme zu beheben, die bei der Verwendung dieser Funktion auftreten können.

Alle meine Hosts können sich gegenseitig pingen, aber ich kann keinen Cluster erstellen. Warum?

Der Clustering-Mechanismus verwendet bestimmte Ports. Wenn Ihre Hosts über diese Ports nicht kommunizieren können (auch wenn sie über andere Ports kommunizieren können), können Sie das Clustering für den Pool nicht aktivieren.

Stellen Sie sicher, dass die Hosts im Pool über die folgenden Ports kommunizieren können:

- TCP: 8892, 8896, 21064
- UDP: 5404, 5405 (kein Multicast)

Wenn es Firewalls oder ähnliches zwischen den Hosts im Pool gibt, stellen Sie sicher, dass diese Ports geöffnet sind.

Wenn Sie HA zuvor im Pool konfiguriert haben, deaktivieren Sie HA, bevor Sie das Clustering aktivieren.

Warum erhalte ich eine Fehlermeldung, wenn ich versuche, einen neuen Host mit einem vorhandenen Clusterpool zu verbinden?

Wenn Clustering für einen Pool aktiviert ist, muss jede Änderung der Poolmitgliedschaft von jedem Mitglied des Clusters genehmigt werden, bevor sie erfolgreich sein kann. Wenn ein Clustermitglied nicht erreichbar ist, schlagen Operationen, die die Clustermitgliedschaft ändern (wie das Hinzufügen oder Entfernen von Hosts), fehl.

So fügen Sie Ihren neuen Host zum Cluster-Pool hinzu:

1. Stellen Sie sicher, dass alle Hosts online sind und kontaktiert werden können.
2. Stellen Sie sicher, dass die Hosts im Pool über die folgenden Ports kommunizieren können:
    - TCP: 8892, 8896, 21064
    - UDP: 5404, 5405 (kein Multicast)
3. Stellen Sie sicher, dass dem beitretenden Host eine IP-Adresse auf der Netzwerkkarte zugewiesen ist, die dem Cluster-Netzwerk des Pools beitritt.
4. Stellen Sie sicher, dass kein Host im Pool offline ist, wenn ein neuer Host versucht, dem Clusterpool beizutreten.

5. Wenn ein Offline-Host nicht wiederhergestellt werden kann, markieren Sie ihn als tot, um ihn aus dem Cluster zu entfernen. Weitere Informationen finden Sie unter Ein Host in meinem Clusterpool ist offline und ich kann ihn nicht wiederherstellen. Wie entferne ich den Host aus meinem Cluster?

Was mache ich, wenn einige Mitglieder des Cluster-Pools dem Cluster nicht automatisch beitreten?

Dieses Problem kann dadurch verursacht werden, dass Mitglieder des Cluster-Pools die Synchronisation verlieren.

Verwenden Sie den folgenden Befehl, um die Mitglieder des geclusterten Pools erneut zu synchronisieren:

```
xe cluster-pool-resync cluster-uuid=<cluster_uuid>
```

Wenn das Problem weiterhin besteht, können Sie versuchen, den GFS2 SR erneut anzuschließen. Sie können diese Aufgabe mithilfe der Xe-CLI oder über XenCenter ausführen.

Hängen Sie den GFS2 SR mithilfe der Xe-CLI erneut an:

1. Nehmen Sie den GFS2 SR vom Pool ab. Führen Sie auf jedem Host den Befehl xe CLI aus `xe pbd-unplug uuid=<uuid_of_pbd>`.
2. Deaktivieren Sie den Cluster-Pool mit dem Befehl `xe cluster-pool-destroy cluster-uuid=<cluster_uuid>`

   Wenn der vorherige Befehl nicht erfolgreich ist, können Sie einen Cluster-Pool zwangsweise deaktivieren, indem Sie `xe cluster-host-force-destroy uuid=<cluster_host>` auf jedem Host im Pool ausführen.
3. Aktivieren Sie den Cluster-Pool erneut, indem Sie den Befehl verwenden `xe cluster-pool-create network-uuid=<network_uuid> [cluster-stack=cluster_stack] [token-timeout=token_timeout] [token-timeout-coefficient=token_timeout_coefficient]`
4. Verbinden Sie den GFS2 SR erneut, indem Sie den Befehl `xe pbd-plug uuid=<uuid_of_pbd>` auf jedem Host ausführen.

Alternativ können Sie XenCenter verwenden, um den GFS2 SR erneut anzuschließen:

1. Klicken Sie auf der Registerkarte **Poolspeicher** mit der rechten Maustaste auf den GFS2 SR und wählen Sie **Trennen…**.
2. Wählen Sie in der Werkzeugleiste **Pool > Eigenschaften**aus.
3. Deaktivieren Sie auf der Registerkarte **Clustering** die Option Clustering **aktivieren**.
4. Klicken Sie auf **OK**, um Ihre Änderung zu übernehmen.

5. Wählen Sie in der Werkzeugleiste **Pool > Eigenschaften**aus.
6. Wählen Sie auf der Registerkarte **Clustering** die Option **Clustering aktivieren** und wählen Sie das Netzwerk aus, das für das Clustering verwendet werden soll.
7. Klicken Sie auf **OK**, um Ihre Änderung zu übernehmen.
8. Klicken Sie auf der Registerkarte **Poolspeicher** mit der rechten Maustaste auf den GFS2 SR und wählen Sie **Reparieren.**

Woher weiß ich, ob mein Host sich umgrenzt hat?

Wenn Ihr Host sich umgrenzt hat, ist er beim Neustart möglicherweise wieder dem Cluster beigetreten. Um zu sehen, ob ein Host sich selbst eingezäunt und wiederhergestellt hat, können Sie in der Datei `/var/opt/xapi-clusterd/boot-times` nachsehen, wann der Host gestartet wurde. Wenn die Datei Startzeiten enthält, von denen Sie nicht erwartet haben, dass sie angezeigt werden, hat sich der Host selbst umgrenzt.

Warum ist mein Host offline? Wie kann ich ihn wiederherstellen?

Es gibt viele mögliche Gründe dafür, dass ein Host offline geht. Je nach Grund kann der Host entweder wiederhergestellt werden oder nicht.

Die folgenden Gründe dafür, dass ein Host offline ist, treten häufiger auf und können durch eine Wiederherstellung des Hosts behoben werden:

- Sauberes Herunterfahren
- Erzwungene Abschaltung
- Vorübergehender Stromausfall
- Reboot

Die folgenden Gründe dafür, dass ein Host offline ist, sind seltener:

- Dauerhafter Host-Hardwarefehler
- Dauerhafter Ausfall der Host-Stromversorgung
- Netzwerkpartition
- Ausfall des Netzwerk-Switches

Diese Probleme können behoben werden, indem Hardware ausgetauscht oder ausgefallene Hosts als tot markiert werden.

Ein Host in meinem Clusterpool ist offline und ich kann ihn nicht wiederherstellen. Wie entferne ich den Host aus meinem Cluster?

Sie können dem Cluster sagen, dass er den Host vergessen soll. Diese Aktion entfernt den Host dauerhaft aus dem Cluster und verringert die Anzahl der Live-Hosts, die für das Quorum erforderlich sind.

Verwenden Sie den folgenden Befehl, um einen nicht wiederherstellbaren Host zu entfernen:

```
xe host-forget uuid=<host_uuid>
```

Dieser Befehl entfernt den Host dauerhaft aus dem Cluster und verringert die Anzahl der Live-Hosts, die für das Quorum erforderlich sind.

> **Hinweis:**
>
> Wenn der Host nicht offline ist, kann dieser Befehl zu Datenverlust führen. Sie werden gebeten, zu bestätigen, dass Sie sich sicher sind, bevor Sie mit dem Befehl fortfahren.

Wenn ein Host vergessen wurde, kann er nicht wieder zum Cluster hinzugefügt werden. Um diesen Host wieder zum Cluster hinzuzufügen, müssen Sie eine Neuinstallation von XenServer auf dem Host durchführen.

Ich habe einen Host repariert, der als tot markiert war. Wie füge ich ihn wieder zu meinem Cluster hinzu?

Ein XenServer-Host, der als tot markiert wurde, kann dem Cluster nicht wieder hinzugefügt werden. Um dieses System wieder zum Cluster hinzuzufügen, müssen Sie eine Neuinstallation von XenServer durchführen. Diese Neuinstallation wird dem Cluster als neuer Host angezeigt.

Was mache ich, wenn mein Cluster ständig das Quorum verliert und seine Hosts sich weiterhin umgrenzen?

Wenn einer oder mehrere der XenServer-Hosts im Cluster in eine Fence-Schleife geraten, weil sie ständig Quorum verlieren und gewinnen, können Sie den Host mit dem Kernel-Befehlszeilenargument `nocluster` starten. Stellen Sie eine Verbindung zur physischen oder seriellen Konsole des Hosts her und bearbeiten Sie die Boot-Argumente in Grub.

Beispiel:

```
/boot/grub/grub.cfg
menuentry 'XenServer' {

        search --label --set root root-oyftuj
```



```
5           multiboot2 /boot/xen.gz dom0_mem=4096M,max:4096M watchdog ucode
               =scan dom0_max_vcpus=1-16 crashkernel=192M,below=4G console=
               vga vga=mode-0x0311
6           module2 /boot/vmlinuz-4.4-xen root=LABEL=root-oyftuj ro nolvm
               hpet=disable xencons=hvc console=hvc0 console=tty0 quiet vga
               =785 splash plymouth.ignore-serial-consoles nocluster
7           module2 /boot/initrd-4.4-xen.img
8    }
9
10   menuentry 'XenServer (Serial)' {
11
12          search --label --set root root-oyftuj
13          multiboot2 /boot/xen.gz com1=115200,8n1 console=com1,vga
               dom0_mem=4096M,max:4096M watchdog ucode=scan dom0_max_vcpus
               =1-16 crashkernel=192M,below=4G
14          module2 /boot/vmlinuz-4.4-xen root=LABEL=root-oyftuj ro nolvm
               hpet=disable console=tty0 xencons=hvc console=hvc0 nocluster
15          module2 /boot/initrd-4.4-xen.img
16   }
17
18   <!--NeedCopy-->
```

Was passiert, wenn der Poolkoordinator in einem Clusterpool neu gestartet wird?

In den meisten Fällen ist das Verhalten beim Herunterfahren oder Neustarten des Poolkoordinators in einem Clusterpool dasselbe wie beim Herunterfahren oder Neustarten eines anderen Poolmitglieds.

Wie der Host heruntergefahren oder neu gestartet wird, kann sich auf das Quorum des Cluster-Pools auswirken. Weitere Informationen zum Quorum finden Sie unter Quorum.

Der einzige Unterschied im Verhalten hängt davon ab, ob HA in Ihrem Pool aktiviert ist:

- Wenn HA aktiviert ist, wird ein neuer Koordinator ausgewählt und der allgemeine Service wird aufrechterhalten.
- Wenn HA nicht aktiviert ist, gibt es keinen Koordinator für den Pool. Laufende VMs auf den verbleibenden Hosts werden weiterhin ausgeführt. Die meisten Verwaltungsvorgänge sind erst verfügbar, wenn der Koordinator neu gestartet wird.

Warum ist mein Pool verschwunden, nachdem ein Host im Cluster-Pool zum Herunterfahren gezwungen wurde?

Wenn Sie einen Host normal (nicht gewaltsam) herunterfahren, wird er vorübergehend aus den Quorumberechnungen entfernt, bis er wieder eingeschaltet wird. Wenn Sie jedoch einen Host zwangsweise herunterfahren oder er nicht mehr mit Strom versorgt wird, wird dieser Host trotzdem bei den Quorumberechnungen berücksichtigt. Wenn Sie beispielsweise einen Pool mit 3 Hosts haben

und 2 von ihnen zwangsweise herunterfahren, wird der verbleibende Host eingezäunt, weil er kein Quorum mehr hat.

Versuchen Sie, Hosts in einem Clusterpool immer sauber herunterzufahren. Weitere Informationen finden Sie unter Verwalten Ihres Clusterpools.

Warum wurden alle Hosts im Clusterpool gleichzeitig neu gestartet?

Es wird davon ausgegangen, dass alle Hosts in einem aktiven Cluster das Quorum verloren haben, wenn die Anzahl der kontaktierbaren Hosts im Pool unter diesen Werten liegt:

- Für einen Pool mit einer geraden Anzahl von Hosts: n/2
- Für einen Pool mit einer ungeraden Anzahl von Hosts: (n+1) /2

Der Buchstabe n gibt die Gesamtzahl der Hosts im Clusterpool an. Weitere Informationen zum Quorum finden Sie unter Quorum.

In dieser Situation sperren sich alle Hosts automatisch ab und Sie sehen, wie alle Hosts neu gestartet werden.

Um zu diagnostizieren, warum der Pool das Quorum verloren hat, können die folgenden Informationen hilfreich sein:

- Überprüfen Sie in XenCenter im Abschnitt **Benachrichtigungen** den Zeitpunkt des Problems, um festzustellen, ob Self-Fencing aufgetreten ist.
- Überprüfen Sie `/var/opt/xapi-clusterd/boot-times` auf den Cluster-Hosts, um zu prüfen, ob zu einem unerwarteten Zeitpunkt ein Neustart stattgefunden hat.
- Prüfen Sie unter `Crit.log`, ob Meldungen zur Selbstabschottung ausgegeben werden.
- Informationen zum Fencing finden Sie in der Ausgabe des Befehls `dlm_tool status`.

  Beispielausgabe für `dlm_tool status`:

```
dlm_tool status

cluster nodeid 1 quorate 1 ring seq 8 8
daemon now 4281 fence_pid 0
node 1 M add 3063 rem 0 fail 0 fence 0 at 0 0
node 2 M add 3066 rem 0 fail 0 fence 0 at 0 0
<!--NeedCopy-->
```

Sammeln Sie beim Sammeln von Protokollen für das Debuggen Diagnoseinformationen von allen Hosts im Cluster. Wenn ein einzelner Host über eine eigene Umzäunung verfügt, verfügen die anderen Hosts im Cluster mit größerer Wahrscheinlichkeit über nützliche Informationen.

Erfassen Sie vollständige Serverstatusberichte für die Hosts in Ihrem Clusterpool. Weitere Informationen finden Sie unter XenServer-Hostprotokolle.

Warum kann ich meinen Cluster-Pool nicht wiederherstellen, obwohl ich Quorum habe?

Wenn Sie einen Clusterpool mit einer geraden Anzahl von Hosts haben, ist die Anzahl der Hosts, die zum *Erreichen* des Quorums erforderlich sind, um eins höher als die Anzahl der Hosts, die für die *Aufrechterhaltung* des Quorums erforderlich sind. Weitere Informationen zum Quorum finden Sie unter Quorum.

Wenn Sie sich in einem Pool mit geraden Nummern befinden und die Hälfte der Hosts wiederhergestellt haben, müssen Sie einen weiteren Host wiederherstellen, bevor Sie den Cluster wiederherstellen können.

Warum sehe ich einen Fehler `Invalid token`, wenn ich die Cluster-Einstellungen ändere?

Wenn Sie die Konfiguration Ihres Clusters aktualisieren, erhalten Sie möglicherweise die folgende Fehlermeldung über ein ungültiges Token (`"[[\"InternalError\",\"Invalid token \"]]"`).

Sie können dieses Problem lösen, indem Sie die folgenden Schritte ausführen:

1. (Optional) Sichern Sie die aktuelle Cluster-Konfiguration, indem Sie einen Serverstatusbericht sammeln, der die xapi-clusterd- und Systemprotokolle enthält.
2. Verwenden Sie XenCenter, um den GFS2 SR vom Clusterpool zu trennen.

   Klicken Sie auf der Registerkarte **Poolspeicher** mit der rechten Maustaste auf den GFS2 SR und wählen Sie **Trennen...**.
3. Führen Sie auf einem beliebigen Host im Cluster diesen Befehl aus, um den Cluster gewaltsam zu zerstören:

   ```
   1 xe cluster-pool-force-destroy cluster-uuid=<uuid>
   ```
4. Verwenden Sie XenCenter, um das Clustering in Ihrem Pool wieder zu aktivieren.

   a) Wählen Sie in der Werkzeugleiste **Pool > Eigenschaften**aus.
   b) Wählen Sie auf der Registerkarte **Clustering** die Option **Clustering aktivieren** und wählen Sie das Netzwerk aus, das für das Clustering verwendet werden soll.
   c) Klicken Sie auf **OK**, um Ihre Änderung zu übernehmen
5. Verwenden Sie XenCenter, um den GFS2 SR erneut an den Pool anzuschließen

   Klicken Sie auf der Registerkarte **Poolspeicher** mit der rechten Maustaste auf den GFS2 SR und wählen Sie **Reparieren.**

layout: doc
description: Use Active Directory to create additional users that can administer XenServer. Configure the user permissions with role-based access control.—

Benutzer verwalten

Durch die Definition von Benutzern, Gruppen, Rollen und Berechtigungen können Sie steuern, wer Zugriff auf Ihre XenServer-Hosts und -Pools hat und welche Aktionen sie ausführen können.

Bei der ersten Installation von XenServer wird XenServer automatisch ein Benutzerkonto hinzugefügt. Dieses Konto ist der lokale Superuser (LSU) oder Root, den XenServer lokal authentifiziert.

Die LSU oder root ist ein spezielles Benutzerkonto, das für die Systemadministration bestimmt ist und über alle Berechtigungen verfügt. In XenServer ist die LSU das Standardkonto bei der Installation. XenServer authentifiziert das LSU-Konto. Die LSU benötigt keinen externen Authentifizierungsdienst. Wenn ein externer Authentifizierungsdienst ausfällt, kann sich die LSU trotzdem anmelden und das System verwalten. Die LSU kann jederzeit über SSH auf den physischen XenServer-Server zugreifen.

Sie können mehr Benutzer erstellen, indem Sie die Active Directory-Konten entweder über die Registerkarte Benutzer von XenCenter oder die xe-CLI hinzufügen. Wenn Ihre Umgebung kein Active Directory verwendet, sind Sie auf das LSU-Konto beschränkt.

> **Hinweis:**
>
> Wenn Sie Benutzer erstellen, weist XenServer neu erstellten Benutzerkonten nicht automatisch RBAC-Rollen zu. Daher haben diese Konten keinen Zugriff auf den XenServer-Pool, bis Sie ihnen eine Rolle zuweisen.

Diese Berechtigungen werden über Rollen erteilt, wie im Abschnitt *Authentifizierung von Benutzern mit Active Directory (AD)* erläutert.

Authentifizieren von Benutzern mit Active Directory (AD)

Wenn Sie mehrere Benutzerkonten auf einem Host oder Pool haben möchten, müssen Sie Active Directory-Benutzerkonten für die Authentifizierung verwenden. Mit AD-Konten können sich XenServer-Benutzer mit ihren Windows-Domänenanmeldeinformationen an einem Pool anmelden.

> **Hinweis:**
>
> Sie können LDAP-Kanalbindung und LDAP-Signatur auf Ihren AD-Domänencontroller aktivieren Weitere Informationen finden Sie unter Microsoft Security Advisory.

Sie können verschiedene Zugriffsebenen für bestimmte Benutzer konfigurieren, indem Sie die Active Directory-Authentifizierung aktivieren, Benutzerkonten hinzufügen und diesen Konten Rollen zuweisen.

Active Directory-Benutzer können die xe-CLI verwenden (entsprechende Argumente `-u` und `-pw` übergeben) und mit XenCenter auch eine Verbindung zum Host herstellen. Die Authentifizierung erfolgt auf Poolbasis pro Ressource.

Die Probanden kontrollieren den Zugriff auf Benutzerkonten. Ein Betreff in XenServer ist einer Entität auf Ihrem Active Directory-Server zugeordnet (entweder einem Benutzer oder einer Gruppe). Wenn Sie die externe Authentifizierung aktivieren, überprüft XenServer die Anmeldeinformationen, die zum Erstellen einer Sitzung verwendet wurden, mit den lokalen Root-Anmeldeinformationen und dann mit der Betreffliste. Um den Zugriff zu ermöglichen, erstellen Sie einen Betreffeintrag für die Person oder Gruppe, für die Sie Zugriff gewähren möchten. Sie können XenCenter oder die xe CLI verwenden, um einen Betreffeintrag zu erstellen.

Wenn Sie mit XenCenter vertraut sind, beachten Sie, dass die Xe-CLI eine etwas andere Terminologie verwendet, um sich auf Active Directory- und Benutzerkontenfunktionen zu beziehen:

XenCenter-Begriff	xe-CLI-Begriff
Benutzer, Benutzer hinzufügen	Fächer, Fächer hinzufügen

Obwohl XenServer Linux-basiert ist, können Sie mit XenServer Active Directory-Konten für XenServer-Benutzerkonten verwenden. Dazu werden Active Directory-Anmeldeinformationen an den Active Directory-Domänencontroller übergeben.

Wenn Sie Active Directory zu XenServer hinzufügen, werden Active Directory-Benutzer und -Gruppen zu XenServer-Themen. Die Themen werden in XenCenter als Benutzer bezeichnet. Benutzer/Gruppen werden bei der Anmeldung mithilfe von Active Directory authentifiziert, wenn Sie ein Subjekt bei XenServer registrieren. Benutzer und Gruppen müssen ihren Benutzernamen nicht mithilfe eines Domainnamens qualifizieren.

Um einen Benutzernamen zu qualifizieren, müssen Sie den Benutzernamen im Format Anmeldename der unteren Ebene eingeben, `mydomain\myuser`z. B.

> **Hinweis:**
>
> Wenn Sie den Benutzernamen nicht qualifiziert haben, versucht XenCenter standardmäßig, Benutzer mit der Domäne, mit der es verbunden ist, bei AD-Authentifizierungsservern anzumelden. Die Ausnahme bildet das LSU-Konto, das XenCenter immer zuerst lokal (also auf dem XenServer) authentifiziert.

Der externe Authentifizierungsprozess funktioniert wie folgt:

1. Die beim Herstellen einer Verbindung mit einem Host angegebenen Anmeldeinformationen werden zur Authentifizierung an den Active Directory-Domänencontroller übergeben.
2. Der Domänencontroller prüft die Anmeldeinformationen. Wenn sie ungültig sind, schlägt die Authentifizierung sofort fehl.
3. Wenn die Anmeldeinformationen gültig sind, wird der Active Directory-Controller abgefragt, um die mit den Anmeldeinformationen verknüpfte Betreff-ID und die Gruppenmitgliedschaft abzurufen.
4. Wenn die Betreff-ID mit der im XenServer gespeicherten übereinstimmt, ist die Authentifizierung erfolgreich.

Wenn Sie einer Domäne beitreten, aktivieren Sie die Active Directory-Authentifizierung für den Pool. Wenn ein Pool jedoch einer Domäne beitritt, können nur Benutzer in dieser Domäne (oder einer Domäne, zu der er Vertrauensbeziehungen hat) eine Verbindung zum Pool herstellen.

> **Hinweis:**
>
> Das manuelle Aktualisieren der DNS-Konfiguration eines DHCP-konfigurierten Netzwerk-PIF wird nicht unterstützt und kann dazu führen, dass die AD-Integration und damit die Benutzerauthentifizierung fehlschlägt oder nicht mehr funktioniert.

Active Directory-Authentifizierung konfigurieren

XenServer unterstützt die Verwendung von Active Directory-Servern unter Windows 2008 oder höher.

Um Active Directory für XenServer-Hosts zu authentifizieren, müssen Sie denselben DNS-Server sowohl für den Active Directory-Server (konfiguriert für Interoperabilität) als auch für den XenServer-Host verwenden.
In einigen Konfigurationen kann der Active Directory-Server das DNS selbst bereitstellen. Dies kann entweder mithilfe von DHCP erreicht werden, um dem XenServer-Host die IP-Adresse und eine Liste von DNS-Servern zur Verfügung zu stellen. Alternativ können Sie die Werte in den PIF-Objekten festlegen oder das Installationsprogramm verwenden, wenn eine manuelle statische Konfiguration verwendet wird.

Wir empfehlen, DHCP zu aktivieren, um Hostnamen zuzuweisen. Weisen Sie die Hostnamen `localhost` oder `linux` nicht Hosts zu.

> **Warnung:**
>
> XenServer-Hostnamen müssen in der gesamten XenServer-Bereitstellung eindeutig sein.

Beachten Sie Folgendes:

- XenServer kennzeichnet seinen AD-Eintrag in der AD-Datenbank mit seinem Hostnamen. Wenn zwei XenServer-Hosts mit demselben Hostnamen derselben AD-Domäne angehören, überschreibt der zweite XenServer den AD-Eintrag des ersten XenServer. Das Überschreiben erfolgt unabhängig davon, ob die Hosts zu denselben oder verschiedenen Pools gehören. Dies kann dazu führen, dass die AD-Authentifizierung auf dem ersten XenServer nicht mehr funktioniert.

  Sie können denselben Hostnamen in zwei XenServer-Hosts verwenden, sofern sie verschiedenen AD-Domänen beitreten.

- Die XenServer-Hosts können sich in unterschiedlichen Zeitzonen befinden, da die UTC-Zeit verglichen wird. Um sicherzustellen, dass die Synchronisierung korrekt ist, können Sie dieselben NTP-Server für Ihren XenServer-Pool und den Active Directory-Server verwenden.
- Pools mit gemischter Authentifizierung werden nicht unterstützt. Sie können keinen Pool haben, in dem einige Hosts im Pool für die Verwendung von Active Directory konfiguriert sind und andere nicht.
- Die XenServer Active Directory-Integration verwendet das Kerberos-Protokoll für die Kommunikation mit den Active Directory-Servern. Daher unterstützt XenServer nicht die Kommunikation mit Active Directory-Servern, die Kerberos nicht verwenden.
- Damit die externe Authentifizierung mit Active Directory erfolgreich ist, müssen die Uhren auf Ihren XenServer-Hosts mit den Uhren auf Ihrem Active Directory-Server synchronisiert werden. Wenn XenServer der Active Directory-Domäne beitritt, wird die Synchronisierung überprüft und die Authentifizierung schlägt fehl, wenn es zu viele Abweichungen zwischen den Servern gibt.

> **Warnung:**
>
> Hostnamen dürfen ausschließlich aus nicht mehr als 63 alphanumerischen Zeichen bestehen und dürfen nicht rein numerisch sein.
>
> Eine Einschränkung in den neuesten SSH-Clients bedeutet, dass SSH nicht für Benutzernamen funktioniert, die eines der folgenden Zeichen enthalten: `{ } [] | &`. Stellen Sie sicher, dass Ihre Benutzernamen und Active Directory-Servernamen keines dieser Zeichen enthalten.

Wenn Sie nach der Aktivierung der Active Directory-Authentifizierung einen Host zu einem Pool hinzufügen, werden Sie aufgefordert, Active Directory auf dem Host zu konfigurieren, der dem Pool

beitritt. Wenn Sie auf dem beitretenden Host zur Eingabe von Anmeldeinformationen aufgefordert werden, geben Sie Active Directory-Anmeldeinformationen mit ausreichenden Rechten ein, um Hosts zu dieser Domäne hinzuzufügen.

Active Directory-Integration

Stellen Sie sicher, dass die folgenden Firewallports für ausgehenden Datenverkehr geöffnet sind, damit XenServer auf die Domänencontroller zugreifen kann.

Port	Protokoll	Verwenden
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS-Namensdienst
139	TCP	NetBIOS-Sitzung (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB über TCP
464	UDP/TCP	Kennwortänderungen für
636	UDP/TCP	LDAP über SSL
3268	TCP	Globale Katalogsuche

Weitere Informationen finden Sie unter Von XenServer verwendete Kommunikationsports.

> **Hinweise:**
>
> - Führen Sie den folgenden Befehl aus, um die Firewall-Regeln auf einem Linux-Computer mit *iptables*anzuzeigen: `iptables -nL`.

Winbind

XenServer verwendet Winbind, um Active Directory-Benutzer (AD) beim AD-Server zu authentifizieren und die Kommunikation mit dem AD-Server zu verschlüsseln.

Winbind unterstützt die folgenden Szenarien nicht:

- Leerzeichen am Anfang oder Ende eines Domänenbenutzers oder eines Domänengruppennamens.

- Domain-Benutzernamen, die mindestens 64 Zeichen enthalten.
- Domänenbenutzernamen, die eines der Sonderzeichen enthalten +<>”=/%@:,;\ ‘
- Domänengruppennamen, die eines der Sonderzeichen enthalten,;\ ‘

Winbind konfigurieren Konfigurieren Sie das Winbind-Verhalten mit den folgenden Konfigurationsoptionen, die in die Datei `/etc/xapi.conf` aufgenommen werden können:

- `winbind_machine_pwd_timeout`: Der Wert dieser Option definiert, wie oft (in Sekunden) das Computerkennwort für diesen XenServer-Host rotiert wird. Definieren Sie einen Wert als Ganzzahl.

  Der Standardwert ist 1209600 Sekunden (14 Tage). Es wird empfohlen, den Standardwert beizubehalten oder den Wert nicht unter den Standardwert zu verringern, um genügend Zeit für die Synchronisierung des neuen Kennworts zwischen den Domänencontrollern zu gewährleisten.

- `winbind_kerberos_encryption_type`: Die Werte für diese Option sind strong, legacy und all. Der Standardwert ist all.

  - Der Wert `all` erlaubt die folgenden Verschlüsselungssammlungen: `aes256-cts-hmac-sha1-96`, `aes128-cts-hmac-sha1-96`, und `arcfour-hmac-md5`
  - Der Wert `strong` erlaubt die folgenden Verschlüsselungssammlungen: und `aes256-cts-hmac-sha1-96aes128-cts-hmac-sha1-96`
  - Der Wert `legacy` erlaubt die folgenden Verschlüsselungssammlungen: `arcfour-hmac-md5`

    Die Legacy-Option ist unsicher und wir empfehlen, sie nur zum Debuggen von Problemen zu verwenden.

  Zur Verbesserung der Sicherheit empfehlen wir, die AES-Verschlüsselung zu erzwingen. Führen Sie hierfür folgende Schritte aus:

  1. Stellen Sie sicher, dass der Domänencontroller `aes256-cts-hmac-sha1-96` und unterstützt `aes128-cts-hmacsha1-96`.
  2. Konfigurieren Sie den Domänencontroller so, dass **die andere Domäne die Kerberos-AES-Verschlüsselung** in der Domänenvertrauensstellung

     Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Methode 3: Konfiguration der Vertrauensstellung zur Unterstützung der AES128- und AES-256-Verschlüsselung anstelle der RC4-Verschlüsselung.
  3. Aktualisieren Sie die `winbind_kerberos_encryption_type` Option, um den Wert zu verwenden `strong`.

4. Starten Sie den Toolstack neu.

   Starten Sie den Toolstack nicht neu, solange HA aktiviert ist. Wenn möglich, deaktivieren Sie HA vorübergehend, bevor Sie den Toolstack neu starten.

- `winbind_cache_time`: Winbind speichert einige Domaininformationen lokal im Cache. Der Wert dieser Option definiert die Anzahl der Sekunden zwischen jeder Cache-Aktualisierung. Die Standardeinstellung ist 60 Sekunden.

Nachdem Sie eine dieser Konfigurationsoptionen aktualisiert haben, starten Sie den Toolstack neu.

Wie verwaltet XenServer das Maschinenkontokennwort für die AD-Integration?

Ähnlich wie bei Windows-Client-Computern aktualisiert Winbind automatisch das Kennwort für das Computerkonto. Winbind aktualisiert das Computerkontokennwort automatisch alle 14 Tage oder wie in der Konfigurationsoption `winbind_machine_pwd_timeout`angegeben.

Externe Authentifizierung in einem Pool aktivieren

Die externe Authentifizierung mit Active Directory kann entweder mit XenCenter oder der CLI mit dem folgenden Befehl konfiguriert werden.

```
xe pool-enable-external-auth auth-type=AD \
  service-name=full-qualified-domain \
  config:user=username \
  config:pass=password
<!--NeedCopy-->
```

Der angegebene Benutzer muss die Berechtigung `Add/remove computer objects or workstations` haben, was die Standardeinstellung für Domänenadministratoren ist.

Wenn Sie in dem von Active Directory und Ihren XenServer-Hosts verwendeten Netzwerk kein DHCP verwenden, richten Sie Ihr DNS wie folgt ein:

1. Richten Sie Ihre Domain-DNS-Suffix-Suchreihenfolge zum Auflösen von Nicht-FQDN-Einträgen

   ```
   xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \
      "other-config:domain=suffix1.com suffix2.com suffix3.com"
   <!--NeedCopy-->
   ```

2. Konfigurieren Sie den DNS-Server für die Verwendung auf Ihren XenServer-Hosts:

   ```
   xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \
     gateway=gateway netmask=netmask uuid=uuid
   <!--NeedCopy-->
   ```


3. Stellen Sie die Verwaltungsschnittstelle manuell so ein, dass sie eine PIF verwendet, die sich im selben Netzwerk wie Ihr DNS-Server befindet:

```
xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die externe Authentifizierung ist eine Pro-Host-Eigenschaft. Wir empfehlen jedoch, dass Sie die externe Authentifizierung pro Pool aktivieren und deaktivieren. Eine Einstellung pro Pool ermöglicht es XenServer, mit Fehlern umzugehen, die bei der Aktivierung der Authentifizierung auf einem bestimmten Host auftreten. XenServer macht auch alle Änderungen rückgängig, die möglicherweise erforderlich sind, um eine konsistente Konfiguration im gesamten Pool sicherzustellen. Verwenden Sie den `host-param-list` Befehl, um die Eigenschaften eines Hosts zu überprüfen und den Status der externen Authentifizierung zu ermitteln, indem Sie die Werte der entsprechenden Felder überprüfen.

Deaktivieren Sie mit XenCenter die Active Directory-Authentifizierung oder den folgenden xe-Befehl:

```
xe pool-disable-external-auth
<!--NeedCopy-->
```

Benutzerauthentifizierung

Um einem Benutzer Zugriff auf Ihren XenServer-Host zu gewähren, müssen Sie einen Betreff für diesen Benutzer oder eine Gruppe hinzufügen, der er angehört. (Transitive Gruppenmitgliedschaften werden ebenfalls wie gewohnt geprüft. Beispiel: Hinzufügen eines Betreffs für Gruppe A, wobei Gruppe A Gruppe B enthält und `user 1` Mitglied der Gruppe B ist, würde den Zugriff auf `user 1` erlauben.) Wenn Sie Benutzerberechtigungen in Active Directory verwalten möchten, können Sie eine einzelne Gruppe erstellen, die Sie dann Benutzer hinzufügen und aus löschen. Alternativ können Sie einzelne Benutzer oder eine Kombination von Benutzern und Gruppen, je nach Ihren Authentifizierungsanforderungen, zu XenServer hinzufügen und löschen. Sie können die Betreffliste über XenCenter oder über die CLI verwalten, wie im folgenden Abschnitt beschrieben.

Bei der Authentifizierung eines Benutzers werden die Anmeldeinformationen zunächst mit dem lokalen Root-Konto abgeglichen, sodass Sie ein System wiederherstellen können, dessen AD-Server ausgefallen ist. Wenn die Anmeldeinformationen (Benutzername und Kennwort) nicht übereinstimmen, wird eine Authentifizierungsanfrage an den AD-Server gestellt. Wenn die Authentifizierung erfolgreich ist, werden die Benutzerinformationen abgerufen und mit der lokalen Betreffliste abgeglichen. Der Zugriff wird verweigert, wenn die Authentifizierung fehlschlägt. Die Validierung anhand der Betreffliste ist erfolgreich, wenn sich der Benutzer oder eine Gruppe in der transitiven Gruppenzugehörigkeit des Benutzers in der Betreffliste befindet.

> **Hinweis:**
>
> Wenn Sie Active Directory-Gruppen verwenden, um Benutzern des Pool-Administrators Zugriff zu gewähren, die Host-SSH-Zugriff benötigen, darf die Größe der AD-Gruppe 500 Benutzer nicht überschreiten.

So fügen Sie XenServer ein AD-Betreff hinzu:

```
xe subject-add subject-name=entity_name
<!--NeedCopy-->
```

Der entity_name ist der Name des Benutzers oder der Gruppe, für die Sie Zugriff gewähren möchten. Sie können die Domäne der Entität einbeziehen (z. B. “xendt\ user1”im Gegensatz zu “Benutzer1”), obwohl das Verhalten dasselbe ist, sofern keine Begriffsklärung erforderlich ist.

Suchen Sie die Betreff-ID des Benutzers. Die Kennung ist der Benutzer oder die Gruppe, die den Benutzer enthält. Durch das Entfernen einer Gruppe wird der Zugriff für alle Benutzer in dieser Gruppe aufgehoben, sofern sie nicht auch in der Betreffliste angegeben sind. Verwenden Sie den `subject list` Befehl, um die Betreff-ID des Benutzers zu finden. :

```
xe subject-list
<!--NeedCopy-->
```

Dieser Befehl gibt eine Liste aller Benutzer zurück.

Um einen Filter auf die Liste anzuwenden, z. B. um die Betreff-ID für einen Benutzer `user1` in der `testad` Domäne zu finden, verwenden Sie den folgenden Befehl:

```
xe subject-list other-config:subject-name='testad\user1'
<!--NeedCopy-->
```

Entfernen Sie den Benutzer mithilfe des `subject-remove` Befehls und geben Sie die im vorherigen Schritt erlernte Fachkennung ein:

```
xe subject-remove subject-uuid=subject_uuid
<!--NeedCopy-->
```

Sie können jede aktuelle Sitzung beenden, die dieser Benutzer bereits authentifiziert hat. Weitere Informationen finden Sie unter *Beenden aller authentifizierten Sitzungen mit xe* und *Beenden einzelner Benutzersitzungen mit xe* im folgenden Abschnitt. Wenn Sie die Sitzungen nicht beenden, können Benutzer mit entzogenen Berechtigungen weiterhin auf das System zugreifen, bis sie sich abmelden.

Führen Sie den folgenden Befehl aus, um die Liste der Benutzer und Gruppen zu identifizieren, die berechtigt sind, auf Ihren XenServer-Host oder -Pool zuzugreifen:

```
xe subject-list
<!--NeedCopy-->
```


Zugriff für einen Benutzer aufheben

Wenn ein Benutzer authentifiziert ist, kann er auf den Host zugreifen, bis er seine Sitzung beendet oder ein anderer Benutzer seine Sitzung beendet. Wenn Sie einen Benutzer aus der Betreffliste entfernen oder ihn aus einer Gruppe in der Betreffliste entfernen, werden nicht automatisch alle bereits authentifizierten Sitzungen des Benutzers widerrufen. Benutzer können weiterhin mit XenCenter oder anderen API-Sitzungen, die sie bereits erstellt haben, auf den Pool zugreifen. XenCenter und die CLI bieten Möglichkeiten, einzelne Sitzungen oder alle aktiven Sitzungen mit Nachdruck zu beenden. In der XenCenter-Dokumentation finden Sie Informationen zu Verfahren mit XenCenter oder im folgenden Abschnitt finden Sie Verfahren zur Verwendung der CLI.

Beenden Sie alle authentifizierten Sitzungen mit xe

Führen Sie den folgenden CLI-Befehl aus, um alle authentifizierten Sitzungen mit xe zu beenden:

```
xe session-subject-identifier-logout-all
<!--NeedCopy-->
```

Beenden einzelner Benutzersitzungen mit xe

1. Bestimmen Sie den Betreff, dessen Sitzung Sie abmelden möchten. Verwenden Sie entweder die Befehle `session-subject-identifier-list` oder `subject-list` xe, um die Betreff-ID zu finden. Der erste Befehl zeigt Benutzer mit Sitzungen an. Der zweite Befehl zeigt alle Benutzer an, kann aber gefiltert werden. Zum Beispiel, indem Sie einen Befehl wie `xe subject-list other-config:subject-name=xendt\\user1` verwenden. Möglicherweise benötigen Sie einen doppelten Backslash (wie gezeigt, abhängig von Ihrer Shell).
2. Verwenden Sie den Befehl `session-subject-logout`, um die im vorherigen Schritt ermittelte Betreff-ID als Parameter zu übergeben, z. B.:

   ```
   xe session-subject-identifier-logout subject-identifier=subject_id
   <!--NeedCopy-->
   ```

Eine AD-Domäne verlassen

> **Warnung:**
>
> Wenn Sie die Domäne verlassen, werden alle Benutzer, die sich mit Active Directory-Anmeldeinformationen am Pool oder Host authentifiziert haben, getrennt.

Verwenden Sie XenCenter, um eine AD-Domäne zu verlassen. Weitere Informationen finden Sie in der XenCenter-Dokumentation. Führen Sie den alternativ Befehl `pool-disable-external-auth` aus und geben Sie bei Bedarf die Pool-UUID an.

> **Hinweis:**
>
> Beim Verlassen der Domäne werden die Host-Objekte nicht aus der AD-Datenbank gelöscht. In der Active Directory-Dokumentation finden Sie Informationen darüber, wie Sie Ihre deaktivierten Host-Einträge erkennen und entfernen können.

Rollenbasierte Zugriffssteuerung

September 19, 2023

Mit der Funktion Role-Based Access Control (RBAC) in XenServer können Sie Benutzer, Rollen und Berechtigungen zuweisen, um zu steuern, wer Zugriff auf Ihren XenServer hat und welche Aktionen sie ausführen können. Das XenServer RBAC-System ordnet einen Benutzer (oder eine Gruppe von Benutzern) definierten Rollen (einem benannten Satz von Berechtigungen) zu. Den Rollen sind XenServer-Berechtigungen zugeordnet, um bestimmte Vorgänge auszuführen.

Berechtigungen werden Benutzern nicht direkt zugewiesen. Benutzer erwerben Berechtigungen über Rollen, die ihnen zugewiesen sind. Bei der Verwaltung einzelner Benutzerberechtigungen muss daher der Benutzer der entsprechenden Rolle zugewiesen werden, was allgemeine Vorgänge vereinfacht. XenServer verwaltet eine Liste autorisierter Benutzer und ihrer Rollen.

Mit RBAC können Sie einschränken, welche Vorgänge verschiedene Benutzergruppen ausführen können, wodurch die Wahrscheinlichkeit eines Unfalls durch einen unerfahrenen Benutzer verringert wird.

RBAC bietet auch eine Überwachungsprotokollfunktion für Konformität und Überwachung.

RBAC hängt von Active Directory für Authentifizierungsdienste ab. Insbesondere führt XenServer eine Liste autorisierter Benutzer auf der Grundlage von Active Directory Directory-Benutzer- und Gruppenkonten. Daher müssen Sie den Pool der Domäne beitreten und Active Directory-Konten hinzufügen, bevor Sie Rollen zuweisen können.

Der lokale Superuser (LSU) oder root ist ein spezielles Benutzerkonto, das für die Systemadministration verwendet wird und über alle Rechte oder Berechtigungen verfügt. Der lokale Superuser ist das Standardkonto bei der Installation in XenServer. Die LSU wird über XenServer authentifiziert und nicht über einen externen Authentifizierungsdienst. Wenn der externe Authentifizierungsdienst ausfällt, kann sich die LSU trotzdem anmelden und das System verwalten. Die LSU kann jederzeit über SSH auf den physischen XenServer-Host zugreifen.

RBAC-Prozess

Im folgenden Abschnitt wird der Standardprozess für die Implementierung von RBAC und das Zuweisen einer Rolle für einen Benutzer oder eine Gruppe beschrieben:

1. Treten Sie der Domänebei. Weitere Informationen finden Sie unter Externe Authentifizierung für einen Pool aktivieren.
2. Fügen Sie dem Pool einen Active Directory-Benutzer oder eine Gruppe hinzu. Das wird ein Thema. Weitere Informationen finden Sie unter So fügen Sie einen Betreff zu RBAChinzu.
3. Weisen Sie die RBAC-Rolle des Subjekts zu (oder ändern) Sie Weitere Informationen finden Sie unter So weisen Sie einem Betreff eine RBAC-Rolle zu.

---

layout: doc
description: Learn about the different roles and permissions that can be assigned to your XenServer users.—

RBAC-Rollen und Berechtigungen

Rollen

XenServer wird mit den folgenden sechs vordefinierten Rollen ausgeliefert:

- *Pool-Administrator* (Pool Admin) —das gleiche wie das lokale Stammverzeichnis. Kann alle Vorgänge ausführen.

  > **Hinweis:**
  >
  > Der lokale Superuser (root) hat die Rolle "Pool Admin". Die Pool-Admin-Rolle hat dieselben Berechtigungen wie der lokale Stamm.
  >
  > Wenn Sie einem Benutzer die Pool-Admin-Rolle entziehen, sollten Sie auch das Root-Kennwort ändern und das Pool-Geheimnis rotieren lassen. Weitere Informationen finden Sie unter Pool-Sicherheit.

- *Pool Operator* (Pool Operator) —kann alles außer dem Hinzufügen/Entfernen von Benutzern und dem Ändern ihrer Rollen tun. Diese Rolle konzentriert sich hauptsächlich auf die Host- und Pool-Verwaltung (d. h. das Erstellen von Speicher, das Erstellen von Pools, das Verwalten der Hosts usw.).

- *Virtual Machine Power Administrator* (VM Power Admin) —erstellt und verwaltet virtuelle Maschinen. Diese Rolle konzentriert sich auf die Bereitstellung von VMs zur Verwendung durch einen VM-Betreiber.
- *Virtual Machine Administrator* (VM Admin) —ähnelt einem VM Power Admin, kann jedoch keine VMs migrieren oder Snapshots ausführen.
- *Virtual Machine Operator* (VM Operator) —ähnlich wie VM Admin, kann aber keine VMs erstellen/löschen —kann aber Lebenszyklusvorgänge starten/stoppen.
- *Schreibgeschützt (schreibgeschützt*) —kann Ressourcenpool- und Leistungsdaten anzeigen.

> **Hinweis:**
>
> - Um Updates auf XenServer 8-Pools anzuwenden, müssen Sie als Pooladministrator oder Pool-Operator oder mit einem lokalen Root-Konto bei XenCenter angemeldet sein.
> - Wenn Sie Active Directory-Gruppen verwenden, um Pooladministrator-Benutzern, die Host-SSH-Zugriff benötigen, Zugriff zu gewähren, darf die Anzahl der Benutzer in der Active Directory-Gruppe 500 nicht überschreiten.

Eine Zusammenfassung der für jede Rolle verfügbaren Berechtigungen und Informationen zu den für jede Berechtigung verfügbaren Vorgängen finden Sie unter *Definitionen von RBAC-Rollen und Berechtigungen* im folgenden Abschnitt.

Wenn Sie einen Benutzer in XenServer erstellen, müssen Sie dem neu erstellten Benutzer zunächst eine Rolle zuweisen, bevor er das Konto verwenden kann. XenServer **weist dem neu erstellten Benutzer nicht** automatisch eine Rolle zu. Daher haben diese Konten keinen Zugriff auf den XenServer-Pool, bis Sie ihnen eine Rolle zuweisen.

1. Ändern Sie das Thema der Rollenzuordnung. Dies erfordert die Berechtigung zum Zuweisen/Ändern der Rolle, die nur einem Pool-Administrator zur Verfügung steht.
2. Ändern Sie die Gruppenmitgliedschaft des Benutzers in Active Directory.

Definitionen von RBAC-Rollen und Berechtigungen

In der folgenden Tabelle wird zusammengefasst, welche Berechtigungen für jede Rolle verfügbar sind. Einzelheiten zu den für jede Berechtigung verfügbaren Vorgängen finden Sie unter *Definitionen von Berechtigungen*.

Rollen-Berechtigungen	Pooladministrator	Poolbetreiber	VM Power Admin	VM-Admin	VM-Betreiber	Lesezugriff
Rollen zuweisen/ändern	X					
Melden Sie sich bei (physischen) Serverkonsolen an (über SSH und XenCenter)	X					
Serverbackup/wiederherstellung	X					
Import/Export von OVF/OVA-Paketen und Disk-Images	X					
Kerne pro Sockel festlegen	X	X	X	X		
Virtuelle Maschinen mit XenServer Conversion Manager konvertieren	X					
Switch-Port-Verriegelung	X	X				
Multipathing	X	X				

Rollen-Berechtigungen	Pooladministrator	Poolbetreiber	VM Power Admin	VM-Admin	VM-Betreiber	Lesezugriff
Aktive Benutzerverbindungen abmelden	X	X				
Überwachen Sie Host- und Dom0-Ressourcen mit NRPE	X					
Überwachen Sie Host- und Dom0-Ressourcen mit SNMP	X					
Benachrichtigungen erstellen und verwerfen	X	X				
Aufgabe eines Benutzers abbrechen	X	X				
Poolmanagement	X	X				
Livemigration	X	X	X			
Live-Speichermigration	X	X	X			
Erweiterte VM-Vorgänge	X	X	X			
VM Erstellen/Löschen von Vorgängen	X	X	X	X		
VM ändern CD-Medien	X	X	X	X	X	

Rollen-Berechtigungen	Pooladministrator	Poolbetreiber	VM Power Admin	VM-Admin	VM-Betreiber	Lesezugriff
VM-Energiezustand ändern	X	X	X	X	X	
VM-Konsolen anzeigen	X	X	X	X	X	
XenCenter Ansichtsverwaltungsvorgänge	X	X	X	X	X	
Eigene Aufgaben abbrechen	X	X	X	X	X	X
Auditprotokolle lesen	X	X	X	X	X	X
Verbindung mit Pool herstellen und alle Poolmetadaten lesen	X	X	X	X	X	X
Konfigurieren der virtuellen GPU	X	X				
Virtuelle GPU-Konfiguration anzeigen	X	X	X	X	X	X
Zugriff auf das Konfigurationslaufwerk (nur CoreOS-VMs)	X					

Rollen-Berechtigungen	Pooladministrator	Poolbetreiber	VM Power Admin	VM-Admin	VM-Betreiber	Lesezugriff
Geplante Snapshots (Hinzufügen und Entfernen von VMs zu vorhandenen Snapshot-Zeitplänen)	X	X	X			
Geplante Snapshots (Snapshot-Zeitpläne hinzufügen/ändern/löschen)	X	X				
Sammeln von Diagnoseinformationen	X	X				
Geänderte Blockverfolgung konfigurieren	X	X	X	X		
Changed Blocks auflisten	X	X	X	X	X	
Konfigurieren von PVS-Accelerator	X	X				
PVS-Beschleunigerkonfiguration anzeigen	X	X	X	X	X	X

Definitionen von Berechtigungen

Rollen zuweisen/ändern:

- Benutzer hinzufügen/entfernen
- Rollen von Benutzern hinzufügen/entfernen
- Aktivieren und deaktivieren Sie die Active Directory-Integration (wird der Domäne hinzugefügt)

Mit dieser Berechtigung kann sich der Benutzer selbst eine Berechtigung erteilen oder eine Aufgabe ausführen.

Warnung: Mit dieser Rolle kann der Benutzer die Active Directory-Integration und alle aus Active Directory hinzugefügten Themen deaktivieren.

Bei Serverkonsolen anmelden:

- Zugriff auf die Serverkonsole über SSH
- Zugriff auf die Serverkonsole über XenCenter

Warnung: Mit Zugriff auf eine Root-Shell kann der Empfänger das gesamte System, einschließlich RBAC, beliebig neu konfigurieren.

Serverbackup/-wiederherstellung VM Erstellen/Löschen von virtuellen Rechnern:

- Backup und Wiederherstellen von Servern
- Backup und Wiederherstellen von Poolmetadaten

Durch die Möglichkeit, ein Backup wiederherzustellen, kann der Beauftragte Änderungen an der RBAC-Konfiguration rückgängig machen.

Import/Export von OVF/OVA-Paketen und Disk-Images:

- Import von OVF- und OVA-Paketen
- Importieren von Datenträgerimages
- Exportieren von VMs als OVF/OVA-Pakete

Kerne pro Sockel einstellen:

- Legen Sie die Anzahl der Kerne pro Socket für die virtuellen CPUs der VM fest

Mit dieser Berechtigung kann der Benutzer die Topologie für die virtuellen CPUs der VM angeben.

Konvertieren Sie VMs mit XenServer Conversion Manager:

- Konvertieren Sie VMware ESXi/vCenter-VMs in XenServer-VMs

Mit dieser Berechtigung kann der Benutzer Workloads von VMware nach XenServer konvertieren, indem er Stapel von VMware ESXi/vCenter-VMs in die XenServer-Umgebung kopiert.

Switch-Port-Verriegelung:

- Steuern Sie den Verkehr in einem Netzwerk

Mit dieser Berechtigung kann der Benutzer standardmäßig den gesamten Datenverkehr in einem Netzwerk blockieren oder bestimmte IP-Adressen definieren, von denen eine VM Datenverkehr senden darf.

Multipathing:

- Multipathing aktivieren
- Deaktivieren Sie Multipathing

Aktive Benutzerverbindungen abmelden:

- Möglichkeit, angemeldete Benutzer zu trennen

Warnungen erstellen/verwerfen:

- Konfigurieren Sie XenCenter so, dass Warnungen generiert werden, wenn die Ressourcenauslastung bestimmte Schwellenwerte überschreitet
- Warnmeldungen aus der Alerts-Ansicht entfernen

Warnung: Ein Benutzer mit dieser Berechtigung kann Warnungen für den gesamten Pool verwerfen.

Hinweis: Die Möglichkeit, Warnungen anzuzeigen, ist Teil der Berechtigung “Mit Pool verbinden”und alle Poolmetadaten lesen.

Aufgabe eines beliebigen Benutzers abbrechen:

- Die ausgeführte Aufgabe eines Benutzers abbrechen

Mit dieser Berechtigung kann der Benutzer beantragen, dass XenServer eine laufende Aufgabe storniert, die von einem beliebigen Benutzer initiiert wurde.

Pool-Verwaltung:

- Pool-Eigenschaften festlegen (Benennung, Standard-SRs)
- Erstellen eines Clusterpools
- Hochverfügbarkeit aktivieren, deaktivieren und konfigurieren
- Neustartprioritäten für Hochverfügbarkeit pro VM festlegen
- Konfigurieren Sie DR und führen Sie DR-Failover-, Failback- und Test-Failover-Vorgänge durch
- Aktivieren, Deaktivieren und Konfigurieren von Workload Balancing (WLB)
- Server zum Pool hinzufügen und daraus entfernen
- Notfallübergang zum Poolkoordinator
- Adresse des Notfallpoolkoordinators
- Notfall-Poolmitglieder
- Neuen Poolkoordinator benennen
- Pool- und Host-Zertifikate verwalten

- Patchen
- Host-Eigenschaften festlegen
- Host-Logging konfigurieren
- Server aktivieren und deaktivieren
- Server herunterfahren, neu starten und einschalten
- Starten Sie toolstack neu
- Berichte über den Systemstatus
- Lizenz anwenden
- Live-Migration aller anderen VMs auf einem Host auf einen anderen Host aufgrund des Wartungsmodus oder der Hochverfügbarkeit
- Host-Management-Schnittstelle und sekundäre Schnittstellen konfigurieren
- Host-Verwaltung deaktivieren
- Crashdumps löschen
- Netzwerke hinzufügen, bearbeiten und entfernen
- Hinzufügen, Bearbeiten und Entfernen von PBDS/PIFS/VLANs/Bonds/SRs
- Secrets hinzufügen, entfernen und abrufen

Diese Berechtigung umfasst alle Aktionen, die zur Verwaltung eines Pools erforderlich sind.

Hinweis: Wenn die Verwaltungsschnittstelle nicht funktioniert, können sich keine Anmeldungen außer lokalen Root-Anmeldungen authentifizieren.

Livemigration:

- Migrieren Sie VMs von einem Host auf einen anderen Host, wenn sich die VMs auf einem von beiden Hosts gemeinsam genutzten Speicher befinden

Speicher-Livemigration:

- Migration von einem Host zu einem anderen Host, wenn sich die VMs nicht auf einem von den beiden Hosts gemeinsam genutzten Speicher befinden
- Verschieben von Virtual Disk (VDIs) von einem SR zu einem anderen SR

Erweiterter VM-Betrieb:

- VM-Speicher anpassen (über Dynamic Memory Control)
- Erstellen eines VM-Snapshots mit Arbeitsspeicher, Erstellung von VM-Snapshots und Rollback von VMs
- VMs migrieren
- Starten von VMs, einschließlich Angabe des physischen Servers
- VMs fortsetzen

Diese Berechtigung bietet dem Beauftragten genügend Rechte, um eine VM auf einem anderen Host zu starten, wenn er mit dem ausgewählten Host XenServer nicht zufrieden ist.

VM-Erstellen/Löschen von Vorgängen:

- Installieren oder löschen
- VMs klonen/kopieren
- Hinzufügen, Entfernen und Konfigurieren von virtuellen Laufplatten/CD-Geräten
- Hinzufügen, Entfernen und Konfigurieren virtueller Netzwerkgeräte
- XVA-Dateien importieren/exportieren
- Änderung der VM-Konfiguration
- Serverbackup/-wiederherstellung

> **Hinweis:**
>
> Die VM-Admin-Rolle kann XVA-Dateien nur in einen Pool mit einem gemeinsam genutzten SR importieren. Die VM-Admin-Rolle verfügt nicht über unzureichende Berechtigungen, um eine XVA-Datei in einen Host oder in einen Pool ohne gemeinsam genutzten Speicher zu importieren.

VM CD-Medien wechseln:

- Aktuelle CD auswerfen
- Neue CD einlegen

Import/Export von OVF/OVA-Paketen; Import von Datenträgerimages

VM ändert den Energiezustand:

- VMs starten (automatische Platzierung)
- VMs herunterfahren
- Starten Sie VMs neu
- VMs aussetzen
- VMs fortsetzen (automatische Platzierung)

Diese Berechtigung umfasst nicht start_on, resume_on und migrate, die Teil der Berechtigung für erweiterte VM-Vorgänge sind.

VM-Konsolen anzeigen:

- VM-Konsolen sehen und mit ihnen interagieren

Mit dieser Berechtigung kann der Benutzer Hostkonsolen nicht anzeigen.

XenCenter View-Verwaltungsvorgänge:

- Erstellen und Ändern globaler XenCenter-Ordner
- Erstellen und Ändern globaler benutzerdefinierter XenCenter-Felder
- Erstellen und Ändern globaler XenCenter-Suchen

Ordner, benutzerdefinierte Felder und Suchen werden von allen Benutzern geteilt, die auf den Pool zugreifen

Stornieren eigener Aufgaben:

- Ermöglicht es einem Benutzer, seine eigenen Aufgaben abzubrechen

Prüfprotokoll lesen:

- Laden Sie das XenServer-Auditprotokoll herunter

Verbinden Sie sich mit Pool und lesen Sie alle Poolmetadaten:

- Melden Sie sich bei Pool an
- Poolmetadaten anzeigen
- Historische Leistungsdaten anzeigen
- Eingeloggte Benutzer anzeigen
- Benutzer und Rollen anzeigen
- Nachrichten ansehen
- Registrieren und Ereignisse erhalten

Konfigurieren der virtuellen GPU:

- Angeben einer poolweiten Platzierungsrichtlinie
- Weisen Sie einer VM eine virtuelle GPU zu
- Entfernen einer virtuellen GPU von einer VM
- Zulässige virtuelle GPU-Typen ändern
- GPU-Gruppe erstellen, zerstören oder zuweisen

Virtuelle GPU-Konfiguration anzeigen:

- GPUs, GPU-Platzierungsrichtlinien und virtuelle GPU-Zuweisungen anzeigen

Geplante Snapshots:

- VMs zu vorhandenen Snapshot-Zeitplänen hinzufügen
- VMs aus vorhandenen Snapshot-Zeitplänen entfernen
- Snapshot-Zeitpläne hinzufügen
- Snapshot-Zeitpläne ändern
- Snapshot-Zeitpläne löschen

Sammeln Sie Diagnoseinformationen von XenServer:

- GC-Sammlung und Heap-Verdichtung einleiten
- Sammeln von Statistiken zur Müllsammlung
- Sammeln von Datenbankstatistiken

- Netzwerkstatistiken sammeln

Geändertes Block-Tracking konfigurieren:

- Geänderte Blockverfolgung aktivieren
- Geänderte Blockverfolgung deaktivieren
- Löschen Sie die mit einem Snapshot verknüpften Daten und behalten Sie die Metadaten bei
- Abrufen der NBD-Verbindungsinformationen für einen VDI

Die geänderte Blockverfolgung kann nur für lizenzierte Instanzen der XenServer Premium Edition aktiviert werden.

Geänderte Blöcke auflisten:

- Vergleichen Sie zwei VDI-Snapshots und listen Sie die Blöcke auf, die sich zwischen ihnen geändert haben

Konfigurieren des PVS-Beschleunigers:

- PVS-Beschleuniger aktivieren
- PVS-Accelerator deaktivieren
- Cache-Konfiguration aktualisieren (PVS-Accelerator)
- Cache-Konfiguration hinzufügen/entfernen (PVS-Accelerator)

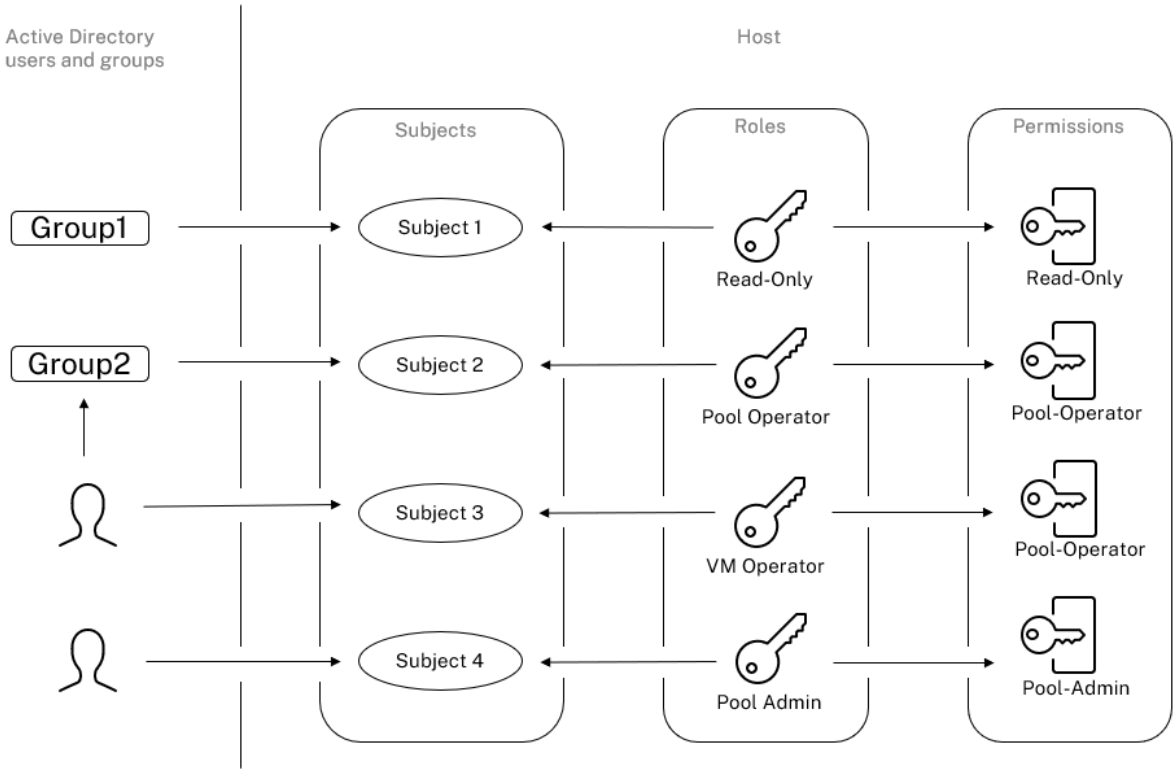
PVS-Accelerator-Konfiguration anzeigen:

- Status von PVS-Accelerator anzeigen

> **Hinweis:**
>
> Manchmal kann ein schreibgeschützter Benutzer eine Ressource nicht in einen Ordner in XenCenter verschieben, selbst nachdem er eine Eingabeaufforderung mit erhöhten Rechten erhalten und die Anmeldeinformationen eines privilegierteren Benutzers angegeben hat. In diesem Fall melden Sie sich als privilegierterer Benutzer bei XenCenter an und versuchen Sie die Aktion erneut.

Wie berechnet XenServer die Rollen für die Sitzung?

1. Der Antragsteller wird über den Active Directory-Server authentifiziert, um zu überprüfen, zu welchen Gruppen der Betreff auch gehören kann.
2. XenServer überprüft dann, welche Rollen sowohl dem Betreff als auch den zugehörigen Gruppen zugewiesen wurden.
3. Da Subjekte Mitglieder mehrerer Active Directory-Gruppen sein können, erben sie alle Berechtigungen der zugehörigen Rollen.



Verwenden Sie RBAC mit der CLI

September 19, 2023

RBAC xe CLI-Befehle

Verwenden Sie die folgenden Befehle, um mit Rollen und Themen zu arbeiten.

So listen Sie alle verfügbaren definierten Rollen auf

Führen Sie den Befehl `xe role-list` aus.

Dieser Befehl gibt eine Liste der aktuell definierten Rollen zurück, zum Beispiel:

```
1     uuid( RO): 0165f154-ba3e-034e-6b27-5d271af109ba
2     name ( RO): pool-admin
3     description ( RO): The Pool Administrator role has full access to
         all
4     features and settings, including accessing Dom0 and managing
         subjects,
```



```
5       roles and external authentication
6
7       uuid ( RO): b9ce9791-0604-50cd-0649-09b3284c7dfd
8       name ( RO): pool-operator
9       description ( RO): The Pool Operator role manages host-  and pool-
           wide resources,
10      including setting up storage, creating resource pools and managing
           patches, and
11      high availability (HA).
12
13      uuid( RO): 7955168d-7bec-10ed-105f-c6a7e6e63249
14      name ( RO): vm-power-admin
15      description ( RO): The VM Power Administrator role has full access
           to VM and
16      template management and can choose where to start VMs and use the
           dynamic memory
17      control and VM snapshot features
18
19      uuid ( RO): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
20      name ( RO): vm-admin
21      description ( RO):  The VM Administrator role can manage VMs and
           templates
22
23      uuid ( RO): fb8d4ff9-310c-a959-0613-54101535d3d5
24      name ( RO): vm-operator
25      description ( RO):  The VM Operator role can use VMs and interact
           with VM consoles
26
27      uuid ( RO): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
28      name ( RO): read-only
29      description ( RO): The Read-Only role can log in with basic read-
           only access
30  <!--NeedCopy-->
```

> **Hinweis:**
>
> Diese Liste von Rollen ist statisch. Sie können keine Rollen hinzufügen, entfernen oder ändern.

So zeigen Sie eine Liste der aktuellen Themen an

Führen Sie den folgenden Befehl aus:

```
1  xe subject-list
2  <!--NeedCopy-->
```

Dieser Befehl gibt eine Liste der XenServer-Benutzer, ihrer UUID und der Rollen zurück, denen sie zugeordnet sind:

```
1       uuid ( RO): bb6dd239-1fa9-a06b-a497-3be28b8dca44
2       subject-identifier ( RO): S
           -1-5-21-1539997073-1618981536-2562117463-2244
```



```
    other-config (MRO): subject-name: example01\user_vm_admin; subject-upn: \
      user_vm_admin@XENDT.NET; subject-uid: 1823475908; subject-gid: 1823474177; \
      subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2244; subject-gecos: \
      user_vm_admin; subject-displayname: user_vm_admin; subject-is-group: false; \
      subject-account-disabled: false; subject-account-expired: false; \
      subject-account-locked: false;subject-password-expired: false
    roles (SRO): vm-admin

    uuid ( RO): 4fe89a50-6a1a-d9dd-afb9-b554cd00c01a
    subject-identifier ( RO): S-1-5-21-1539997073-1618981536-2562117463-2245
    other-config (MRO): subject-name: example02\user_vm_op; subject-upn: \
      user_vm_op@XENDT.NET; subject-uid: 1823475909; subject-gid: 1823474177; \
      subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2245; \
      subject-gecos: user_vm_op; subject-displayname: user_vm_op; \
      subject-is-group: false; subject-account-disabled: false; \
      subject-account-expired: false; subject-account-locked: \
      false; subject-password-expired: false
    roles (SRO): vm-operator

    uuid ( RO): 8a63fbf0-9ef4-4fef-b4a5-b42984c27267
    subject-identifier ( RO): S-1-5-21-1539997073-1618981536-2562117463-2242
    other-config (MRO): subject-name: example03\user_pool_op; \
      subject-upn: user_pool_op@XENDT.NET; subject-uid: 1823475906; \
      subject-gid: 1823474177; subject-s id:
      S-1-5-21-1539997073-1618981536-2562117463-2242; \
      subject-gecos: user_pool_op; subject-displayname: user_pool_op; \
      subject-is-group: false; subject-account-disabled: false; \
      subject-account-expired: false; subject-account-locked: \
      false; subject-password-expired: false
      roles (SRO): pool-operator
<!--NeedCopy-->
```

So fügen Sie einen Betreff zu RBAC hinzu

Um vorhandenen AD-Benutzern die Verwendung von RBAC zu ermöglichen, erstellen Sie eine Betreffinstanz in XenServer, entweder direkt für den AD-Benutzer oder für die enthaltenen Gruppen:

Führen Sie den folgenden Befehl aus, um eine neue Betreffinstanz hinzuzufügen:

```
xe subject-add subject-name=AD user/group
<!--NeedCopy-->
```


So weisen Sie einem Betreff eine RBAC-Rolle zu

Nachdem Sie einen Betreff hinzugefügt haben, können Sie ihn einer RBAC-Rolle zuweisen. Sie können entweder mit ihrer UUID oder ihrem Namen auf die Rolle verweisen:

Führen Sie den Befehl aus:

```
xe subject-role-add uuid=subject uuid role-uuid=role_uuid
<!--NeedCopy-->
```

Oder

```
xe subject-role-add uuid=subject uuid role-name=role_name
<!--NeedCopy-->
```

Mit dem folgenden Befehl wird beispielsweise der Pooladministrator-Rolle ein Betreff mit der UUID `b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4` hinzugefügt:

```
xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name
   =pool-admin
<!--NeedCopy-->
```

So ändern Sie die RBAC-Rolle eines Subjekts

Um die Rolle eines Benutzers zu ändern, müssen Sie ihn aus seiner vorhandenen Rolle entfernen und zu einer neuen Rolle hinzufügen:

Führen Sie die folgenden Befehle aus:

```
xe subject-role-remove uuid=subject_uuid role-name=role_name_to_remove
xe subject-role-add uuid=subject_uuid role-name=role_name_to_add
<!--NeedCopy-->
```

Der Benutzer muss sich abmelden und wieder anmelden, um sicherzustellen, dass die neue Rolle wirksam wird. Dazu ist die Berechtigung „Aktive Benutzerverbindungen abmelden“erforderlich, die einem Pooladministrator oder Poolbetreiber zur Verfügung steht.

Wenn Sie einem Benutzer die Pool-Admin-Rolle entziehen, sollten Sie auch das Root-Passwort ändern und das Pool-Geheimnis rotieren lassen. Weitere Informationen finden Sie unter Pool-Sicherheit.

> **Warnung:**
>
> Wenn Sie einen Pool-Admin-Betreff hinzufügen oder entfernen, kann es einige Sekunden dauern, bis alle Hosts im Pool SSH-Sitzungen akzeptieren, die mit diesem Thema verknüpft sind.

Auditing

Das RBAC-Überwachungsprotokoll zeichnet jeden Vorgang auf, der von einem angemeldeten Benutzer ausgeführt wurde.

- Die Nachricht zeichnet die Betreff-ID und den Benutzernamen auf, die mit der Sitzung verknüpft sind, die den Vorgang aufgerufen hat.
- Wenn ein Betreff einen Vorgang aufruft, der nicht autorisiert ist, wird der Vorgang protokolliert.
- Jeder erfolgreiche Vorgang wird ebenfalls aufgezeichnet. Wenn der Vorgang fehlgeschlagen ist, wird der Fehlercode protokolliert.

Überwachungsprotokoll xe CLI-Befehle

Mit dem folgenden Befehl werden alle verfügbaren Datensätze der RBAC-Überwachungsdatei im Pool in eine Datei heruntergeladen. Wenn der optionale Parameter ‘seit’vorhanden ist, werden nur die Datensätze von diesem bestimmten Zeitpunkt heruntergeladen.

```
xe audit-log-get [since=timestamp] filename=output filename
<!--NeedCopy-->
```

So rufen Sie alle Prüfaufzeichnungen aus dem Pool ab

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

Um Prüfaufzeichnungen des Pools seit einem genauen Millisekunden-Zeitstempel zu erhalten

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z \
    filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

Um Prüfaufzeichnungen des Pools seit einem genauen Minutenzeitstempel zu erhalten

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get since=2009-09-24T17:56Z \
    filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```


layout: doc
description: Understand the concepts involved in XenServer networking, including networks, VLANs, and NIC bonds.—

Netzwerke

Dieser Abschnitt bietet einen Überblick über XenServer-Netzwerke, einschließlich Netzwerke, VLANs und NIC-Verbindungen. Außerdem wird erläutert, wie Sie Ihre Netzwerkkonfiguration verwalten und Fehler beheben können.

> **Wichtig:**
>
> vSwitch ist der Standard-Netzwerkstack von XenServer. Befolgen Sie die Anweisungen in vSwitch-Netzwerken, um den Linux-Netzwerkstapel zu konfigurieren.

Wenn Sie bereits mit den Netzwerkkonzepten von XenServer vertraut sind, können Sie mit Netzwerkverwaltung weitermachen, um Informationen zu den folgenden Abschnitten zu erhalten:

- Netzwerke für eigenständige XenServer-Hosts erstellen
- Erstellen Sie Netzwerke für XenServer-Hosts, die in einem Ressourcenpool konfiguriert sind
- Erstellen Sie VLANs für XenServer-Hosts, entweder eigenständig oder als Teil eines Ressourcenpools
- Bindungen für eigenständige XenServer-Hosts erstellen
- Erstellen Sie Bindungen für XenServer-Hosts, die in einem Ressourcenpool konfiguriert sind

> **Hinweis:**
>
> Der Begriff “Verwaltungsschnittstelle”wird verwendet, um die IP-fähige Netzwerkkarte zu bezeichnen, die den Verwaltungsverkehr überträgt. Der Begriff “sekundäre Schnittstelle”wird verwendet, um eine IP-fähige Netzwerkkarte anzugeben, die für den Speicherverkehr konfiguriert ist.

Unterstützung von Netzwerken

XenServer unterstützt bis zu 16 physische Netzwerkschnittstellen (oder bis zu 4 verbundene Netzwerkschnittstellen) pro Host und bis zu 7 virtuelle Netzwerkschnittstellen pro VM.

> **Hinweis:**
>
> XenServer ermöglicht die automatisierte Konfiguration und Verwaltung von NICs mithilfe der XE-Befehlszeilenschnittstelle (CLI). Bearbeiten Sie die Host-Netzwerkkonfigurationsdateien nicht direkt.

vSwitch-Netzwerke

vSwitch-Netzwerke unterstützen Open Flow.

- Unterstützt feinkörnige Sicherheitsrichtlinien zur Steuerung des Datenverkehrs, der zu und von einer VM gesendet wird.
- Bietet einen detaillierten Überblick über das Verhalten und die Leistung des gesamten Datenverkehrs, der in der virtuellen Netzwerkumgebung gesendet wird.

Ein vSwitch vereinfacht die IT-Verwaltung in virtualisierten Netzwerkumgebungen erheblich. Alle VM-Konfigurationen und Statistiken bleiben an die VM gebunden, auch wenn die VM von einem physischen Host im Ressourcenpool zu einem anderen migriert.

Führen Sie den folgenden Befehl aus, um festzustellen, welcher Netzwerkstapel konfiguriert ist:

```
xe host-list params=software-version
<!--NeedCopy-->
```

Suchen Sie in der Befehlsausgabe nach `network_backend`. Wenn der vSwitch als Netzwerkstapel konfiguriert ist, wird die Ausgabe wie folgt angezeigt:

```
network_backend: openvswitch
<!--NeedCopy-->
```

Wenn die Linux-Brücke als Netzwerkstapel konfiguriert ist, wird die Ausgabe wie folgt angezeigt:

```
network_backend: bridge
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um zum Linux-Netzwerkstapel zurückzukehren:

```
xe-switch-network-backend bridge
<!--NeedCopy-->
```

Starten Sie Ihren Host nach Ausführung dieses Befehls neu.

Überblick über das XenServer-Netzwerk

In diesem Abschnitt werden die allgemeinen Netzwerkkonzepte in der XenServer-Umgebung beschrieben.

XenServer erstellt während der Installation ein Netzwerk für jede physische Netzwerkkarte. Wenn Sie einem Pool einen Host hinzufügen, werden die Standardnetzwerke zusammengeführt. Dadurch wird sichergestellt, dass alle physischen Netzwerkkarten mit demselben Gerätenamen an dasselbe Netzwerk angeschlossen sind.

In der Regel fügen Sie ein Netzwerk hinzu, um ein internes Netzwerk zu erstellen, ein neues VLAN mit einer vorhandenen Netzwerkkarte einzurichten oder eine NIC-Bindung zu erstellen.

Sie können in XenServer vier verschiedene Netzwerktypen konfigurieren:

- **Externe Netzwerke** haben eine Zuordnung zu einer physikalischen Netzwerkschnittstelle. Externe Netzwerke bilden eine Brücke zwischen einer virtuellen Maschine und der mit dem Netzwerk verbundenen physischen Netzwerkschnittstelle. Externe Netzwerke ermöglichen es einer virtuellen Maschine, eine Verbindung zu Ressourcen herzustellen, die über die physische Netzwerkkarte des Hosts verfügbar sind.
- **Gebundene Netzwerke** stellen eine Verbindung zwischen zwei oder mehr NICs her, um einen einzigen, leistungsstarken Kanal zwischen der virtuellen Maschine und dem Netzwerk zu schaffen.
- **Private Einzelserver Netzwerke** haben keine Zuordnung zu einer physikalischen Netzwerkschnittstelle. Private Netzwerke mit einem Server können verwendet werden, um Konnektivität zwischen den virtuellen Maschinen auf einem bestimmten Host ohne Verbindung zur Außenwelt bereitzustellen.

> **Hinweis:**
>
> Einige Netzwerkoptionen verhalten sich bei Verwendung mit eigenständigen XenServer-Hosts anders als bei Ressourcenpools. Dieser Abschnitt enthält Abschnitte zu allgemeinen Informationen, die sowohl für eigenständige Hosts als auch für Pools gelten, gefolgt von spezifischen Informationen und Verfahren für jeden.

Netzwerk-Objekte

In diesem Abschnitt werden drei Arten von serverseitigen Softwareobjekten verwendet, um Netzwerkeinheiten darzustellen. Diese Objekte sind:

- Ein *PIF*, der eine physische Netzwerkkarte auf einem Host darstellt. PIF-Objekte haben einen Namen und eine Beschreibung, eine UUID, die Parameter der NIC, die sie repräsentieren, sowie das Netzwerk und den Host, mit dem sie verbunden sind.
- Ein *VIF*, das eine virtuelle Netzwerkkarte auf einer virtuellen Maschine darstellt. VIF-Objekte haben einen Namen und eine Beschreibung, eine UUID sowie das Netzwerk und die VM, mit der sie verbunden sind.

- Ein *Netzwerk*, bei dem es sich um einen virtuellen Ethernet-Switch auf einem Host handelt. Netzwerkobjekte haben einen Namen und eine Beschreibung, eine UUID und die Sammlung von VIFs und PIFs, die mit ihnen verbunden sind.

XenCenter und die xe CLI ermöglichen Ihnen die Konfiguration von Netzwerkoptionen. Sie können die für Verwaltungsvorgänge verwendete Netzwerkkarte steuern und erweiterte Netzwerkfunktionen wie VLANs und NIC-Bonds erstellen.

Netzwerke

Jeder XenServer-Host verfügt über ein oder mehrere Netzwerke, bei denen es sich um virtuelle Ethernet-Switches handelt. Netzwerke, die nicht mit einem PIF verknüpft sind, werden als *intern*betrachtet. Interne Netzwerke können verwendet werden, um nur Konnektivität zwischen VMs auf einem bestimmten XenServer-Host ohne Verbindung zur Außenwelt bereitzustellen. Mit einem PIF verknüpfte Netzwerke werden als *extern*betrachtet. Externe Netzwerke bieten eine Brücke zwischen VIFs und dem mit dem Netzwerk verbundenen PIF und ermöglichen die Konnektivität zu Ressourcen, die über die NIC des PIF verfügbar sind.

VLANs

VLANs, wie im IEEE 802.1Q-Standard definiert, ermöglichen es einem einzelnen physischen Netzwerk, mehrere logische Netzwerke zu unterstützen. XenServer-Hosts unterstützen VLANs auf verschiedene Weise.

> **Hinweis:**
>
> - Wir empfehlen, GFS2 SR nicht mit einem VLAN zu verwenden, da ein bekanntes Problem besteht, bei dem Sie Hosts in einem Clusterpool nicht hinzufügen oder entfernen können, wenn sich das Clusternetzwerk in einem Nicht-Management-VLAN befindet.
> - Alle unterstützten VLAN-Konfigurationen gelten gleichermaßen für Pools und eigenständige Hosts sowie für gebundene und nicht gebundene Konfigurationen.

Verwenden von VLANs mit virtuellen Maschinen Switch-Ports, die als 802.1Q-VLAN-Trunk-Ports konfiguriert sind, können mit den XenServer-VLAN-Funktionen verwendet werden, um virtuelle Gastnetzwerkschnittstellen (VIFs) mit bestimmten VLANs zu verbinden. In diesem Fall führt der XenServer-Host die VLAN-Tagging/Untagging-Funktionen für den Gast aus, der keine VLAN-Konfiguration kennt.

XenServer-VLANs werden durch zusätzliche PIF-Objekte dargestellt, die VLAN-Schnittstellen darstellen, die einem angegebenen VLAN-Tag entsprechen. Sie können XenServer-Netzwerke mit dem PIF verbinden, der die physische Netzwerkkarte darstellt, um den gesamten Datenverkehr

auf der Netzwerkkarte zu sehen. Verbinden Sie alternativ Netzwerke mit einem PIF, der ein VLAN darstellt, um nur den Datenverkehr mit dem angegebenen VLAN-Tag zu sehen. Sie können ein Netzwerk auch so verbinden, dass es nur den nativen VLAN-Verkehr sieht, indem Sie es an VLAN 0 anhängen.

Verfahren zum Erstellen von VLANs für XenServer-Hosts, entweder eigenständig oder Teil eines Ressourcenpools, finden Sie unter VLANs erstellen.

Wenn Sie möchten, dass der Gast die VLAN-Tagging- und Untagging-Funktionen ausführt, muss der Gast die VLANs kennen. Wenn Sie das Netzwerk für Ihre VMs konfigurieren, konfigurieren Sie die Switch-Ports als VLAN-Trunk-Ports, erstellen Sie jedoch keine VLANs für den XenServer-Host. Verwenden Sie stattdessen VIFs in einem normalen Nicht-VLAN-Netzwerk.

Verwenden von VLANs mit Verwaltungsschnittstellen Die Verwaltungsschnittstelle kann in einem VLAN mithilfe eines Switch-Ports konfiguriert werden, der als Trunk-Port oder Zugriffsmodus Port konfiguriert ist. Verwenden Sie XenCenter oder xe CLI, um ein VLAN einzurichten und es zur Verwaltungsschnittstelle zu machen. Weitere Informationen finden Sie unter Verwaltungsschnittstelle.

Verwenden von VLANs mit dedizierten Speicher-NICs Dedizierte Speicher-NICs können für die Verwendung nativer VLAN- oder Zugriffsmode-Ports konfiguriert werden, wie im vorherigen Abschnitt für Verwaltungsschnittstellen beschrieben. Dedizierte Speicher-NICs werden auch als IP-fähige NICs oder sekundäre Schnittstellen bezeichnet. Sie können dedizierte Speicher-NICs für die Verwendung von Trunk-Ports und XenServer-VLANs konfigurieren, wie im vorherigen Abschnitt für virtuelle Maschinen beschrieben. Weitere Informationen finden Sie unter Konfigurieren einer dedizierten Speicher-NIC.

Kombinieren von Verwaltungsschnittstellen und Gast-VLANs auf einer einzigen Host-NIC Ein einzelner Switch-Port kann sowohl mit Trunk als auch mit nativen VLANs konfiguriert werden, sodass eine Host-NIC für eine Verwaltungsschnittstelle (im nativen VLAN) und zum Verbinden von Gast-VIFs mit bestimmten VLAN-IDs verwendet werden kann.

Jumbo-Rahmen

Jumbo-Frames können verwendet werden, um die Leistung des Datenverkehrs in Speichernetzwerken und VM-Netzwerken zu optimieren. Jumbo-Frames sind Ethernet-Frames mit mehr als 1.500 Byte Nutzlast. Jumbo-Frames werden in der Regel verwendet, um einen besseren Durchsatz zu erzielen, die Belastung des Systembusspeichers zu reduzieren und den CPU-Overhead zu reduzieren.

> **Hinweis:**
>
> XenServer unterstützt Jumbo Frames nur, wenn vSwitch als Netzwerkstack auf allen Hosts im Pool verwendet wird.

Anforderungen für die Verwendung von Jumbo-Frames Beachten Sie bei der Verwendung von Jumbo-Frames Folgendes:

- Jumbo-Frames werden auf Poolebene konfiguriert
- vSwitch muss als Netzwerk-Backend auf allen Hosts im Pool konfiguriert werden
- Jedes Gerät im Subnetz muss für die Verwendung von Jumbo-Frames konfiguriert sein
- Das Aktivieren von Jumbo-Frames im Verwaltungsnetzwerk wird nicht unterstützt

Um Jumbo-Frames zu verwenden, stellen Sie die Maximum Transmission Unit (MTU) auf einen Wert zwischen 1500 und 9216 ein. Sie können XenCenter oder die xe CLI verwenden, um die MTU festzulegen.

NIC-Bindungen

NIC-Bonds, manchmal auch als NIC-Teaming bezeichnet, verbessern die Resilienz und Bandbreite von XenServer-Hosts, indem sie es Administratoren ermöglichen, zwei oder mehr NICs zusammen zu konfigurieren. NIC-Bonds funktionieren logischerweise als eine Netzwerkkarte und alle gebundenen NICs teilen sich eine MAC-Adresse.

Wenn eine Netzwerkkarte in der Bindung ausfällt, wird der Netzwerkverkehr des Hosts automatisch über die zweite Netzwerkkarte umgeleitet. XenServer unterstützt bis zu acht verbundene Netzwerke.

XenServer unterstützt Aktiv-Aktiv-, Aktiv-Passiv- und LACP-Bonding-Modi. Die Anzahl der unterstützten NICs und der unterstützte Bonding-Modus variieren je nach Netzwerkstapel:

- LACP-Bonding ist nur für den vSwitch verfügbar, wohingegen aktiv-aktiv und aktiv-passiv sowohl für den vSwitch als auch für die Linux-Bridge verfügbar sind.
- Wenn der vSwitch der Netzwerkstapel ist, können Sie entweder zwei, drei oder vier Netzwerkkarten verbinden.
- Wenn die Linux-Brücke der Netzwerkstapel ist, können Sie nur zwei Netzwerkkarten verbinden.

Alle Bonding-Modi unterstützen Failover. Nicht in allen Modi können jedoch alle Links für alle Verkehrstypen aktiv sein. XenServer unterstützt das Zusammenfügen der folgenden Arten von NICs:

- **NICs (nicht verwaltet)**. Sie können NICs verbinden, die XenServer ausschließlich für den VM-Verkehr verwendet. Das Verbinden dieser Netzwerkkarten sorgt nicht nur für Stabilität, sondern gleicht dadurch auch den Datenverkehr von mehreren virtuellen Rechnern zwischen den NICs aus.
- **Management-Schnittstellen**. Sie können eine Verwaltungsschnittstelle an eine andere Netzwerkkarte binden, sodass die zweite Netzwerkkarte ein Failover für den Verwaltungsdatenverkehr bietet. Die Konfiguration einer LACP-Link-Aggregations-Bindung bietet zwar einen Lastenausgleich für den Verwaltungsdatenverkehr, Active-Active-NIC-Bonding jedoch nicht. Sie können ein VLAN auf gebundenen NICs erstellen, und die Host-Management-Schnittstelle kann diesem VLAN zugewiesen werden.
- **Sekundäre Schnittstellen**. Sie können NICs binden, die Sie als sekundäre Schnittstellen konfiguriert haben (z. B. für Speicher). Für die meisten iSCSI-Softwareinitiatorspeicher empfehlen wir jedoch, Multipathing anstelle von NIC-Bonding zu konfigurieren, wie unter Designing XenServer Network Configurations beschrieben.

  In diesem Abschnitt wird der Begriff IP-basierter Speicherverkehr verwendet, um iSCSI- und NFS-Datenverkehr gemeinsam zu beschreiben.

Sie können eine Bindung erstellen, wenn ein VIF bereits eine der Schnittstellen verwendet, die gebunden werden: Der VM-Verkehr migriert automatisch zur neuen gebundenen Schnittstelle.

In XenServer steht ein zusätzlicher PIF für eine NIC-Bond. XenServer-NIC-Bonds subsumieren die zugrunde liegenden physischen Geräte (PIFs) vollständig.

> **Hinweise:**
>
> - Das Erstellen einer Bindung, die nur eine Netzwerkkarte enthält, wird nicht unterstützt.
> - Bei den gebundenen NICs kann es sich um unterschiedliche Modelle handeln.
> - NIC-Bindungen werden auf NICs, die FCoE-Datenverkehr übertragen, nicht unterstützt.

Bewährte Methoden

Halten Sie sich bei der Einrichtung Ihrer NIC-Bonds an diese bewährten Methoden:

- Verbinden Sie die Verbindungen des Bonds mit verschiedenen physischen Netzwerk-Switches, nicht nur mit den Ports desselben Switches.
- Stellen Sie sicher, dass die einzelnen Switches Strom von verschiedenen, unabhängigen Stromverteilungseinheiten (PDUs) beziehen.
- Wenn möglich, platzieren Sie die PDUs in Ihrem Rechenzentrum an verschiedenen Phasen der Stromversorgung oder sogar an Einspeisungen, die von verschiedenen Versorgungsunternehmen bereitgestellt werden.

- Erwägen Sie die Verwendung von unterbrechungsfreien Stromversorgungen, um sicherzustellen, dass die Netzwerk-Switches und -Hosts weiterhin funktionieren oder bei einem Stromausfall ordnungsgemäß heruntergefahren werden können.

Diese Maßnahmen erhöhen die Widerstandsfähigkeit gegen Software-, Hardware- oder Stromausfälle, die sich auf Ihre Netzwerk-Switches auswirken können.

Wichtige Punkte zur IP-Adressierung

Gebundene NICs haben entweder eine IP-Adresse oder keine IP-Adressen wie folgt:

- **Management- und Speichernetzwerke**.
  - Wenn Sie eine Verwaltungsschnittstelle oder eine sekundäre Schnittstelle binden, wird der Bindung eine einzelne IP-Adresse zugewiesen. Das heißt, jede Netzwerkkarte hat keine eigene IP-Adresse. XenServer behandelt die beiden NICs als eine logische Verbindung.
  - Wenn Bindungen für Nicht-VM-Datenverkehr verwendet werden, z. B. um eine Verbindung zu freigegebenem Netzwerkspeicher oder XenCenter für die Verwaltung herzustellen, konfigurieren Sie eine IP-Adresse für die Bindung. Wenn Sie jedoch bereits einer der Netzwerkkarten eine IP-Adresse zugewiesen haben (d. h. eine Verwaltungsschnittstelle oder eine sekundäre Schnittstelle erstellt haben), wird diese IP-Adresse automatisch der gesamten Bindung zugewiesen.
  - Wenn Sie eine Verwaltungsschnittstelle oder eine sekundäre Schnittstelle ohne IP-Adresse an eine Netzwerkkarte binden, nimmt die Bindung die IP-Adresse der jeweiligen Schnittstelle an.
  - Wenn Sie eine getaggte VLAN-Verwaltungsschnittstelle und eine sekundäre Schnittstelle verbinden, wird das Verwaltungs-VLAN auf dieser gebundenen Netzwerkkarte erstellt.
- **VM-Netzwerke**. Wenn gebundene NICs für den VM-Verkehr verwendet werden, müssen Sie keine IP-Adresse für die Bindung konfigurieren. Dies liegt daran, dass die Bindung auf Layer 2 des OSI-Modells, der Datenverbindungsschicht, ausgeführt wird und auf dieser Ebene keine IP-Adressierung verwendet wird. IP-Adressen für virtuelle Maschinen sind mit VIFs verknüpft.

Bonding-Typen

XenServer bietet drei verschiedene Arten von Bindungen, die alle entweder über die CLI oder XenCenter konfiguriert werden können:

- Active-Active-Modus mit ausgewogenem VM-Datenverkehr zwischen den gebundenen NICs. Siehe Aktiv-Aktiv-Bindung.

- Aktiv-Passiv-Modus, bei dem nur eine Netzwerkkarte aktiv Datenverkehr überträgt. Siehe Aktiv-Passiv-Verklebung.
- LACP Link Aggregation, bei der aktive und Standby-NICs zwischen dem Switch und dem Host ausgehandelt werden. Siehe LACP Link Aggregation Control Protocol Bindung.

> **Hinweis:**
>
> Das Bonding wird mit einer Aufwärtsverzögerung von 31.000 ms und einer Abwärtsverzögerung von 200 ms eingerichtet. Die scheinbar lange Aufwärtsverzögerung ist aufgrund der Zeit, die einige Switches benötigen, um den Port zu aktivieren, absichtlich. Ohne Verzögerung, wenn eine Verbindung nach einem Ausfall zurückkommt, kann die Bindung den Verkehr auf sie ausgleichen, bevor der Switch bereit ist, den Verkehr weiterzuleiten. Um beide Verbindungen auf einen anderen Switch zu verschieben, bewegen Sie einen und warten Sie dann 31 Sekunden, bis er erneut verwendet wird, bevor Sie den anderen bewegen. Informationen zum Ändern der Verzögerung finden Sie unter Ändern der Verzögerung für Bonds.

Status der Bindung

XenServer stellt den Status für Verbindungen in den Ereignisprotokollen für jeden Host bereit. Wenn eine oder mehrere Links in einem Bond ausfallen oder wiederhergestellt werden, wird dies im Ereignisprotokoll vermerkt. Ebenso können Sie den Status der Bindungen abfragen, indem Sie den Parameter `links-up` verwenden, wie im folgenden Beispiel gezeigt:

```
1 xe bond-param-get uuid=bond_uuid param-name=links-up
2 <!--NeedCopy-->
```

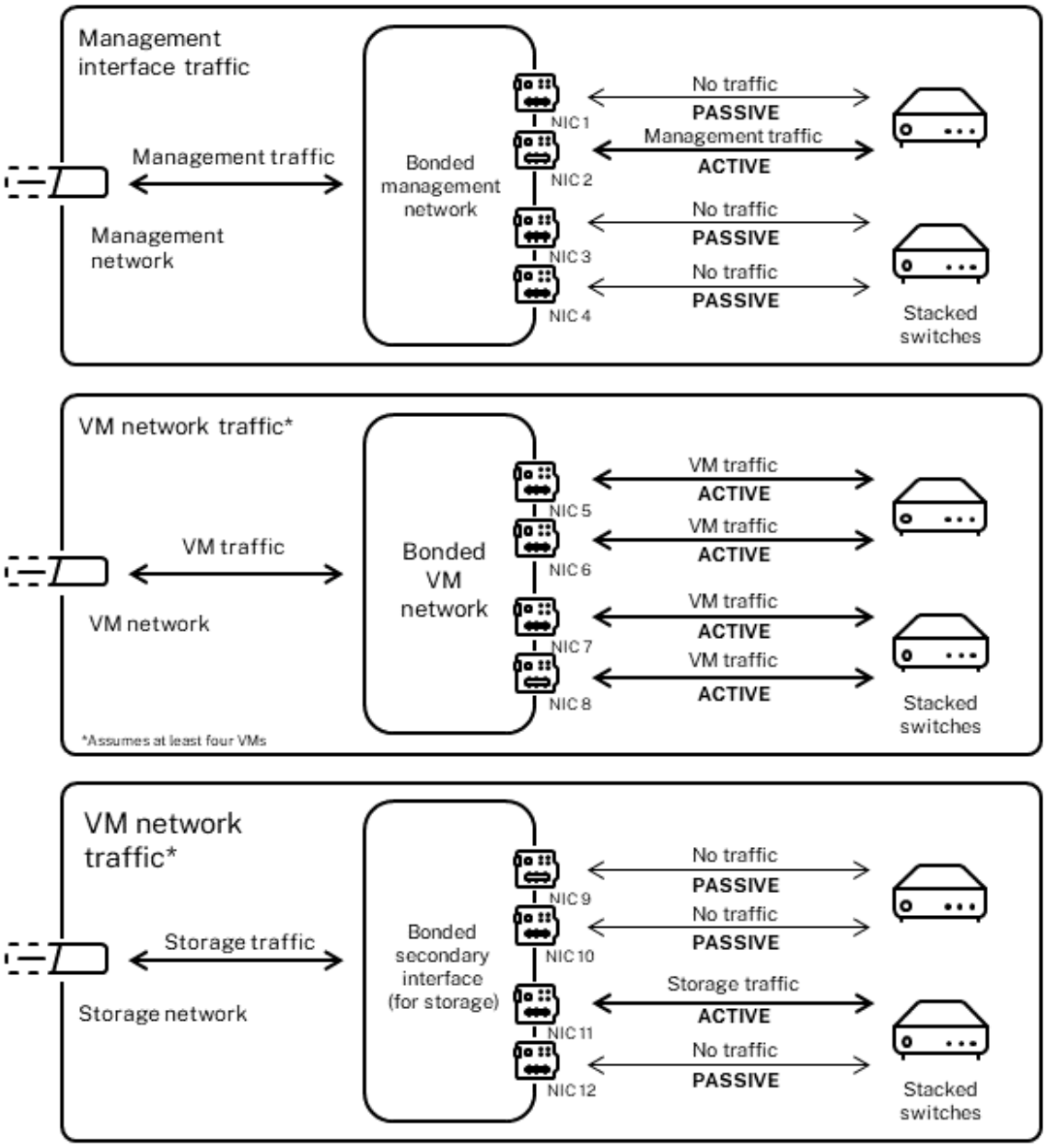
XenServer überprüft den Status von Links in Bonds etwa alle fünf Sekunden. Wenn daher im Fünf-Sekunden-Fenster mehr Links in dem Bond ausfallen, wird der Fehler erst bei der nächsten Statusüberprüfung protokolliert.

Bondingereignisprotokolle werden auf der Registerkarte XenCenter Logs angezeigt. Für Benutzer, die XenCenter nicht ausführen, werden Ereignisprotokolle auch in `/var/log/xensource.log` auf jedem Host angezeigt.

Aktiv-aktive Verklebung

Active-Active ist eine aktive/aktive Konfiguration für den Gastverkehr: Beide NICs können den VM-Verkehr gleichzeitig weiterleiten. Wenn Bindungen für den Verwaltungsverkehr verwendet werden, kann nur eine Netzwerkkarte in der Bindung den Datenverkehr weiterleiten: Die andere Netzwerkkarte bleibt ungenutzt und bietet Failoverunterstützung. Der Aktiv-Aktiv-Modus ist der Standardverbindungsmodus, wenn entweder die Linux-Brücke oder der vSwitch-Netzwerkstapel aktiviert ist

Wenn Active-Active-Bonding mit der Linux-Brücke verwendet wird, können Sie nur zwei Netzwerkkarten verbinden. Wenn Sie den vSwitch als Netzwerkstapel verwenden, können Sie entweder zwei, drei oder vier Netzwerkkarten im Active-Active-Modus verbinden. Im aktiv-aktiven Modus ist das Verbinden von drei oder vier NICs jedoch nur für den VM-Verkehr von Vorteil, wie in der folgenden Abbildung gezeigt.



Active-active bonds (vSwitch network stack)

XenServer kann nur dann Datenverkehr über zwei oder mehr NICs senden, wenn der Verbindung mehr

als eine MAC-Adresse zugeordnet ist. XenServer kann die virtuellen MAC-Adressen in der VIF verwenden, um Datenverkehr über mehrere Links zu senden. Speziell:

- **VM-Verkehr**. Sofern Sie die Bindung auf NICs aktivieren, die nur VM-Datenverkehr (Gast) übertragen, sind alle Verbindungen aktiv und die NIC-Bindung kann den verteilten VM-Verkehr über die Netzwerkkarten ausgleichen Der Datenverkehr eines einzelnen VIF wird niemals zwischen Netzwerkkarten aufgeteilt.
- **Verwaltung oder Speicherverkehr**. Nur einer der Links (NICs) in der Bindung ist aktiv und die anderen NICs bleiben ungenutzt, sofern der Datenverkehr nicht zu ihnen übergeht. Die Konfiguration einer Verwaltungsschnittstelle oder einer sekundären Schnittstelle in einem gebundenen Netzwerk sorgt für Ausfallsicherheit.
- **Gemischter Verkehr**. Wenn die gebundene Netzwerkkarte eine Mischung aus IP-basiertem Speicherverkehr und Gastverkehr trägt, wird nur der Gast- und Steuerdomänenverkehr mit einem Lastenausgleich durchgeführt. Bei der Steuerdomäne handelt es sich im Wesentlichen um eine virtuelle Maschine, sodass sie wie die anderen Gäste eine Netzwerkkarte verwendet. XenServer verteilt den Datenverkehr der Steuerdomäne auf die gleiche Weise wie den VM-Verkehr.

Datenverkehr ausgleichen XenServer verteilt den Datenverkehr zwischen Netzwerkkarten mithilfe der Quell-MAC-Adresse des Pakets. Da für den Verwaltungsdatenverkehr nur eine Quell-MAC-Adresse vorhanden ist, kann im Active-Active-Modus nur eine NIC verwendet werden, und der Datenverkehr ist nicht ausgeglichen. Der Verkehrsausgleich basiert auf zwei Faktoren:

- Die virtuelle Maschine und die zugehörige VIF senden oder empfangen den Datenverkehr
- Die Menge der gesendeten Daten (in Kilobyte).

XenServer bewertet die Datenmenge (in Kilobyte), die jede Netzwerkkarte sendet und empfängt. Wenn die über eine Netzwerkkarte gesendete Datenmenge die Datenmenge übersteigt, die über die andere Netzwerkkarte gesendet wird, gleicht XenServer aus, welche VIFs welche NICs verwenden. Die gesamte Ladung des VIF wird übertragen. Die Last eines VIF wird niemals auf zwei Netzwerkkarten aufgeteilt.

Die aktiv-aktive NIC-Bindung kann zwar einen Lastenausgleich für den Datenverkehr von mehreren VMs ermöglichen, kann jedoch keine einzelne VM mit dem Durchsatz von zwei Netzwerkkarten bereitstellen. Jede VIF verwendet jeweils nur einen der Links in einem Bond. Da XenServer den Datenverkehr regelmäßig neu verteilt, werden VIFs nicht dauerhaft einer bestimmten Netzwerkkarte in der Bindung zugewiesen.

Der Active-Active-Modus wird manchmal als Source Load Balancing (SLB) -Bonding bezeichnet, da XenServer SLB verwendet, um die Last auf gebündelte Netzwerkschnittstellen zu verteilen. SLB

wird aus dem Open-Source-Modus Adaptive Load Balancing (ALB) abgeleitet und verwendet die ALB-Funktionalität erneut, um die Last über die NICs hinweg dynamisch neu zu verteilen.

Beim Rebalancing wird die Anzahl der Byte, die über jede sekundäre (Schnittstelle) gehen, über einen bestimmten Zeitraum verfolgt. Wenn ein zu sendendes Paket eine neue Quell-MAC-Adresse enthält, wird es der sekundären Schnittstelle mit der geringsten Auslastung zugewiesen. Der Verkehr wird in regelmäßigen Abständen neu ausbalanciert.

Jede MAC-Adresse hat eine entsprechende Last und XenServer kann ganze Lasten zwischen NICs verschieben, abhängig von der Datenmenge, die eine VM sendet und empfängt. Für aktiv-aktiven Datenverkehr kann der gesamte Datenverkehr von einer VM auf nur einer Netzwerkkarte gesendet werden.

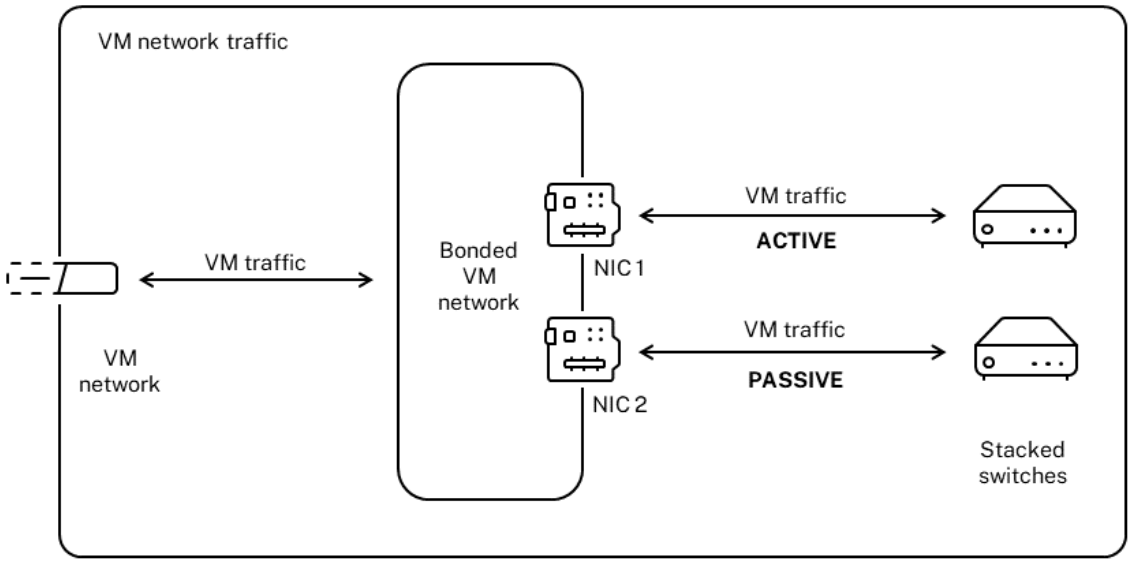
> **Hinweis:**
>
> Active-Active-Bonding erfordert keine Switch-Unterstützung für EtherChannel oder 802.3ad (LACP).

Aktiv-Passiv Bonding

Eine Aktiv-Passiv-Bindung leitet den Verkehr nur über eine der NICs. Wenn die aktive Netzwerkkarte die Netzwerkkonnektivität verliert, wechselt der Datenverkehr auf die andere Netzwerkkarte in der Verbindung. Aktiv-Passiv-Bindungen leiten den Datenverkehr über die aktive Netzwerkkarte. Der Verkehr verlagert sich auf die passive Netzwerkkarte, wenn die aktive Netzwerkkarte ausfällt.

Aktiv-Passiv-Bindung ist in der Linux-Bridge und im vSwitch-Netzwerkstapel verfügbar. Bei Verwendung mit der Linux-Brücke können Sie zwei Netzwerkkarten miteinander verbinden. Bei Verwendung mit dem vSwitch können Sie nur zwei, drei oder vier Netzwerkkarten miteinander verbinden. Unabhängig von der Art des Datenverkehrs ist beim Binden von Netzwerkkarten im aktiv-passiven Modus jedoch nur eine Verbindung aktiv und es findet kein Lastenausgleich zwischen den Links statt.

Die folgende Abbildung zeigt zwei verbundene NICs, die im aktiv-passiven Modus konfiguriert sind.



Active-passive bond

Der Active-Active-Modus ist die Standard-Bonding-Konfiguration in XenServer. Wenn Sie Bonds mit der CLI konfigurieren, müssen Sie einen Parameter für den aktiv-passiven Modus angeben. Andernfalls wird eine aktiv-aktive Bindung hergestellt. Sie müssen den aktiv-Passiv-Modus nicht konfigurieren, da ein Netzwerk Verwaltungsdatenverkehr oder Speicherverkehr überträgt.

Aktiv-Passiv kann eine gute Wahl für die Ausfallsicherheit sein, da es mehrere Vorteile bietet. Bei Aktiv-Passiv-Bindungen bewegt sich der Verkehr nicht zwischen den NICs. In ähnlicher Weise können Sie beim Aktiv-Passiv-Bonding zwei Switches für Redundanz konfigurieren, erfordert jedoch kein Stapeln. Wenn der Verwaltungs-Switch stirbt, können gestapelte Switches eine einzelne Ausfallstelle sein.

Der Aktiv-Passiv-Modus erfordert keine Switch-Unterstützung für EtherChannel oder 802.3ad (LACP).

Erwägen Sie die Konfiguration des aktiv-passiven Modus in Situationen, in denen Sie keinen Lastenausgleich benötigen oder wenn Sie nur Datenverkehr auf einer Netzwerkkarte senden möchten.

> **Wichtig:**
>
> Nachdem Sie VIFs erstellt haben oder Ihr Pool in Produktion ist, seien Sie vorsichtig mit dem Wechseln und Erstellen von Bindungen.

LACP Link Aggregation Control Protocol Bindung

Das LACP Link Aggregation Control Protocol ist eine Art von Bindung, die eine Gruppe von Ports bündelt und sie wie einen einzigen logischen Kanal behandelt. LACP-Bonding bietet Failover und kann die gesamte verfügbare Bandbreite erhöhen.

Im Gegensatz zu anderen Bonding-Modi erfordert das LACP-Bonding die Konfiguration beider Seiten der Links: Erstellen einer Bindung auf dem Host und Erstellen einer Link Aggregation Group (LAG) für jede Bindung auf dem Switch. Siehe Switchkonfiguration für LACP-Bonds. Sie müssen den vSwitch als Netzwerkstapel konfigurieren, um die LACP-Bindung verwenden zu können. Außerdem müssen Ihre Switches den IEEE 802.3ad-Standard unterstützen.

Ein Vergleich der aktiv-aktiven SLB-Bindung und der LACP-Bindung:

Aktiv-aktive SLB-Bindung Vorteile:

- Kann mit jedem Switch auf der Hardwarekompatibilitätsliste verwendet werden.
- Benötigt keine Switches, die das Stapeln unterstützen.
- Unterstützt vier NICs.

Überlegungen:

- Für den optimalen Lastausgleich ist mindestens eine Netzwerkkarte pro VIF erforderlich.
- Speicher- oder Verwaltungsverkehr kann nicht auf mehrere Netzwerkkarten aufgeteilt werden.
- Der Lastenausgleich findet nur statt, wenn mehrere MAC-Adressen vorhanden sind.

LACP-Bindung Vorteile:

- Alle Links können unabhängig von der Verkehrsart aktiv sein.
- Der Verkehrsausgleich hängt nicht von den Quell-MAC-Adressen ab, sodass alle Verkehrstypen ausgeglichen werden können.

Überlegungen:

- Switches müssen den IEEE 802.3ad-Standard unterstützen.
- Erfordert eine Switch-seitige Konfiguration.
- Wird nur für den vSwitch unterstützt.
- Benötigt einen einzelnen Switch oder einen gestapelten Switch.

Datenverkehr ausgleichen XenServer unterstützt zwei LACP-Bonding-Hashing-Typen. Der Begriff Hashing beschreibt, wie die NICs und der Switch den Datenverkehr verteilen —(1) Lastenausgleich basierend auf IP und Port von Quell- und Zieladressen und (2) Lastenausgleich basierend auf der Quell-MAC-Adresse.

Je nach Hash-Typ und Verkehrsmuster kann die LACP-Bindung den Datenverkehr möglicherweise gleichmäßiger verteilen als die aktiv-aktive NIC-Bindung.

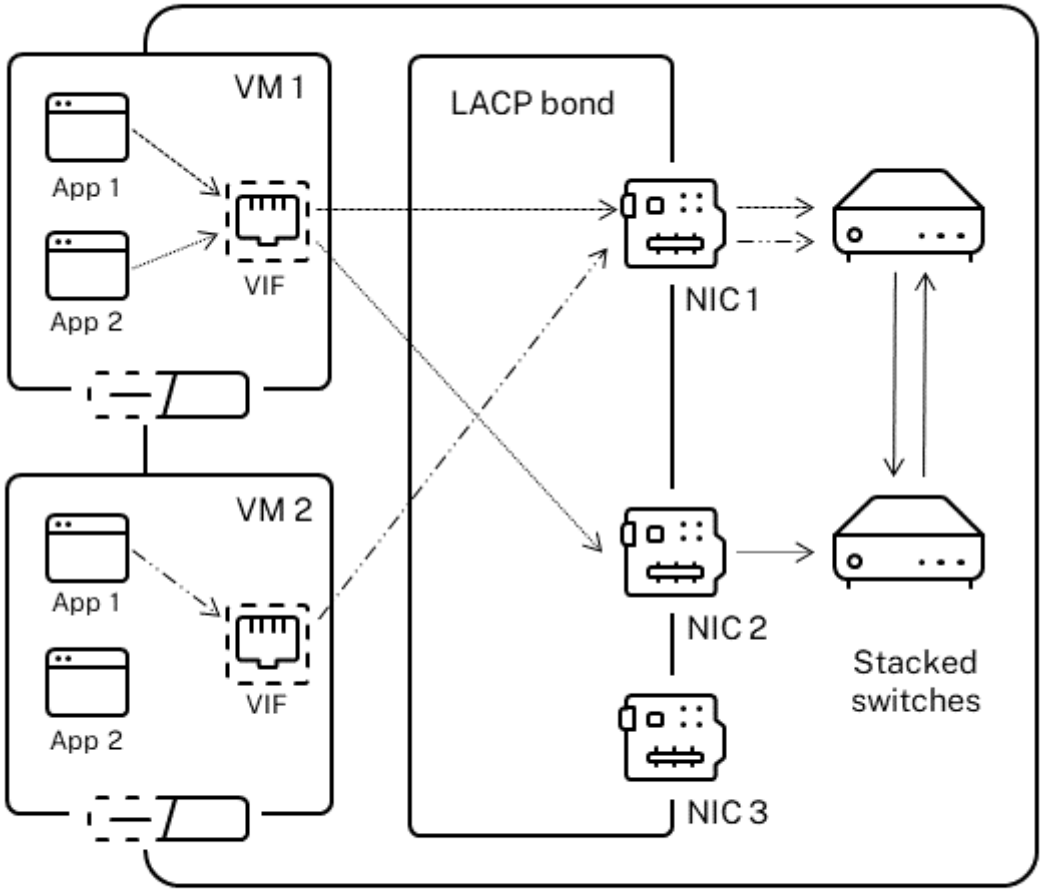
> **Hinweis:**
>
> Sie konfigurieren Einstellungen für ausgehenden und eingehenden Datenverkehr getrennt auf dem Host und dem Switch: Die Konfiguration muss nicht auf beiden Seiten übereinstimmen.

Lastenausgleich basierend auf IP und Port der Quell- und Zieladressen.

Dieser Hashing-Typ ist der standardmäßige LACP-Bonding-Hashing-Algorithmus. Wenn sich die Quell- oder Ziel-IP oder die Portnummern unterscheiden, kann der Datenverkehr von einem Gast über zwei Links verteilt werden.

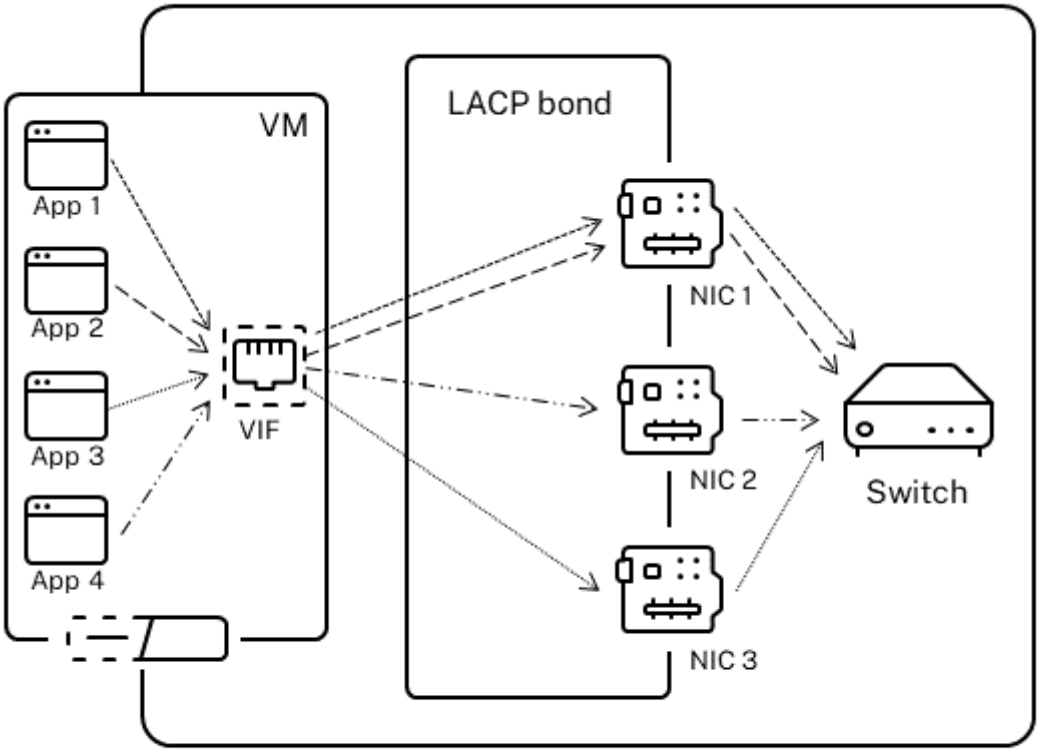
Wenn auf einer virtuellen Maschine mehrere Anwendungen ausgeführt werden, die unterschiedliche IP- oder Portnummern verwenden, verteilt dieser Hashing-Typ den Datenverkehr über mehrere Links. Durch die Verteilung des Datenverkehrs hat der Gast die Möglichkeit, den Gesamtdurchsatz zu nutzen. Mit diesem Hashing-Typ kann ein Gast den gesamten Durchsatz mehrerer Netzwerkkarten nutzen.

Wie in der folgenden Abbildung dargestellt, kann dieser Hashing-Typ den Datenverkehr von zwei verschiedenen Anwendungen auf einer virtuellen Maschine auf zwei verschiedene NICs verteilen.



Load balancing based on IP and port of source and destination addresses

Die Konfiguration der LACP-Bindung basierend auf IP und Port der Quell- und Zieladresse ist vorteilhaft, wenn Sie den Datenverkehr zweier verschiedener Anwendungen auf derselben VM ausgleichen möchten. Zum Beispiel, wenn nur eine virtuelle Maschine für die Verwendung einer Bindung von drei NICs konfiguriert ist.

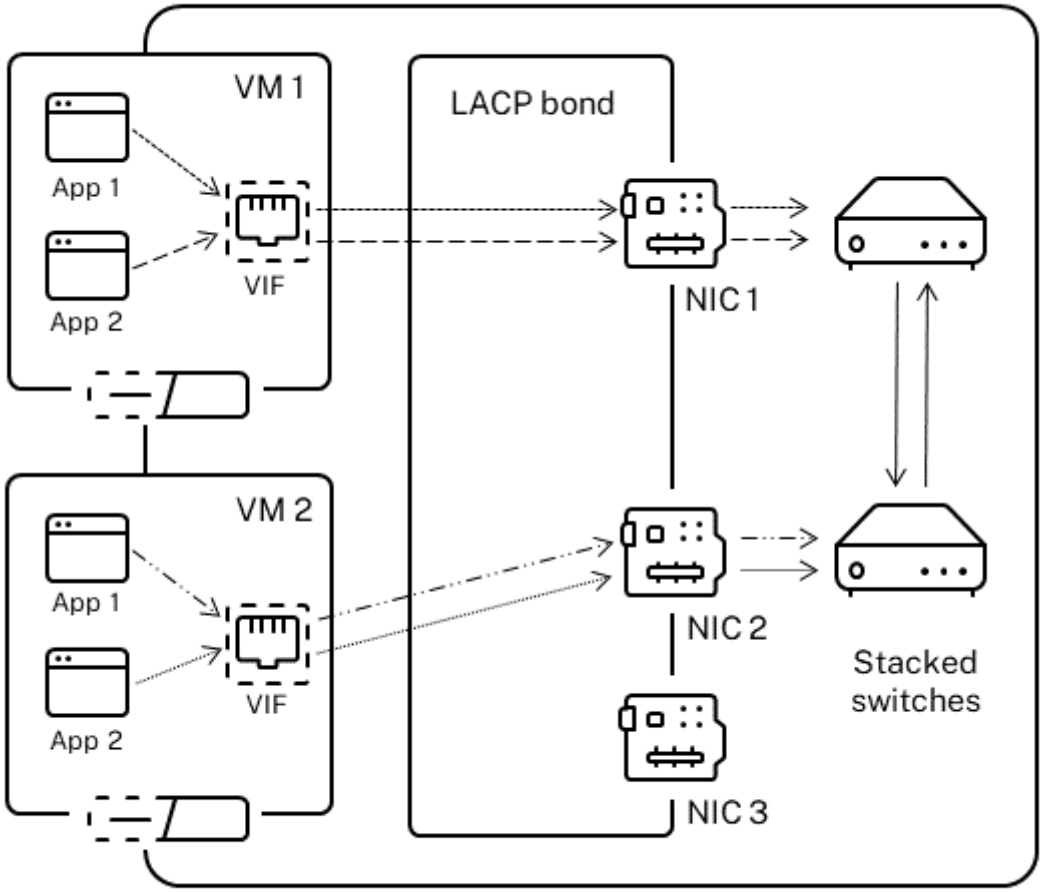


Load balancing based on IP and port of source and destination addresses

Der Balancing-Algorithmus für diesen Hashing-Typ verwendet fünf Faktoren, um den Datenverkehr über die NICs zu verteilen: Quell-IP-Adresse, Quellportnummer, Ziel-IP-Adresse, Zielportnummer und Quell-MAC-Adresse.

Lastenausgleich basierend auf der Quell-MAC-Adresse.

Diese Art des Lastenausgleichs funktioniert gut, wenn sich mehrere virtuelle Maschinen auf demselben Host befinden. Der Datenverkehr wird basierend auf der virtuellen MAC-Adresse der VM, von der der Datenverkehr stammt, ausgeglichen. XenServer sendet ausgehenden Datenverkehr mit demselben Algorithmus wie beim Active-Active-Bonding. Der Datenverkehr desselben Gastes wird nicht auf mehrere Netzwerkkarten aufgeteilt. Daher ist dieser Hashing-Typ nicht geeignet, wenn weniger VIFs als NICs vorhanden sind: Der Lastausgleich ist nicht optimal, da der Datenverkehr nicht auf Netzwerkkarten aufgeteilt werden kann.



Load balancing based on source MAC address

Switch-Konfiguration

Abhängig von Ihren Redundanzanforderungen können Sie die Netzwerkkarten in der Verbindung entweder mit denselben oder mit separaten gestapelten Switches verbinden. Wenn Sie eine der Netzwerkkarten mit einem zweiten, redundanten Switch verbinden und eine Netzwerkkarte oder ein Switch ausfällt, wird der Datenverkehr auf die andere Netzwerkkarte umgeleitet. Das Hinzufügen eines zweiten Switches verhindert auf folgende Weise einen einzelnen Ausfallpunkt in Ihrer Konfiguration:

- Wenn Sie eine der Links in einer gebundenen Verwaltungsschnittstelle mit einem zweiten Switch verbinden und der Switch ausfällt, bleibt das Verwaltungsnetzwerk online und die Hosts können weiterhin miteinander kommunizieren.
- Wenn Sie eine Verbindung (für jeden Verkehrstyp) mit einem zweiten Switch verbinden und die Netzwerkkarte oder der Switch ausfällt, bleiben die virtuellen Maschinen im Netzwerk, während

ihr Datenverkehr auf den anderen NIC/Switch umschlägt.

Verwenden Sie gestapelte Switches, wenn Sie gebundene NICs mit mehreren Switches verbinden möchten und den LACP-Bondingmodus konfiguriert haben. Der Begriff "gestapelte Switches" wird verwendet, um die Konfiguration mehrerer physischer Switches zu beschreiben, die als ein einziger logischer Switch funktionieren. Sie müssen die Switches physisch und über die Switch-Verwaltungssoftware zusammenfügen, damit die Switches gemäß den Richtlinien des Switch-Herstellers als eine einzige logische Vermittlungseinheit fungieren. In der Regel ist das Stapeln von Switches nur über proprietäre Erweiterungen verfügbar, und Switch-Anbieter können diese Funktionalität unter anderen Bedingungen vermarkten.

> **Hinweis:**
>
> Wenn Sie Probleme mit aktiv-aktiven Bonds haben, kann die Verwendung von gestapelten Switches erforderlich sein. Aktiv-Passiv-Bonds erfordern keine gestapelten Switches.

Switch-Konfiguration für LACP-Bindungen Da die spezifischen Details der Switch-Konfiguration je nach Hersteller variieren, sollten Sie bei der Konfiguration von Switches für die Verwendung mit LACP-Bindungen einige wichtige Punkte beachten:

- Der Switch muss LACP und den IEEE 802.3ad-Standard unterstützen.
- Wenn Sie die LAG-Gruppe auf dem Switch erstellen, müssen Sie eine LAG-Gruppe für jede LACP-Bindung auf dem Host erstellen. Wenn Sie beispielsweise über einen Pool mit fünf Hosts verfügen und eine LACP-Bindung auf den NICs 4 und 5 auf jedem Host erstellt haben, müssen Sie fünf LAG-Gruppen auf dem Switch erstellen. Eine Gruppe für jeden Portsatz, der den NICs auf dem Host entspricht.

  Möglicherweise müssen Sie auch Ihre VLAN-ID zu Ihrer LAG-Gruppe hinzufügen.
- Für XenServer-LACP-Bindungen muss die Einstellung Static Mode in der LAG-Gruppe auf Deaktiviert gesetzt werden.

Wie bereits in der *Switch-Konfiguration*erwähnt, sind Stapel-Switches erforderlich, um LACP-Bindungen mit mehreren Switches zu verbinden.

Erstkonfiguration des Netzwerks nach der Einrichtung

Die XenServer-Host-Netzwerkkonfiguration wird bei der ersten Hostinstallation angegeben. Optionen wie die IP-Adresskonfiguration (DHCP/Static), die als Verwaltungsschnittstelle verwendete Netzwerkkarte und der Hostname werden auf der Grundlage der bei der Installation angegebenen Werte festgelegt.

Wenn ein Host über mehrere Netzwerkkarten verfügt, hängt die nach der Installation vorhandene Konfiguration davon ab, welche Netzwerkkarte für Verwaltungsvorgänge während der Installation ausgewählt wurde:

- PIFs werden für jede Netzwerkkarte im Host erstellt.
- Die PIF der für die Verwendung als Verwaltungsschnittstelle ausgewählten NIC wird mit den bei der Installation angegebenen IP-Adressierungsoptionen konfiguriert.
- Für jedes PIF wird ein Netzwerk erstellt (“Netzwerk 0”, “Netzwerk 1”usw.)
- Jedes Netzwerk ist mit einem PIF verbunden
- Die IP-Adressierungsoptionen bleiben für alle PIFs außer dem PIF, der als Verwaltungsschnittstelle verwendet wird, nicht konfiguriert.

Wenn ein Host über eine einzelne Netzwerkkarte verfügt, ist nach der Installation die folgende Konfiguration vorhanden:

- Es wird ein einzelnes PIF erstellt, das der einzelnen Netzwerkkarte des Hosts entspricht.
- Der PIF ist mit den bei der Installation angegebenen IP-Adressierungsoptionen konfiguriert und ermöglicht die Verwaltung des Hosts.
- Der PIF ist für die Verwendung in Host-Verwaltungsvorgängen festgelegt.
- Ein einzelnes Netzwerk, Netzwerk 0, wird erstellt
- Netzwerk 0 ist mit dem PIF verbunden, um externe Konnektivität zu virtuellen Rechnern zu ermöglichen

Wenn eine Installation von XenServer in einem markierten VLAN-Netzwerk durchgeführt wird, ist nach der Installation die folgende Konfiguration vorhanden:

- PIFs werden für jede Netzwerkkarte im Host erstellt.
- Der PIF für das markierte VLAN auf der Netzwerkkarte, die für die Verwendung als Verwaltungsschnittstelle ausgewählt wurde, wird mit der bei der Installation angegebenen IP-Adresskonfiguration konfiguriert.
- Für jedes PIF wird ein Netzwerk erstellt (z. B. Netzwerk 1, Netzwerk 2 usw.). Ein zusätzliches VLAN-Netzwerk wird erstellt (z. B. für ein poolweites Netzwerk, das mit eth0 im VLAN<TAG> verknüpft ist)
- Jedes Netzwerk ist mit einem PIF verbunden. Der VLAN-PIF ist für die Verwendung in Host-Verwaltungsvorgängen festgelegt.

In beiden Fällen ermöglicht die resultierende Netzwerkkonfiguration die Verbindung zum XenServer-Host über XenCenter, die Xe-CLI und jede andere Verwaltungssoftware, die auf separaten Computern

ausgeführt wird, über die IP-Adresse der Verwaltungsschnittstelle. Die Konfiguration bietet auch externe Netzwerke für virtuelle Maschinen, die auf dem Host erstellt wurden.

Das für Verwaltungsvorgänge verwendete PIF ist das einzige PIF, das jemals während der XenServer-Installation mit einer IP-Adresse konfiguriert wurde. Externe Netzwerke für VMs werden durch die Überbrückung von PIFs zu VIFs mithilfe des Netzwerkobjekts erreicht, das als virtueller Ethernet-Switch fungiert.

Die Schritte, die für Netzwerkfunktionen wie VLANs, NIC-Bindungen und das Zuweisen einer NIC für den Speicherverkehr erforderlich sind, werden in den folgenden Abschnitten behandelt.

Netzwerkkonfiguration ändern

Sie können Ihre Netzwerkkonfiguration ändern, indem Sie das Netzwerkobjekt ändern. Dazu führen Sie einen Befehl aus, der sich entweder auf das Netzwerkobjekt oder das VIF auswirkt.

Ändern des Netzwerkobjekts

Sie können Aspekte eines Netzwerks ändern, z. B. die Framegröße (MTU), die Namensbezeichnung, die Namensbeschreibung, den Zweck und andere Werte. Verwenden Sie den xe-Befehl `network-param-set` und die zugehörigen Parameter, um die Werte zu ändern.

Wenn Sie den xe-Befehl `network-param-set` ausführen, ist der einzige erforderliche Parameter `uuid`.

Optionale Parameter sind:

- `default_locking_mode`. Siehe Vereinfachung der Konfiguration des VIF-Sperrmodus in der Cloud.
- `name-label`
- `name-description`
- `MTU`
- `purpose`. Informationen finden Sie unter Hinzufügen eines Zwecks zu einem Netzwerk.
- `other-config`

Wenn kein Wert für einen Parameter angegeben wird, wird der Parameter auf einen Nullwert gesetzt. Um ein (Schlüssel, Wert) -Paar in einem Map-Parameter festzulegen, verwenden Sie die Syntax `map-param:key=value`.

Änderung der Aufwärtverzögerung für Bindungen

Die Bindung wird standardmäßig mit einer Aufwärtsverzögerung von 31.000 ms eingerichtet, um zu verhindern, dass der Datenverkehr nach einem Ausfall auf eine Netzwerkkarte neu verteilt wird. Die Aufwärtsverzögerung scheint zwar lang zu sein, ist aber für alle Bonding-Modi wichtig und nicht nur für aktiv-aktiv.

Wenn Sie jedoch die entsprechenden Einstellungen für Ihre Umgebung kennen, können Sie die Aufwärtsverzögerung für Bindungen mit dem folgenden Verfahren ändern.

Stellen Sie die Aufwärtsverzögerung in Millisekunden:

```
xe pif-param-set uuid=<uuid of bond interface PIF> other-config:bond-
    updelay=<delay in ms>
<!--NeedCopy-->
```

Um die Änderung wirksam werden zu lassen, müssen Sie die physische Schnittstelle abziehen und dann erneut anschließen:

```
xe pif-unplug uuid=<uuid of bond interface PIF>
<!--NeedCopy-->
```

```
xe pif-plug uuid=<uuid of bond interface PIF>
<!--NeedCopy-->
```

Verwalten von Netzwerken

February 24, 2024

Die Netzwerkkonfigurationsverfahren in diesem Abschnitt unterscheiden sich je nachdem, ob Sie einen eigenständigen Host oder einen Host konfigurieren, der Teil eines Ressourcenpools ist.

Netzwerke auf einem eigenständigen Host erstellen

Da während der Host-Installation für jedes PIF externe Netzwerke erstellt werden, ist das Erstellen zusätzlicher Netzwerke normalerweise nur erforderlich, um:

- Verwenden Sie ein privates Netzwerk
- Unterstützt erweiterte Vorgänge wie VLANs oder NIC-Bonding

Informationen zum Hinzufügen oder Löschen von Netzwerken mit XenCenter finden Sie unter Hinzufügen eines neuen Netzwerks in der XenCenter-Dokumentation.

Öffnen Sie die XenServer-Host-Textkonsole.

Erstellen Sie das Netzwerk mit dem Befehl network-create, der die UUID des neu erstellten Netzwerks zurückgibt:

```
xe network-create name-label=mynetwork
<!--NeedCopy-->
```

Zu diesem Zeitpunkt ist das Netzwerk nicht mit einem PIF verbunden und daher intern.

Erstellen von Netzwerken in Ressourcenpools

Alle XenServer-Hosts in einem Ressourcenpool müssen dieselbe Anzahl von physischen Netzwerkkarten haben. Diese Anforderung wird nicht strikt durchgesetzt, wenn ein Host mit einem Pool verbunden ist. Eine der NICs wird immer als *Verwaltungsschnittstelle bezeichnet, die für den XenServer-Verwaltungsdatenverkehr*verwendet wird.

Da sich alle Hosts in einem Pool ein gemeinsames Netzwerk teilen. Es ist wichtig, dieselbe physische Netzwerkkonfiguration für XenServer-Hosts in einem Pool zu haben. PIFs auf den einzelnen Hosts werden basierend auf dem Gerätenamen mit poolweiten Netzwerken verbunden. Beispielsweise haben alle XenServer-Hosts in einem Pool mit eth0-NIC eine entsprechende PIF, die an das poolweite Netzwerk `Network 0` angeschlossen ist. Das Gleiche gilt für Hosts mit eth1-NICs und anderen NICs `Network 1`, die in mindestens einem XenServer-Host im Pool vorhanden sind.

Wenn ein XenServer-Host eine andere Anzahl von NICs hat als andere Hosts im Pool, können Komplikationen auftreten. Die Komplikationen können auftreten, da nicht alle Pool-Netzwerke für alle Pool-Hosts gültig sind. Wenn sich beispielsweise die Hosts *host1* und *host2* im selben Pool befinden und *host1* über vier Netzwerkkarten verfügt und *host2* nur über zwei verfügt, sind nur die Netzwerke, die mit PIFs verbunden sind, die eth0 und eth1 entsprechen, auf *host2*gültig. Virtuelle Rechner auf *host1* mit VIFs, die mit Netzwerken verbunden sind, die eth2 und eth3 entsprechen, können nicht auf Host *host2*migriert werden.

Erstellen von VLANs

Für Hosts in einem Ressourcenpool können Sie den `pool-vlan-create` Befehl verwenden. Dieser Befehl erstellt das VLAN und erstellt und fügt automatisch die erforderlichen PIFs auf den Hosts im Pool ein. Weitere Informationen finden Sie unter `pool-vlan-create`.

Öffnen Sie die XenServer-Hostkonsole.

Erstellen Sie ein Netzwerk für die Verwendung mit dem VLAN. Die UUID des neuen Netzwerks wird zurückgegeben:

```
xe network-create name-label=network5
```



```
<!--NeedCopy-->
```

Verwenden Sie den Befehl `pif-list`, um die UUID der PIF zu finden, der der physischen Netzwerkkarte entspricht, die das gewünschte VLAN-Tag unterstützt. Die UUIDs und Gerätenamen aller PIFs werden zurückgegeben, einschließlich aller vorhandenen VLANs:

```
xe pif-list
<!--NeedCopy-->
```

Erstellen Sie ein VLAN-Objekt, das den gewünschten physischen PIF- und VLAN-Tag auf allen VMs angibt, die mit dem neuen VLAN verbunden werden sollen. Ein neuer PIF wird erstellt und an das angegebene Netzwerk angeschlossen. Die UUID des neuen PIF-Objekts wird zurückgegeben.

```
xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
<!--NeedCopy-->
```

Hängen Sie VM-VIFs an das neue Netzwerk an. Weitere Informationen finden Sie unter Netzwerke auf einem eigenständigen Host erstellen.

Erstellen von NIC-Bindungen auf einem eigenständigen Host

Wir empfehlen die Verwendung von XenCenter zum Erstellen von NIC-Bonds. Weitere Informationen finden Sie unter Konfigurieren von NICs.

In diesem Abschnitt wird beschrieben, wie Sie mit der Xe-CLI NIC-Schnittstellen auf XenServer-Hosts verbinden, die sich nicht in einem Pool befinden. Informationen zur Verwendung der Xe-CLI zum Erstellen von NIC-Bindungen auf XenServer-Hosts, die einen Ressourcenpool bilden, finden Sie unter *Erstellen von NIC-Bindungen in Ressourcenpools*.

Erstellen einer NIC-Verbindung

Wenn Sie eine Netzwerkkarte binden, absorbiert die Bindung den PIF/NIC, der als Verwaltungsschnittstelle verwendet wird. Die Verwaltungsschnittstelle wird automatisch auf den Bond-PIF verschoben.

1. Verwenden Sie den Befehl `network-create`, um ein Netzwerk für die Verwendung mit der gebundenen NIC zu erstellen. Die UUID des neuen Netzwerks wird zurückgegeben:

   ```
   xe network-create name-label=bond0
   <!--NeedCopy-->
   ```

2. Verwenden Sie den Befehl `pif-list`, um die UUIDs der PIFs zu bestimmen, die in der Bindung verwendet werden sollen:


```
xe pif-list
<!--NeedCopy-->
```

3. Führen Sie einen der folgenden Schritte aus:

   - Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den Befehl `bond-create`, um die Bindung zu erstellen. Trennen Sie die Parameter durch Kommas und geben Sie die neu erstellte Netzwerk-UUID und die UUIDs der zu verbindenden PIFs an:

     ```
     xe bond-create network-uuid=network_uuid /
          pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
     <!--NeedCopy-->
     ```

     Geben Sie zwei UUIDs ein, wenn Sie zwei NICs und vier UUIDs verbinden, wenn Sie vier Netzwerkkarten verbinden. Die UUID für die Bindung wird nach Ausführung des Befehls zurückgegeben.

   - Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie dieselbe Syntax, fügen Sie den optionalen Parameter `mode` hinzu und geben Sie `lacp` oder `active-backup` an:

     ```
     xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1
         , /
          pif_uuid_2,pif_uuid_3,pif_uuid_4 /
          mode=balance-slb | active-backup | lacp
     <!--NeedCopy-->
     ```

Steuern Sie die MAC-Adresse der Bindung

Wenn Sie die Verwaltungsschnittstelle verbinden, wird die verwendete PIF/NIC als Verwaltungsschnittstelle subsumiert. Wenn der Host DHCP verwendet, entspricht die MAC-Adresse der Bindung der verwendeten PIF/NIC. Die IP-Adresse der Verwaltungsschnittstelle kann unverändert bleiben.

Sie können die MAC-Adresse der Bindung so ändern, dass sie sich von der MAC-Adresse für die (aktuelle) Verwaltungsschnittstellen-NIC unterscheidet. Da die Bindung jedoch aktiviert ist und sich die verwendete MAC/IP-Adresse ändert, werden vorhandene Netzwerksitzungen zum Host verworfen.

Sie können die MAC-Adresse für einen Bond auf zwei Arten steuern:

- Im Befehl `bond-create` kann ein optionaler Parameter `mac` angegeben werden. Mit diesem Parameter können Sie die Bond-MAC-Adresse auf eine beliebige Adresse setzen.
- Wenn der `mac` Parameter nicht angegeben ist, verwendet XenServer die MAC-Adresse der Verwaltungsschnittstelle, wenn es sich um eine der Schnittstellen in der Bindung handelt.

Wenn die Verwaltungsschnittstelle nicht Teil des Bonds ist, sondern eine andere Verwaltungsschnittstelle, verwendet die Bindung die MAC-Adresse (und auch die IP-Adresse) dieser Verwaltungsschnittstelle. Wenn keine der Netzwerkkarten in der Bindung eine Verwaltungsschnittstelle ist, verwendet die Bindung den MAC der zuerst benannten NIC.

NIC-Bonds rückgängig machen

Wenn der XenServer-Host auf eine nicht gebundene Konfiguration zurückgesetzt wird, konfiguriert der `bond-destroy` Befehl automatisch die primäre Netzwerkkarte als Schnittstelle für die Verwaltungsschnittstelle. Daher werden alle VIFs auf die Verwaltungsschnittstelle verschoben. Wenn sich die Verwaltungsschnittstelle eines Hosts auf einer getaggten VLAN-gebundenen Schnittstelle befindet, wird das Verwaltungs-VLAN beim Ausführen von `bond-destroy` auf die primäre Netzwerkkarte verschoben.

Der Begriff primäre Netzwerkkarte bezieht sich auf den PIF, aus dem die MAC- und IP-Konfiguration beim Erstellen der Bindung kopiert wurde. Beim Verbinden von zwei NICs lautet die primäre Netzwerkkarte:

1. Die Netzwerkkarte der Verwaltungsschnittstelle (wenn die Verwaltungsschnittstelle eine der gebundenen NICs ist).
2. Jede andere Netzwerkkarte mit einer IP-Adresse (wenn die Verwaltungsschnittstelle nicht Teil der Bindung war).
3. Die erste benannte NIC. Sie können herausfinden, um welches es sich handelt, indem Sie Folgendes ausführen:

```
xe bond-list params=all
<!--NeedCopy-->
```

NIC-Bindungen in Ressourcenpools erstellen

Erstellen Sie nach Möglichkeit NIC-Bindungen als Teil der anfänglichen Erstellung eines Ressourcenpools, bevor Sie dem Pool weitere Hosts hinzufügen oder VMs erstellen. Dadurch kann die Bond-Konfiguration automatisch auf Hosts repliziert werden, wenn sie mit dem Pool verbunden werden, und reduziert die Anzahl der erforderlichen Schritte.

Das Hinzufügen einer NIC-Bindung zu einem vorhandenen Pool erfordert eine der folgenden Optionen:

- Verwenden Sie die CLI, um die Bindungen auf dem Poolkoordinator und dann auf jedem Mitglied des Pools zu konfigurieren.

- Verwenden Sie die CLI, um Bindungen auf dem Poolkoordinator zu konfigurieren und dann jedes Poolmitglied neu zu starten, sodass es seine Einstellungen vom Poolkoordinator erbt.
- Verwenden von XenCenter zur Konfiguration der Bindungen auf dem Poolkoordinator. XenCenter synchronisiert automatisch die Netzwerkeinstellungen auf den Mitgliedshosts mit dem Poolkoordinator, sodass Sie die Mitgliedshosts nicht neu starten müssen.

Zur Vereinfachung und zur Vermeidung von Fehlkonfigurationen empfehlen wir die Verwendung von XenCenter zum Erstellen von NIC-Bonds. Weitere Informationen finden Sie unter Konfigurieren von NICs.

In diesem Abschnitt wird die Verwendung der Xe-CLI zum Erstellen gebundener NIC-Schnittstellen auf XenServer-Hosts beschrieben, die einen Ressourcenpool bilden. Informationen zur Verwendung der xe CLI zum Erstellen von NIC-Bindungen auf einem eigenständigen Host finden Sie unter *Erstellen von NIC-Bonds auf einem eigenständigen Host*.

> **Warnung:**
>
> Versuchen Sie nicht, Netzwerkbindungen zu erstellen, wenn Hochverfügbarkeit aktiviert ist. Der Prozess der Bond-Erstellung stört den laufenden Heartbeat mit hoher Verfügbarkeit und führt dazu, dass Hosts sich selbst abgrenzen (sich selbst herunterfahren). Die Hosts können nicht ordnungsgemäß neu gestartet werden und benötigen möglicherweise den Befehl `host-emergency-ha-disable` zum Wiederherstellen.

Wählen Sie den Host aus, der der Poolkoordinator sein soll. Der Poolkoordinator gehört standardmäßig zu einem unbenannten Pool. Um einen Ressourcenpool mit der CLI zu erstellen, benennen Sie den vorhandenen namenlosen Pool um:

```
xe pool-param-set name-label="New Pool" uuid=pool_uuid
<!--NeedCopy-->
```

Erstellen Sie die NIC-Bindung wie unter Erstellen einer NIC-Verbindungbeschrieben.

Öffnen Sie eine Konsole auf einem Host, dem Sie dem Pool beitreten möchten, und führen Sie den Befehl aus:

```
xe pool-join master-address=host1 master-username=root master-password=
   password
<!--NeedCopy-->
```

Die Netzwerk- und Bondinformationen werden automatisch auf den neuen Host repliziert. Die Verwaltungsschnittstelle wird automatisch von der Host-Netzwerkkarte, auf der sie ursprünglich konfiguriert wurde, in das gebundene PIF verschoben. Das heißt, die Verwaltungsschnittstelle wird nun in den Bond aufgenommen, sodass der gesamte Bond als Verwaltungsschnittstelle fungiert.

Verwenden Sie den Befehl `host-list`, um die UUID des zu konfigurierenden Hosts zu finden:


```
xe host-list
<!--NeedCopy-->
```

> **Warnung:**
>
> Versuchen Sie nicht, Netzwerkbindungen zu erstellen, solange Hochverfügbarkeit aktiviert ist. Der Prozess der Bond-Erstellung stört den laufenden Heartbeat mit hoher Verfügbarkeit und führt dazu, dass Hosts sich selbst abgrenzen (sich selbst herunterfahren). Die Hosts können möglicherweise nicht ordnungsgemäß neu gestartet werden, und Sie müssen den Befehl `host-emergency-ha-disable` zum Wiederherstellen ausführen.

Konfigurieren einer dedizierten Speicher-NIC

Sie können XenCenter oder die xe CLI verwenden, um einer NIC eine IP-Adresse zuzuweisen und sie einer bestimmten Funktion wie Speicherverkehr zuzuweisen. Wenn Sie eine Netzwerkkarte mit einer IP-Adresse konfigurieren, erstellen Sie dazu eine sekundäre Schnittstelle. (Der IP-fähige NIC XenServer, der für die Verwaltung verwendet wird, wird als Verwaltungsschnittstelle bezeichnet.)

Wenn Sie eine sekundäre Schnittstelle für einen bestimmten Zweck reservieren möchten, stellen Sie sicher, dass die entsprechende Netzwerkkonfiguration vorhanden ist. Dadurch wird sichergestellt, dass die Netzwerkkarte nur für den gewünschten Datenverkehr verwendet wird. Um eine Netzwerkkarte für den Speicherverkehr zuzuweisen, konfigurieren Sie die Netzwerkkarte, das Speicherziel, den Switch und das VLAN so, dass auf das Ziel nur über die zugewiesene Netzwerkkarte zugegriffen werden kann. Wenn Ihre physische und IP-Konfiguration den über die Speicher-NIC gesendeten Datenverkehr nicht einschränkt, können Sie Datenverkehr, z. B. Verwaltungsdatenverkehr, über die sekundäre Schnittstelle senden.

Wenn Sie eine neue sekundäre Schnittstelle für den Speicherverkehr erstellen, müssen Sie ihr eine IP-Adresse zuweisen, die lautet:

- im selben Subnetz wie der Speichercontroller, falls zutreffend, und
- Nicht im selben Subnetz wie alle anderen sekundären Schnittstellen oder die Verwaltungsschnittstelle.

Wenn Sie sekundäre Schnittstellen konfigurieren, muss sich jede sekundäre Schnittstelle in einem separaten Subnetz befinden. Wenn Sie beispielsweise zwei weitere sekundäre Schnittstellen für den Speicher konfigurieren möchten, benötigen Sie IP-Adressen in drei verschiedenen Subnetzen —ein Subnetz für die Verwaltungsschnittstelle, ein Subnetz für Secondary Interface 1 und ein Subnetz für Secondary Interface 2.

Wenn Sie Bonding für die Ausfallsicherheit Ihres Speicherverkehrs verwenden, sollten Sie die Verwendung von LACP anstelle der Linux-Brückenbindung in Betracht ziehen. Um LACP-Bonding zu verwen-

den, müssen Sie den vSwitch als Ihren Netzwerkstapel konfigurieren. Weitere Informationen finden Sie unter vSwitch-Netzwerke.

> **Hinweis:**
>
> Stellen Sie bei der Auswahl einer Netzwerkkarte zur Konfiguration als sekundäre Schnittstelle für die Verwendung mit iSCSI- oder NFS-SRs sicher, dass die dedizierte Netzwerkkarte ein separates IP-Subnetz verwendet, das nicht von der Verwaltungsschnittstelle weitergeleitet werden kann. Wenn dies nicht erzwungen wird, kann der Speicherverkehr aufgrund der Reihenfolge, in der Netzwerkschnittstellen initialisiert werden, nach einem Neustart des Hosts über die Hauptverwaltungsschnittstelle geleitet werden.

Stellen Sie sicher, dass sich der PIF in einem separaten Subnetz befindet oder dass das Routing entsprechend Ihrer Netzwerktopologie konfiguriert ist, um den gewünschten Datenverkehr über den ausgewählten PIF zu erzwingen.

Richten Sie eine IP-Konfiguration für den PIF ein und fügen Sie entsprechende Werte für den Modus-Parameter hinzu. Wenn Sie statische IP-Adressierung verwenden, fügen Sie die IP-, Netmask-, Gateway- und DNS-Parameter hinzu:

```
1 xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
2 <!--NeedCopy-->
```

Setzen Sie den Parameter disallow-unplug des PIF auf true:

```
1 xe pif-param-set disallow-unplug=true uuid=pif-uuid
2 <!--NeedCopy-->
```

```
1 xe pif-param-set other-config:management_purpose="Storage" uuid=pif-
     uuid
2 <!--NeedCopy-->
```

Wenn Sie eine sekundäre Schnittstelle für Speicher verwenden möchten, die auch von der Verwaltungsschnittstelle geroutet werden kann (wenn Sie bedenken, dass diese Konfiguration nicht die beste Vorgehensweise ist), haben Sie zwei Möglichkeiten:

- Stellen Sie nach einem Neustart des Hosts sicher, dass die sekundäre Schnittstelle korrekt konfiguriert ist. Verwenden Sie die Befehle `xe pbd-unplug` und `xe pbd-plug`, um die Speicherverbindungen auf dem Host neu zu initialisieren. Dieser Befehl startet die Speicherverbindung neu und leitet sie über die richtige Schnittstelle weiter.
- Alternativ können `xe pif-forget` Sie die Schnittstelle aus der XenServer-Datenbank löschen und sie manuell in der Steuerdomäne konfigurieren. `xe pif-forget` ist eine erweiterte Option und erfordert, dass Sie mit der manuellen Konfiguration von Linux-Netzwerken vertraut sind.

SR-IOV-fähige NICs verwenden

Single Root I/O Virtualization (SR-IOV) ist eine Virtualisierungstechnologie, mit der ein einzelnes PCI-Gerät als mehrere PCI-Geräte auf dem physischen System angezeigt werden kann. Das eigentliche physische Gerät ist als physische Funktion (PF) bekannt, während die anderen als virtuelle Funktionen (VF) bekannt sind. Der Hypervisor kann einer virtuellen Maschine (VM) eine oder mehrere VFs zuweisen: Der Gast kann das Gerät dann so verwenden, als wäre es direkt zugewiesen.

Durch Zuweisen einer oder mehrerer NIC-VFs zu einer VM kann der Netzwerkverkehr den virtuellen Switch Bypass. Bei der Konfiguration verhält sich jede VM so, als würde sie die NIC direkt verwenden, wodurch der Verarbeitungsaufwand reduziert und die Leistung verbessert wird.

Vorteile von SR-IOV

Ein SR-IOV-VF hat eine bessere Leistung als VIF. Es kann die hardwarebasierte Trennung zwischen Datenverkehr von verschiedenen VMs über dieselbe Netzwerkkarte sicherstellen (unter Umgehung des XenServer-Netzwerkstapels).

Mit dieser Funktion können Sie:

- Aktivieren Sie SR-IOV auf NICs, die SR-IOV unterstützen.
- Deaktivieren Sie SR-IOV auf NICs, die SR-IOV unterstützen.
- Verwalten Sie SR-IOV-VFs als VF-Ressourcenpool.
- Weisen Sie SR-IOV-VFs einer VM zu.
- Konfigurieren Sie SR-IOV-VFs (z. B. MAC-Adresse, VLAN, Rate).
- Führen Sie Tests durch, um zu überprüfen, ob SR-IOV als Teil des automatisierten Zertifizierungskits unterstützt wird.

Konfiguration der Anlage

Konfigurieren Sie die Hardwareplattform korrekt, um SR-IOV zu unterstützen. Die folgenden Technologien sind erforderlich:

- I/O-MMU-Virtualisierung (AMD-VI und Intel VT-d)
- Alternative Routing-ID-Interpretation (ARI)
- Adressübersetzungsdienste (ATS)
- Zugriffssteuerungsdienste (ACS)

Informationen zur Konfiguration der Systemfirmware zur Aktivierung der genannten Technologien finden Sie in der Dokumentation, die Ihrem System beiliegt.

Ermöglichen eines SR-IOV-Netzwerks auf einer NIC

Verwenden Sie in XenCenter den Assistenten für **Neues Netzwerk** auf der Registerkarte **Netzwerk**, um ein SR-IOV-Netzwerk auf einer Netzwerkkarte zu erstellen und zu aktivieren.

Weisen Sie der virtuellen Schnittstelle ein SR-IOV-Netzwerk zu (VM-Ebene)

Verwenden Sie in XenCenter auf VM-Ebene den Assistenten zum **Hinzufügen einer virtuellen Schnittstelle** auf der Registerkarte **Netzwerk**, um ein SR-IOV-fähiges Netzwerk als virtuelle Schnittstelle für diese VM hinzuzufügen. Weitere Informationen finden Sie unter Neues Netzwerk hinzufügen.

Unterstützte NICs und Gäste

Eine Liste der unterstützten Hardwareplattformen und Netzwerkkarten finden Sie unter Hardwarekompatibilitätsliste. In der Dokumentation des Anbieters für einen bestimmten Gast erfahren Sie, ob er SR-IOV unterstützt.

Einschränkungen

- Für bestimmte Netzwerkkarten, die Legacy-Treiber verwenden (z. B. Intel I350-Familie), muss der Host neu gestartet werden, um SR-IOV auf diesen Geräten zu aktivieren oder zu deaktivieren.
- Ein SR-IOV-Netzwerk auf Poolebene mit unterschiedlichen NIC-Typen wird nicht unterstützt.
- Ein SR-IOV-VF und ein normaler VIF von derselben Netzwerkkarte können aufgrund der Einschränkungen der NIC-Hardware möglicherweise nicht miteinander kommunizieren. Damit diese virtuellen Maschinen kommunizieren können, stellen Sie sicher, dass die Kommunikation das Muster VF zu VF oder VIF zu VIF verwendet und nicht VF zu VIF.
- Die Quality of Service-Einstellungen für einige SR-IOV-VFs werden nicht wirksam, da sie keine Begrenzung der Netzwerkgeschwindigkeit unterstützen.
- Die Durchführung von Livemigration, Suspend und Checkpoint wird auf virtuellen Rechnern, die einen SR-IOV-VF verwenden, nicht unterstützt.
- SR-IOV-VFs unterstützen kein Hot-Plugging.
- SR-IOV-VFs unterstützen keinen Netzwerkstart.
- Bei einigen NICs mit älteren NIC-Treibern kann ein Neustart auch nach einem Neustart des Hosts erforderlich sein, was darauf hinweist, dass die Netzwerkkarte SR-IOV nicht aktivieren kann.

- Wenn Ihre VM über einen SR-IOV-VF verfügt, sind Funktionen, die eine Livemigration erfordern, nicht möglich. Dies liegt daran, dass die VM direkt an den physischen SR-IOV-fähigen NIC-VF gebunden ist.
- SR-IOV kann in einer Umgebung eingesetzt werden, die Hochverfügbarkeit nutzt. SR-IOV wird jedoch in der Kapazitätsplanung nicht berücksichtigt. VMs, denen SR-IOV-VFs zugewiesen sind, werden nach bestem Ermessen neu gestartet, wenn sich im Pool ein Host mit entsprechenden Ressourcen befindet. Zu diesen Ressourcen gehören SR-IOV-fähig im richtigen Netzwerk und eine kostenlose VF.
- SR-IOV-VFs werden mit dem PVS-Accelerator nicht unterstützt.

Konfigurieren von SR-IOV-VFs für Legacy-Treiber

In der Regel kann die maximale Anzahl von VFs, die eine NIC unterstützen kann, automatisch bestimmt werden. Für NICs, die Legacy-Treiber verwenden (z. B. Intel I350-Familie), ist der Grenzwert in der Treibermodul-Konfigurationsdatei definiert. Das Limit muss möglicherweise manuell angepasst werden. Um es auf das Maximum zu setzen, öffnen Sie die Datei mit einem Editor und ändern Sie die Zeile ab:

```
## VFs-maxvfs-by-user:
<!--NeedCopy-->
```

Um beispielsweise die maximale VFs auf 4 festzulegen, damit die `igb`-Treiberbearbeitung `/etc/modprobe.d/igb.conf` liest:

```
## VFs-param: max_vfs
## VFs-maxvfs-by-default: 7
## VFs-maxvfs-by-user: 4
options igb max_vfs=0
<!--NeedCopy-->
```

> **Hinweise:**
>
> - Der Wert muss kleiner oder gleich dem Wert in der Zeile sein `VFs-maxvfs-by-default`.
> - Ändern Sie keine andere Zeile in diesen Dateien.
> - Nehmen Sie die Änderungen vor, bevor Sie SR-IOV aktivieren.

CLI

Unter SR-IOV-Befehle finden Sie CLI-Anweisungen zum Erstellen, Löschen, Anzeigen von SR-IOV-Netzwerken und Zuweisen eines SR-IOV-VF zu einer VM.

Steuern Sie die Rate der ausgehenden Daten (QoS)

Um die Menge der *ausgehenden* Daten zu begrenzen, die eine VM pro Sekunde senden kann, legen Sie einen optionalen Quality of Service (QoS) -Wert für virtuelle VM-Schnittstellen (VIFs) fest. Mit dieser Einstellung können Sie eine maximale Übertragungsrate für ausgehende Pakete in *Kilobyte* pro Sekunde angeben.

Der Quality of Service-Wert begrenzt die Übertragungsrate *von* der VM. Die Einstellung Quality of Service schränkt die Datenmenge, die die VM empfangen kann, nicht ein. Wenn ein solches Limit erwünscht ist, empfehlen wir, die Rate eingehender Pakete weiter oben im Netzwerk zu begrenzen (z. B. auf Switch-Ebene).

Abhängig vom im Pool konfigurierten Netzwerkstapel können Sie den Wert Quality of Service auf virtuellen VM-Schnittstellen (VIFs) an einer von zwei Stellen festlegen. Sie können diesen Wert entweder mit der xe CLI oder in XenCenter festlegen.

- **XenCenter** Sie können den Grenzwert für die Quality of Service-Übertragungsrate im Eigenschaftendialogfeld der virtuellen Schnittstelle festlegen.
- **xe-Befehle** Sie können die Quality of Service-Übertragungsrate über die CLI mithilfe der Befehle im folgenden Abschnitt festlegen.

Beispiel eines CLI-Befehls für QoS

Um eine VIF über die CLI auf eine maximale Übertragungsrate von 100 Kilobyte pro Sekunde zu beschränken, verwenden Sie den Befehl `vif-param-set`:

```
xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der Parameter `kbps` gibt *Kilobyte* pro Sekunde (Kbps) an, nicht Kilobit pro Sekunde (kbps).

Ändern der Netzwerkkonfigurationsoptionen

In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkkonfiguration Ihres XenServer-Hosts ändern. Folgendes ist eingeschlossen:

- Änderung des Hostnamens (d. h. des Domain Name System (DNS) -Namens)
- Hinzufügen oder Löschen von DNS-Servern
- IP-Adressen ändern

- Ändern der Netzwerkkarte, die als Verwaltungsschnittstelle verwendet wird
- Hinzufügen einer neuen physischen Netzwerkkarte zum Server
- Hinzufügen eines Zwecks zu einem Netzwerk
- ARP-Filterung aktivieren (Switch-Port-Sperrung)

Hostname

Der System-Hostname, auch als Domain- oder DNS-Name bekannt, wird in der poolweiten Datenbank definiert und mit dem CLI-Befehl `xe host-set-hostname-live`wie folgt geändert:

```
xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
<!--NeedCopy-->
```

Der zugrunde liegende Hostname der Steuerdomäne ändert sich dynamisch, um den neuen Hostnamen wiederzugeben.

DNS-Server

Verwenden Sie den `pif-reconfigure-ip` Befehl, um DNS-Server in der IP-Adressierungskonfiguration des XenServer-Hosts hinzuzufügen oder zu löschen. Zum Beispiel für ein PIF mit einer statischen IP:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip IP=IP
   netmask=netmask
<!--NeedCopy-->
```

Ändern der IP-Adresskonfiguration für einen eigenständigen Host

Sie können die xe-CLI verwenden, um die Konfiguration der Netzwerkschnittstelle zu ändern. Ändern Sie die zugrunde liegenden Netzwerkkonfigurationsskripte nicht direkt.

Um die IP-Adresskonfiguration eines PIF zu ändern, verwenden Sie den CLI-Befehl `pif-reconfigure-ip`. Einzelheiten zu den Parametern des Befehls `pif-reconfigure-ip` finden Sie unter `pif-reconfigure-ip`. Im folgenden Abschnitt finden Sie Informationen zum Ändern von Host-IP-Adressen in Ressourcenpools.

Ändern der IP-Adresskonfiguration in Ressourcenpools

XenServer-Hosts in Ressourcenpools haben eine einzige Management-IP-Adresse, die für die Verwaltung und Kommunikation mit und von anderen Hosts im Pool verwendet wird. Die Schritte, die zum

Ändern der IP-Adresse der Verwaltungsschnittstelle eines Hosts erforderlich sind, unterscheiden sich für Poolkoordinator und andere Hosts.

> **Hinweis:**
>
> Sie müssen vorsichtig sein, wenn Sie die IP-Adresse eines Hosts und andere Netzwerkparameter ändern. Abhängig von der Netzwerktopologie und den vorgenommenen Änderungen können Verbindungen zum Netzwerkspeicher verloren gehen. In diesem Fall muss der Speicher mit der Funktion **Speicher reparieren** in XenCenter oder mit dem CLI-Befehl `pbd-plug` neu angeschlossen werden. Aus diesem Grund empfehlen wir, dass Sie virtuelle Maschinen vom Host weg migrieren, bevor Sie die IP-Konfiguration ändern.

Verwenden Sie den CLI-Befehl `pif-reconfigure-ip`, um die IP-Adresse wie gewünscht festzulegen. Einzelheiten zu den Parametern des Befehls `pif-reconfigure-ip` finden Sie unter `pif-reconfigure-ip`.

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
<!--NeedCopy-->
```

Verwenden Sie den `host-list` CLI-Befehl, um zu bestätigen, dass der Mitgliedshost erfolgreich wieder eine Verbindung zum Poolkoordinator hergestellt hat, indem Sie überprüfen, ob alle anderen XenServer-Hosts im Pool sichtbar sind:

```
xe host-list
<!--NeedCopy-->
```

Das Ändern der IP-Adresse des Poolkoordinator-XenServer-Hosts erfordert zusätzliche Schritte. Dies liegt daran, dass jedes Poolmitglied die angekündigte IP-Adresse des Poolkoordinators für die Kommunikation verwendet. Die Poolmitglieder wissen nicht, wie sie den Poolkoordinator kontaktieren sollen, wenn sich seine IP-Adresse ändert.

Verwenden Sie nach Möglichkeit eine dedizierte IP-Adresse, die sich während der gesamten Lebensdauer des Pools für Poolkoordinatoren wahrscheinlich nicht ändern wird.

Verwenden Sie den CLI-Befehl `pif-reconfigure-ip`, um die IP-Adresse wie gewünscht festzulegen:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
<!--NeedCopy-->
```

Wenn sich die IP-Adresse des Poolkoordinators ändert, wechseln alle Mitgliedshosts in einen Notfallmodus, wenn sie den Poolkoordinator nicht kontaktieren können.

Verwenden Sie auf dem Poolkoordinator den Befehl `pool-recover-slaves`, um den Poolkoordinator zu zwingen, jedes Poolmitglied zu kontaktieren und es über die neue IP-Adresse des Poolkoordinators zu informieren:


```
xe pool-recover-slaves
<!--NeedCopy-->
```

Verwaltungsoberfläche

Wenn Sie XenServer auf einem Host installieren, wird eine seiner NICs als *Verwaltungsschnittstelle bestimmt: die NIC, die für den XenServer-Verwaltungsverkehr*verwendet wird. Die Verwaltungsschnittstelle wird für XenCenter-Verbindungen zum Host (z. B. Citrix Virtual Apps and Desktops) und für die Host-zu-Host-Kommunikation verwendet.

Verwenden Sie den Befehl `pif-list`, um zu ermitteln, welcher PIF der NIC entspricht, die als Verwaltungsschnittstelle verwendet werden soll. Die UUID jedes PIF wird zurückgegeben.

```
xe pif-list
<!--NeedCopy-->
```

Verwenden Sie den Befehl `pif-param-list`, um die IP-Adressierungskonfiguration für den PIF zu überprüfen, der für die Verwaltungsschnittstelle verwendet wird. Verwenden Sie ggf. den Befehl `pif-reconfigure-ip`, um die IP-Adressierung für den zu verwendenden PIF zu konfigurieren.

```
xe pif-param-list uuid=pif_uuid
<!--NeedCopy-->
```

Verwenden Sie den CLI-Befehl `host-management-reconfigure`, um die für die Verwaltungsschnittstelle verwendete PIF zu ändern. Wenn dieser Host Teil eines Ressourcenpools ist, *muss dieser Befehl auf der Mitgliedshost-Konsole ausgegeben werden*:

```
xe host-management-reconfigure pif-uuid=pif_uuid
<!--NeedCopy-->
```

Verwenden Sie den Befehl `network-list`, um zu ermitteln, welche PIF der Netzwerkkarte entspricht, die als Verwaltungsschnittstelle für alle Hosts im Pool verwendet werden soll. Die UUID des poolweiten Netzwerks wird zurückgegeben.

```
xe network-list
<!--NeedCopy-->
```

Verwenden Sie den Befehl `network-param-list`, um die PIF-UUIDs aller Hosts im Pool abzurufen. Verwenden Sie den Befehl `pif-param-list`, um die IP-Adressierungskonfiguration für das PIF für die Verwaltungsschnittstelle zu überprüfen. Verwenden Sie ggf. den Befehl `pif-reconfigure-ip`, um die IP-Adressierung für den zu verwendenden PIF zu konfigurieren.

```
xe pif-param-list uuid=pif_uuid
<!--NeedCopy-->
```


Verwenden Sie den CLI-Befehl `pool-management-reconfigure`, um die PIF zu ändern, die für die in der Liste Netzwerke aufgeführte Verwaltungsschnittstelle verwendet wird.

```
xe pool-management-reconfigure network-uuid=network_uuid
<!--NeedCopy-->
```

Verwendung von Port 80 beschränken

Sie können entweder HTTPS über Port 443 oder HTTP über Port 80 verwenden, um mit XenServer zu kommunizieren. Aus Sicherheitsgründen können Sie den TCP-Port 80 auf der Verwaltungsschnittstelle schließen. Standardmäßig ist Port 80 immer noch geöffnet. Wenn Sie es schließen, müssen alle externen Clients, die die Verwaltungsschnittstelle verwenden, HTTPS über Port 443 verwenden, um eine Verbindung zu XenServer herzustellen. Bevor Sie jedoch Port 80 schließen, überprüfen Sie, ob alle Ihre API-Clients (insbesondere Citrix Virtual Apps and Desktops) HTTPS über Port 443 verwenden können.

Informationen zum Schließen von Port 80 finden Sie unter `https-only` xe CLI-Befehl.

Deaktivieren des Verwaltungszugriffs

Verwenden Sie den CLI-Befehl `host-management-disable`, um den Remotezugriff auf die Verwaltungskonsole vollständig zu deaktivieren.

> **Warnung:**
>
> Wenn die Verwaltungsschnittstelle deaktiviert ist, müssen Sie sich auf der physischen Host-Konsole anmelden, um Verwaltungsaufgaben ausführen zu können. Externe Schnittstellen wie XenCenter funktionieren nicht, wenn die Verwaltungsschnittstelle deaktiviert ist.

Fügen Sie eine neue physische Netzwerkkarte hinzu

1. Installieren Sie wie gewohnt eine neue physische Netzwerkkarte auf Ihrem XenServer-Host.
2. Starten Sie Ihren XenServer-Host neu.
3. Listen Sie alle physischen Netzwerkkarten für diesen XenServer-Host auf, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list host-uuid=<host_uuid>
   ```

4. Wenn Sie die zusätzliche Netzwerkkarte nicht sehen, suchen Sie mit dem folgenden Befehl nach neuen physischen Schnittstellen:

   ```
   xe pif-scan host-uuid=<host_uuid>
   ```


Mit diesem Befehl wird ein neues PIF-Objekt für die neue NIC erstellt.

5. Führen Sie die physischen Netzwerkkarten auf dem XenServer-Host erneut auf, um sicherzustellen, dass die neue Netzwerkkarte sichtbar ist:

```
xe pif-list host-uuid=<host_uuid>
```

6. Die neue PIF wird anfänglich als nicht verbunden (`currently-attached ( RO): false`) aufgeführt. Verwenden Sie den folgenden Befehl, um es aufzurufen:

```
xe pif-plug uuid=<uuid_of_pif>
```

Alternativ können Sie XenCenter verwenden, um erneut nach neuen Netzwerkkarten zu suchen. Weitere Informationen finden Sie unter Konfiguration von Netzwerkkarten in der XenCenter-Dokumentation.

Entfernen einer physischen Netzwerkkarte

Stellen Sie vor dem Entfernen der Netzwerkkarte sicher, dass Sie die UUID des entsprechenden PIF kennen. Entfernen Sie die physische Netzwerkkarte wie gewohnt von Ihrem XenServer-Host. Führen Sie nach dem Neustart des Hosts den XE-CLI-Befehl aus, `pif-forget uuid=<UUID>` um das PIF-Objekt zu zerstören.

Hinzufügen eines Zwecks zu einem Netzwerk

Der Netzwerkzweck kann verwendet werden, um einem Netzwerk zusätzliche Funktionen hinzuzufügen. Zum Beispiel die Möglichkeit, das Netzwerk zu verwenden, um NBD-Verbindungen herzustellen.

Verwenden Sie den`xe network-param-add` folgenden Befehl, um einen Netzwerkzweck hinzuzufügen:

```
xe network-param-add param-name=purpose param-key=purpose uuid=network-
    uuid
<!--NeedCopy-->
```

Verwenden Sie den`xe network-param-remove` folgenden Befehl, um einen Netzwerkzweck zu löschen:

```
xe network-param-remove param-name=purpose param-key=purpose uuid=
    network-uuid
<!--NeedCopy-->
```

Derzeit sind die verfügbaren Werte für den Netzwerkzweck `nbd` und `insecure_nbd`. Weitere Informationen finden Sie im XenServer Changed Block Tracking Guide.

Switch Port-Verriegelung verwenden

Mit der XenServer-Switchport-Sperrfunktion können Sie den Datenverkehr kontrollieren, der von unbekannten, nicht vertrauenswürdigen oder potenziell feindlichen VMs gesendet wird, indem Sie deren Fähigkeit einschränken, so zu tun, als hätten sie eine MAC- oder IP-Adresse, die ihnen nicht zugewiesen wurde. Sie können die Befehle zum Sperren von Ports verwenden, um standardmäßig den gesamten Datenverkehr in einem Netzwerk zu blockieren oder bestimmte IP-Adressen zu definieren, von denen eine einzelne VM Datenverkehr senden darf.

Die Switch-Port-Sperrung ist eine Funktion, die für öffentliche Cloud-Dienstanbieter in Umgebungen entwickelt wurde, die sich mit internen Bedrohungen befassen. Diese Funktion unterstützt öffentliche Cloud-Dienstanbieter mit einer Netzwerkarchitektur, in der jede VM über eine öffentliche, mit dem Internet verbundene IP-Adresse verfügt. Da Cloud-Mandanten nicht vertrauenswürdig sind, können Sie Sicherheitsmaßnahmen wie den Spoofing-Schutz verwenden, um sicherzustellen, dass Mandanten andere virtuelle Maschinen in der Cloud nicht angreifen können.

Durch die Verwendung der Switch-Port-Sperrung können Sie Ihre Netzwerkkonfiguration vereinfachen, indem Sie allen Ihren Mandanten oder Gästen ermöglichen, dasselbe Layer-2-Netzwerk zu verwenden.

Eine der wichtigsten Funktionen der Port-Locking-Befehle ist, dass sie den Datenverkehr einschränken können, den ein nicht vertrauenswürdiger Gast sendet. Dies schränkt die Fähigkeit des Gastes ein, so zu tun, als hätte er eine MAC- oder IP-Adresse, die er nicht wirklich besitzt. Insbesondere können Sie diese Befehle verwenden, um zu verhindern, dass ein Gast:

- Anspruch auf eine andere als die vom XenServer-Administrator angegebene IP- oder MAC-Adresse geltend machen, die er verwenden kann
- Abfangen, Spoofing oder Unterbrechen des Datenverkehrs anderer VMs

Anforderungen

- Die XenServer-Switch-Port-Sperrfunktion wird auf den Linux Bridge- und vSwitch-Netzwerkstapeln unterstützt.
- Wenn Sie die rollenbasierte Zugriffssteuerung (RBAC) in Ihrer Umgebung aktivieren, muss der Benutzer, der die Switch-Port-Sperrung konfiguriert, mit einem Konto angemeldet sein, das mindestens eine Pool-Operator- oder Pool-Admin-Rolle hat. Wenn RBAC in Ihrer Umgebung nicht aktiviert ist, muss der Benutzer mit dem Root-Konto für den Poolkoordinator angemeldet sein.
- Wenn Sie die Switch-Port-Sperrbefehle ausführen, können Netzwerke online oder offline sein.
- Bei Windows-Gästen wird das Symbol für getrennte Netzwerke nur angezeigt, wenn die XenServer VM Tools auf dem Gast installiert sind.

Hinweise Ohne Switch-Port-Sperrkonfigurationen sind VIFs auf "network_default"und Netzwerke auf "unlocked"gesetzt.

Die Konfiguration der Switch-Port-Sperrung wird nicht unterstützt, wenn Controller von Drittanbietern in der Umgebung verwendet werden.

Das Sperren von Switch-Ports verhindert nicht, dass Cloud-Mandanten:

- Durchführen eines Angriffs auf IP-Ebene auf einen anderen Mandanten/Benutzer. Die Switch-Port-Sperre verhindert jedoch, dass sie den Angriff auf IP-Ebene ausführen, wenn sie versuchen, dies auf folgende Weise zu tun, und die Switch-Port-Sperre konfiguriert ist: a) die Identität eines anderen Mandanten in der Cloud oder eines anderen Benutzers oder b) das Abfangen des für einen anderen Benutzer bestimmten Datenverkehrs.
- Erschöpfende Netzwerkressourcen.
- Empfang von Datenverkehr, der für andere virtuelle Maschinen bestimmt ist, durch normales Switch-Flutverhalten (für Broadcast-MAC-Adressen oder unbekannte Ziel-MAC-Adressen)

Ebenso schränkt die Switch-Port-Sperrung nicht ein, wohin eine VM Datenverkehr senden kann.

Hinweise zur Umsetzung Sie können die Switch-Port-Sperrfunktion entweder über die Befehlszeile oder die XenServer-API implementieren. In großen Umgebungen, in denen die Automatisierung ein Hauptanliegen ist, ist die typischste Implementierungsmethode jedoch die Verwendung der API.

Beispiele In diesem Abschnitt finden Sie Beispiele dafür, wie das Sperren von Switch-Ports bestimmte Arten von Angriffen verhindern kann. In diesen Beispielen ist VM-c eine virtuelle Maschine, die ein feindlicher Mandant (Tenant C) least und für Angriffe verwendet. VM-a und VM-b sind virtuelle Maschinen, die von nicht angreifenden Mandanten geleast werden.

Beispiel 1: Wie das Sperren von Switch-Ports die ARP-Spoofing-Verhinderung verhindern kann:

ARP-Spoofing wird verwendet, um auf die Versuche eines Angreifers hinzuweisen, seine MAC-Adresse mit der IP-Adresse eines anderen Knotens zu verknüpfen. ARP-Spoofing kann möglicherweise dazu führen, dass der Datenverkehr des Knotens stattdessen an den Angreifer gesendet wird. Um dieses Ziel zu erreichen, sendet der Angreifer gefälschte (gefälschte) ARP-Nachrichten an ein Ethernet-LAN.

Szenario:

Virtuelle Maschine A (VM-a) möchte IP-Verkehr von VM-a zur virtuellen Maschine B (VM-b) senden, indem sie ihn an die IP-Adresse von VM-b adressiert. Der Besitzer von Virtual Machine C möchte ARP-Spoofing verwenden, um so zu tun, als wäre seine VM, VM-c, tatsächlich VM-b.

1. VM-c sendet einen spekulativen Stream von ARP-Antworten an VM-a. In den ARP-Antworten wird behauptet, dass die MAC-Adresse in der Antwort (c_Mac) mit der IP-Adresse b_IP verknüpft ist

   Ergebnis: Da der Administrator die Switch-Port-Sperrung aktiviert hat, werden diese Pakete alle verworfen, da die Aktivierung der Switch-Port-Sperrung den Identitätswechsel verhindert.

2. VM-b sendet eine ARP-Antwort an VM-a und behauptet, dass die MAC-Adresse in der Antwort (b_Mac) mit der IP-Adresse b_IP verknüpft ist.

   Ergebnis: VM-a empfängt die ARP-Antwort von VM-b.

Beispiel 2: IP-Spoofing-Verhinderung:

IP-Adress-Spoofing ist ein Prozess, der die Identität von Paketen verbirgt, indem Internetprotokoll-Pakete (IP) mit einer gefälschten Quell-IP-Adresse erstellt werden.

Szenario:

Mandant C versucht, einen Denial-of-Service-Angriff durchzuführen, indem er seinen Host, Host-C, auf einem Remote-System verwendet, um seine Identität zu verschleiern.

Versuch 1:

Mandant C setzt die IP-Adresse und MAC-Adresse von Host-C auf die IP- und MAC-Adressen von VM-A (a_IP und a_Mac). Mandant C weist Host-C an, IP-Verkehr an ein Remote-System zu senden.

Ergebnis: Die Host-C-Pakete werden verworfen. Das liegt daran, dass der Administrator die Switch-Port-Sperrung aktiviert hat Die Host-C-Pakete werden verworfen, da die Aktivierung der Switch-Port-Sperrung den Identitätswechsel verhindert.

Versuch 2:

Mandant C setzt die IP-Adresse von Host-C auf die IP-Adresse von VM-A (a_IP) und behält ihren ursprünglichen c_Mac bei.

Mandant C weist Host-C an, IP-Verkehr an ein Remote-System zu senden.

Ergebnis: Die Host-C-Pakete werden verworfen. Dies liegt daran, dass der Administrator die Switch-Port-Sperrung aktiviert hat, wodurch Identitätswechsel verhindert werden.

Beispiel 3: Webhosting:

Szenario:

Alice ist Infrastrukturadministratorin.

Einer ihrer Mandanten, Mandant B, hostet mehrere Websites von seiner VM “VM-b”aus. Jede Website benötigt eine eigene IP-Adresse, die auf derselben virtuellen Netzwerkschnittstelle (VIF) gehostet wird.

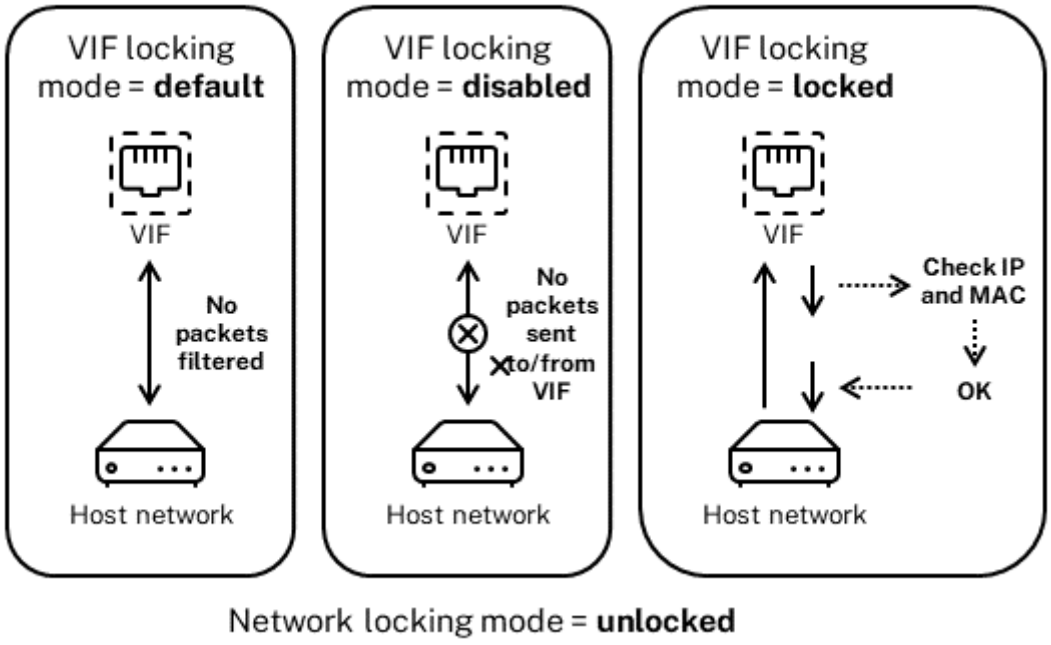
Alice konfiguriert das VIF von Host-B neu, sodass es an einen einzigen MAC, aber viele IP-Adressen gebunden ist.

So funktioniert die Switch-Port-Verriegelung Mit der Switch-Port-Sperrfunktion können Sie die Paketfilterung auf einer oder mehreren von zwei Ebenen steuern:

- **VIF-Ebene**. Die Einstellungen, die Sie im VIF konfigurieren, legen fest, wie Pakete gefiltert werden. Sie können das VIF so einstellen, dass verhindert wird, dass die VM Datenverkehr sendet, das VIF so einschränken, dass es nur Datenverkehr mit der zugewiesenen IP-Adresse senden kann, oder der VM erlauben, Datenverkehr an eine beliebige IP-Adresse im Netzwerk zu senden, die mit dem VIF verbunden ist.
- **Netzwerk-Ebene**. Das XenServer-Netzwerk bestimmt, wie Pakete gefiltert werden. Wenn der Sperrmodus eines VIF auf eingestellt ist `network_default`, bezieht er sich auf die Sperreinstellung auf Netzwerkebene, um zu bestimmen, welcher Datenverkehr zugelassen werden soll.

Unabhängig davon, welchen Netzwerkstapel Sie verwenden, funktioniert die Funktion auf dieselbe Weise. Wie in den folgenden Abschnitten ausführlicher beschrieben, unterstützt die Linux-Brücke jedoch die Switch-Port-Sperrung in IPv6 nicht vollständig.

VIF-Sperrmodus-Zustände Die XenServer-Switchport-Sperrfunktion bietet einen Sperrmodus, mit dem Sie VIFs in vier verschiedenen Zuständen konfigurieren können. Diese Zustände gelten nur, wenn das VIF an eine laufende virtuelle Maschine angeschlossen ist.



- **network_default**. Wenn der Status der VIF auf festgelegt ist, verwendet XenServer den `default-locking-mode` Netzwerkparameter `network_default`, um zu bestimmen, ob und wie Pakete gefiltert werden sollen, die über die VIF übertragen werden. Das Verhalten hängt davon ab, ob für das zugehörige Netzwerk der Standard-Sperrmodus des Netzwerks auf Deaktiviert oder entsperrt eingestellt ist:

  -`default-locking-mode=disabled`, XenServer wendet eine Filterregel an, sodass die VIF den gesamten Datenverkehr verwirft.

  -`default-locking-mode`=freigeschaltet, XenServer entfernt alle mit der VIF verknüpften Filterregeln. Standardmäßig ist der Standard-Sperrmodus Parameter auf `unlocked` eingestellt.

  Informationen zum Parameter `default-locking-mode` finden Sie unter Netzwerkbefehle.

  Der standardmäßige Sperrmodus des Netzwerks hat keine Auswirkung auf angeschlossene VIFs, deren Sperrzustand etwas anderes ist als `network_default`.

  > **Hinweis:**
  >
  > Sie können `default-locking-mode` für ein Netzwerk, an das aktive VIFs angeschlossen sind, nicht ändern.

- **Gesperrt**. XenServer wendet Filterregeln an, sodass nur Datenverkehr, der zu/von den angegebenen MAC- und IP-Adressen gesendet wird, über die VIF gesendet werden darf. Wenn in diesem Modus keine IP-Adressen angegeben sind, kann die VM keinen Datenverkehr über dieses VIF in diesem Netzwerk senden.

  Um die IP-Adressen anzugeben, von denen die VIF Datenverkehr akzeptiert, verwenden Sie die IPv4- oder IPv6-IP-Adressen mit den Parametern `ipv4_allowed` oder `ipv6_allowed`. Wenn Sie jedoch die Linux-Brücke konfiguriert haben, geben Sie keine IPv6-Adressen ein.

  Mit XenServer können Sie IPv6-Adressen eingeben, wenn die Linux-Bridge aktiv ist. XenServer kann jedoch nicht auf der Grundlage der eingegebenen IPv6-Adressen filtern. Der Grund dafür ist, dass die Linux-Brücke keine Module zum Filtern von NDP-Paketen (NDP) hat. Daher kann kein vollständiger Schutz implementiert werden, und Gäste können sich als ein anderer Gast ausgeben, indem sie NDP-Pakete fälschen. Wenn Sie also auch nur eine IPv6-Adresse angeben, lässt XenServer den gesamten IPv6-Verkehr die VIF passieren. Wenn Sie keine IPv6-Adressen angeben, lässt XenServer keinen IPv6-Verkehr an die VIF weiterleiten.

- **Freigeschaltet**. Der gesamte Netzwerkverkehr kann das VIF durchlaufen. Das heißt, es werden keine Filter auf Datenverkehr angewendet, der zum oder vom VIF geht.

- **Deaktiviert**. Es darf kein Verkehr durch das VIF fließen. (Das heißt, XenServer wendet eine Filterregel an, sodass die VIF den gesamten Datenverkehr verwirft.)

Konfigurieren der Switch-Port- In diesem Abschnitt werden drei verschiedene Verfahren beschrieben:

- Beschränken Sie VIFs auf die Verwendung einer bestimmten IP-Adresse
- Fügen Sie eine IP-Adresse zu einer vorhandenen Liste mit eingeschränkten Rechten hinzu. Zum Beispiel, um einer VIF eine IP-Adresse hinzuzufügen, wenn die VM läuft und mit dem Netzwerk verbunden ist (z. B. wenn Sie ein Netzwerk vorübergehend offline schalten).
- Entfernen einer IP-Adresse aus einer vorhandenen Liste mit eingeschränkten Rechten

Wenn der Sperrmodus eines VIF auf `locked` eingestellt ist, können nur die Adressen verwendet werden, die in den Parametern `ipv4-allowed` oder `ipv6-allowed` angegeben sind.

Da VIFs in einigen relativ seltenen Fällen mehr als eine IP-Adresse haben können, ist es möglich, mehrere IP-Adressen für ein VIF anzugeben.

Sie können diese Verfahren ausführen, bevor oder nachdem das VIF angeschlossen wurde (oder die VM gestartet wurde).

Ändern Sie den Standardsperrmodus in gesperrt, falls dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

```
1 xe vif-param-set uuid=vif-uuid locking-mode=locked
2 <!--NeedCopy-->
```

`vif-uuid` stellt die UUID der VIF dar, die Sie zum Senden von Datenverkehr zulassen möchten. Um die UUID zu erhalten, führen Sie den xe-Befehl `vif-list` auf dem Host aus. `vm-uuid` Zeigt die virtuelle Maschine an, für die die Informationen angezeigt werden. Die Geräte-ID zeigt die Gerätenummer des VIF an.

Führen Sie den Befehl `vif-param-set` aus, um die IP-Adressen anzugeben, von denen die virtuelle Maschine Datenverkehr senden kann. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Geben Sie ein oder mehrere IPv4-IP-Adressen-Ziele an. Beispiel:

```
1 xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list
     of ipv4-addresses
2 <!--NeedCopy-->
```

- Geben Sie ein oder mehrere IPv6-IP-Adressen-Ziele an. Beispiel:

```
1 xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list
     of ipv6-addresses
2 <!--NeedCopy-->
```

Sie können mehrere IP-Adressen angeben, indem Sie sie durch ein Komma trennen, wie im vorherigen Beispiel gezeigt.

Nachdem Sie das Verfahren zum Beschränken eines VIF auf die Verwendung einer bestimmten IP-Adresse ausgeführt haben, können Sie eine oder mehrere IP-Adressen hinzufügen, die das VIF verwenden kann.

Führen Sie den Befehl `vif-param-add` aus, um die IP-Adressen zur vorhandenen Liste hinzuzufügen. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Geben Sie die IPv4-IP-Adresse an. Beispiel:

```
xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list
   of ipv4-addresses
<!--NeedCopy-->
```

- Geben Sie die IPv6-IP-Adresse an. Beispiel:

```
xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list
   of ipv6-addresses
<!--NeedCopy-->
```

Wenn Sie ein VIF auf die Verwendung von zwei oder mehr IP-Adressen beschränken, können Sie eine dieser IP-Adressen aus der Liste löschen.

Führen Sie den Befehl `vif-param-remove` aus, um die IP-Adressen aus der vorhandenen Liste zu löschen. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Geben Sie die zu löschende IPv4-IP-Adresse an. Beispiel:

```
xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated
   list of ipv4-addresses
<!--NeedCopy-->
```

- Geben Sie die zu löschende IPv6-IP-Adresse an. Beispiel:

```
xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated
   list of ipv6-addresses
<!--NeedCopy-->
```

Verhindern, dass eine virtuelle Maschine Datenverkehr von einem bestimmten Netzwerk sendet oder empfängt Das folgende Verfahren verhindert, dass eine virtuelle Maschine über eine bestimmte VIF kommuniziert. Wenn eine VIF eine Verbindung zu einem bestimmten XenServer-Netzwerk herstellt, können Sie mit diesem Verfahren verhindern, dass eine virtuelle Maschine Datenverkehr von einem bestimmten Netzwerk sendet oder empfängt. Dies bietet eine detailliertere Steuerung als die Deaktivierung eines gesamten Netzwerks.

Wenn Sie den CLI-Befehl verwenden, müssen Sie das VIF nicht trennen, um den Sperrmodus des VIF einzustellen. Der Befehl ändert die Filterregeln, während das VIF ausgeführt wird. In diesem Fall scheint die Netzwerkverbindung immer noch vorhanden zu sein, jedoch verwirft das VIF alle Pakete, die die VM zu senden versucht.

> **Tipp:**
>
> Um die UUID einer VIF zu finden, führen Sie den xe-Befehl `vif-list` auf dem Host aus. Die Geräte-ID zeigt die Gerätenummer des VIF an.

Um zu verhindern, dass ein VIF Datenverkehr empfängt, deaktivieren Sie das mit dem Netzwerk verbundene VIF, von dem aus Sie verhindern möchten, dass die VM Datenverkehr empfängt:

```
xe vif-param-set uuid=vif-uuid locking-mode=disabled
<!--NeedCopy-->
```

Sie können die VIF auch in XenCenter deaktivieren, indem Sie auf der Registerkarte Netzwerk der VM die virtuelle Netzwerkschnittstelle auswählen und auf Deaktivieren klicken.

Aufhebung der Beschränkung eines VIF auf eine IP-Adresse Gehen Sie wie folgt vor, um zum standardmäßigen (ursprünglichen) Sperrmoduszustand zurückzukehren. Wenn Sie eine VIF erstellen, konfiguriert XenServer sie standardmäßig so, dass sie nicht auf die Verwendung einer bestimmten IP-Adresse beschränkt ist.

Um eine VIF in einen entsperrten Zustand zurückzusetzen, ändern Sie den Standardsperrmodus der VIF in “Entsperrt”. Wenn dieser Modus nicht bereits verwendet wird, führen Sie den folgenden Befehl aus:

```
xe vif-param-set uuid=vif_uuid locking-mode=unlocked
<!--NeedCopy-->
```

Vereinfachte Konfiguration des VIF-Sperrmodus in der Cloud Anstatt die Befehle für den VIF-Sperrmodus für jedes VIF auszuführen, können Sie sicherstellen, dass alle VIFs standardmäßig deaktiviert sind. Um dies zu tun, müssen Sie die Paketfilterung auf Netzwerkebene ändern. Wenn Sie die Paketfilterung ändern, bestimmt das XenServer-Netzwerk, wie Pakete gefiltert werden, wie im vorherigen Abschnitt *So funktioniert Switch-Port-Sperren*beschrieben.

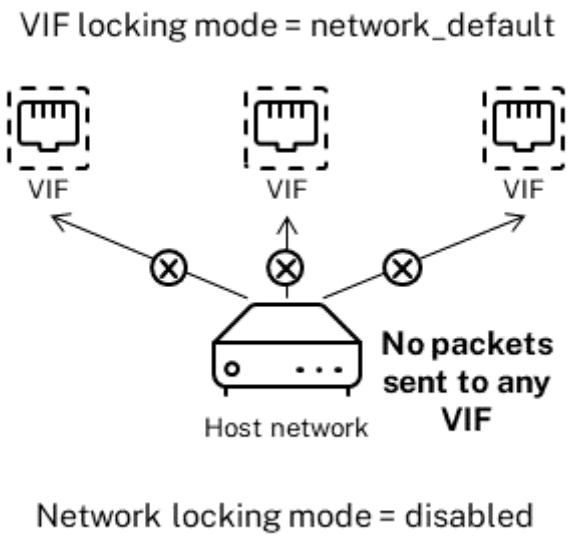
Insbesondere bestimmt die Einstellung **`default`**`-locking-mode` eines Netzwerks, wie sich neue VIFs mit Standardeinstellungen verhalten. Wann immer `locking-mode` für VIF auf **`default`** eingestellt ist, bezieht sich das VIF auf den Netzwerksperrmodus (**`default`**`-locking-mode`), um zu bestimmen, ob und wie Pakete gefiltert werden, die durch das VIF übertragen werden:

- **Freigeschaltet**. Wenn der **`default`**`-locking-mode` Netzwerkparameter auf gesetzt ist `unlocked`, ermöglicht XenServer der VM, Datenverkehr an jede IP-Adresse im Netzwerk zu senden, mit der die VIF eine Verbindung herstellt.
- **Deaktiviert**. Wenn der **`default`**`-locking-mode` Parameter auf gesetzt ist `disabled`, wendet XenServer eine Filterregel an, sodass die VIF den gesamten Datenverkehr verwirft.

Standardmäßig ist **default**-locking-mode für alle Netzwerke, die in XenCenter erstellt wurden und die CLI verwenden, auf unlocked festgelegt.

Indem Sie den Sperrmodus des VIF auf den Standardwert (network_default) setzen, können Sie eine grundlegende Standardkonfiguration (auf Netzwerkebene) für alle neu erstellten VIFs erstellen, die eine Verbindung zu einem bestimmten Netzwerk herstellen.

Diese Abbildung zeigt, wie die VIF **default**-locking-mode für das Netzwerk verwendet, um sein Verhalten zu bestimmen, wenn locking-mode für die VIF auf die Standardeinstellung (network_default) eingestellt ist.



Beispielsweise werden VIFs standardmäßig mit der Einstellung locking-mode auf network_default erstellt. Wenn Sie das **default**-locking-mode= eines Netzwerks festlegen disabled, werden alle neuen VIFs, für die Sie den Sperrmodus nicht konfiguriert haben, deaktiviert. Die VIFs bleiben deaktiviert, bis Sie entweder (a) den Parameter locking-mode des einzelnen VIF ändern oder (b) die locking-mode der VIFs explizit auf “entsperrt”setzen. Dies ist hilfreich, wenn Sie einer bestimmten VM genug vertrauen, sodass Sie ihren Datenverkehr überhaupt nicht filtern möchten.

So ändern Sie die Standardeinstellung für den Sperrmodus eines Netzwerks:

Ändern Sie nach dem Erstellen des Netzwerks den Standardsperrmodus, indem Sie den folgenden Befehl ausführen:

```
1 xe network-param-set uuid=network-uuid default-locking-mode=[unlocked|
     disabled]
2 <!--NeedCopy-->
```


> **Hinweis:**
>
> Um die UUID für ein Netzwerk abzurufen, führen Sie den xe-Befehl `network-list` aus. Dieser Befehl zeigt die UUIDs für alle Netzwerke auf dem Host an, auf dem Sie den Befehl ausgeführt haben.

So überprüfen Sie die Standardeinstellung für den Sperrmodus eines Netzwerks:

Führen Sie einen der folgenden Befehle aus:

```
xe network-param-get uuid=network-uuid param-name=default-locking-mode
<!--NeedCopy-->
```

ODER

```
xe network-list uuid=network-uuid params=default-locking-mode
<!--NeedCopy-->
```

Netzwerkeinstellungen für die Filterung des VIF-Datenverkehrs verwenden Das folgende Verfahren weist eine VIF auf einer virtuellen Maschine an, die **`default`**`-locking-mode` XenServer-Netzwerkeinstellungen im Netzwerk selbst zu verwenden, um zu bestimmen, wie der Datenverkehr gefiltert werden soll.

1. Ändern Sie den VIF-Sperrstatus in `network_default`, falls dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

   ```
   xe vif-param-set uuid=vif_uuid locking-mode=network_default
   <!--NeedCopy-->
   ```

2. Ändern Sie den Standardsperrmodus in `unlocked`, falls dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

   ```
   xe network-param-set uuid=network-uuid default-locking-mode=
      unlocked
   <!--NeedCopy-->
   ```

Fehlerbehebung bei Netzwerkproblemen

February 24, 2024

Wenn Sie Probleme mit der Netzwerkkonfiguration haben, stellen Sie zunächst sicher, dass Sie keine der Steuerdomänendateien `ifcfg-*` direkt geändert haben. Der Host-Agent der Steuerdomäne verwaltet die `ifcfg`-Dateien direkt, und alle Änderungen werden überschrieben.

Diagnose einer Netzwerkbeschädigung

Bei einigen Netzwerkkartenmodellen sind Firmware-Upgrades des Anbieters erforderlich, um unter Last oder wenn bestimmte Optimierungen aktiviert sind, zuverlässig zu funktionieren. Wenn Sie einen beschädigten Datenverkehr zu VMs feststellen, versuchen Sie, die neueste Firmware von Ihrem Anbieter zu beziehen und verwenden Sie sie dann, um Ihre Hardware zu aktualisieren.

Wenn das Problem weiterhin besteht, können Sie die CLI verwenden, um die Empfangs- oder Übertragungs-Offload-Optimierungen auf der physischen Schnittstelle zu deaktivieren.

> **Warnung:**
>
> Das Deaktivieren von Empfangs- oder Übertragungs-Offload-Optimierungen kann zu Leistungseinbußen und erhöhter CPU-Auslastung führen

Bestimmen Sie zunächst die UUID der physikalischen Schnittstelle. Sie können das `device`-Feld wie folgt filtern:

```
xe pif-list device=eth0
<!--NeedCopy-->
```

Stellen Sie als Nächstes den folgenden Parameter auf dem PIF ein, um den TX-Offload zu deaktivieren:

```
xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
<!--NeedCopy-->
```

Schließen Sie abschließend den PIF erneut an oder starten Sie den Host neu, damit die Änderung wirksam wird.

Zurücksetzen des Notfallnetzwerks

Falsche Netzwerkeinstellungen können zum Verlust der Netzwerkkonnektivität führen. Wenn keine Netzwerkkonnektivität besteht, kann auf den XenServer-Host über XenCenter oder Remote-SSH nicht mehr zugegriffen werden. Emergency Network Reset bietet einen einfachen Mechanismus zum Wiederherstellen und Zurücksetzen des Netzwerks eines Hosts.

Die Funktion zum Zurücksetzen des Netzwerks im Notfall ist über die CLI mit dem Befehl `xe-reset-networking` und im Abschnitt **Netzwerk- und Verwaltungsschnittstelle** von `xsconsole` verfügbar.

Zu den falschen Einstellungen, die zum Verlust der Netzwerkkonnektivität führen, gehören das Umbenennen von Netzwerkschnittstellen, das Erstellen von Bonds oder VLANs oder Fehler beim Ändern der Verwaltungsschnittstelle. Zum Beispiel die falsche IP-Adresse eingeben. Möglicherweise möchten Sie dieses Dienstprogramm auch in den folgenden Szenarien ausführen:

- wenn ein Rolling-Pool-Upgrade, ein manuelles Upgrade, eine Hotfixinstallation oder eine Treiberinstallation zu einem Mangel an Netzwerkkonnektivität führt oder
- Wenn ein Poolkoordinator oder Host in einem Ressourcenpool keine Verbindung zu anderen Hosts aufnehmen kann.

Verwenden Sie das Dienstprogramm `xe-reset-networking` nur im Notfall, da es die Konfiguration für alle PIFs, Bindungen, VLANs und Tunnel löscht, die dem Host zugeordnet sind. Gastnetzwerke und VIFs werden beibehalten. Im Rahmen dieses Dienstprogramms werden virtuelle Maschinen zwangsweise heruntergefahren. Bevor Sie diesen Befehl ausführen, fahren Sie die VMs nach Möglichkeit sauber herunter. Bevor Sie einen Reset anwenden, können Sie die Verwaltungsschnittstelle ändern und angeben, welche IP-Konfiguration, DHCP oder Static verwendet werden kann.

Wenn der Poolkoordinator ein Zurücksetzen des Netzwerks erfordert, setzen Sie zuerst das Netzwerk auf dem Poolkoordinator zurück, bevor Sie einen Netzwerk-Reset für Poolmitglieder anwenden. Wenden Sie die Netzwerkrücksetzung auf alle verbleibenden Hosts im Pool an, um sicherzustellen, dass die Netzwerkkonfiguration des Pools homogen ist. Die Homogenität des Netzwerks ist ein wichtiger Faktor für die Livemigration.

> **Hinweis:**
>
> Wenn sich die IP-Adresse des Poolkoordinators (die Verwaltungsschnittstelle) infolge eines Netzwerk-Resets ändert `xe host-management-reconfigure`, oder wenden Sie den Befehl network reset auf andere Hosts im Pool an. Dadurch wird sichergestellt, dass sich die Poolmitglieder unter seiner neuen IP-Adresse wieder mit dem Poolkoordinator verbinden können. In diesem Fall muss die IP-Adresse des Poolkoordinators angegeben werden.
>
> Das Zurücksetzen des Netzwerks wird NICHT unterstützt, wenn Hochverfügbarkeit aktiviert ist. Um die Netzwerkkonfiguration in diesem Szenario zurückzusetzen, müssen Sie zuerst die Hochverfügbarkeit manuell deaktivieren und dann den Befehl zum Zurücksetzen des Netzwerks ausführen.

Überprüfung des Netzwerkrücksetzens

Nachdem Sie den Konfigurationsmodus angegeben haben, der nach dem Zurücksetzen des Netzwerks verwendet werden soll, `xsconsole` und die CLI-Anzeigeeinstellungen, die nach dem Neustart des Hosts angewendet werden. Es ist eine letzte Möglichkeit, Änderungen vorzunehmen, bevor der Befehl zum Zurücksetzen des Netzwerks im Notfall angewendet wird. Nach dem Neustart kann die neue Netzwerkkonfiguration in XenCenter und überprüft werden `xsconsole`. Wählen Sie in XenCenter bei ausgewähltem Host die Registerkarte **Netzwerk** aus, um die neue Netzwerkkonfiguration anzuzeigen. Im Bereich Netzwerk und Verwaltungsschnittstelle in **xsconsole** werden diese Informationen angezeigt.

> **Hinweis:**
>
> Führen Sie einen Notfall-Netzwerk-Reset für andere Poolmitglieder durch, um Bindungen, VLANs oder Tunnel aus der neuen Konfiguration des Poolkoordinators zu replizieren.

Verwenden der CLI zum Zurücksetzen des Netzwerks

Die folgende Tabelle zeigt die verfügbaren optionalen Parameter, die beim Ausführen des Befehls `xe-reset-networking` verwendet werden können.

> **Warnung:**
>
> Die Benutzer sind dafür verantwortlich, die Gültigkeit der Parameter für den Befehl `xe-reset-networking` sicherzustellen und die Parameter sorgfältig zu überprüfen. Wenn Sie ungültige Parameter angeben, können Netzwerkkonnektivität und -konfiguration verloren gehen. In diesem Fall empfehlen wir Ihnen, den Befehl `xe-reset-networking` noch einmal auszuführen, ohne Parameter zu verwenden.
>
> Das Zurücksetzen der Netzwerkkonfiguration eines gesamten Pools **muss** auf dem Poolkoordinator beginnen, gefolgt von einem Netzwerk-Reset auf allen verbleibenden Hosts im Pool.

Parameter	Erforderlich/optional	Beschreibung
`-m`, `--master`	Optional	IP-Adresse der Verwaltungsschnittstelle des Poolkoordinators. Standardmäßig wird die IP-Adresse des letzten bekannten Poolkoordinators verwendet.
`--device`	Optional	Gerätename der Verwaltungsschnittstelle. Standardmäßig wird der bei der Installation angegebene Gerätename verwendet.

Parameter	Erforderlich/optional	Beschreibung
`--mode=static`	Optional	Aktiviert die folgenden vier Netzwerkparameter für die statische IP-Konfiguration für die Verwaltungsschnittstelle. Falls nicht angegeben, wird das Netzwerk mithilfe von DHCP konfiguriert.
`--ip`	Erforderlich, falls `mode=static`	Die IP-Adresse für die Verwaltungsschnittstelle des Hosts. Nur gültig wenn `mode=static`.
`--netmask`	Erforderlich, falls `mode=static`	Netzwerkmaske für die Verwaltungsschnittstelle. Nur gültig wenn `mode=static`.
`--gateway`	Optional	Gateway für die Verwaltungsschnittstelle. Nur gültig wenn `mode=static`.
`--dns`	Optional	DNS-Server für die Verwaltungsschnittstelle. Nur gültig wenn `mode=static`.
`--vlan`	Optional	VLAN-Tag für die Verwaltungsschnittstelle. Standardmäßig wird das bei der Installation angegebene VLAN-Tag verwendet.

Befehlszeilenbeispiele für Poolkoordinatoren Beispiele für Befehle, die auf einen Poolkoordinator angewendet werden können:

Um das Netzwerk für die DHCP-Konfiguration zurückzusetzen:

```
xe-reset-networking
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für die statische IP-Konfiguration zurück:

```
xe-reset-networking --mode= static --ip=ip-address \
    --netmask=netmask --gateway=gateway \
    --dns=dns
<!--NeedCopy-->
```


So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück, wenn nach der Ersteinrichtung eine andere Schnittstelle zur Verwaltungsschnittstelle wurde:

```
xe-reset-networking --device=device-name
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für die statische IP-Konfiguration zurück, wenn nach der Ersteinrichtung eine andere Schnittstelle zur Verwaltungsschnittstelle wurde:

```
xe-reset-networking --device=device-name --mode=static \
    --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für die Verwaltungsschnittstelle im VLAN zurück:

```
xe-reset-networking --vlan=VLAN TAG
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der Befehl `reset-network` kann auch zusammen mit den IP-Konfigurationseinstellungen verwendet werden.

Befehlszeilenbeispiele für Poolmitglieder Alle vorherigen Beispiele gelten auch für Poolmitglieder. Zusätzlich kann die IP-Adresse des Poolkoordinators angegeben werden (was erforderlich ist, wenn sie sich geändert hat).

Um das Netzwerk für die DHCP-Konfiguration zurückzusetzen:

```
xe-reset-networking
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für DHCP zurück, wenn die IP-Adresse des Poolkoordinators geändert wurde:

```
xe-reset-networking --master=pool-coordinator-ip-address
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für die statische IP-Konfiguration zurück, vorausgesetzt, die IP-Adresse des Poolkoordinators hat sich nicht geändert:

```
xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
<!--NeedCopy-->
```

So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück, wenn die Verwaltungsschnittstelle und die IP-Adresse des Poolkoordinators nach der ersten Einrichtung geändert wurden:


```
xe-reset-networking --device=device-name --master=pool-coordinator-ip-
    address
<!--NeedCopy-->
```

---

layout: doc
description: Understand the concepts involved in XenServer storage.—

Speicher

In diesem Abschnitt wird beschrieben, wie physische Speicherhardware virtuellen Maschinen (VMs) zugeordnet wird und welche Softwareobjekte von der Verwaltungs-API zur Ausführung speicherbezogener Aufgaben verwendet werden. Ausführliche Abschnitte zu jedem der unterstützten Speichertypen enthalten die folgenden Informationen:

- Verfahren zum Erstellen von Speicher für VMs über die CLI mit typspezifischen Gerätekonfigurationsoptionen
- Generieren von Snapshots für Backup-Zwecke
- Best Practices für die Verwaltung von Speicher

Speicherrepositories (SRs)

Ein Speicherrepository (SR) ist ein bestimmtes Speicherziel, in dem Virtual Machine (VM) Virtual Disk Images (VDIs) gespeichert sind. Ein VDI ist eine Speicherabstraktion, die ein virtuelles Datenträgerlaufwerk (HDD) darstellt.

SRs sind flexibel, mit integrierter Unterstützung für die folgenden Laufwerke:

Lokal verbunden:

- SATA
- SCSI
- SAS
- NVMe

Die lokale physische Speicherhardware darf ein Datenträgerlaufwerk (HDD) oder ein Solid-State-Laufwerk (SSD) sein.

Remote-Verbindung:

- iSCSI

- NFS
- SAS
- SMB (nur Version 3)
- Fibre-Channel

> **Hinweis:**
>
> NVMe über Fibre-Channel und NVMe über TCP werden nicht unterstützt.

Die SR- und VDI-Abstraktionen ermöglichen die Bereitstellung erweiterter Speicherfunktionen auf Speicherzielen, die sie unterstützen. Zum Beispiel erweiterte Funktionen wie *Thin Provisioning*, VDI-Snapshots und schnelles Klonen. Für Speichersubsysteme, die erweiterte Vorgänge nicht direkt unterstützen, wird ein Software-Stack bereitgestellt, der diese Funktionen implementiert. Dieser Software-Stack basiert auf Microsofts Virtual Hard Disk (VHD) -Spezifikation.

Ein Speicherrepository ist eine persistente Datenstruktur auf dem Datenträger. Bei SR-Typen, die ein zugrunde liegendes Blockgerät verwenden, werden beim Erstellen eines SRs alle vorhandenen Daten auf dem angegebenen Speicherziel gelöscht. Andere Speichertypen wie NFS erstellen parallel zu vorhandenen SRs einen Container auf dem Speicher-Array.

Jeder XenServer-Host kann mehrere SRs und verschiedene SR-Typen gleichzeitig verwenden. Diese SRs können zwischen Hosts geteilt oder für bestimmte Hosts reserviert werden. Gemeinsam genutzter Speicher wird zwischen mehreren Hosts innerhalb eines definierten Ressourcenpools gepoolt. Ein gemeinsam genutztes SR muss für jeden Host im Pool über das Netzwerk zugänglich sein. Alle Hosts in einem einzigen Ressourcenpool müssen mindestens eine gemeinsam genutzte SR haben. Gemeinsam genutzter Speicher kann nicht von mehreren Pools gemeinsam genutzt werden.

SR-Befehle bieten Vorgänge zum Erstellen, Zerstören, Ändern der Größe, Klonen, Verbinden und Erkennen der einzelnen VDIs, die sie enthalten. CLI-Vorgänge zum Verwalten von Speicherrepositories sind in SR-Befehlen beschrieben.

> **Warnung:**
>
> XenServer unterstützt für keinen SR-Typ Snapshots auf der externen SAN-Ebene einer LUN.

Virtuelles Disk-Image (VDI)

Ein Virtual Disk-Image (VDI) ist eine Speicherabstraktion, die ein virtuelles Datenträgerlaufwerk (HDD) darstellt. VDIs sind die grundlegende Einheit des virtualisierten Speichers in XenServer. VDIs sind persistente Objekte auf der Datenträger, die unabhängig von XenServer-Hosts existieren. CLI-Vorgänge zur Verwaltung von VDIs sind in VDI-Befehlenbeschrieben. Die Darstellung der Daten auf dem Datenträger unterscheidet sich je nach SR-Typ. Eine separate Speicher-Plug-In-Schnittstelle für jedes SR, die SM-API genannt wird, verwaltet die Daten.

Physische Blockgeräte (PBDs)

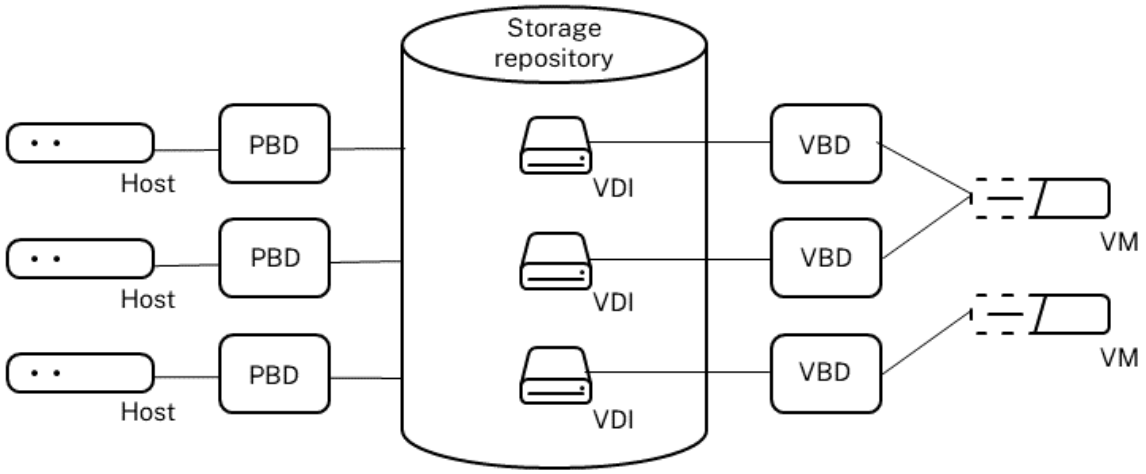
Physische Blockgeräte stellen die Schnittstelle zwischen einem physischen Server und einem angeschlossenen SR dar. PBDs sind Connectorobjekte, mit denen ein bestimmtes SR einem Host zugeordnet werden kann. PBDs speichern die Gerätekonfigurationsfelder, die verwendet werden, um eine Verbindung zu einem bestimmten Speicherziel herzustellen und mit diesem zu interagieren. Die NFS-Gerätekonfiguration umfasst beispielsweise die IP-Adresse des NFS-Servers und den zugehörigen Pfad, den der XenServer-Host bereitstellt. PBD-Objekte verwalten die Laufzeitanhänge einer bestimmten SR an einen bestimmten XenServer-Host. CLI-Operationen in Bezug auf PBDs werden in PBD-Befehlenbeschrieben.

Virtuelle Blockgeräte (VBDs)

Virtuelle Blockgeräte sind Connector-Objekte (ähnlich der oben beschriebenen PBD), die Zuordnungen zwischen VDIs und VMs ermöglichen. VBDs bieten nicht nur einen Mechanismus zum Anhängen eines VDI an eine VM, sondern ermöglichen auch die Feinabstimmung von Parametern in Bezug auf die Datenträger-I/O-Priorität und die Statistiken eines bestimmten VDI sowie die Frage, ob dieser VDI gestartet werden kann. CLI-Operationen in Bezug auf VBDs werden in VBD-Befehlenbeschrieben.

Zusammenfassung der Speicherobjekte

Das folgende Bild ist eine Zusammenfassung der Beziehung der bisher dargestellten Speicherobjekte:



Datenformate virtueller Datenträger

Im Allgemeinen gibt es die folgenden Arten der Zuordnung von physischem Speicher zu einem VDI:

1. *Logische volumebasierte virtuelle Datenträger auf einer LUN: Der standardmäßige block-basierte XenServer-Speicher fügt einen logischen Volume-Manager* auf einer Datenträger ein. Dieser Datenträger ist entweder ein lokal angeschlossenes Gerät (LVM) oder eine an das SAN angeschlossene LUN über Fibre Channel, iSCSI oder SAS. VDIs werden im Volume Manager als Volumes dargestellt und im VHD-Format gespeichert, um die Thin-Bereitstellung von Referenzknoten auf Snapshot und Klon zu ermöglichen.
2. *Dateibasiertes QCOW2 auf einer LUN:* VM-Images werden als Thin-Provisioning-Dateien im QCOW2-Format auf einem gemeinsam genutzten GFS2-Datenträgerdateisystem auf einer LUN gespeichert, die entweder über iSCSI-Softwareinitiator oder Hardware-HBA angeschlossen ist.
3. *Dateibasierte VHD auf einem Dateisystem:* VM-Images werden als Thin-Provisioning-Dateien im VHD-Format entweder in einem lokalen, nicht gemeinsam genutzten Dateisystem (EXT3/EXT4-SR), einem gemeinsam genutzten NFS-Ziel (NFS-SR) oder einem Remote-SMB-Ziel (SMB-SR) gespeichert.
4. *Dateibasiertes QCOW2 auf einem Dateisystem:* VM-Images werden als Thin-Provision-Dateien im QCOW2-Format auf einem lokalen, nicht gemeinsam genutzten XFS-Dateisystem gespeichert.

VDI-Typen

Für GFS2- und XFS-SRs werden QCOW2-VDIs erstellt.

Für andere SR-Typen werden VDIs im VHD-Format erstellt. Sie können zum Zeitpunkt des Erstellens des VDI die Option “Raw”verwenden. Diese Option kann nur mit der xe CLI angegeben werden.

> **Hinweis:**
>
> Wenn Sie einen Roh-VDI auf einem LVM-basierten SR oder HBA/LUN-per-VDI SR erstellen, kann die besitzende VM möglicherweise auf Daten zugreifen, die Teil eines zuvor gelöschten VDI (jedes Formats) waren, der zu einer beliebigen VM gehört. Wir empfehlen Ihnen, Ihre Sicherheitsanforderungen zu berücksichtigen, bevor Sie diese Option verwenden.
>
> Raw-VDIs auf einem NFS-, EXT- oder SMB SR ermöglichen keinen Zugriff auf die Daten zuvor gelöschter VDIs, die zu einer VM gehören.

Um zu überprüfen, ob ein VDI mit `type=raw` erstellt wurde, überprüfen Sie seine `sm-config`-Zuordnung. Die xe-Befehle `sr-param-list` und `vdi-param-list` können jeweils für diesen Zweck verwendet werden.

Erstellen eines virtuellen Rohdatenträgers über die xe CLI

1. Führen Sie den folgenden Befehl aus, um einen VDI mit der UUID des SRs zu erstellen, in dem Sie das virtuelle Laufwerk platzieren möchten:

```
xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size
    \
        name-label=VDI name sm-config:type=raw
<!--NeedCopy-->
```

2. Hängen Sie das neue virtuelle Laufwerk an eine VM an. Verwenden Sie die Datenträger-Tools innerhalb der VM zum Partitionieren und Formatieren oder verwenden Sie die neue Datenträger auf andere Weise. Sie können den Befehl `vbd-create` verwenden, um ein VBD zu erstellen, um den virtuellen Datenträger Ihrer VM zuzuordnen.

Zwischen VDI-Formaten konvertieren

Es ist nicht möglich, eine direkte Konvertierung zwischen den Raw- und VHD-Formaten durchzuführen. Stattdessen können Sie einen VDI erstellen (entweder roh, wie oben beschrieben, oder VHD) und dann Daten von einem vorhandenen Volume hinein kopieren. Verwenden Sie die xe CLI, um sicherzustellen, dass der neue VDI eine virtuelle Größe hat, die mindestens so groß ist wie der VDI, von dem Sie kopieren. Sie können dies tun, indem Sie das entsprechende Feld `virtual-size` überprüfen, z. B. mit dem Befehl `vdi-param-list`. Sie können diesen neuen VDI dann an eine VM anhängen und Ihr bevorzugtes Tool innerhalb der VM verwenden, um eine direkte Blockkopie der Daten zu erstellen. Zum Beispiel Standard-Datenträgerverwaltungstools in Windows oder der Befehl `dd` in Linux. Wenn das neue Volume ein VHD-Volume ist, verwenden Sie ein Tool, mit dem Sie vermeiden können, leere Sektoren auf den Datenträger zu schreiben. Durch diese Aktion kann sichergestellt werden, dass der Speicherplatz im zugrunde liegenden Speicherrepository optimal genutzt wird. Ein dateibasierter Kopieransatz ist möglicherweise besser geeignet.

VHD-basierte und QCow2-basierte VDIs

VHD- und QCOW2-Images können *verkettet*werden, sodass zwei VDIs gemeinsame Daten gemeinsam nutzen können. In Fällen, in denen eine VHD- oder QCow2-unterstützte VM geklont wird, teilen sich die resultierenden VMs zum Zeitpunkt des Klonens die gemeinsamen Daten auf dem Datenträger. Jede VM nimmt ihre eigenen Änderungen in einer isolierten Copy-on-Write-Version des VDI vor. Mit dieser Funktion können solche VMs schnell aus Vorlagen geklont werden, was eine sehr schnelle Bereitstellung und Bereitstellung neuer VMs ermöglicht.

Wenn VMs und ihre zugehörigen VDIs im Laufe der Zeit geklont werden, werden Bäume verketteter VDIs erstellt. Wenn einer der VDIs in einer Kette gelöscht wird, rationalisiert XenServer die anderen VDIs in der Kette, um nicht benötigte VDIs zu entfernen. Dieser *Koaleszenzprozess* läuft asynchron.

Die Menge des zurückgewonnenen Datenträgerspeichers und die für die Ausführung des Vorgangs benötigte Zeit hängen von der Größe des VDI und der Menge der gemeinsam genutzten Daten ab.

Sowohl das VHD- als auch das QCOW2-Format unterstützen *Thin Provisioning*. Die Imagedatei wird automatisch in feinkörnigen Chunks erweitert, während die VM Daten auf den Datenträger schreibt. Bei dateibasierter VHD und GFS2-basierter QCOW2 hat dieser Ansatz den erheblichen Vorteil, dass VM-Image-Dateien nur so viel Speicherplatz auf dem physischen Speicher beanspruchen, wie erforderlich. Bei LVM-basierter VHD muss der zugrunde liegende logische Volume-Container auf die virtuelle Größe des VDI angepasst sein. Nicht genutzter Speicherplatz auf der zugrunde liegenden Copy-on-Write-Instanzdatenträger wird jedoch zurückgewonnen, wenn ein Snapshot oder Klon auftritt Der Unterschied zwischen den beiden Verhaltensweisen kann auf folgende Weise beschrieben werden:

- Bei *LVM-basierten VHD-Images* verbrauchen die unterschiedlichen Datenträgerknoten innerhalb der Kette nur so viele Daten, wie auf den Datenträger geschrieben wurden. Die Blattknoten (VDI-Klone) bleiben jedoch vollständig auf die virtuelle Größe der Datenträger vergrößert. Snapshot-Blattknoten (VDI-Snapshots) bleiben ungebunden, wenn sie nicht verwendet werden, und können schreibgeschützt angehängt werden, um die verkleinerte Zuweisung beizubehalten. Snapshot-Knoten, die mit Lese-/Schreibzugriff verbunden sind, werden beim Anhängen vollständig aufgeblasen und beim Trennen entleert.
- Bei *dateibasierten VHDs* und *GFS2-basierten QCOW2-Images* verbrauchen alle Knoten nur so viele Daten, wie geschrieben wurde. Die Blattknotendateien werden erweitert, um Daten aufzunehmen, während sie aktiv geschrieben werden. Wenn ein 100-GB-VDI für eine VM zugewiesen wird und ein Betriebssystem installiert ist, entspricht die VDI-Datei physisch nur der Größe der Betriebssystemdaten auf dem Datenträger sowie einigen kleineren Metadatenaufwand.

Beim Klonen von VMs basierend auf einer einzelnen VHD- oder QCOW2-Vorlage bildet jede untergeordnete VM eine Kette, in der neue Änderungen in die neue VM geschrieben werden. Alte Blöcke werden direkt aus der übergeordneten Vorlage gelesen. Wenn die neue VM in eine weitere Vorlage umgewandelt wurde und mehr VMs geklont wurden, führt die resultierende Kette zu einer Leistungsminderung. XenServer unterstützt eine maximale Kettenlänge von 30. Nähern Sie sich dieser Grenze nicht ohne guten Grund. Im Zweifelsfall “kopieren”Sie die VM mit XenCenter oder verwenden Sie den Befehl `vm -copy`, der die Kettenlänge auf 0 zurücksetzt.

VHD-spezifische Hinweise zur Koaleszenz Für ein SR ist immer nur ein Koaleszenzprozess aktiv. Dieser Prozessthread läuft auf dem SR-Poolkoordinator.

Wenn auf dem Poolkoordinator kritische VMs ausgeführt werden, können Sie die folgenden Schritte ergreifen, um gelegentliche langsame I/O-Vorgänge zu vermeiden:

- Migrieren Sie die VM auf einen anderen Host als den SR- Poolkoordinator

- Stellen Sie die Datenträger-E/A-Priorität auf eine höhere Ebene und passen Sie den Scheduler an Weitere Informationen finden Sie unter Priorisierung von I/O-Anforderungen für virtuelle Datenträger.

---

layout: doc
description: Create storage repositories for use in your XenServer environment.—

Erstellen Sie ein Speicher-Repository

Sie können den Assistenten für **neues Speicher-Repository** in XenCenter verwenden, um Speicherrepositorys (SRs) zu erstellen. Der Assistent führt Sie durch die Konfigurationsschritte. Verwenden Sie alternativ die CLI und den Befehl `sr-create`. Der Befehl `sr-create` erstellt ein SR auf dem Speichersubstrat (wodurch möglicherweise alle vorhandenen Daten zerstört werden). Außerdem werden das SR-API-Objekt und ein entsprechender PBD-Datensatz erstellt, sodass VMs den Speicher verwenden können. Bei erfolgreicher Erstellung des SRs wird das PBD automatisch angeschlossen. Wenn das `shared=true` SR-Flag gesetzt ist, wird ein PBD-Datensatz für jeden XenServer im Ressourcenpool erstellt und angeschlossen.

Wenn Sie ein SR für IP-basierten Speicher (iSCSI oder NFS) erstellen, können Sie eine der folgenden Optionen als Speichernetzwerk konfigurieren: die Netzwerkkarte, die den Verwaltungsdatenverkehr verarbeitet, oder eine neue Netzwerkkarte für den Speicherverkehr. Informationen zum Zuweisen einer IP-Adresse zu einer Netzwerkkarte finden Sie unter Konfigurieren einer dedizierten Speicher-NIC.

Alle XenServer SR-Typen unterstützen VDI-Größenänderung, schnelles Klonen und Snapshot. SRs, die auf dem LVM SR-Typ (lokal, iSCSI oder HBA) basieren, bieten Thin Provisioning für Snapshots und versteckte übergeordnete Knoten. Die anderen SR-Typen (EXT3/EXT4, NFS, GFS2) unterstützen die vollständige Thin Provisioning, auch für virtuelle Datenträger, die aktiv sind.

> **Warnungen:**
>
> - Wenn VHD-VDIs nicht an eine VM angeschlossen sind, z. B. für einen VDI-Snapshot, werden sie standardmäßig als dünn bereitgestellt gespeichert. Wenn Sie versuchen, den VDI erneut anzuhängen, stellen Sie sicher, dass ausreichend Datenträgerspeicher verfügbar ist, damit der VDI dick bereitgestellt werden kann. VDI-Klone werden dick bereitgestellt.
> - XenServer unterstützt für keinen SR-Typ Snapshots auf der externen SAN-Ebene einer LUN.
> - Versuchen Sie nicht, eine SR zu erstellen, bei der die LUN-ID der Ziel-LUN größer als 255 ist. Stellen Sie sicher, dass Ihr Ziel die LUN mit einer LUN-ID verfügbar macht, die kleiner oder

gleich 255 ist, bevor Sie diese LUN verwenden, um eine SR zu erstellen.

- Wenn Sie Thin Provisioning auf einem dateibasierten SR verwenden, stellen Sie sicher, dass Sie den freien Speicherplatz auf Ihrem SR überwachen. Wenn die SR-Nutzung auf 100% ansteigt, schlagen weitere Schreibvorgänge von VMs fehl. Diese fehlgeschlagenen Schreibvorgänge können zum Einfrieren oder Absturz der VM führen.

Die maximal unterstützten VDI-Größen sind:

Format des Speicherrepository	Maximale VDI-Größe
EXT3/EXT4	2 TiB
GFS2 (mit iSCSI oder HBA)	16 TiB
XFS	16 TiB
LVM	2 TiB
LVMoFCOE (veraltet)	2 TiB
LVMoHBA	2 TiB
LVMoiSCSI	2 TiB
NFS	2 TiB
SMB	2 TiB

Lokales LVM

Der Typ Local LVM stellt Datenträger innerhalb einer lokal angeschlossenen Volume-Gruppe dar.

Standardmäßig verwendet XenServer den lokalen Datenträger auf dem physischen Host, auf dem sie installiert ist. Der Linux Logical Volume Manager (LVM) wird zur Verwaltung des VM-Speichers verwendet. Ein VDI wird im VHD-Format in einem logischen LVM-Volume der angegebenen Größe implementiert.

Hinweis:

Die Blockgröße einer LVM-LUN muss 512 Byte betragen. Um Speicher mit physischen Blöcken von 4 KB zu verwenden, muss der Speicher auch die Emulation von 512-Byte-Zuweisungsblöcken unterstützen (die logische Blockgröße muss 512 Byte betragen).

Überlegungen zur LVM-Leistung

Die Snapshot- und Fast-Clon-Funktionalität für LVM-basierte SRs ist mit einem inhärenten Leistungsaufwand verbunden. Wenn optimale Leistung erforderlich ist, unterstützt XenServer zusätzlich

zum Standard-VHD-Format die Erstellung von VDIs im *Rohformat* . Die XenServer-Snapshot-Funktionalität wird auf Raw-VDIs nicht unterstützt.

> **Warnung:**
>
> Versuchen Sie nicht, einen Snapshot einer VM zu erstellen, an die `type=raw`-Datenträger angeschlossen sind. Diese Aktion kann dazu führen, dass ein teilweiser Snapshot erstellt wird. In dieser Situation können Sie die verwaisten Snapshot-VDIs identifizieren, indem Sie das Feld `snapshot-of` markieren und dann löschen.

Erstellen eines lokalen LVM SRs

Ein LVM SR wird standardmäßig bei der Host-Installation erstellt.

Die Gerätekonfigurationsparameter für LVM SRs sind:

Parametername	Beschreibung	Erforderlich?
`device`	Gerätename auf dem lokalen Host, der für die SR verwendet werden soll. Sie können auch eine durch Kommas getrennte Liste von Namen angeben.	Ja

Verwenden Sie den Befehl, um ein lokales LVM SR auf `/dev/sdb` zu erstellen.

```
    xe sr-create host-uuid=valid_uuid content-type=user \
    name-label="Example Local LVM SR" shared=false \
    device-config:device=/dev/sdb type=lvm
<!--NeedCopy-->
```

Lokales EXT3/EXT4

Die Verwendung von EXT3/EXT4 ermöglicht Thin Provisioning auf lokalem Speicher Der Standard-Speicherrepository-Typ ist jedoch LVM, da er eine konsistente Schreibleistung bietet und ein Überschreiben des Speichers verhindert. Wenn Sie EXT3/EXT4 verwenden, wird die Leistung in den folgenden Fällen möglicherweise reduziert:

- Bei der Durchführung von VM-Lebenszyklusvorgängen wie VM-Erstellen und Aussetzen/Fortsetzen
- Beim Erstellen großer Dateien innerhalb der VM

Lokale Datenträger EXT3/EXT4 SRs müssen mit der XenServer-CLI konfiguriert werden.

Ob ein lokaler EXT-SR EXT3 oder EXT4 verwendet, hängt davon ab, mit welcher Version von XenServer er erstellt wurde:

- Wenn Sie den lokalen EXT SR auf einer früheren Version von Citrix Hypervisor oder XenServer erstellt und dann auf XenServer 8 aktualisiert haben, verwendet er EXT3.
- Wenn Sie den lokalen EXT-SR auf XenServer 8 erstellt haben, verwendet er EXT4.

> **Hinweis:**
>
> Die Blockgröße eines EXT3/EXT4-Datenträgers muss 512 Byte sein. Um Speicher mit physischen Blöcken von 4 KB zu verwenden, muss der Speicher auch die Emulation von 512-Byte-Zuweisungsblöcken unterstützen (die logische Blockgröße muss 512 Byte betragen).

Erstellen eines lokalen EXT4 SR (`ext`)

Gerätekonfigurationsparameter für Ext-SRs:

Parametername	Beschreibung	Erforderlich?
`device`	Gerätename auf dem lokalen Host, der für die SR verwendet werden soll. Sie können auch eine durch Kommas getrennte Liste von Namen angeben.	Ja

Verwenden Sie den folgenden Befehl, um ein lokales EXT4 SR auf `/dev/sdb` zu erstellen:

```
    xe sr-create host-uuid=valid_uuid content-type=user \
       name-label="Example Local EXT4 SR" shared=false \
       device-config:device=/dev/sdb type=ext
<!--NeedCopy-->
```

Lokales XFS

Die Verwendung von XFS ermöglicht Thin Provisioning auf lokalem Speicher. Mit dem lokalen XFS-Typ können Sie lokale Speichergeräte mit physischen Blöcken von 4 KB erstellen, ohne dass eine logische Blockgröße von 512 Byte erforderlich ist.

Erstellen einer lokalen XFS-SR

Gerätekonfigurationsparameter für XFS-SRs:

Parametername	Beschreibung	Erforderlich?
`device`	Gerätename auf dem lokalen Host, der für die SR verwendet werden soll. Sie können auch eine durch Kommas getrennte Liste von Namen angeben.	Ja

Verwenden Sie den folgenden Befehl, um eine lokale XFS-SR auf `/dev/sdb` zu erstellen:

```
    xe sr-create host-uuid=valid_uuid content-type=user \
       name-label="Example Local XFS SR" shared=false \
       device-config:device=/dev/sdb type=xfs
<!--NeedCopy-->
```

udev

Der Typ udev steht für Geräte, die mit dem Udev-Gerätemanager als VDIs angeschlossen wurden.

XenServer hat zwei SRs vom Typ udev, die Wechselspeicher darstellen. Eine ist für die CD oder DVD im physischen CD- oder DVD-ROM-Laufwerk des XenServer-Hosts. Die andere ist für ein USB-Gerät vorgesehen, das an einen USB-Anschluss des XenServer-Hosts angeschlossen ist. VDIs, die die Medien darstellen, kommen und gehen, wenn Datenträger oder USB-Sticks eingelegt und entfernt werden.

ISO-Image

Der ISO-Typ verarbeitet CD-Images, die als Dateien im ISO-Format gespeichert sind. Dieser SR-Typ eignet sich zum Erstellen gemeinsam genutzter ISO-Bibliotheken.

Die folgenden ISO-SR-Typen sind verfügbar:

- `nfs_iso`: Der NFS ISO SR-Typ verarbeitet CD-Images, die als Dateien im ISO-Format gespeichert sind, das als NFS-Freigabe verfügbar ist.
- `cifs`: Der SR-Typ Windows File Sharing (SMB/CIFS) verarbeitet CD-Images, die als Dateien im ISO-Format gespeichert sind, die als Windows-Freigabe (SMB/CIFS) verfügbar sind.

`location`Wenn Sie den Speichertyp, der für die SR verwendet werden soll, nicht angeben, verwendet XenServer den Gerätekonfigurationsparameter, um den Typ zu bestimmen.

Gerätekonfigurationsparameter für ISO-SRs:

Parametername	Beschreibung	Erforderlich?
`location`	Bereitstellungspfad.	Ja
`type`	Speichertyp, der für den SR verwendet werden soll: `cifs` oder `nfs_iso`.	Nein
`nfsversion`	Für den Speichertyp NFS die zu verwendende Version des NFS-Protokolls: 3, 4, 4.0 oder 4.1.	Nein
`vers`	Für den Speichertyp CIFS/SMB die zu verwendende Version von SMB: 1.0 oder 3.0. Die Standardeinstellung ist 3.0.	Nein
`username`	Für den Speichertyp CIFS/SMB, wenn ein Benutzername für den Windows-Dateiserver erforderlich ist.	Nein
`cifspassword_secret`	(Empfohlen) Für den Speichertyp CIFS/SMB können Sie anstelle eines Kennworts ein Geheimnis für den Windows-Dateiserver übergeben.	Nein
`cifspassword`	Für den Speichertyp CIFS/SMB, wenn ein Kennwort für den Windows-Dateiserver erforderlich ist. Wir empfehlen, stattdessen den Parameter `cifspassword_secret` zu verwenden.	Nein

> **Hinweis:**
>
> Wenn Sie den Befehl `sr-create` ausführen, empfehlen wir, das Argument `device-config:cifspassword_secret` zu verwenden, anstatt das Kennwort in der Befehlszeile anzugeben. Weitere Informationen finden Sie unter Secrets.

Für Speicher-Repositorys, die eine Bibliothek von ISOs speichern, muss der Parameter `content-`

`type` beispielsweise auf `iso` festgelegt werden. Beispiel:

```
1     xe sr-create host-uuid=valid_uuid content-type=iso  type=iso name-
         label="Example ISO SR" \
2       device-config:location=<path_to_mount> device-config:type=nfs_iso
3 <!--NeedCopy-->
```

Sie können NFS oder SMB verwenden, um das ISO-SR bereitzustellen. Weitere Informationen zur Verwendung dieser SR-Typen finden Sie unter NFS und SMB.

Wir empfehlen, dass Sie SMB Version 3 verwenden, um ISO SR auf dem Windows-Dateiserver zu mounten. Version 3 ist standardmäßig ausgewählt, da sie sicherer und robuster ist als SMB-Version 1.0. Sie können ISO SR jedoch mit dem folgenden Befehl mit SMB Version 1 mounten:

```
1      xe sr-create content-type=iso type=iso shared=true device-config:
          location=<path_to_mount>
2      device-config:username=<username> device-config:cifspassword=<
          password> \
3      device-config:type=cifs device-config:vers=1.0 name-label="Example
           ISO SR"
4 <!--NeedCopy-->
```

Software-iSCSI-Unterstützung

XenServer unterstützt gemeinsam genutzte SRs auf iSCSI-LUNs. iSCSI wird mit dem Open-iSCSI-Software-iSCSI-Initiator oder mit einem unterstützten iSCSI-Hostbusadapter (HBA) unterstützt. Die Schritte zur Verwendung von iSCSI-HBAs sind identisch mit den Schritten für Fibre-Channel-HBAs. Beide Schritte sind unter Create a Shared LVM over Fibre Channel/ Fibre Channel over Ethernet/ iSCSI HBA oder SAS SRbeschrieben.

Gemeinsame iSCSI-Unterstützung unter Verwendung des Software-iSCSI-Initiators wird basierend auf dem Linux Volume Manager (LVM) implementiert. Diese Funktion bietet dieselben Leistungsvorteile, die LVM-VDIs im lokalen Datenträgergehäuse bieten. Gemeinsam genutzte iSCSI-SRs, die den softwarebasierten Host-Initiator verwenden, können die Agilität von VMs mithilfe der Live-Migration unterstützen: VMs können auf jedem XenServer-Host in einem Ressourcenpool gestartet und ohne merkliche Ausfallzeiten zwischen ihnen migriert werden.

iSCSI-SRs verwenden die gesamte LUN, die bei der Erstellung angegeben wurde, und dürfen sich nicht über mehr als eine LUN erstrecken. CHAP-Unterstützung wird für die Clientauthentifizierung sowohl während der Datenpfadinitialisierung als auch während der LUN-Erkennungsphase bereitgestellt.

> **Hinweis:**
>
> Die Blockgröße einer iSCSI-LUN muss 512 Byte betragen. Um Speicher mit physischen Blöcken

> von 4 KB zu verwenden, muss der Speicher auch die Emulation von 512-Byte-Zuweisungsblöcken unterstützen (die logische Blockgröße muss 512 Byte betragen).

XenServer-Host-iSCSI-Konfiguration

Alle iSCSI-Initiatoren und -Ziele müssen einen eindeutigen Namen haben, um sicherzustellen, dass sie im Netzwerk eindeutig identifiziert werden können. Ein Initiator hat eine iSCSI-Initiatoradresse und ein Ziel hat eine iSCSI-Zieladresse. Zusammenfassend werden diese Namen als iSCSI Qualified Names oder IQNs bezeichnet.

XenServer-Hosts unterstützen einen einzelnen iSCSI-Initiator, der während der Hostinstallation automatisch mit einem zufälligen IQN erstellt und konfiguriert wird. Der einzelne Initiator kann verwendet werden, um gleichzeitig eine Verbindung zu mehreren iSCSI-Zielen herzustellen.

iSCSI-Ziele ermöglichen üblicherweise die Zugriffssteuerung mithilfe der IQN-Listen des iSCSI-Initiators. Alle iSCSI-Ziele/LUNs, auf die Ihr XenServer-Host zugreift, müssen so konfiguriert sein, dass sie den Zugriff durch den Initiator-IQN des Hosts zulassen. In ähnlicher Weise müssen Ziele/LUNs, die als gemeinsam genutzte iSCSI-SRs verwendet werden sollen, so konfiguriert werden, dass sie den Zugriff aller Host-IQNs im Ressourcenpool ermöglichen.

> **Hinweis:**
>
> iSCSI-Ziele, die keine Zugriffssteuerung bieten, beschränken in der Regel den LUN-Zugriff auf einen einzelnen Initiator, um die Datenintegrität zu gewährleisten. Wenn eine iSCSI-LUN als gemeinsam genutzte SR für mehrere Hosts in einem Pool verwendet wird, stellen Sie sicher, dass der Multiinitiatorzugriff für die angegebene LUN aktiviert ist.

Der IQN-Wert des XenServer-Hosts kann mit XenCenter oder mithilfe der CLI mit dem folgenden Befehl angepasst werden, wenn der iSCSI-Softwareinitiator verwendet wird:

```
1     xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=
         new_initiator_iqn
2 <!--NeedCopy-->
```

> **Warnung:**
>
> - Jedes iSCSI-Ziel und jeder Initiator muss über einen eindeutigen IQN verfügen. Wenn eine nicht eindeutige IQN-ID verwendet wird, kann es zu Datenbeschädigungen oder Verweigerung des LUN-Zugriffs kommen.
> - Ändern Sie nicht den IQN des XenServer-Hosts mit angeschlossenen iSCSI-SRs. Dies kann zu Fehlern bei der Verbindung zu neuen Zielen oder vorhandenen SRs führen.

Software-FCoE-Speicher (veraltet)

Software-FCoE bietet ein Standardrahmen, an das Hardwarehersteller ihre FCoE-fähige Netzwerkkarte anschließen und die gleichen Vorteile eines hardwarebasierten FCoE nutzen können. Diese Funktion macht die Verwendung teurer HBAs überflüssig.

> **Hinweis:**
>
> Software-FCoE ist veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie einen Software-FCoE-Speicher erstellen, schließen Sie die Konfiguration manuell ab, die erforderlich ist, um eine LUN für den Host verfügbar zu machen. Diese Konfiguration umfasst die Konfiguration der FCoE-Fabric und die Zuweisung von LUNs zum Public World Wide Name (PWWN) Ihres SAN. Nachdem Sie diese Konfiguration abgeschlossen haben, wird die verfügbare LUN als SCSI-Gerät in die CNA des Hosts eingebunden. Das SCSI-Gerät kann dann für den Zugriff auf die LUN verwendet werden, als wäre es ein lokal angeschlossenes SCSI-Gerät. Informationen zum Konfigurieren des physischen Switches und des Arrays zur Unterstützung von FCoE finden Sie in der Dokumentation des Herstellers.

> **Hinweis:**
>
> Software-FCoE kann mit Open vSwitch und Linux Bridge als Netzwerk-Backend verwendet werden.

Erstellen eines Software-FCoE SRs

Vor dem Erstellen eines Software-FCoE SRs müssen Kunden sicherstellen, dass FCoE-fähige NICs an den Host angeschlossen sind.

Die Gerätekonfigurationsparameter für FCoE SRs sind:

Parametername	Beschreibung	Erforderlich?
`SCSIid`	Die SCSI-Bus-ID der Ziel-LUN	Ja

Führen Sie den folgenden Befehl aus, um ein gemeinsames FCoE SR zu erstellen:

```
1     xe sr-create type=lvmofcoe \
2     name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
3 <!--NeedCopy-->
```


Hardware-Hostbusadapter (HBAs)

Dieser Abschnitt behandelt verschiedene Vorgänge, die für die Verwaltung von SAS-, Fibre-Channel- und iSCSI-HBAs erforderlich sind.

Beispiel für eine QLogic iSCSI HBA-Einrichtung

Einzelheiten zur Konfiguration von QLogic Fibre Channel und iSCSI HBAs finden Sie auf der Cavium-Website .

Sobald der HBA physisch auf dem XenServer-Host installiert ist, konfigurieren Sie den HBA mit den folgenden Schritten:

1. Stellen Sie die IP-Netzwerkkonfiguration für den HBA ein. In diesem Beispiel wird von DHCP und HBA-Port 0 ausgegangen. Geben Sie die entsprechenden Werte an, wenn Sie eine statische IP-Adressierung oder einen Multiport-HBA verwenden.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
   <!--NeedCopy-->
   ```

2. Fügen Sie ein beständiges iSCSI-Ziel zu Port 0 des HBA hinzu.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0
      iscsi_target_ip_address
   <!--NeedCopy-->
   ```

3. Verwenden Sie den xe-Befehl `sr-probe`, um eine erneute Suche des HBA-Controller zu erzwingen und verfügbare LUNs anzuzeigen. Weitere Informationen finden Sie unter Sondieren eines SR und Erstellen eines gemeinsam genutzten LVM über Fibre-Channel/ Fibre-Channel über Ethernet/ iSCSI HBA oder SAS SR.

HBA-basierte SAS-, FC- oder iSCSI-Geräteeinträge entfernen

> **Hinweis:**
>
> Dieser Schritt ist nicht erforderlich. Wir empfehlen, dass nur Hauptbenutzer diesen Vorgang ausführen, wenn dies erforderlich ist.

Jede HBA-basierte LUN hat einen entsprechenden globalen Gerätepfadeintrag unter `/dev/disk/by-scsibus` im Format `<SCSIid>-<adapter>:<bus>:<target>:<lun>` und einen Standardgerätepfad unter `/dev`. Gehen Sie folgendermaßen vor, um die Geräteeinträge für LUNs zu entfernen, die nicht mehr als SRs verwendet werden:

1. Verwenden Sie `sr-forget` oder nach `sr-destroy` Bedarf, um die SR aus der XenServer-Hostdatenbank zu entfernen. Einzelheiten finden Sie unter SRs entfernen .

2. Entfernen Sie die Zoning-Konfiguration innerhalb des SAN für die gewünschte LUN auf dem gewünschten Host.
3. Verwenden Sie den Befehl `sr-probe`, um die Werte ADAPTER, BUS, TARGET und LUNs zu ermitteln, die der zu entfernenden LUN entsprechen. Weitere Informationen finden Sie unter Sonde und SR.
4. Entfernen Sie die Geräteeinträge mit dem folgenden Befehl:

```
echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/
   delete
<!--NeedCopy-->
```

> **Warnung:**
>
> Stellen Sie sicher, dass Sie sicher sind, welche LUN Sie entfernen. Durch versehentliches Entfernen einer für den Host-Betrieb erforderlichen LUN, z. B. des Boot- oder Root-Geräts, wird der Host unbrauchbar.

Gemeinsam genutzter LVM-Speicher

Der Shared LVM-Typ stellt Datenträger als logische Volumes innerhalb einer Volume-Gruppe dar, die auf einer iSCSI-LUN (FC oder SAS) erstellt wurde.

> **Hinweis:**
>
> Die Blockgröße einer iSCSI-LUN muss 512 Byte betragen. Um Speicher mit physischen Blöcken von 4 KB zu verwenden, muss der Speicher auch die Emulation von 512-Byte-Zuweisungsblöcken unterstützen (die logische Blockgröße muss 512 Byte betragen).

Erstellen eines gemeinsam genutzten LVM über iSCSI SR mithilfe des Software-iSCSI-Initiators

Gerätekonfigurationsparameter für LVMoiSCSI SRs:

Parametername	Beschreibung	Erforderlich?
`target`	Die IP-Adresse oder der Hostname des iSCSI-Filers, der das SR hostet. Dies kann auch eine kommagetrennte Werteliste sein.	Ja
`targetIQN`	Die IQN-Zieladresse des iSCSI-Filers, der das SR hostet	Ja

Parametername	Beschreibung	Erforderlich?
`SCSIid`	Die SCSI-Bus-ID der Ziel-LUN	Ja
`chapuser`	Der für die CHAP-Authentifizierung zu verwendende Benutzername	Nein
`chappassword_secret`	(Empfohlen) Geheime ID für das Kennwort, das für die CHAP-Authentifizierung verwendet werden soll. Geben Sie ein Geheimnis anstelle eines Kennworts weiter.	Nein
`chappassword`	Das Kennwort, das für die CHAP-Authentifizierung verwendet werden soll. Wir empfehlen, stattdessen den Parameter `chappassword_secret` zu verwenden.	Nein
`port`	Die Netzwerkportnummer, auf der das Ziel abgefragt werden soll	Nein
`usediscoverynumber`	Der zu verwendende iSCSI-Record-Index	Nein
`incoming_chapuser`	Der Benutzername, den der iSCSI-Filter verwendet, um sich gegen den Host zu authentifizieren.	Nein
`incoming_chappassword`	Das Kennwort, das der iSCSI-Filter zur Authentifizierung gegen den Host verwendet.	Nein

> **Hinweis:**
>
> Wenn Sie den Befehl `sr-create` ausführen, empfehlen wir, das Argument `device-config: chappassword_secret` zu verwenden, anstatt das Kennwort in der Befehlszeile anzugeben. Weitere Informationen finden Sie unter Secrets.

Verwenden Sie den folgenden Befehl, um ein gemeinsam genutztes LVMoiSCSI SR auf einer bestimmten LUN eines iSCSI-Ziels zu erstellen.


```
    xe sr-create host-uuid=valid_uuid content-type=user \
    name-label="Example shared LVM over iSCSI SR" shared=true \
    device-config:target=target_ip= device-config:targetIQN=target_iqn=
        \
    device-config:SCSIid=scsci_id \
    type=lvmoiscsi
<!--NeedCopy-->
```

Erstellen eines gemeinsam genutzten LVM über Fibre-Channel/ Fibre-Channel über Ethernet/ iSCSI HBA oder SAS SR

SRs vom Typ LVMoHBA können mit der xe CLI oder XenCenter erstellt und verwaltet werden.

Gerätekonfigurationsparameter für LVMoHBA SRs:

Parametername	Beschreibung	Erforderlich?
SCSIid	SCSI-ID des Geräts	Ja

Um ein gemeinsam genutztes LVMoHBA SR zu erstellen, führen Sie die folgenden Schritte auf jedem Host im Pool aus:

1. Zonieren Sie jedem XenServer-Host im Pool eine oder mehrere LUNs. Dieser Prozess ist sehr spezifisch für die verwendeten SAN-Geräte. Weitere Informationen finden Sie in Ihrer SAN-Dokumentation.
2. Verwenden Sie bei Bedarf die im XenServer-Host enthaltene HBA-CLI, um den HBA zu konfigurieren:
   - Emulex: /bin/sbin/ocmanager
   - QLogic FC: /opt/QLogic_Corporation/SANsurferCLI
   - QLogic iSCSI: /opt/QLogic_Corporation/SANsurferiCLI

   Ein Beispiel für die QLogic iSCSI-HBA-Konfiguration finden Sie unter *Hardware-Host-Busadapter (HBAs)* im vorherigen Abschnitt. Weitere Informationen zu Fibre-Channel- und iSCSI-HBAs finden Sie auf den Websites Broadcom und Cavium .
3. Verwenden Sie den Befehl sr-probe, um den globalen Gerätepfad der HBA-LUN zu bestimmen. Der Befehl sr-probe erzwingt einen Neuscan der im System installierten HBAs, um neue LUNs zu erkennen, die für den Host in Zonen unterteilt wurden. Der Befehl gibt eine Liste von Eigenschaften für jede gefundene LUN zurück. Geben Sie den Parameter an host-uuid, um sicherzustellen, dass die Sonde auf dem gewünschten Host erfolgt.

Der globale Gerätepfad, der als <path>-Eigenschaft zurückgegeben wird, ist für alle Hosts im Pool gemeinsam. Daher muss dieser Pfad beim Erstellen des SRs als Wert für den Parameter device-config:device verwendet werden.

Wenn mehrere LUNs vorhanden sind, verwenden Sie den Anbieter, die LUN-Größe, die LUN-Seriennummer oder die SCSI-ID der <path>-Eigenschaft, um die gewünschte LUN zu identifizieren.

```
xe sr-probe type=lvmohba \
host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31
Error code: SR_BACKEND_FAILURE_90
Error parameters: , The request is missing the device
   parameter, \
<?xml version="1.0" ?>
<Devlist>
    <BlockDevice>
        <path>
            /dev/disk/by-id/scsi-360
               a98000686669496734463876653 36f
        </path>
        <vendor>
            HITACHI
        </vendor>
        <serial>
            730157980002
        </serial>
        <size>
            80530636800
        </size>
        <adapter>
            4
        </adapter>
        <channel>
            0
        </channel>
        <id>
            4
        </id>
        <lun>
            2
        </lun>
        <hba>
            qla2xxx
        </hba>
    </BlockDevice>
    <Adapter>
        <host>
            Host4
        </host>
        <name>
            qla2xxx
        </name>
```



```
            <manufacturer>
                QLogic HBA Driver
            </manufacturer>
            <id>
                4
            </id>
        </Adapter>
    </Devlist>
<!--NeedCopy-->
```

4. Erstellen Sie auf dem Poolkoordinator den SR. Geben Sie den globalen Gerätepfad an, der in der <path>-Eigenschaft von sr-probe zurückgegeben wird. PBDs werden für jeden Host im Pool automatisch erstellt und angeschlossen.

```
    xe sr-create host-uuid=valid_uuid \
    content-type=user \
    name-label="Example shared LVM over HBA SR" shared=true \
    device-config:SCSIid=device_scsi_id type=lvmohba
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können die XenCenter Repair Storage Repository-Funktion verwenden, um die PBD-Erstellung neu zu versuchen und Teile des Vorgangs sr-create zu blockieren. Diese Funktion kann in Fällen nützlich sein, in denen das LUN-Zoning für einen oder mehrere Hosts in einem Pool nicht korrekt war, als das SR erstellt wurde. Korrigieren Sie das Zoning für die betroffenen Hosts und verwenden Sie die Funktion "Speicherrepository reparieren", anstatt das SR zu entfernen und neu zu erstellen.

Gemeinsam genutzter GFS2-Blockspeicher mit Thin-Provisioning

Beim Thin Provisioning wird der verfügbare Speicher besser genutzt, indem VDIs Datenträgerspeicherplatz zugewiesen wird, während die Daten auf das virtuelle Laufwerk geschrieben werden, anstatt die volle virtuelle Größe des VDI im Voraus zuzuweisen. Thin Provisioning ermöglicht es Ihnen, den auf einem gemeinsam genutzten Speicher-Array benötigten Speicherplatz und damit Ihre Gesamtbetriebskosten (TCO) erheblich zu reduzieren.

Thin Provisioning für gemeinsam genutzten Blockspeicher ist in den folgenden Fällen von besonderem Interesse:

- Sie möchten eine höhere Raumeffizienz. Images werden spärlich und nicht dicht verteilt.
- Sie möchten die Anzahl der I/O-Vorgänge pro Sekunde auf Ihrem Speicher-Array reduzieren. GFS2-SR ist der erste SR-Typ, der das Speicherlesecaching auf gemeinsam genutztem Blockspeicher unterstützt.
- Sie verwenden ein allgemeines Basisimage für mehrere virtuelle Maschinen. Die Images einzelner VMs benötigen dann in der Regel noch weniger Speicherplatz.

- Sie verwenden Schnappschüsse. Jeder Snapshot ist ein Image und jedes Image ist jetzt spärlich.
- Ihr Speicher unterstützt kein NFS und unterstützt nur Blockspeicher. Wenn Ihr Speicher NFS unterstützt, empfehlen wir Ihnen, NFS anstelle von GFS2 zu verwenden.
- Sie möchten VDIs erstellen, die größer als 2 TiB sind. Der GFS2 SR unterstützt VDIs mit einer Größe von bis zu 16 TiB.

> **Hinweis:**
>
> Wir empfehlen, GFS2 SR nicht mit einem VLAN zu verwenden, da ein bekanntes Problem besteht, bei dem Sie Hosts in einem Clusterpool nicht hinzufügen oder entfernen können, wenn sich das Clusternetzwerk in einem Nicht-Management-VLAN befindet.

Der gemeinsam genutzte GFS2-SR-Typ erstellt ein GFS2-Dateisystem auf einer iSCSI- oder HBA-LUN. VDIs werden im GFS2 SR als Dateien im QCOW2-Bildformat gespeichert.

Weitere Informationen zur Verwendung von GFS2-Speicher finden Sie unter Gemeinsam genutzter GFS2-Blockspeicher mit Thin-Provisioning.

NFS und SMB

Freigaben auf NFS-Servern (die jede Version von NFSv4 oder NFSv3 unterstützen) oder auf SMB-Servern (die SMB 3 unterstützen) können sofort als SR für virtuelle Laufwerke verwendet werden. VDIs werden nur im Microsoft VHD-Format gespeichert. Da diese SRs gemeinsam genutzt werden können, ermöglichen VDIs, die auf gemeinsam genutzten SRs gespeichert sind, außerdem:

- VMs, die auf beliebigen XenServer-Hosts in einem Ressourcenpool gestartet werden sollen
- VM-Migration zwischen XenServer-Hosts in einem Ressourcenpool mithilfe der Livemigration (ohne merkliche Ausfallzeiten)

> **Wichtig:**
>
> - Die Unterstützung für SMB3 ist auf die Möglichkeit beschränkt, mithilfe des 3-Protokolls eine Verbindung zu einer Freigabe herzustellen. Zusätzliche Funktionen wie Transparent Failover hängen von der Funktionsverfügbarkeit im Upstream-Linux-Kernel ab und werden in XenServer 8 nicht unterstützt.
> - Clustered SMB wird von XenServer nicht unterstützt.
> - Für NFSv4 wird nur der Authentifizierungstyp AUTH_SYS unterstützt.
> - SMB-Speicher ist für Kunden der XenServer Premium Edition verfügbar.
> - Sowohl für NFS- als auch für SMB-Speicher wird dringend empfohlen, ein dediziertes Speichernetzwerk mit mindestens zwei gebundenen Verbindungen zu verwenden, idealerweise für unabhängige Netzwerk-Switches mit redundanter Stromversorgung.
> - Wenn Sie SMB-Speicher verwenden, entfernen Sie die Freigabe nicht aus dem Speicher,

> bevor Sie den SMB-SR trennen.

VDIs, die auf dateibasierten SRs gespeichert sind, werden *dünn bereitgestellt*. Die Image-Datei wird zugewiesen, während die VM Daten auf den Datenträger schreibt. Dieser Ansatz hat den erheblichen Vorteil, dass die VM-Image-Dateien nur so viel Speicherplatz auf dem Speicher beanspruchen, wie erforderlich ist. Wenn beispielsweise ein 100-GB-VDI für eine VM zugewiesen ist und ein Betriebssystem installiert ist, spiegelt die VDI-Datei nur die Größe der auf den Datenträger geschriebenen Betriebssystemdaten wider und nicht die gesamten 100 GB.

VHD-Dateien können auch verkettet werden, sodass zwei VDIs gemeinsame Daten gemeinsam nutzen können. In Fällen, in denen eine dateibasierte VM geklont wird, teilen sich die resultierenden VMs zum Zeitpunkt des Klonens die gemeinsamen Daten auf dem Datenträger. Jede VM nimmt ihre eigenen Änderungen in einer isolierten Copy-on-Write-Version des VDI vor. Mit dieser Funktion können dateibasierte VMs schnell aus Vorlagen geklont werden, was eine sehr schnelle Bereitstellung und Bereitstellung neuer VMs ermöglicht.

> **Hinweis:**
>
> Die maximal unterstützte Länge von VHD-Ketten beträgt 30.

Dateibasierte SRs- und VHD-Implementierungen in XenServer gehen davon aus, dass sie die volle Kontrolle über das SR-Verzeichnis auf dem Dateiserver haben. Administratoren dürfen den Inhalt des SR-Verzeichnisses nicht ändern, da durch diese Aktion der Inhalt von VDIs beschädigt werden kann.

XenServer wurde für Speicher der Enterprise-Klasse optimiert, der nichtflüchtiges RAM verwendet, um Schreibanforderungen schnell zu bestätigen und gleichzeitig ein hohes Maß an Datenschutz vor Ausfällen zu gewährleisten. XenServer wurde mit Data OnTap 7.3 und 8.1 ausgiebig gegen Network Appliance FAS2020- und FAS3210-Speicher getestet

> **Warnung:**
>
> Da VDIs auf dateibasierten SRs als Thin Provisioning erstellt werden, müssen Administratoren sicherstellen, dass die dateibasierten SRs über ausreichend Speicherplatz für alle erforderlichen VDIs verfügen. XenServer-Hosts erzwingen nicht, dass der für VDIs auf dateibasierten SRs erforderliche Speicherplatz vorhanden ist.
>
> Stellen Sie sicher, dass Sie den freien Speicherplatz auf Ihrem SR überwachen. Wenn die SR-Nutzung auf 100% ansteigt, schlagen weitere Schreibvorgänge von VMs fehl. Diese fehlgeschlagenen Schreibvorgänge können zum Einfrieren oder Absturz der VM führen.

Erstellen eines gemeinsam genutzten NFS-SR (NFS)

Um ein NFS-SR zu erstellen, müssen Sie den Hostnamen oder die IP-Adresse des NFS-Servers angeben. Sie können das SR auf jedem gültigen Zielpfad erstellen. Verwenden Sie den Befehl `sr-probe`, um eine Liste der vom Server exportierten gültigen Zielpfade anzuzeigen.

In Szenarien, in denen XenServer mit Low-End-Speicher verwendet wird, wartet es vorsichtig, bis alle Schreibvorgänge bestätigt wurden, bevor Bestätigungen an VMs weitergegeben werden. Dieser Ansatz verursacht erhebliche Leistungskosten und kann gelöst werden, indem der Speicher so eingestellt wird, dass der SR-Einhängepunkt als Export im asynchronen Modus dargestellt wird. Asynchrone Exporte bestätigen Schreibvorgänge, die nicht wirklich auf dem Datenträger sind. Überlegen Sie sich in diesen Situationen sorgfältig die Risiken eines Scheiterns.

> **Hinweis:**
>
> Der NFS-Server muss so konfiguriert sein, dass er den angegebenen Pfad zu allen Hosts im Pool exportiert. Wenn diese Konfiguration nicht erfolgt, schlägt das Erstellen des SRs und das Einstecken des PBD-Datensatzes fehl.

Die XenServer NFS-Implementierung verwendet standardmäßig TCP. Wenn es Ihre Situation zulässt, können Sie die Implementierung so konfigurieren, dass UDP in Szenarien verwendet wird, in denen möglicherweise ein Leistungsvorteil besteht. Um diese Konfiguration durchzuführen, geben Sie beim Erstellen eines SR den Parameter `device-config` mit `useUDP=true` an.

Die folgenden Parameter `device-config` werden mit NFS-SRs verwendet:

Parametername	Beschreibung	Erforderlich?
`server`	IP-Adresse oder Hostname des NFS-Servers	Ja
`serverpath`	Pfad, einschließlich des NFS-Einhängepunkts, zum NFS-Server, der das SR hostet	Ja
`nfsversion`	Gibt die zu verwendende Version von NFS an. Wenn Sie `nfsversion="4"` angeben, verwendet der SR NFS v4.0, v4.1 oder v4.2, je nachdem, was verfügbar ist. Wenn Sie eine spezifischere Version von NFS auswählen möchten, können Sie `nfsversion="4.0"` usw. angeben. Es kann nur ein Wert für `nfsversion` angegeben werden.	Nein
`useUDP`	Konfigurieren Sie den SR so, dass er UDP anstelle des Standard-TCP verwendet.	Nein

Verwenden Sie zum Beispiel den folgenden Befehl, um ein gemeinsam genutztes NFS-SR auf `192.168.1.10:/export1` mit einer beliebigen Version 4 von NFS zu erstellen, die vom Filer zur Verfügung gestellt wird:

```
    xe sr-create content-type=user \
    name-label="shared NFS SR" shared=true \
    device-config:server=192.168.1.10 device-config:serverpath=/export1
        type=nfs \
    device-config:nfsversion="4"
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um speziell mit NFS Version 4.0 ein nicht gemeinsam genutztes NFS-SR auf `192.168.1.10:/export1` zu erstellen:

```
    xe sr-create host-uuid=host_uuid content-type=user \
    name-label="Non-shared NFS SR" \
    device-config:server=192.168.1.10 device-config:serverpath=/export1
        type=nfs \
    device-config:nfsversion="4.0"
<!--NeedCopy-->
```

Erstellen eines gemeinsam genutzten SMB-SRs (SMB)

Um ein SMB-SR zu erstellen, geben Sie den Hostnamen oder die IP-Adresse des SMB-Servers, den vollständigen Pfad der exportierten Freigabe und die entsprechenden Anmeldeinformationen an.

Gerätekonfigurationsparameter für SMB SRs:

Parametername	Beschreibung	Erforderlich?
`server`	Vollständiger Pfad zur Freigabe auf dem Server	Ja
`username`	Benutzerkonto mit RW-Zugriff zum Teilen	Optional
`password_secret`	(Empfohlen) Geheime ID für das Kennwort für das Benutzerkonto, die anstelle des Kennworts verwendet werden kann.	Optional
`password`	Kennwort für das Benutzerkonto. Wir empfehlen, stattdessen den Parameter `password_secret` zu verwenden.	Optional

> **Hinweis:**
>
> Wenn Sie den Befehl `sr-create` ausführen, empfehlen wir, das Argument `device-config:password_secret` zu verwenden, anstatt das Kennwort in der Befehlszeile anzugeben. Weitere Informationen finden Sie unter Secrets.

Um beispielsweise ein gemeinsam genutztes SMB-SR auf `192.168.1.10:/share1` zu erstellen, verwenden Sie den folgenden Befehl:

```
1     xe sr-create content-type=user \
2     name-label="Example shared SMB SR" shared=true \
3     device-config:server=//192.168.1.10/share1 \
4     device-config:username=valid_username device-config:password_secret
         =valid_password_secret type=smb
5 <!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um ein nicht gemeinsam genutztes SMB-SR zu erstellen:

```
1     xe sr-create host-uuid=host_uuid content-type=user \
2     name-label="Non-shared SMB SR" \
3     device-config:server=//192.168.1.10/share1 \
4     device-config:username=valid_username device-config:password_secret
         =valid_password_secret type=smb
5 <!--NeedCopy-->
```

LVM über Hardware HBA

Der LVM-über-Hardware-HBA-Typ stellt Datenträger als VHDs auf logischen Volumes innerhalb einer Volume-Gruppe dar, die auf einer HBA-LUN erstellt wurde und beispielsweise hardwarebasierte iSCSI- oder FC-Unterstützung bietet.

XenServer-Hosts unterstützen Fibre-Channel-SANs über Emulex- oder QLogic-Hostbusadapter (HBAs). Die gesamte Fibre-Channel-Konfiguration, die erforderlich ist, um eine Fibre-Channel-LUN für den Host verfügbar zu Diese Konfiguration umfasst Speichergeräte, Netzwerkgeräte und den HBA innerhalb des XenServer-Hosts. Nachdem die gesamte FC-Konfiguration abgeschlossen ist, macht der HBA ein von der FC-LUN unterstütztes SCSI-Gerät für den Host verfügbar. Das SCSI-Gerät kann dann für den Zugriff auf die FC-LUN verwendet werden, als wäre es ein lokal angeschlossenes SCSI-Gerät.

Verwenden Sie den Befehl `sr-probe`, um die LUN-unterstützten SCSI-Geräte aufzulisten, die auf dem Host vorhanden sind. Dieser Befehl erzwingt einen Scan nach neuen LUN-gestützten SCSI-Geräten. Der von `sr-probe` für ein LUN-gestütztes SCSI-Gerät zurückgegebene Pfadwert ist auf allen Hosts mit Zugriff auf die LUN konsistent. Daher muss dieser Wert verwendet werden, wenn gemeinsam genutzte SRs erstellt werden, auf die alle Hosts in einem Ressourcenpool zugreifen können.

Dieselben Funktionen gelten für QLogic iSCSI-HBAs.

Weitere Informationen zum Erstellen von gemeinsam genutzten HBA-basierten FC- und iSCSI-SRs finden Sie unter Erstellen von Speicherrepositories .

> **Hinweis:**
>
> Die XenServer-Unterstützung für Fibre Channel unterstützt keine direkte Zuordnung einer LUN zu einer VM. HBA-basierte LUNs müssen dem Host zugeordnet und für die Verwendung in einem SR angegeben werden. VDIs innerhalb des SRs sind für VMs als standardmäßige Blockgeräte verfügbar.
>
> Die Blockgröße einer LVM-über-HBA-LUN muss 512 Byte betragen. Um Speicher mit physischen Blöcken von 4 KB zu verwenden, muss der Speicher auch die Emulation von 512-Byte-Zuweisungsblöcken unterstützen (die logische Blockgröße muss 512 Byte betragen).

---

layout: doc
description: “Thin provisioning better utilizes the available storage by allocating disk storage space to VDIs as data is written to the virtual disk, rather than allocating the full virtual size of the VDI in advance. The shared GFS2 type represents disks as a filesystem created on an iSCSI or HBA LUN.”
—

Gemeinsam genutzter GFS2-Blockspeicher mit Thin-Provisioning

Beim Thin Provisioning wird der verfügbare Speicher besser genutzt, indem VDIs Datenträgerspeicherplatz zugewiesen wird, während die Daten auf das virtuelle Laufwerk geschrieben werden, anstatt die volle virtuelle Größe des VDI im Voraus zuzuweisen. Thin Provisioning ermöglicht es Ihnen, den auf einem gemeinsam genutzten Speicher-Array benötigten Speicherplatz und damit Ihre Gesamtbetriebskosten (TCO) erheblich zu reduzieren.

Thin Provisioning für gemeinsam genutzten Blockspeicher ist in den folgenden Fällen von besonderem Interesse:

- Sie möchten eine höhere Raumeffizienz. Images werden spärlich und nicht dicht verteilt.
- Sie möchten die Anzahl der I/O-Vorgänge pro Sekunde auf Ihrem Speicher-Array reduzieren. GFS2-SR ist der erste SR-Typ, der das Speicherlesecaching auf gemeinsam genutztem Blockspeicher unterstützt.
- Sie verwenden ein allgemeines Basisimage für mehrere virtuelle Maschinen. Die Images einzelner VMs benötigen dann in der Regel noch weniger Speicherplatz.
- Sie verwenden Schnappschüsse. Jeder Snapshot ist ein Image und jedes Image ist jetzt spärlich.
- Sie möchten VDIs erstellen, die größer als 2 TiB sind. Der GFS2 SR unterstützt VDIs mit einer Größe von bis zu 16 TiB.

- Ihr Speicher unterstützt weder NFS noch SMB3 und unterstützt nur Blockspeicher. Wenn Ihr Speicher NFS oder SMB3 unterstützt, empfehlen wir Ihnen, diese SR-Typen anstelle von GFS2 zu verwenden.
- Ihr Speicher unterstützt kein Thin Provisioning von LUNs. Wenn Ihr Speicher Thin Provision-LUNs verwendet, können Probleme auftreten und Ihnen der Speicherplatz ausgeht, wenn Sie ihn mit GFS2 kombinieren. Die Kombination von GFS2 mit einer Thin-Provision-LUN bietet nicht viele zusätzliche Vorteile und wird nicht empfohlen.

> **Hinweis:**
>
> Wir empfehlen, GFS2 SR nicht mit einem VLAN zu verwenden, da ein bekanntes Problem besteht, bei dem Sie Hosts in einem Clusterpool nicht hinzufügen oder entfernen können, wenn sich das Clusternetzwerk in einem Nicht-Management-VLAN befindet.

Der gemeinsam genutzte GFS2-Typ stellt Datenträger als Dateisystem dar, das auf einer iSCSI- oder HBA-LUN erstellt wurde. Auf einem GFS2 SR gespeicherte VDIs werden im QCOW2-Imageformat gespeichert.

In diesem Artikel wird beschrieben, wie Sie Ihre GFS2-Umgebung mithilfe der Xe-CLI einrichten. Informationen zum Einrichten einer GFS2-Umgebung mithilfe von XenCenter finden Sie in derXenCenter-Produktdokumentation.

1. Planen Sie Ihre GFS2-Umgebung

Um die Vorteile von Thin Provisioning auf gemeinsam genutztem Blockspeicher ohne das Risiko eines Datenverlusts nutzen zu können, muss Ihr Pool ein gutes Maß an Zuverlässigkeit und Konnektivität bieten. Es ist entscheidend, dass die Hosts im Ressourcenpool, die GFS2 verwenden, zuverlässig miteinander kommunizieren können. Um dies sicherzustellen, erfordert XenServer, dass Sie einen Clusterpool mit Ihrem GFS2 SR verwenden. Wir empfehlen Ihnen außerdem, Ihre Umgebung zu entwerfen und die XenServer-Funktionen so zu konfigurieren, dass sie so viel Stabilität und Redundanz wie möglich bieten.

Bevor Sie Ihren XenServer-Pool für die Verwendung mit GFS2-SRs einrichten, sollten Sie die folgenden Anforderungen und Empfehlungen für eine ideale GFS2-Umgebung lesen:

- **Empfehlung:** Konfigurieren Sie eine redundante Netzwerkinfrastruktur.
- **Empfohlen:** Erstellen Sie ein dediziertes gebundenesNetzwerk
- **Erforderlich:** Richten Sie einen Clusterpool ein
- **Optional:** Erhöhen Sie den Speicher Ihrer Steuerdomäne
- **Empfehlung:** Speicher-Multipathing konfigurieren

- **Erforderlich:** Erstellen Sie eine GFS2-SR

Ein geclusterter Pool mit GFS2-SRs weist einige Verhaltensunterschiede zu anderen Pool- und SR-Typen auf. Weitere Informationen finden Sie unter Einschränkungen.

2. Konfiguration einer redundanten Netzwerkinfrastruktur

Ein gebundenes Netzwerk verbindet zwei oder mehr NICs miteinander, um einen einzigen Kanal für den Netzwerkverkehr zu schaffen. Wir empfehlen, dass Sie ein gebundenes Netzwerk für Ihren Clusterpool-Verkehr verwenden. Bevor Sie Ihr gebündeltes Netzwerk einrichten, stellen Sie jedoch sicher, dass Ihre Netzwerkhardwarekonfiguration die Redundanz im gebundenen Netzwerk fördert. Erwägen Sie, so viele dieser Empfehlungen umzusetzen, wie es für Ihr Unternehmen und Ihre Umgebung möglich ist.

Die folgenden bewährten Methoden erhöhen die Widerstandsfähigkeit gegen Software-, Hardware- oder Stromausfälle, die sich auf Ihre Netzwerk-Switches auswirken können.

- Stellen Sie sicher, dass Sie separate physische Netzwerk-Switches für die Verwendung im gebündelten Netzwerk zur Verfügung haben, nicht nur Ports auf demselben Switch.
- Stellen Sie sicher, dass die einzelnen Switches Strom von verschiedenen, unabhängigen Stromverteilungseinheiten (PDUs) beziehen.
- Wenn möglich, platzieren Sie die PDUs in Ihrem Rechenzentrum an verschiedenen Phasen der Stromversorgung oder sogar an Einspeisungen, die von verschiedenen Versorgungsunternehmen bereitgestellt werden.
- Erwägen Sie die Verwendung von unterbrechungsfreien Stromversorgungen, um sicherzustellen, dass die Netzwerk-Switches und Server weiterhin funktionieren oder bei einem Stromausfall ordnungsgemäß heruntergefahren werden können.

3. Erstellen Sie ein dediziertes gebundenes Netzwerk

Es ist wichtig sicherzustellen, dass Hosts in einem Clusterpool zuverlässig miteinander kommunizieren können. Das Erstellen eines Verbundnetzwerks für diesen Pool-Verkehr erhöht die Ausfallsicherheit Ihres Clusterpools.

Ein gebundenes Netzwerk stellt eine Verbindung zwischen zwei oder mehr NICs her, um einen einzigen, leistungsstarken Kanal zu erstellen, den Ihr Clusterpool für Cluster-Heartbeat-Verkehr verwenden kann. Wir empfehlen dringend, dieses gebündelte Netzwerk nicht für anderen Datenverkehr zu verwenden. Erstellen Sie ein separates Netzwerk für den Pool, das für die Verwaltung des Datenverkehrs verwendet werden soll.

> **Warnung:**
>
> Wenn Sie dieser Empfehlung nicht folgen, besteht ein höheres Risiko, Netzwerkpakete für die Clusterverwaltung zu verlieren. Der Verlust von Netzwerkpaketen für die Clusterverwaltung kann dazu führen, dass Ihr Clusterpool das Quorum verliert und einige oder alle Hosts im Pool sich selbst umzäunen.
>
> Wenn Ihr Cluster ein Fencing hat oder ein Problem in dieser nicht empfohlenen Konfiguration auftritt, werden Sie vom XenServer-Support im Laufe der Untersuchung möglicherweise gebeten, dasselbe Problem in einer empfohlenen Konfiguration zu reproduzieren.

So erstellen Sie ein gebundenes Netzwerk, das als Clusternetzwerk verwendet werden soll:

1. Wenn Sie eine Firewall zwischen den Hosts in Ihrem Pool haben, stellen Sie sicher, dass Hosts über die folgenden Ports im Cluster-Netzwerk kommunizieren können:

   - TCP: 8892, 8896, 21064
   - UDP: 5404, 5405

   Weitere Informationen finden Sie unter Von XenServer verwendete Kommunikationsports.

2. Öffnen Sie eine Konsole auf dem XenServer-Host, den Sie als Poolkoordinator verwenden möchten.

3. Erstellen Sie ein Netzwerk zur Verwendung mit der gebundenen NIC, indem Sie den folgenden Befehl verwenden:

   ```
   xe network-create name-label=bond0
   <!--NeedCopy-->
   ```

   Die UUID des neuen Netzwerks wird zurückgegeben.

4. Suchen Sie die UUIDs der PIFs, die in der Bindung verwendet werden sollen, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

5. Erstellen Sie Ihr gebundenes Netzwerk entweder im aktiv-aktiven Modus, im aktiv-passiven Modus oder im LACP-Bond-Modus. Führen Sie je nach dem Bond-Modus, den Sie verwenden möchten, eine der folgenden Aktionen aus:

   - Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den Befehl `bond-create`, um die Bindung zu erstellen. Trennen Sie die Parameter durch Kommas und geben Sie die neu erstellte Netzwerk-UUID und die UUIDs der zu verbindenden PIFs an:


```
xe bond-create network-uuid=<network_uuid> /
    pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4>
<!--NeedCopy-->
```

Geben Sie zwei UUIDs ein, wenn Sie zwei NICs und vier UUIDs verbinden, wenn Sie vier Netzwerkkarten verbinden. Die UUID für die Bindung wird nach Ausführung des Befehls zurückgegeben.

- Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie dieselbe Syntax, fügen Sie den optionalen Parameter `mode` hinzu und geben Sie `lacp` oder `active-backup` an:

```
xe bond-create network-uuid=<network_uuid> /
    pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4> /
    mode=balance-slb | active-backup | lacp
<!--NeedCopy-->
```

Nachdem Sie Ihr gebundenes Netzwerk auf dem Poolkoordinator erstellt haben und andere XenServer-Hosts mit dem Pool verbinden, werden die Netzwerk- und Bindungsinformationen automatisch auf den beitretenden Server repliziert.

Weitere Informationen finden Sie unter Netzwerk.

> **Hinweis:**
>
> - Um die IP-Adresse des Cluster-Netzwerks mithilfe von XenCenter zu ändern, müssen Clustering und GFS2 vorübergehend deaktiviert werden.
> - Ändern Sie nicht die Bindung Ihres Clusternetzwerks, während der Cluster aktiv ist und über laufende VMs verfügt. Diese Aktion kann dazu führen, dass Hosts im Cluster neu gestartet werden (Fencing).
> - Wenn Sie in Ihrem Clusternetzwerk einen IP-Adresskonflikt haben (mehrere Hosts mit derselben IP-Adresse), an dem mindestens ein Host mit aktiviertem Clustering beteiligt ist, wird der Cluster nicht korrekt gebildet und die Hosts können bei Bedarf kein Fencing durchführen. Um dieses Problem zu beheben, lösen Sie den IP-Adresskonflikt.

So testen Sie die Failover-Zeiten für Ihr aktiv-passives gebundenes Netzwerk:

Bei verbundenen Netzwerken, die den Aktiv-Passiv-Modus verwenden, gibt es beim Ausfall der aktiven Verbindung eine Failover-Phase, in der die Netzwerkverbindung unterbrochen wird, während die passive Verbindung aktiv wird. Wenn die Zeit, die für das Failover Ihres Aktiv-Passiv-Verbundnetzwerks benötigt wird, länger als das Cluster-Timeout ist, können einige oder alle Hosts in Ihrem Clusterpool immer noch eingezäunt sein.

Sie können die Failoverzeit Ihres verbundenen Netzwerks testen, indem Sie das Netzwerk mithilfe einer der folgenden Methoden zum Failover zwingen:

- Durch physisches Herausziehen der Netzwerkkabel
- Durch Deaktivieren von Switch-Ports an einer Netzwerkverbindung

Wiederholen Sie den Test mehrmals, um sicherzustellen, dass das Ergebnis konsistent ist.

Der Cluster-Timeout-Wert Ihres Pools hängt davon ab, wie viele Hosts sich in Ihrem Cluster befinden. Führen Sie den folgenden Befehl aus, um den Wert `token-timeout` für den Pool in Sekunden zu ermitteln:

```
1 xe cluster-param-get uuid=<cluster_uuid> param-name=token-timeout
```

Wenn die Failover-Zeit wahrscheinlich über dem Timeout-Wert liegt, sind Ihre Netzwerkinfrastruktur und Konfiguration möglicherweise nicht zuverlässig genug, um einen Clusterpool zu unterstützen.

4. Richten Sie einen Clusterpool ein

Um gemeinsam genutzten GFS2-Speicher zu verwenden, muss der XenServer-Ressourcenpool ein Clusterpool sein. Aktivieren Sie das Clustering in Ihrem Pool, bevor Sie ein GFS2-SR erstellen.

Ein Clusterpool ist ein Pool von XenServer-Hosts, die enger miteinander verbunden und koordiniert sind als Hosts in nicht geclusterten Pools. Die Hosts im Cluster kommunizieren ständig miteinander in einem ausgewählten Netzwerk. Alle Hosts im Cluster kennen den Status jedes Hosts im Cluster. Diese Host-Koordination ermöglicht es dem Cluster, den Zugriff auf den Inhalt des GFS2-SRs zu steuern. Um sicherzustellen, dass der Clusterpool immer in Verbindung bleibt, muss jeder Host in einem Cluster immer mit mindestens der Hälfte der Hosts im Cluster kommunizieren (einschließlich sich selbst). Dieser Zustand ist als Host mit Quorum bekannt. Wenn ein Host kein Quorum hat, wird er neu gestartet und entfernt sich selbst aus dem Cluster. Diese Aktion wird als “Fechten”bezeichnet.

Weitere Informationen finden Sie unter Clustered-Pools.

Bevor Sie mit der Einrichtung Ihres Clusterpools beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Planen Sie, einen Pool mit 3 bis 16 Hosts zu erstellen.

  Verwenden Sie nach Möglichkeit eine ungerade Anzahl von Hosts in einem Clusterpool, da dadurch sichergestellt wird, dass Hosts immer feststellen können, ob sie Quorun haben. Es wird empfohlen, Clustering nur in Pools mit mindestens drei Hosts zu verwenden, da Pools von zwei Hosts empfindlich auf das Selbst-Fencing des gesamten Pools reagieren.

  Clusterpools unterstützen nur bis zu 16 Hosts pro Pool.

- Alle XenServer-Hosts im Clusterpool müssen über mindestens 2 GiB Steuerdomänenspeicher verfügen.

- Alle Hosts im Cluster müssen statische IP-Adressen für das Cluster-Netzwerk verwenden.
- Wenn Sie einen vorhandenen Pool clustern, stellen Sie sicher, dass die Hochverfügbarkeit deaktiviert ist. Sie können die Hochverfügbarkeit erneut aktivieren, nachdem das Clustering aktiviert wurde.

So verwenden Sie die xe CLI zum Erstellen eines Clusterpool:

1. Erstellen Sie einen Ressourcenpool mit mindestens drei XenServer-Hosts.

   Wiederholen Sie die folgenden Schritte auf jedem beitretenden XenServer-Host, der nicht der Poolkoordinator ist:

   a) Öffnen Sie eine Konsole auf dem XenServer-Host.

   b) Verbinden Sie den XenServer-Host mit dem Pool auf dem Poolkoordinator, indem Sie den folgenden Befehl verwenden:

   ```
   xe pool-join master-address=<master_address> /
       master-username=<administrators_username> /
       master-password=<password>
   <!--NeedCopy-->
   ```

   Der Wert des `master-address` Parameters muss auf den vollqualifizierten Domänennamen des XenServer-Hosts gesetzt werden, der der Poolkoordinator ist. Das `password` muss das Administratorkennwort sein, das bei der Installation des Poolkoordinators festgelegt wurde.

   Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

2. Stellen Sie für jedes PIF, das zu diesem Netzwerk gehört, ein `disallow-unplug=true`.

   a) Suchen Sie die UUIDs der PIFs, die zum Netzwerk gehören, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list
   <!--NeedCopy-->
   ```

   b) Führen Sie den folgenden Befehl auf einem XenServer-Host in Ihrem Ressourcenpool aus:

   ```
   xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
   <!--NeedCopy-->
   ```

3. Aktivieren Sie das Clustering in Ihrem Pool. Führen Sie den folgenden Befehl auf einem XenServer-Host in Ihrem Ressourcenpool aus:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   <!--NeedCopy-->
   ```

   Geben Sie die UUID des gebundenen Netzwerks an, das Sie in einem früheren Schritt erstellt haben.

5. Erhöhen Sie den Speicher Ihrer Steuerdomäne

Wenn Sie auf Ihren Hosts nicht genügend Steuerdomänenspeicher haben, kann es in Ihrem Pool zu Netzwerkinstabilität kommen. Netzwerkinstabilität kann bei einem Clusterpool mit GFS2-SRs zu Problemen führen.

Es ist wichtig sicherzustellen, dass Ihr Clusterpool über eine angemessene Menge an Steuerdomänenspeicher verfügt. Hinweise zum Ändern der Größe des Steuerdomänenspeichers und zum Überwachen des Speicherverhaltens finden Sie unter Speicherauslastung.

6. Speicher-Multipathing konfigurieren

Stellen Sie sicher, dass Storage-Multipathing zwischen Ihrem Clusterpool und Ihrem GFS2-SR eingerichtet ist.

Multipathing leitet den Speicherdatenverkehr aus Redundanzgründen über mehrere Pfade an ein Speichergerät weiter. Auf allen Strecken kann während des normalen Betriebs aktiver Verkehr herrschen, was zu einem erhöhten Durchsatz führt.

Bevor Sie Multipathing aktivieren, überprüfen Sie, ob die folgenden Anweisungen zutreffen:

- Ihr Ethernet- oder Fibre-Switch ist so konfiguriert, dass mehrere Ziele auf Ihrem Speicherserver verfügbar sind.

  Beispielsweise gibt ein iSCSI-Speicher-Backend, das nach `sendtargets` für ein bestimmtes Portal abgefragt wird, mehrere Ziele zurück, wie im folgenden Beispiel:

  ```
  iscsiadm -m discovery --type sendtargets --portal 192.168.0.161
  192.168.0.161:3260,1 iqn.strawberry:litchie
  192.168.0.204:3260,2 iqn.strawberry:litchie
  ```

  Sie können jedoch eine zusätzliche Konfiguration durchführen, um iSCSI-Multipath für Arrays zu aktivieren, die nur ein einziges Ziel verfügbar machen. Weitere Informationen finden Sie unter iSCSI Multipath für Arrays, die nur ein einziges Zielverfügbar machen.

- Nur für iSCSI hat die Steuerdomäne (dom0) eine IP-Adresse in jedem Subnetz, das vom Multipath-Speicher verwendet wird.

  Stellen Sie sicher, dass Sie für jeden Pfad zum Speicher über eine Netzwerkkarte verfügen und dass auf jeder Netzwerkkarte eine IP-Adresse konfiguriert ist. Wenn Sie beispielsweise vier Pfade zu Ihrem Speicher wünschen, müssen Sie über vier Netzwerkkarten verfügen, für die jeweils eine IP-Adresse konfiguriert ist.

- Nur für iSCSI hat jedes iSCSI-Ziel und jeder iSCSI-Initiator einen eigenen IQN.

- Nur für iSCSI arbeiten die iSCSI-Zielports im Portalmodus.

- Nur für HBA sind mehrere HBAs an die Switch-Fabric angeschlossen.
- Verwenden Sie nach Möglichkeit mehrere redundante Switches.

So aktivieren Sie Multipathing mit der xe-CLI

Wir empfehlen, dass Sie Multipathing für alle Hosts in Ihrem Pool aktivieren, *bevor Sie die SR* erstellen. Wenn Sie die SR erstellen, bevor Sie Multipathing aktivieren, müssen Sie Ihre Hosts in den Wartungsmodus versetzen, um Multipathing zu aktivieren.

1. Öffnen Sie eine Konsole auf dem XenServer-Host.
2. Trennen Sie alle PBDs auf dem Host mit dem folgenden Befehl:

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   <!--NeedCopy-->
   ```

   Sie können den Befehl verwenden `xe pbd-list`, um die UUID der PBDs zu finden.
3. Setzen Sie den Wert des Parameters `multipathing` auf **`true`**, indem Sie den folgenden Befehl verwenden:

   ```
   xe host-param-set uuid=<host uuid> multipathing=true
   <!--NeedCopy-->
   ```
4. Wenn auf den Hosts, die im Einzelpfadmodus ausgeführt werden, SRs mit mehreren Pfaden vorhanden sind:

   - Migrieren oder unterbrechen Sie alle laufenden Gäste mit virtuellen Datenträgern in den betroffenen SRs.
   - Schließen Sie die PBD aller betroffenen SRs erneut an, um sie mithilfe von Multipathing erneut zu verbinden:

     ```
     xe pbd-plug uuid=<pbd_uuid>
     <!--NeedCopy-->
     ```
5. Wiederholen Sie diese Schritte, um Multipathing auf allen Hosts im Pool zu aktivieren.

Stellen Sie sicher, dass Sie Multipathing auf allen Hosts im Pool aktivieren. Die gesamte Verkabelung und, im Fall von iSCSI, die Subnetzkonfigurationen müssen mit den entsprechenden NICs auf jedem Host übereinstimmen.

Weitere Informationen finden Sie unter Speicher-Multipathing.

7. Erstellen Sie eine GFS2-SR

Erstellen Sie Ihre gemeinsam genutzte GFS2 SR auf einer iSCSI- oder HBA-LUN, die für alle XenServer-Hosts in Ihrem Ressourcenpool sichtbar ist. Wir empfehlen nicht, eine Thin-Provision-LUN mit GFS2 zu verwenden. Wenn Sie diese Konfiguration wählen, müssen Sie jedoch sicherstellen, dass die LUN immer über genügend Speicherplatz verfügt, damit XenServer darauf schreiben kann.

Sie können einem Clusterpool bis zu 62 GFS2-SRs hinzufügen.

Wenn Sie Ihr blockbasiertes Speichergerät zuvor für Thick Provisioning mit LVM verwendet haben, wird dies von XenServer erkannt. XenCenter bietet Ihnen die Möglichkeit, die vorhandene LVM-Partition zu verwenden oder den Datenträger zu formatieren und eine GFS2-Partition einzurichten.

Erstellen eines gemeinsam genutzten GFS2 über iSCSI SR

Sie können GFS2 über iSCSI-SRs mit XenCenter erstellen. Weitere Informationen finden Sie unter Software-iSCSI-Speicher in der XenCenter-Produktdokumentation .

Alternativ können Sie die xe CLI verwenden, um ein GFS2 über iSCSI SR zu erstellen.

Gerätekonfigurationsparameter für GFS2-SRs:

Parametername	Beschreibung	Erforderlich?
`provider`	Die Blockanbieter-Implementierung. In diesem Fall, `iscsi`.	Ja
`target`	Die IP-Adresse oder der Hostname des iSCSI-Filers, der hostet	Ja
`targetIQN`	Das IQN-Ziel des iSCSI-Filers, der das SR hostet	Ja
`SCSIid`	SCSI-ID des Geräts	Ja

Sie können die für diese Parameter zu verwendenden Werte mit dem Befehl `xe sr-probe-ext` finden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
   config> sm-config:=<sm_config>
<!--NeedCopy-->
```

1. Führen Sie zunächst den folgenden Befehl aus:


```
xe sr-probe-ext type=gfs2 device-config:provider=iscsi
<!--NeedCopy-->
```

Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben, und enthält bei jedem Schritt eine Liste möglicher Werte.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.
3. Wenn die Befehlsausgabe mit beginnt `Found the following complete configurations that can be used to create SRs:`, können Sie den SR mithilfe des `xe sr-create` Befehls und der von Ihnen angegebenen `device-config` Parameter suchen.

   Beispielausgabe:

   “‘Es
   wurden die folgenden vollständigen Konfigurationen gefunden, die zur Erstellung von SRs verwendet werden können:
   Konfiguration 0:
   scsiID:
   36001405852f77532a064687aea8a5b3f TargetIQN: iqn.2009-01.example.com:iscsi192a25d6
   Ziel : 198.51.100.27 Anbieter: iscsi

   Configuration 0 extra information:
   “‘

Um ein gemeinsam genutztes GFS2-SR auf einer bestimmten LUN eines iSCSI-Ziels zu erstellen, führen Sie den folgenden Befehl auf einem Server in Ihrem Clusterpool aus:

```
xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
   device-config:provider=iscsi device-config:targetIQN=<target_iqns> \
   device-config:target=<portal_address> device-config:SCSIid=<scsci_id
      >
```

Wenn das iSCSI-Ziel nicht erreichbar ist, während GFS2-Dateisysteme gemountet sind, kann es sein, dass einige Hosts im Clusterpool neu gestartet werden (Fencing).

Weitere Informationen zum Arbeiten mit iSCSI SRs finden Sie unter Software-iSCSI-Unterstützung.

Erstellen eines gemeinsam genutzten GFS2 über HBA SR

Sie können GFS2 über HBA-SRs erstellen, indem Sie XenCenter verwenden. Weitere Informationen finden Sie unter Hardware-HBA-Speicher in der XenCenter-Produktdokumentation.

Alternativ können Sie die xe CLI verwenden, um ein GFS2 über HBA SR zu erstellen.

Gerätekonfigurationsparameter für GFS2-SRs:

Parametername	Beschreibung	Erforderlich?
provider	Die Blockanbieter-Implementierung. In diesem Fall, hba.	Ja
SCSIid	SCSI-ID des Geräts	Ja

Sie können die für den SCSIid-Parameter zu verwendenden Werte mit dem Befehl xe sr-probe-ext finden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Führen Sie zunächst den folgenden Befehl aus:

   ```
   xe sr-probe-ext type=gfs2 device-config:provider=hba
   ```

   Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben, und enthält bei jedem Schritt eine Liste möglicher Werte.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.

3. Wenn die Befehlsausgabe mit beginnt Found the following complete configurations that can be used to create SRs:, können Sie den SR mithilfe des xe sr-create Befehls und der von Ihnen angegebenen device-config Parameter suchen.

   Beispielausgabe:

   “‘Es
   wurden die folgenden vollständigen Konfigurationen gefunden, die zur Erstellung von SRs verwendet werden können:
   Konfiguration 0:
   scsiID:
   36001405852f77532a064687aea8a5b3f TargetIQN: iqn.2009-01.example.com:iscsi192a25d6 Ziel : 198.51.100.27 Anbieter: iscsi

   Configuration 0 extra information:
   “‘

Um ein gemeinsam genutztes GFS2-SR auf einer bestimmten LUN eines HBA-Ziels zu erstellen, führen Sie den folgenden Befehl auf einem Server in Ihrem Clusterpool aus:

```
xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
  device-config:provider=hba device-config:SCSIid=<device_scsi_id>
<!--NeedCopy-->
```

Weitere Informationen zum Arbeiten mit HBA-SRs finden Sie unter Hardware-Hostbusadapter.

Was kommt als Nächstes?

Nachdem Sie Ihre GFS2-Umgebung eingerichtet haben, ist es wichtig, dass Sie die Stabilität Ihres Clusterpools aufrechterhalten, indem Sie sicherstellen, dass er über ein Quorum verfügt. Weitere Informationen finden Sie unter Verwalten Ihres Clusterpools.

Wenn Probleme mit Ihrer GFS2-Umgebung auftreten, finden Sie weitere Informationen unter Problembehandlung bei Clusterpools.

Sie können Ihren GFS2 SR genauso verwalten wie andere SRs. Sie können beispielsweise dem Speicher-Array Kapazität hinzufügen, um die Größe der LUN zu erhöhen. Weitere Informationen finden Sie unter Live-LUN-Erweiterung.

Einschränkungen

Gemeinsam genutzter GFS2-Speicher weist derzeit die folgenden Einschränkungen auf:

- Wie bei jeder Thin-Provisioning-SR schlagen weitere Schreibvorgänge von VMs fehl, wenn die GFS2 SR-Nutzung auf 100% ansteigt. Diese fehlgeschlagenen Schreibvorgänge können dann zu Ausfällen innerhalb der VM, möglichen Datenbeschädigungen oder beidem führen.
- XenCenter zeigt eine Warnung an, wenn Ihre SR-Auslastung auf 80% ansteigt. Stellen Sie sicher, dass Sie Ihren GFS2 SR auf diese Warnung überwachen und gegebenenfalls die entsprechenden Maßnahmen ergreifen. Bei einem GFS2 SR führt eine hohe Auslastung zu einer Leistungsverschlechterung. Wir empfehlen, dass Sie Ihre SR-Nutzung unter 80% halten.
- VM-Migration mit Speichermigration (live oder offline) wird für VMs, deren VDIs sich auf einem GFS2-SR befinden, nicht unterstützt. Sie können auch keine VDIs von einem anderen SR-Typ auf eine GFS2 SR migrieren.
- Der FCoE-Transport wird mit GFS2-SRs nicht unterstützt.
- Trim/Unmap wird auf GFS2 SRs nicht unterstützt.
- CHAP wird auf GFS2 SRs nicht unterstützt.
- Leistungsmetriken sind für GFS2 SRs und Datenträger auf diesen SRs nicht verfügbar.
- Die geänderte Blockverfolgung wird für VDIs, die auf GFS2 SRs gespeichert sind, nicht unterstützt.
- Sie können VDIs, die größer als 2 TiB sind, nicht als VHD oder OVA/OVF exportieren. Sie können jedoch VMs mit VDIs, die größer als 2 TiB sind, im XVA-Format exportieren.
- Wir empfehlen nicht, eine Thin-Provision-LUN mit GFS2 zu verwenden. Wenn Sie diese Konfiguration wählen, müssen Sie jedoch sicherstellen, dass die LUN immer über genügend Speicherplatz verfügt, damit XenServer darauf schreiben kann.

- Sie können nicht mehr als 62 GFS2 SRs in Ihrem Pool haben.
- Clusterpools unterstützen nur bis zu 16 Hosts pro Pool.
- Um HA in Ihrem Clusterpool zu aktivieren, muss der Heartbeat-SR ein GFS2-SR sein.
- Für Clusterverkehr empfehlen wir dringend, ein gebundenes Netzwerk zu verwenden, das mindestens zwei verschiedene Netzwerk-Switches verwendet. Verwenden Sie dieses Netzwerk nicht für andere Zwecke.
- Um die IP-Adresse des Cluster-Netzwerks mithilfe von XenCenter zu ändern, müssen Clustering und GFS2 vorübergehend deaktiviert werden.
- Ändern Sie nicht die Bindung Ihres Clusternetzwerks, während der Cluster aktiv ist und über laufende VMs verfügt. Diese Aktion kann dazu führen, dass Hosts im Cluster neu gestartet werden (Fencing).
- Wenn Sie in Ihrem Clusternetzwerk einen IP-Adresskonflikt haben (mehrere Hosts mit derselben IP-Adresse), an dem mindestens ein Host mit aktiviertem Clustering beteiligt ist, wird der Cluster nicht korrekt gebildet und die Hosts können bei Bedarf kein Fencing durchführen. Um dieses Problem zu beheben, lösen Sie den IP-Adresskonflikt.

---

layout: doc
description: Create and manage storage repositories in your XenServer environment.—

Verwalten von Speicherrepositories

In diesem Abschnitt wird beschrieben, wie Speicher-Repository-Typen erstellt und für Ihren XenServer-Host verfügbar gemacht werden. Es deckt auch verschiedene Vorgänge ab, die für die laufende Verwaltung von Speicherrepositories (SRs) erforderlich sind, einschließlich Live-VDI-Migration.

Erstellen von Speicherrepositories

In diesem Abschnitt wird erklärt, wie Sie Storage Repositories (SRs) verschiedener Typen erstellen und sie Ihrem XenServer-Host zur Verfügung stellen. In den bereitgestellten Beispielen wird das Erstellen von SRs über die xe-CLI behandelt. Einzelheiten zur Verwendung des Assistenten für **neues Speicherrepository** zum Hinzufügen von SRs mit XenCenter finden Sie in der XenCenter-Dokumentation.

> **Hinweis:**
>
> Lokale SRs vom Typ `lvm`, `ext` und `xfs` können nur mit der xe-CLI erstellt werden. Nach dem Erstellen können Sie alle SR-Typen entweder über XenCenter oder die xe-CLI verwalten.

Es gibt zwei grundlegende Schritte zum Erstellen eines Speicherrepositorys für die Verwendung auf einem Host über die CLI:

1. Prüfen Sie den SR-Typ, um Werte für alle erforderlichen Parameter zu ermitteln.
2. Erstellen Sie das SR, um das SR-Objekt und die zugehörigen PBD-Objekte zu initialisieren, schließen Sie die PBDs an und aktivieren Sie das SR.

Diese Schritte unterscheiden sich je nach Art des zu erstellenden SRs im Detail. In allen Beispielen gibt der Befehl `sr-create` bei Erfolg die UUID des erstellten SR zurück.

SRs können *zerstört* werden, wenn sie nicht mehr verwendet werden, um das physische Gerät freizugeben. SRs können auch *vergessen* werden, die SR von einem XenServer-Host zu trennen und an einen anderen anzuhängen. Weitere Informationen finden Sie im folgenden Abschnitt unter *SRs entfernen* .

Testen eines SR

Der Befehl `sr-probe` kann auf folgende Weise verwendet werden:

- So identifizieren Sie unbekannte Parameter für die Erstellung eines SRs
- So geben Sie eine Liste vorhandener SRs zurück

In beiden Fällen wird mit `sr-probe` ein SR-Typ und ein oder mehrere `device-config`-Parameter für diesen SR-Typ angegeben. Wenn ein unvollständiger Satz von Parametern angegeben wird, gibt der Befehl `sr-probe` eine Fehlermeldung zurück, die angibt, dass Parameter fehlen und die möglichen Optionen für die fehlenden Parameter angezeigt werden. Wenn ein vollständiger Satz von Parametern geliefert wird, wird eine Liste der vorhandenen SRs zurückgegeben. Die gesamte `sr-probe`-Ausgabe wird als XML zurückgegeben.

Ein bekanntes iSCSI-Ziel kann beispielsweise durch Angabe seines Namens oder seiner IP-Adresse untersucht werden. Der Satz von IQNs, der auf dem Ziel verfügbar ist, wird zurückgegeben:

```
1     xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10
2
3     Error code: SR_BACKEND_FAILURE_96
4     Error parameters: , The request is missing or has an incorrect
         target IQN parameter, \
5     <?xml version="1.0" ?>
6     <iscsi-target-iqns>
7         <TGT>
```



```
            <Index>
                0
            </Index>
            <IPAddress>
                192.168.1.10
            </IPAddress>
            <TargetIQN>
                iqn.192.168.1.10:filer1
            </TargetIQN>
        </TGT>
    </iscsi-target-iqns>
<!--NeedCopy-->
```

Wenn Sie dasselbe Ziel erneut prüfen und sowohl den Namen/die IP-Adresse als auch den gewünschten IQN angeben, wird der Satz von `SCSIids` (LUNs) zurückgegeben, die auf dem Ziel/IQN verfügbar sind.

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=iqn.192.168.1.10:filer1

    Error code: SR_BACKEND_FAILURE_107
    Error parameters: , The SCSIid parameter is missing or incorrect, \
    <?xml version="1.0" ?>
    <iscsi-target>
        <LUN>
            <vendor>
                IET
            </vendor>
            <LUNid>
                0
            </LUNid>
            <size>
                42949672960
            </size>
            <SCSIid>
                149455400000000000000000002000000b70200000f000000
            </SCSIid>
        </LUN>
    </iscsi-target>
<!--NeedCopy-->
```

Wenn Sie dasselbe Ziel prüfen und alle drei Parameter angeben, wird eine Liste von SRs zurückgegeben, die in der LUN vorhanden sind, falls vorhanden.

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000
       b70200000f000000

    <?xml version="1.0" ?>
    <SRlist>
        <SR>
```



```
 8               <UUID>
 9                   3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
10               </UUID>
11               <Devlist>
12                   /dev/disk/by-id/scsi-149455400000000000000000002000000
                        b70200000f000000
13               </Devlist>
14           </SR>
15       </SRlist>
16   <!--NeedCopy-->
```

Die folgenden Parameter können für jeden SR-Typ geprüft werden:

SR-Typ	Die Parameter `device-config`, in der Reihenfolge der Abhängigkeit	Kann untersucht werden?	Erforderlich für `sr-create`?
`lvmoiscsi`	`target`	Nein	Ja
	`chapuser`	Nein	Nein
	`chappassword`	Nein	Nein
	`targetIQN`	Ja	Ja
	`SCSIid`	Ja	Ja
`lvmohba`	`SCSIid`	Ja	Ja
`lvmofcoe`	`SCSIid`	Ja	Ja
`nfs`	`server`	Nein	Ja
	`serverpath`	Ja	Ja
`smb`	`server`	Nein	Ja
	`username`	Nein	Nein
	`password`	Nein	Nein
`lvm`	`device`	Nein	Ja
`ext`	`device`	Nein	Ja

Informationen zum Testen einer GFS2-SR finden Sie unter Erstellen einer GFS2-SR.

SRs entfernen

Ein Speicherrepository (SR) kann entweder vorübergehend oder dauerhaft entfernt werden.

Trennen: Unterbricht die Zuordnung zwischen dem Speichergerät und dem Pool oder Host (PBD Unplug). Auf das SR (und ihre VDIs) kann nicht mehr zugegriffen werden. Der Inhalt der VDIs und die Metainformationen, die von VMs für den Zugriff auf die VDIs verwendet werden, werden beibehalten. Detach kann verwendet werden, wenn Sie ein SR vorübergehend offline nehmen, z. B. für Wartungsarbeiten. Ein abgelöstes SR kann später wieder angebracht werden.

Vergessen: Behält den Inhalt des SRs auf dem physischen Datenträger bei, aber die Informationen, die eine VM mit ihren VDIs verbinden, werden dauerhaft gelöscht. Ermöglicht es Ihnen beispielsweise, die SR erneut an einen anderen XenServer-Host anzuschließen, ohne den SR-Inhalt zu entfernen.

Zerstören: Löscht den Inhalt des SRs von dem physischen Datenträger.

> **Hinweis:**
>
> Wenn Sie SMB-Speicher verwenden, entfernen Sie die Freigabe nicht aus dem Speicher, bevor Sie den SMB-SR trennen.

Für Destroy or Forget muss das an das SR angeschlossene PBD vom Host getrennt werden.

1. Trennen Sie die PBD, um die SR vom entsprechenden XenServer-Host zu trennen:

   ```
   xe pbd-unplug uuid=pbd_uuid
   <!--NeedCopy-->
   ```

2. Verwenden Sie den Befehl `sr-destroy`, um ein SR zu entfernen. Der Befehl zerstört die SR, löscht die SR und die entsprechende PBD aus der XenServer-Hostdatenbank und löscht den SR-Inhalt von der physischen Datenträger:

   ```
   xe sr-destroy uuid=sr_uuid
   <!--NeedCopy-->
   ```

3. Verwenden Sie den Befehl `sr-forget`, um ein SR zu vergessen. Der Befehl entfernt die SR und die entsprechende PBD aus der XenServer-Hostdatenbank, lässt jedoch den tatsächlichen SR-Inhalt auf dem physischen Medium intakt:

   ```
   xe sr-forget uuid=sr_uuid
   <!--NeedCopy-->
   ```

> **Hinweis:**
>
> Es kann einige Zeit dauern, bis das Softwareobjekt, das dem SR entspricht, bereinigt wird.

Einführen eines SRs

Um ein zuvor *vergessenes* SR wieder einzuführen, erstellen Sie ein PBD. Schließen Sie die PBD manuell an die entsprechenden XenServer-Hosts an, um den SR zu aktivieren.

Im folgenden Beispiel wird ein SR vom Typ `lvmoiscsi` eingeführt.

1. Prüfen Sie das vorhandene SR, um ihre UUID zu ermitteln:

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000
       b70200000f000000
<!--NeedCopy-->
```

2. Führen Sie die vorhandene SR-UUID ein, die vom Befehl `sr-probe` zurückgegeben wurde. Die UUID des neuen SRs wird zurückgegeben:

```
xe sr-introduce content-type=user name-label="Example Shared LVM
   over iSCSI SR" \
    shared=true uuid=valid_sr_uuid type=lvmoiscsi
<!--NeedCopy-->
```

3. Erstellen Sie ein PBD für das SR. Die UUID der neuen PBD wird zurückgegeben:

```
xe pbd-create type=lvmoiscsi host-uuid=valid_uuid sr-uuid=
   valid_sr_uuid \
    device-config:target=192.168.0.1 \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000
       b70200000f000000
<!--NeedCopy-->
```

4. Schließen Sie das PBD an, um das SR anzuschließen:

```
xe pbd-plug uuid=pbd_uuid
<!--NeedCopy-->
```

5. Überprüfen Sie den Status des PBD-Steckers. Wenn dies gelingt, ist die `currently-attached`-Eigenschaft wahr:

```
xe pbd-list sr-uuid=sr_uuid
<!--NeedCopy-->
```

> **Hinweis:**
>
> Führen Sie die Schritte 3 bis 5 für jeden Host im Ressourcenpool aus. Diese Schritte können auch mit der Funktion “Speicherrepository reparieren”in XenCenter ausgeführt werden.

Live-LUN-Erweiterung

Um die Kapazitätsanforderungen zu erfüllen, müssen Sie dem Speicher-Array möglicherweise Kapazität hinzufügen, um die Größe der für den XenServer-Host bereitgestellten LUN zu erhöhen. Mit der Live-LUN-Erweiterung können Sie die Größe der LUN ohne VM-Ausfallzeiten erhöhen.

Nachdem Sie Ihrem Speicher-Array mehr Kapazität hinzugefügt haben, geben Sie


```
xe sr-scan sr-uuid=sr_uuid
<!--NeedCopy-->
```

Dieser Befehl scannt das SR neu, und jede zusätzliche Kapazität wird hinzugefügt und zur Verfügung gestellt.

Dieser Vorgang ist auch in XenCenter verfügbar. Wählen Sie das zu ändernde SR aus, und klicken Sie dann auf **Neu scannen**.

> **Warnungen:**
>
> - Es ist nicht möglich, LUNs zu verkleinern oder zu kürzen. Das Reduzieren der LUN-Größe auf dem Speicher-Array kann zu Datenverlust führen.

Live-VDI-Migration

Die Live-VDI-Migration ermöglicht es dem Administrator, das Virtual Disk Image (VDI) der virtuellen Maschine zu verlagern, ohne die VM herunterzufahren. Diese Funktion ermöglicht administrative Vorgänge wie:

- Verschieben einer VM vom günstigen lokalen Speicher zu einem schnellen, stabilen, Array-gestützten Speicher.
- Verschieben einer VM von einer Entwicklungs- in eine Produktionsumgebung.
- Wechseln zwischen Speicherebenen, wenn eine VM durch Speicherkapazität begrenzt ist.
- Durchführung von Speicher-Array-Upgrades.

Einschränkungen und Hinweise

Die Live-VDI-Migration unterliegt den folgenden Einschränkungen und Vorbehalte:

- Im Ziel-Repository muss ausreichend Speicherplatz verfügbar sein.

So verschieben Sie virtuelle Datenträger mit XenCenter

1. Wählen Sie im Bereich **Ressourcen** das SR aus, in dem der virtuelle Datenträger gespeichert ist, und klicken Sie dann auf die Registerkarte **Speicher**.
2. Wählen Sie in der Liste **Virtuelle Laufwerke** das virtuelle Laufwerk aus, das Sie verschieben möchten, und klicken Sie dann auf **Verschieben**.
3. Wählen Sie im Dialogfeld **Virtuellen Datenträger verschieben** das Ziel-SR aus, auf das Sie den VDI verschieben möchten.

> **Hinweis:**
>
> Stellen Sie sicher, dass das SR ausreichend Speicherplatz für einen anderen virtueller Datenträger hat: Der verfügbare Speicherplatz wird in der Liste der verfügbaren SRs angezeigt.

4. Klicken Sie auf **Verschieben**, um das virtuelle Laufwerk zu verschieben.

Eine xe-CLI-Referenz finden Sie unter `vdi-pool-migrate`.

Kalte VDI-Migration zwischen SRs (Offline-Migration)

Mit einer VM verknüpfte VDIs können von einem SR auf ein anderes kopiert werden, um Wartungsanforderungen oder Tiered Storage-Konfigurationen zu erfüllen. XenCenter ermöglicht es Ihnen, eine VM und alle ihre VDIs auf dasselbe oder ein anderes SR zu kopieren. Eine Kombination aus XenCenter und der xe CLI kann zum Kopieren einzelner VDIs verwendet werden.

Eine xe-CLI-Referenz finden Sie unter `vm-migrate`.

Kopieren Sie alle VDIs einer VM auf ein anderes SR

Die XenCenter Copy-VM-Funktion erstellt Kopien aller VDIs für eine ausgewählte VM auf demselben oder einem anderen SR. Die Quell-VM und VDIs sind standardmäßig nicht betroffen. Um die VM auf das ausgewählte SR zu verschieben, anstatt eine Kopie zu erstellen, wählen Sie im Dialogfeld “Virtuelle Maschine kopieren”die Option “Ursprüngliche VM entfernen”aus.

1. Fahren Sie die VM herunter.
2. Wählen Sie in XenCenter die VM aus und wählen Sie dann die **VM**aus > Option**VM kopieren** .
3. Wählen Sie das gewünschte Ziel-SR aus.

Einzelne VDIs auf ein anderes SR kopieren

Eine Kombination der xe CLI und XenCenter kann verwendet werden, um einzelne VDIs zwischen SRs zu kopieren.

1. Fahren Sie die VM herunter.
2. Verwenden Sie die xe-CLI, um die UUIDs der zu verschiebenden VDIs zu identifizieren. Wenn die VM über ein DVD-Laufwerk verfügt, wird `vdi-uuid` als `not in database` aufgeführt und kann ignoriert werden.

```
xe vbd-list vm-uuid=valid_vm_uuid
<!--NeedCopy-->
```


> **Hinweis:**
>
> Der Befehl `vbd-list` zeigt sowohl die VBD- als auch die VDI-UUIDs an. Achten Sie darauf, die VDI-UUIDs und nicht die VBD-UUIDs aufzuzeichnen.

3. Wählen Sie in XenCenter die Registerkarte **VM-Speicher** aus. Wählen Sie für jeden zu verschiebenden VDI den VDI aus und klicken Sie auf die Schaltfläche **Trennen** . Dieser Schritt kann auch mit dem Befehl `vbd-destroy` ausgeführt werden.

   > **Hinweis:**
   >
   > Wenn Sie den Befehl `vbd-destroy` zum Trennen der VDI-UUIDs verwenden, überprüfen Sie zunächst, ob für die VBD der Parameter `other-config:owner` auf **`true`** eingestellt ist. Stellen Sie diesen Parameter auf ein **`false`**. Durch das Ausgeben des Befehls `vbd-destroy` mit `other-config:owner=true` wird auch der zugehörige VDI zerstört.

4. Verwenden Sie den Befehl `vdi-copy`, um alle VM-VDIs zu kopieren, die auf das gewünschte SR verschoben werden sollen.

   ```
   xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
   <!--NeedCopy-->
   ```

5. Wählen Sie in XenCenter die Registerkarte **VM-Speicher** aus. Klicken Sie auf die Schaltfläche **Anhängen** und wählen Sie die VDIs von dem neuen SR aus. Dieser Schritt kann auch mit dem Befehl `vbd-create` ausgeführt werden.

6. Um die ursprünglichen VDIs zu löschen, wählen Sie in XenCenter die Registerkarte **Speicher** des ursprünglichen SRs aus. Die ursprünglichen VDIs werden mit einem leeren Wert für das VM-Feld aufgeführt. Verwenden Sie die Schaltfläche **Löschen**, um den VDI zu löschen.

Lokale Fibre-Channel-SRs in gemeinsame SRs umwandeln

Verwenden Sie die xe CLI und das XenCenter **Repair Storage Repository** Feature, um ein lokales FC-SR in ein gemeinsam genutztes FC-SR zu konvertieren:

1. Aktualisieren Sie alle Hosts im Ressourcenpool auf XenServer 8.
2. Stellen Sie sicher, dass alle Hosts im Pool die LUN des SRs entsprechend in Zonen eingeteilt haben. Weitere Informationen über den Befehl `sr-probe` zum Prüfen, ob die LUN auf jedem Host vorhanden ist, finden Sie unter Prüfen eines SR.
3. Konvertieren Sie das SR in Shared:

   ```
   xe sr-param-set shared=true uuid=local_fc_sr
   <!--NeedCopy-->
   ```


4. Das SR wird in XenCenter von der Host-Ebene auf die Poolebene verschoben, was darauf hinweist, dass es jetzt freigegeben ist. Das SR ist mit einem roten Ausrufezeichen gekennzeichnet, um anzuzeigen, dass es derzeit nicht an allen Hosts im Pool angeschlossen ist.
5. Wählen Sie das SR und dann den **Speicher** > Option "**Speicherrepository reparieren**".
6. Klicken Sie auf **Reparieren**, um eine PBD für jeden Host im Pool zu erstellen und anzuschließen.

Mit Discard Speicherplatz für blockbasierten Speicher auf dem Backing-Array zurückgewinnen

Sie können die Speicherrückgewinnung verwenden, um ungenutzte Blöcke auf einer dünn bereitgestellten LUN freizugeben. Nachdem der Speicherplatz freigegeben wurde, kann das Speicher-Array diesen zurückgewonnenen Speicherplatz wiederverwenden.

> **Hinweis:**
>
> Die Speicherrückgewinnung ist nur bei einigen Arten von Speicher-Arrays verfügbar. Um festzustellen, ob Ihr Array diese Funktion unterstützt und ob eine bestimmte Konfiguration erforderlich ist, lesen Sie die Hardwarekompatibilitätsliste und die spezifische Dokumentation Ihres Speicheranbieters.

So fordern Sie den Speicherplatz über XenCenter zurück:

1. Wählen Sie die **Infrastrukturansicht** und dann den Host oder Pool aus, der mit der SR verbunden ist.
2. Klicken Sie auf die Registerkarte **Speicher**.
3. Wählen Sie das SR aus der Liste aus und klicken Sie auf **Freigegebenen Speicherplatz zurückgewinnen**.
4. Klicken Sie **Ja**, um den Vorgang zu bestätigen.
5. Klicken Sie auf **Benachrichtigungen** und dann auf **Ereignisse**, um den Status des Vorgangs anzuzeigen.

Für weitere Informationen drücken Sie F1 in XenCenter, um auf die Onlinehilfe zuzugreifen.

Um Speicherplatz über die xe CLI zurückzugewinnen, können Sie den folgenden Befehl verwenden:

```
xe host-call-plugin host-uuid=host_uuid \
    plugin=trim fn=do_trim args:sr_uuid=sr_uuid
```

> **Hinweise:**
>
> - Der Vorgang ist nur für LVM-basierte SRs verfügbar, die auf dünn bereitgestellten LUNs im Array basieren. Lokale SSDs können auch von der Speicherrückgewinnung profitieren.

> - Für dateibasierte SRs wie NFS und EXT3/EXT4 ist keine Speicherrückgewinnung erforderlich. Die Schaltfläche **Freigegebenen Speicherplatz zurückgewinnen** ist in XenCenter für diese SR-Typen nicht verfügbar.
> - Wenn Sie den xe-Befehl zur Speicherrückgewinnung für ein dateibasiertes SR oder ein thick-provisioned LVM-basiertes SR ausführen, gibt der Befehl einen Fehler zurück.
> - Die Speicherrückgewinnung ist ein intensiver Vorgang und kann zu einer Verschlechterung der Speicher-Array-Leistung führen. Starten Sie diesen Vorgang daher nur, wenn eine Speicherrückgewinnung auf dem Array erforderlich ist. Wir empfehlen, dass Sie diese Arbeit außerhalb der Spitzenauslastungszeiten des Arrays einplanen.

Beim Löschen von Snapshots automatisch Speicherplatz zurückgewinnen

Beim Löschen von Snapshots mit XenServer wird der auf LVM-basierten SRs zugewiesene Speicherplatz automatisch zurückgewonnen und ein VM-Neustart ist nicht erforderlich. Dieser Vorgang wird als “Online-Koaleszenz”bezeichnet. Online-Koaleszierung gilt für alle Arten von SR.

In bestimmten Fällen kann die automatisierte Speicherrückgewinnung möglicherweise nicht fortgesetzt werden. Wir empfehlen, das Offline-Coalesce-Tool in den folgenden Szenarien zu verwenden:

- Unter Bedingungen, bei denen ein VM-I/O-Durchsatz erheblich
- Unter Bedingungen, in denen nach einem bestimmten Zeitraum kein Platz mehr zurückgewonnen wird

> **Hinweise:**
>
> - Die Ausführung des Offline-Coalesce-Tools führt zu einigen Ausfallzeiten für die VM, da die ausgeführten Vorgänge zum Anhalten/Wiederaufnehmen ausgeführt werden.
> - Bevor Sie das Tool ausführen, löschen Sie alle Snapshots und Klone, die Sie nicht mehr benötigen. Das Tool beansprucht angesichts der verbleibenden Snapshots/Klone so viel Speicherplatz wie möglich. Wenn Sie den gesamten Speicherplatz zurückfordern möchten, löschen Sie alle Snapshots und Klone.
> - VM-Datenträger müssen sich entweder auf freigegebenem oder lokalem Speicher für einen einzelnen Host befinden. VMs mit Datenträgern in beiden Speichertypen können nicht koalesziert werden.

Mit dem Offline-Coalesce-Tool Speicherplatz zurückgewinnen

Aktivieren Sie die versteckten Objekte mit XenCenter. Klicken Sie auf **Ansicht** > **Versteckte** Objekte. Wählen Sie im Bereich Ressource die VM aus, für die Sie die UUID abrufen möchten. Die UUID wird auf der Registerkarte **Allgemein** angezeigt.

Wählen Sie im Bereich **Ressourcen** den RessourcenPoolkoordinator (den ersten Host in der Liste) aus. Auf der Registerkarte **Allgemein** wird die UUID angezeigt. Wenn Sie keinen Ressourcenpool verwenden, wählen Sie den Host der VM aus.

1. Öffnen Sie eine Konsole auf dem Host und führen Sie den folgenden Befehl aus:

```
xe host-call-plugin host-uuid=host-UUID \
    plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=VM-UUID
<!--NeedCopy-->
```

   Wenn die VM-UUID beispielsweise 9bad4022-2c2d-dee6-abf5-1b6195b1dad5 ist und die Host-UUID b8722062-de95-4d95-9baa-a5fe343898ea, führen Sie den folgenden Befehl aus:

```
xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea
     \
    plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2
       c2d-dee6-abf5-1b6195b1dad5
<!--NeedCopy-->
```

2. Dieser Befehl setzt die VM an (sofern sie nicht bereits heruntergefahren ist), initiiert den Speicherrückgewinnungsprozess und setzt die VM dann fort.

> **Hinweise:**
>
> Wir empfehlen, die VM manuell herunterzufahren oder anzuhalten, bevor Sie das Offline-Coalesce-Tool ausführen. Sie können die VM entweder mit XenCenter oder der XenServer-CLI herunterfahren oder anhalten. Wenn Sie das Coalesce-Tool auf einer laufenden VM ausführen, unterbricht das Tool die VM automatisch, führt die erforderlichen VDI-Coalesce-Operationen durch und setzt die VM fort. Agile VMs werden möglicherweise auf einem anderen Host neu gestartet.
>
> Wenn sich die Virtual Disk Images (VDIs), die zusammengeführt werden sollen, auf gemeinsam genutztem Speicher befinden, müssen Sie das Offline-Koaleszentool auf dem Poolkoordinator ausführen.
>
> Wenn sich die VDIs, die zusammengeführt werden sollen, im lokalen Speicher befinden, führen Sie das Offline-Koaleszenz-Tool auf dem Host aus, an den der lokale Speicher angeschlossen ist.

Arbeiten mit Datenträger-I/O

Sie können den Datenträger-I/O-Scheduler und die Datenträger-I/O-Prioritätseinstellungen konfigurieren, um die Leistung Ihrer Datenträger zu ändern.

> **Hinweis:**
>
> Die in diesem Abschnitt beschriebenen Datenträger-I/O-Funktionen gelten nicht für EqualLogic-, NetApp- oder NFS-Speicher.

Anpassen des Datenträger-E/A-Schedulers

Für die allgemeine Leistung wird der Standarddatenträgerplaner `noop` auf alle neuen SR-Typen angewendet. Der `noop`-Scheduler bietet die fairste Leistung für konkurrierende VMs, die auf dasselbe Gerät zugreifen.

1. Passen Sie den Disk Scheduler an, indem Sie den folgenden Befehl verwenden:

   ```
   xe sr-param-set other-config:scheduler=<option> uuid=<sr_uuid>
   <!--NeedCopy-->
   ```

   Der Wert von `<option>` kann einer der folgenden Begriffe sein: `noop`, `cfq` oder `deadline`.

2. Trennen Sie die entsprechende PBD und stecken Sie sie wieder ein, damit der Scheduler-Parameter wirksam wird.

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   xe pbd-plug uuid=<pbd_uuid>
   <!--NeedCopy-->
   ```

Um die Priorisierung von Datenträger-I/O-Anforderungen anzuwenden, überschreiben Sie die Standardeinstellung und weisen Sie den Datenträgerplaner `cfq` dem SR zu.

Priorisierung von I/O-Anforderungen für virtuelle Datenträger

Virtuelle Laufwerke verfügen über optionale Prioritätseinstellungen für I/O-Anfragen. Sie können diese Einstellungen verwenden, um I/O auf dem Datenträger einer bestimmten virtuellen Maschine gegenüber anderen zu priorisieren.

Bevor Sie die Prioritätsparameter für Datenträger-I/O-Anforderungen für eine VBD konfigurieren, stellen Sie sicher, dass der Datenträgerplaner für die SR entsprechend eingestellt wurde. Der Scheduler-Parameter muss auf dem SR auf `cfq` festgelegt sein und das zugehörige PBD getrennt und wieder angeschlossen werden. Informationen zum Anpassen des Schedulers finden Sie unter Anpassen des Datenträger-I/O-Schedulers.

Bei gemeinsam genutztem SR, bei dem mehrere Hosts auf dieselbe LUN zugreifen, wird die Prioritätseinstellung auf VBDs angewendet, die von demselben Host aus auf die LUN zugreifen. Diese Einstellungen werden nicht auf alle Hosts im Pool angewendet.

Der Host sendet eine Anfrage an den Remotespeicher, aber die Priorisierung der Anfragen erfolgt durch den Remotespeicher.

Datenträger-I/O-Anforderungsparameter festlegen Diese Einstellungen können auf vorhandene virtuelle Laufwerke angewendet werden, indem Sie den Befehl `xe vbd-param-set` mit den folgenden Parametern verwenden:

- `qos_algorithm_type` - Dieser Parameter muss auf den Wert `ionice` festgelegt werden. Dies ist der einzige Algorithmus, der für virtuelle Datenträger unterstützt wird.
- `qos_algorithm_param` - Verwenden Sie diesen Parameter, um Schlüssel/Wert-Paare festzulegen. Für virtuelle Datenträger nimmt `qos_algorithm_param` einen Schlüssel `sched`, und je nach Wert ist auch ein Schlüssel **`class`** erforderlich.

  Der Schlüssel `qos_algorithm_param:sched` kann einen der folgenden Werte haben:

  - `sched=rt` oder `sched=real-time` —Dieser Wert setzt den Planungsparameter auf Echtzeitpriorität, was einen Parameter **`class`** erfordert, um einen Wert festzulegen.
  - `sched=idle` - Dieser Wert setzt den Scheduling-Parameter auf die Leerlauf-Priorität, sodass kein Parameter **`class`** erforderlich ist, um einen Wert festzulegen.
  - `sched=anything` - Dieser Wert setzt den Planungsparameter auf die Best-Effort-Priorität, was einen Parameter **`class`** erfordert, um einen Wert festzulegen.

  Der Schlüssel `qos_algorithm_param:class` kann einen der folgenden Werte haben:

  - Eines der folgenden Schlüsselwörter: `highest`, `high`, `normal`, `low`, `lowest`.
  - Eine Ganzzahl zwischen 0 und 7, wobei 7 die höchste Priorität und 0 die niedrigste Priorität hat. Beispielsweise erhalten I/O-Anforderungen mit einer Priorität von 5 Vorrang vor I/O-Anforderungen mit einer Priorität von 2.

Beispiel Die folgenden CLI-Befehle legen beispielsweise fest, dass die VBD des virtuellen Laufwerks die Echtzeitpriorität verwendet 5:

```
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_type=ionice
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:sched=rt
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:class=5
xe sr-param-set uuid=<sr_uuid> other-config:scheduler=cfq
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
<!--NeedCopy-->
```

Multipathing

November 9, 2023

Dynamische Multipathing-Unterstützung ist für Fibre-Channel- und iSCSI-Speicher-Backends verfügbar.

XenServer verwendet Linux Native Multipathing (DM-MP), die generische Linux-Multipathing-Lösung, als Multipath-Handler. XenServer ergänzt diesen Handler jedoch um zusätzliche Funktionen, sodass XenServer herstellerspezifische Funktionen von Speichergeräten erkennen kann.

Die Konfiguration von Multipathing bietet Redundanz für den Remote-Speicherverkehr bei teilweisem Konnektivitätsverlust. Multipathing leitet den Speicherverkehr über mehrere Pfade an ein Speichergerät weiter, um Redundanz und erhöhten Durchsatz zu gewährleisten. Sie können bis zu 16 Pfade zu einer einzelnen LUN verwenden. Multipathing ist eine aktiv-aktive Konfiguration. Standardmäßig verwendet Multipathing je nach Speicher-Array-Typ entweder Round-Robin- oder Multibus-Lastausgleich. Alle Strecken haben während des normalen Betriebs aktiven Verkehr, was zu einem erhöhten Durchsatz führt.

> **Wichtig:**
>
> Wir empfehlen, dass Sie Multipathing für alle Hosts in Ihrem Pool aktivieren, *bevor Sie die SR* erstellen. Wenn Sie die SR erstellen, bevor Sie Multipathing aktivieren, müssen Sie Ihre Hosts in den Wartungsmodus versetzen, um Multipathing zu aktivieren.

NIC-Bonding kann auch Redundanz für den Speicherverkehr bieten. Für iSCSI-Speicher empfehlen wir, nach Möglichkeit Multipathing anstelle von NIC-Bonding zu konfigurieren.

Multipathing ist in den folgenden Szenarien nicht wirksam:

- NFS-Speichergeräte
- Sie haben eine begrenzte Anzahl von Netzwerkkarten und müssen iSCSI-Verkehr und Dateiverkehr (NFS oder SMB) über dieselbe Netzwerkkarte leiten

In diesen Fällen sollten Sie stattdessen die NIC-Bindung verwenden. Weitere Informationen zum NIC-Bonding finden Sie unter Netzwerk.

Voraussetzungen

Bevor Sie Multipathing aktivieren, überprüfen Sie, ob die folgenden Anweisungen zutreffen:

- Auf Ihrem Speicherserver sind mehrere Ziele verfügbar.

  Beispielsweise gibt ein iSCSI-Speicher-Backend, das nach `sendtargets` für ein bestimmtes Portal abgefragt wird, mehrere Ziele zurück, wie im folgenden Beispiel:

```
iscsiadm -m discovery --type sendtargets --portal 192.168.0.161
192.168.0.161:3260,1 iqn.strawberry:litchie
192.168.0.204:3260,2 iqn.strawberry:litchie
```


Sie können jedoch eine zusätzliche Konfiguration durchführen, um iSCSI-Multipath für Arrays zu aktivieren, die nur ein einziges Ziel verfügbar machen. Weitere Informationen finden Sie unter iSCSI Multipath für Arrays, die nur ein einziges Zielverfügbar machen.

- Nur für iSCSI hat die Steuerdomäne (dom0) eine IP-Adresse in jedem Subnetz, das vom Multipath-Speicher verwendet wird.

  Stellen Sie sicher, dass Sie für jeden Pfad, den Sie zum Speicher haben möchten, über eine Netzwerkkarte verfügen und dass auf jeder Netzwerkkarte eine IP-Adresse konfiguriert ist. Wenn Sie beispielsweise vier Pfade zu Ihrem Speicher wünschen, müssen Sie über vier Netzwerkkarten verfügen, für die jeweils eine IP-Adresse konfiguriert ist.
- Nur für iSCSI hat jedes iSCSI-Ziel und jeder iSCSI-Initiator einen eigenen IQN.
- Nur für iSCSI arbeiten die iSCSI-Zielports im Portalmodus.
- Nur für HBA sind mehrere HBAs an die Switch-Fabric angeschlossen.

Multipathing aktivieren

Sie können Multipathing in XenCenter oder auf der xe-CLI aktivieren.

So aktivieren Sie Multipathing über XenCenter

1. Klicken Sie im Bereich XenCenter **Resources** mit der rechten Maustaste auf den Host und wählen Sie In den **Wartungsmodus wechseln**.
2. Warten Sie, bis der Host wieder im Bereich **Ressourcen** mit dem Symbol für den Wartungsmodus (ein blaues Quadrat) angezeigt wird, bevor Sie fortfahren.
3. Klicken Sie auf der Registerkarte **Allgemein** für den Host auf **Eigenschaften** und wechseln Sie dann zur Registerkarte **Multipathing** .
4. Um Multipathing zu aktivieren, **aktivieren Sie das Kontrollkästchen Multipathing auf diesem Server** aktivieren.
5. Klicken Sie auf **OK**, um die neue Einstellung zu übernehmen. Es gibt eine kurze Verzögerung, während XenCenter die neue Speicherkonfiguration speichert.
6. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus beenden**.
7. Wiederholen Sie diese Schritte, um Multipathing auf allen Hosts im Pool zu aktivieren.

Stellen Sie sicher, dass Sie Multipathing auf allen Hosts im Pool aktivieren. Die gesamte Verkabelung und, im Fall von iSCSI, die Subnetzkonfigurationen müssen mit den entsprechenden NICs auf jedem Host übereinstimmen.

So aktivieren Sie Multipathing mit der xe-CLI

1. Öffnen Sie eine Konsole auf dem XenServer-Host.
2. Trennen Sie alle PBDs auf dem Host mit dem folgenden Befehl:

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   <!--NeedCopy-->
   ```

   Sie können den Befehl verwenden `xe pbd-list`, um die UUID der PBDs zu finden.
3. Setzen Sie den Wert des Parameters `multipathing` auf **`true`**, indem Sie den folgenden Befehl verwenden:

   ```
   xe host-param-set uuid=<host uuid> multipathing=true
   <!--NeedCopy-->
   ```
4. Wenn auf dem Server SRs vorhanden sind, die im Single-Path-Modus ausgeführt werden, aber mehrere Pfade haben:

   - Migrieren oder sperren Sie alle laufenden Gäste mit virtuellen Datenträgern in den betroffenen SRs
   - Schließen Sie die PBD aller betroffenen SRs erneut an, um sie mithilfe von Multipathing erneut zu verbinden:

     ```
     xe pbd-plug uuid=<pbd_uuid>
     <!--NeedCopy-->
     ```
5. Wiederholen Sie diese Schritte, um Multipathing auf allen Hosts im Pool zu aktivieren.

Stellen Sie sicher, dass Sie Multipathing auf allen Hosts im Pool aktivieren. Die gesamte Verkabelung und, im Fall von iSCSI, die Subnetzkonfigurationen müssen mit den entsprechenden NICs auf jedem Host übereinstimmen.

Deaktivieren Sie Multipathing

Sie können Multipathing in XenCenter oder in der xe-CLI deaktivieren.

Deaktivieren von Multipathing über XenCenter

1. Klicken Sie im Bereich XenCenter **Resources** mit der rechten Maustaste auf den Host und wählen Sie In den **Wartungsmodus wechseln**.
2. Warten Sie, bis der Host wieder im Bereich **Ressourcen** mit dem Symbol für den Wartungsmodus (ein blaues Quadrat) angezeigt wird, bevor Sie fortfahren.

3. Klicken Sie auf der Registerkarte **Allgemein** für den Host auf **Eigenschaften** und wechseln Sie dann zur Registerkarte **Multipathing** .
4. Um Multipathing zu deaktivieren, deaktivieren **Sie das Kontrollkästchen Multipathing auf diesem Server aktivieren** .
5. Klicken Sie auf **OK**, um die neue Einstellung zu übernehmen. Es gibt eine kurze Verzögerung, während XenCenter die neue Speicherkonfiguration speichert.
6. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus beenden**.
7. Wiederholen Sie diese Schritte, um Multipathing auf allen Hosts im Pool zu konfigurieren.

So deaktivieren Sie Multipathing mit der xe-CLI

1. Öffnen Sie eine Konsole auf dem XenServer-Host.
2. Trennen Sie alle PBDs auf dem Host mit dem folgenden Befehl:

```
xe pbd-unplug uuid=<pbd_uuid>
<!--NeedCopy-->
```

   Sie können den Befehl verwenden `xe pbd-list`, um die UUID der PBDs zu finden.

3. Setzen Sie den Wert des Parameters `multipathing` auf **`false`**, indem Sie den folgenden Befehl verwenden:

```
xe host-param-set uuid=<host uuid> multipathing=false
<!--NeedCopy-->
```

4. Wenn auf dem Server SRs vorhanden sind, die im Single-Path-Modus ausgeführt werden, aber mehrere Pfade haben:
   - Migrieren oder sperren Sie alle laufenden Gäste mit virtuellen Datenträgern in den betroffenen SRs
   - Trennen Sie die PBD aller betroffenen SRs und schließen Sie sie erneut an, um sie mithilfe von Multipathing erneut zu verbinden:

```
xe pbd-plug uuid=<pbd_uuid>
<!--NeedCopy-->
```

5. Wiederholen Sie diese Schritte, um Multipathing auf allen Hosts im Pool zu deaktivieren.

Konfigurieren von Multipathing

Um eine zusätzliche Multipath-Konfiguration durchzuführen, erstellen Sie Dateien mit dem Suffix `.conf` im Verzeichnis `/etc/multipath/conf.d`. Fügen Sie die zusätzliche Konfiguration in diesen Dateien hinzu. Multipath durchsucht das Verzeichnis alphabetisch nach Dateien, die auf `.conf` enden, und liest daraus die Konfigurationsinformationen.

Bearbeiten Sie die Datei nicht `/etc/multipath.conf`. Diese Datei wird durch Updates für XenServer überschrieben.

Multipath-Werkzeuge

Die Multipath-Unterstützung in XenServer basiert auf dem Device-Mapper. `multipathd components` Die Storage Manager-API verwaltet die automatische Aktivierung und Deaktivierung von Multipath-Knoten. Im Gegensatz zu den Standardtools `dm-multipath` in Linux werden Device Mapper-Knoten nicht automatisch für alle LUNs im System erstellt. Device Mapper-Knoten werden nur bereitgestellt, wenn LUNs aktiv von der Speicherverwaltungsebene verwendet werden. Daher ist es nicht erforderlich, eines der `dm-multipath` CLI-Tools zum Abfragen oder Aktualisieren von DM-Tabellenknoten in XenServer zu verwenden.

Wenn es notwendig ist, den Status von Device-Mapper-Tabellen manuell abzufragen oder aktive Device Mapper-Multipath-Knoten im System aufzulisten, verwenden Sie das Dienstprogramm `mpathutil`:

```
mpathutil list
<!--NeedCopy-->
```

```
mpathutil status
<!--NeedCopy-->
```

iSCSI-Multipath für Arrays, die nur ein einziges Ziel verfügbar machen

Sie können XenServer so konfigurieren, dass iSCSI-Multipath mit Speicher-Arrays verwendet wird, die nur ein einzelnes iSCSI-Ziel und ein IQN über eine IP-Adresse verfügbar machen. Sie können diese Schritte beispielsweise befolgen, um Dell EqualLogic PS und FS Unified Series Storage-Arrays einzurichten.

Standardmäßig stellt XenServer nur eine Verbindung pro iSCSI-Ziel her. Daher wird bei der Standardkonfiguration empfohlen, NIC-Bonding zu verwenden, um Failover und Lastausgleich zu erreichen. Das in diesem Abschnitt beschriebene Konfigurationsverfahren beschreibt eine alternative Konfiguration, bei der mehrere iSCSI-Verbindungen für ein einzelnes iSCSI-Ziel hergestellt werden. NIC-Bonding ist nicht erforderlich.

> **Hinweis:**
>
> Die folgende Konfiguration wird nur für Server unterstützt, die ausschließlich an Speicher-Arrays angeschlossen sind, die nur ein einziges iSCSI-Ziel verfügbar machen. Diese Speicher-Arrays müssen für dieses Verfahren mit XenServer qualifiziert sein.

So konfigurieren Sie Multipath:

1. Machen Sie ein Backup aller Daten, die Sie schützen möchten.
2. Klicken Sie im Bereich XenCenter **Resources** mit der rechten Maustaste auf den Host und wählen Sie In den **Wartungsmodus wechseln**.
3. Warten Sie, bis der Host wieder im Bereich **Ressourcen** mit dem Symbol für den Wartungsmodus (ein blaues Quadrat) angezeigt wird, bevor Sie fortfahren.
4. Klicken Sie auf der Registerkarte **Allgemein** für den Host auf **Eigenschaften** und wechseln Sie dann zur Registerkarte **Multipathing** .
5. Um Multipathing zu aktivieren, **aktivieren Sie das Kontrollkästchen Multipathing auf diesem Server** aktivieren.
6. Klicken Sie auf **OK**, um die neue Einstellung zu übernehmen. Es gibt eine kurze Verzögerung, während XenCenter die neue Speicherkonfiguration speichert.
7. Konfigurieren Sie in der Hostkonsole zwei bis vier Open-iSCSI-Schnittstellen. Jede iSCSI-Schnittstelle wird verwendet, um einen separaten Pfad einzurichten. Die folgenden Schritte zeigen den Ablauf für zwei Schnittstellen:

   a) Konfigurieren Sie zwei iSCSI-Schnittstellen und führen Sie die folgenden Befehle aus:

   ```
   iscsiadm -m iface --op new -I c_iface1
   iscsiadm -m iface --op new -I c_iface2
   ```

   Stellen Sie sicher, dass die Schnittstellennamen das Präfix `c_`haben Wenn die Schnittstellen diesen Benennungsstandard nicht verwenden, werden sie ignoriert und stattdessen wird die Standardschnittstelle verwendet.

   > **Hinweis:**
   >
   > Diese Konfiguration führt dazu, dass die Standardschnittstelle für alle Verbindungen verwendet wird. Dies zeigt an, dass alle Verbindungen über eine einzige Schnittstelle hergestellt werden.

   b) Binden Sie die iSCSI-Schnittstellen mithilfe der folgenden Befehle an xenbr1 und xenbr2:

   ```
   iscsiadm -m iface --op update -I c_iface1 -n iface.
       net_ifacename -v xenbr1
   ```



```
iscsiadm -m iface --op update -I c_iface2 -n iface.
    net_ifacename -v xenbr2
```

> **Hinweis:**
>
> Bei dieser Konfiguration wird vorausgesetzt, dass die für die Steuerdomäne konfigurierten Netzwerkschnittstellen (einschließlich xenbr1 und xenbr2) und xenbr0 für die Verwaltung verwendet werden. Es wird auch davon ausgegangen, dass die für das Speichernetzwerk verwendeten NIC-Karten NIC1 und NIC2 sind.
> Wenn dies nicht der Fall ist, verwenden Sie Ihre Netzwerktopologie, um die Netzwerkschnittstellen und NIC-Karten zu ermitteln, die in diesen Befehlen verwendet werden sollen.

8. Klicken Sie im Bereich XenCenter **Resources** mit der rechten Maustaste auf den Host und wählen Sie **Exit Maintenance Mode**. Setzen Sie Ihre virtuellen Maschinen noch nicht fort.
9. Führen Sie in der Hostkonsole die folgenden Befehle aus, um die Sitzungen zu ermitteln und sich bei ihnen anzumelden:

```
iscsiadm -m discovery -t st -p <IP of SAN>
iscsiadm -m node -L all
```

10. Löschen Sie die veralteten Einträge mit alten Sitzungsinformationen, indem Sie die folgenden Befehle verwenden:

```
cd /var/lib/iscsi/send_targets/<IP of SAN and port, use ls command
    to check that>
rm -rf <iqn of SAN target for that particular LUN>

cd /var/lib/iscsi/nodes/
rm -rf <entries for that particular SAN>
```

11. Trennen Sie die LUN und hängen Sie sie erneut an. Dazu gibt es mehrere Methoden:

    - Nachdem Sie die vorherigen Schritte auf allen Hosts in einem Pool ausgeführt haben, können Sie XenCenter verwenden, um die LUN für den gesamten Pool zu trennen und erneut anzuhängen.
    - Alternativ können Sie die PBD für jeden Host trennen und zerstören und dann die SR reparieren.

      a) Führen Sie die folgenden Befehle aus, um die PBD zu trennen und zu zerstören:

         i. Finden der UUID des SRs:

```
xe sr-list
```

         ii. Rufen Sie die Liste der PBDs ab, die mit dem SR verknüpft sind:


```
xe pbd-list sr-uuid=<sr_uuid>
```

iii. Suchen Sie in der Ausgabe des vorherigen Befehls nach der UUID der PBD des iSCSI-Speicherrepositorys mit einer nicht übereinstimmenden SCSI-ID.

iv. Trennen und vernichten Sie die identifizierte PBD.

```
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-destroy uuid=<pbd_uuid>
```

b) Reparieren Sie den Speicher in XenCenter.

12. Sie können jetzt Ihre virtuellen Maschinen fortsetzen.

Speicher-Lese-Caching

December 6, 2023

Das Lesecaching verbessert die Datenträgerleistung einer VM, da die Daten nach dem ersten Lesen von einem externen Datenträger im freien Speicher des Hosts zwischengespeichert werden. Es verbessert die Leistung in Situationen, in denen viele VMs von einer einzigen Basis-VM geklont werden, da es die Anzahl der von dem Datenträger gelesenen Blöcke drastisch reduziert. Zum Beispiel in der Citrix Virtual Desktops-Umgebung Machine Creation Services (MCS)-Umgebungen.

Die Leistungsverbesserung kann immer dann beobachtet werden, wenn Daten mehr als einmal von dem Datenträger gelesen werden, da sie im Speicher zwischengespeichert werden. Diese Änderung macht sich am deutlichsten in der Verschlechterung des Dienstes bemerkbar, die in schweren E/A-Situationen auftritt Zum Beispiel in den folgenden Situationen:

- Wenn eine beträchtliche Anzahl von Endbenutzern innerhalb eines sehr engen Zeitrahmens hochfährt (Boot-Storm)
- Wenn eine erhebliche Anzahl von VMs zur gleichen Zeit Malware-Scans ausführen soll (Antiviren-stürme).

Das Lesecaching ist standardmäßig aktiviert, wenn Sie über den entsprechenden Lizenztyp verfügen.

> **Hinweis:**
>
> Storage Read Caching ist für Kunden der XenServer Premium Edition verfügbar.

Lesecache aktivieren und deaktivieren

Für dateibasierte SR-Typen wie NFS und EXT3/EXT4 SR-Typen ist Lese-Caching standardmäßig aktiviert. Die Lese-Zwischenspeicherung ist für alle anderen SRs deaktiviert.

Führen Sie den folgenden Befehl aus, um das Lesecaching für ein bestimmtes SR über die xe-CLI zu deaktivieren:

```
xe sr-param-set uuid=sr-uuid other-config:o_direct=true
<!--NeedCopy-->
```

Um den Lesecache für ein bestimmtes SR über XenCenter zu deaktivieren, rufen Sie das **Eigenschaftendialogfeld** für das SR auf. Auf der Registerkarte "**Lesezwischenspeicherung** "können Sie das Lesezwischenspeichern aktivieren oder deaktivieren.

Weitere Informationen finden Sie unter SR-Eigenschaften ändern.

Einschränkungen

- Das Lesecaching ist nur für NFS- und EXT3/EXT4-SRs verfügbar. Es ist nicht für andere SR-Typen verfügbar.
- Der Lesecache gilt nur für schreibgeschützte VDIs und VDI-Eltern. Diese VDIs sind dort vorhanden, wo VMs aus "Fast Clone"oder Datenträger-Snapshots erstellt werden. Die größten Leistungsverbesserungen können erzielt werden, wenn viele VMs aus einem einzigen "goldenen" Image geklont werden.
- Leistungsverbesserungen hängen von der Menge an freiem Speicher ab, die in der Control Domain (dom0) des Hosts verfügbar ist. Durch Erhöhen der Größe des dom0-Speichers kann dem Lese-Cache mehr Speicher zugewiesen werden. Informationen zum Konfigurieren des dom0-Speichers finden Sie unter CTX134951.
- Wenn das Speicherlese-Caching aktiviert ist, führt ein Cache-Fehler dazu, dass I/O serialisiert wird. Dies kann manchmal teurer sein als das Ausschalten des Lesecachings, da bei ausgeschaltetem Lese-Caching I/O parallelisiert werden kann. Um die Auswirkungen von Cache-Fehlern zu reduzieren, erhöhen Sie den verfügbaren dom0-Speicher oder deaktivieren Sie das Lesecaching für den SR.

Vergleich mit IntelliCache

IntelliCache und speicherbasiertes Lese-Caching ergänzen sich in gewisser Hinsicht. IntelliCache speichert nicht nur auf einer anderen Ebene, sondern speichert auch Schreibvorgänge zusätzlich zu Lesevorgängen. IntelliCache speichert Lesevorgänge aus dem Netzwerk auf einem lokalen Datenträger. Im Speicherlesecaching werden die Lesevorgänge aus dem Netzwerk oder dem Datenträger

in den Hostspeicher zwischengespeichert. Der Vorteil des speicherinternen Lesecachings besteht darin, dass der Speicher immer noch eine Größenordnung schneller ist als eine Solid-State-Disk (SSD). Die Leistung bei Boot-Storms und anderen schweren I/O-Situationen verbessert sich

Sowohl Read-Caching als auch IntelliCache können gleichzeitig aktiviert werden. In diesem Fall speichert IntelliCache die Lesevorgänge aus dem Netzwerk auf einen lokalen Datenträger. Lesevorgänge von diesem lokalen Datenträger werden im Speicher mit Lese-Caching zwischengespeichert.

Stellen Sie die Lese-Cache-Größe

Die Lesecacheleistung kann optimiert werden, indem der Steuerdomäne von XenServer (dom0) mehr Speicher zur Verfügung gestellt wird.

> **Wichtig:**
>
> Stellen Sie die Lesecachegröße auf ALLEN Hosts im Pool zur Optimierung einzeln ein. Alle nachfolgenden Änderungen an der Größe des Lesecaches müssen auch auf allen Hosts im Pool festgelegt werden.

Öffnen Sie auf dem XenServer-Host eine lokale Shell und melden Sie sich als Root an.

Führen Sie den folgenden Befehl aus, um die Größe des Lesecaches festzulegen:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
<!--NeedCopy-->
```

Stellen Sie sowohl den Anfangs- als auch den Maximalwert auf denselben Wert ein. Um beispielsweise den dom0-Speicher auf 20.480 MiB zu setzen:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
<!--NeedCopy-->
```

> **Wichtig:**
>
> Starten Sie alle Hosts neu, nachdem Sie die Größe des Lesecaches geändert

Wie kann ich die aktuelle dom0-Speicherzuweisung anzeigen?

Um die aktuellen dom0-Speichereinstellungen anzuzeigen, geben Sie Folgendes ein:

```
free -m
<!--NeedCopy-->
```

Die Ausgabe von `free -m` zeigt die aktuellen dom0-Speichereinstellungen. Der Wert kann aufgrund verschiedener Gemeinkosten geringer sein als erwartet. Die folgende Beispieltabelle zeigt die Ausgabe von einem Host, bei dem dom0 auf 2,6 GiB eingestellt ist.


```
|                     | Total  | Used | Free  | Shared | Buffer/cache |
    Available |
|---------------------|--------|------|-------|--------|--------------|----------
| Mem:                | 2450   | 339  | 1556  | 9      | 554          |
    2019      |
| Swap:               | 1023   | 0    | 1023  |        |              |
              |
<!--NeedCopy-->
```

Welcher Wertebereich kann verwendet werden? Da die XenServer Control Domain (dom0) 64-Bit ist, können große Werte verwendet werden, beispielsweise 32.768 MiB. Wir empfehlen jedoch, **den dom0-Speicher nicht unter 1 GiB zu reduzieren**.

XenCenter Displaynotizen

Der gesamte Arbeitsspeicher des Hosts kann als Xen-Hypervisor, dom0, VMs und freien Speicher betrachtet werden. Obwohl dom0 und VM-Speicher normalerweise eine feste Größe haben, verwendet der Xen-Hypervisor eine variable Speichermenge. Die Menge des verwendeten Speichers hängt von verschiedenen Faktoren ab. Zu diesen Faktoren gehören die Anzahl der virtuellen Maschinen, die zu einem beliebigen Zeitpunkt auf dem Host ausgeführt werden, und wie diese VMs konfiguriert sind. Es ist nicht möglich, die Menge an Speicher zu begrenzen, die Xen verwendet. Durch die Begrenzung des Arbeitsspeichers kann Xen nicht mehr genügend Arbeitsspeicher haben und verhindert, dass neue VMs gestartet werden, selbst wenn der Host über freien Speicher verfügt.

Um den einem Host zugewiesenen Speicher anzuzeigen, wählen Sie in XenCenter den Host aus, und klicken Sie dann auf die Registerkarte **Speicher** .

Das Feld XenServer zeigt die *Summe* des Speichers an, der dom0 - *und* Xen-Speicher zugewiesen ist. Daher kann die angezeigte Speichermenge höher sein als vom Administrator angegeben. Die Speichergröße kann beim Starten und Stoppen von VMs variieren, auch wenn der Administrator eine feste Größe für dom0 festgelegt hat.

Grafikübersicht

January 19, 2024

Dieser Abschnitt bietet einen Überblick über die virtuelle Bereitstellung professioneller 3D-Grafikanwendungen und Workstations in XenServer. Die Angebote umfassen GPU-Passthrough

(für NVIDIA-, AMD- und Intel-GPUs) und hardwarebasierte GPU-Sharing mit NVIDIA vGPU™ und Intel GVT-G™.

Graphics Virtualization ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zu den XenServer-Editionen und zum Upgrade finden Sie auf der XenServer-Website. Weitere Informationen finden Sie unter Lizenzierung.

GPU-Durchgang

In einem virtualisierten System werden die meisten physikalischen Systemkomponenten gemeinsam genutzt. Diese Komponenten werden durch den Hypervisor als mehrere virtuelle Instanzen für mehrere Clients dargestellt. Eine Pass-Through-GPU wird überhaupt nicht abstrahiert, sondern bleibt ein physisches Gerät. Jede gehostete virtuelle Maschine (VM) erhält ihre eigene dedizierte GPU, wodurch die Software-Abstraktion und die damit verbundene Leistungseinbuße entfallen.

Mit XenServer können Sie einer Windows- oder Linux-VM, die auf demselben Host läuft, eine physische GPU (im XenServer-Host) zuweisen. Diese GPU-Pass-Through-Funktion ist für Grafik-Power-Benutzer wie CAD-Designer gedacht.

Gemeinsam genutzte GPU (vGPU)

Mit einer gemeinsam genutzten GPU (vGPU) kann eine physische GPU von mehreren VMs gleichzeitig verwendet werden. Da ein Teil einer physischen GPU verwendet wird, ist die Leistung höher als bei emulierter Grafik, und es ist keine Karte pro VM erforderlich. Diese Funktion ermöglicht die Ressourcenoptimierung und steigert die Leistung der VM. Die Grafikbefehle jeder virtuellen Maschine werden direkt an die GPU übergeben, ohne vom Hypervisor übersetzt zu werden.

Mehrere gemeinsam genutzte GPU (vGPU)

Mit mehreren vGPU können mehrere virtuelle GPUs gleichzeitig von einer einzigen VM verwendet werden. Es können nur bestimmte vGPU-Profile verwendet werden, und alle an eine einzelne VM angeschlossenen vGPUs müssen vom gleichen Typ sein. Diese zusätzlichen vGPUs können zur Rechenverarbeitung verwendet werden. Weitere Informationen zur Anzahl der vGPUs, die für eine einzelne VM unterstützt werden, finden Sie unter Konfigurations-Limits.

Diese Funktion ist nur für NVIDIA-GPUs verfügbar. Weitere Informationen zu den physischen GPUs, die die Funktion mit mehreren vGPUs unterstützen, finden Sie in der NVIDIA-Dokumentation.

Herstellersupport

In der folgenden Tabelle ist die Gastunterstützung für die Funktionen GPU-Passthrough, gemeinsam genutzte GPU (vGPU) und mehrere gemeinsam genutzte GPU (vGPU) aufgeführt:

	GPU-Passthrough für Windows-VMs	GPU-Passthrough für Linux-VMs	Gemeinsam genutzte GPU (vGPU) für Windows-VMs	Gemeinsam genutzte GPU (vGPU) für Linux-VMs	Mehrere gemeinsam genutzte GPU (vGPU) für Windows-VMs	Mehrere gemeinsam genutzte GPU (vGPU) für Linux-VMs
AMD	JA					
Intel	JA		JA (veraltet)			
NVIDIA	JA	JA	JA	JA	JA (siehe Hinweis)	JA (siehe Hinweis)

> **Hinweis:**
>
> - Nur einige der Gastbetriebssysteme unterstützen mehrere vGPU. Weitere Informationen finden Sie unter Unterstützung und Einschränkungen für Gäste.
> - Nur einige der Gastbetriebssysteme unterstützen die vGPU-Livemigration. Weitere Informationen finden Sie unter Herstellersupport.

Je nach verwendeter Grafikkarte benötigen Sie möglicherweise ein Anbieterabonnement oder eine Lizenz.

vGPU Livemigration

vGPU Livemigration ermöglicht eine VM, die eine virtuelle GPU verwendet, um Livemigration, Speicher-Livemigration oder VM-Aussetzung durchzuführen. VMs mit vGPU-Livemigrationsfunktionen können migriert werden, um Ausfallzeiten zu vermeiden.

Mit der vGPU-Livemigration können Sie auch rollierende Pool-Upgrades auf Pools durchführen, die vGPU-fähige VMs hosten. Weitere Informationen finden Sie unter Rolling-Pool-Upgrades.

Um vGPU-Livemigration oder VM-Aussetzung zu verwenden, muss Ihre VM auf einer Grafikkarte ausgeführt werden, die diese Funktion unterstützt. Auf Ihrer VM müssen auch die unterstützten Treiber des GPU-Anbieters installiert sein.

> **Warnung:**
>
> Die Größe des GPU-Status im NVIDIA-Treiber kann während der vGPU-Livemigration zu einer Ausfallzeit von 5 Sekunden oder mehr führen.

Bei der Verwendung der vGPU-Livemigration gelten die folgenden Einschränkungen:

- Die Livemigration ist nicht mit GPU-Passthrough kompatibel.
- Bei VMs müssen die entsprechenden vGPU-Treiber installiert sein, um mit allen vGPU-Livemigrationsfunktionen unterstützt zu werden. Die Gasttreiber müssen für alle Gäste installiert sein, die die vGPU-Funktion verwenden.
- Neustart- und Herunterfahrenvorgänge auf einer VM werden während einer laufenden Migration nicht unterstützt. Diese Vorgänge können dazu führen, dass die Migration fehlschlägt.
- Linux-VMs werden mit keiner vGPU-Livemigrationsfunktion unterstützt.
- Die Livemigration durch die Workload Balancing-Appliance wird für vGPU-fähige VMs nicht unterstützt. Die Workload Balancing-Appliance kann keine Kapazitätsplanung für VMs durchführen, an die eine vGPU angeschlossen ist.
- Nach der Migration einer VM mithilfe der vGPU-Livemigration ist die Gast-VNC-Konsole möglicherweise beschädigt. Verwenden Sie ICA, RDP oder eine andere netzwerkbasierte Methode für den Zugriff auf VMs, nachdem eine vGPU-Livemigration durchgeführt wurde.
- Die VDI-Migration verwendet Livemigration und erfordert daher ausreichend vGPU-Speicherplatz auf dem Host, um eine Kopie der vGPU-Instanz auf dem Host zu erstellen. Wenn die physischen GPUs vollständig genutzt werden, ist eine VDI-Migration möglicherweise nicht möglich.

Herstellersupport

In der folgenden Tabelle ist die Unterstützung für die vGPU-Livemigration aufgeführt:

	GPU-Passthrough für Windows-VMs	GPU-Passthrough für Linux-VMs	Gemeinsam genutzte GPU (vGPU) für Windows-VMs	Gemeinsam genutzte GPU (vGPU) für Linux-VMs	Mehrere gemeinsam genutzte GPU (vGPU) für Windows-VMs	Mehrere gemeinsam genutzte GPU (vGPU) für Linux-VMs
NVIDIA			JA		JA	

Weitere Informationen zu den Grafikkarten, die diese Funktion unterstützen, finden Sie in den herstellerspezifischen Abschnitten dieses Handbuchs. Kunden benötigen je nach verwendeter Grafikkarte möglicherweise ein Anbieterabonnement oder eine Lizenz.

Unterstützung und Einschränkungen für Gäste

XenServer unterstützt die folgenden Gastbetriebssysteme für virtuelle GPUs.

NVIDIA vGPU

Mit einem Sternchen (*) markierte Betriebssysteme unterstützen auch mehrere vGPU.

Windows-Gäste:

- Windows 10 (64 Bit) *
- Windows 11 (64 Bit) *
- Windows Server 2016 (64 Bit) *
- Windows Server 2019 (64 Bit) *
- Windows Server 2022 (64 Bit) *

Linux-Gäste:

- RHEL 7 *
- RHEL 8 *
- RHEL 9 *
- CentOS 7
- CentOS Stream 9
- Ubuntu 18.04 * (veraltet)
- Ubuntu 20.04 *
- Ubuntu 22.04 *
- Rocky Linux 8 *
- Rocky Linux 9 *

Intel GVT-G (veraltet)

Windows-Gäste:

- Windows 10 (64-Bit)
- Windows Server 2016 (64-Bit)

Einschränkungen

- VMs mit einer virtuellen GPU werden von Dynamic Memory Control nicht unterstützt.
- XenServer erkennt und gruppiert automatisch identische physische GPUs auf Hosts im selben Pool. Wenn sie einer Gruppe von GPUs zugewiesen wird, kann eine VM auf jedem Host im Pool gestartet werden, der über eine verfügbare GPU in der Gruppe verfügt.
- Alle Grafiklösungen (NVIDIA vGPU, Intel GVT-D, Intel GVT-G und vGPU Passthrough) können in einer Umgebung mit hoher Verfügbarkeit verwendet werden. VMs, die diese Grafiklösungen verwenden, können jedoch nicht mit hoher Verfügbarkeit geschützt werden. Diese VMs können nach bestem Ermessen neu gestartet werden, während es Hosts mit den entsprechenden freien Ressourcen gibt.

Hosts für Grafiken vorbereiten

February 24, 2024

Dieser Abschnitt enthält schrittweise Anweisungen zur Vorbereitung von XenServer auf unterstützte grafische Virtualisierungstechnologien. Die Angebote umfassen NVIDIA vGPU, Intel GVT-d und Intel GVT-G.

NVIDIA vGPU

NVIDIA vGPU ermöglicht mehreren virtuellen Maschinen (VM) den gleichzeitigen, direkten Zugriff auf eine einzelne physische GPU. Es verwendet NVIDIA-Grafiktreiber, die auf nicht virtualisierten Betriebssystemen bereitgestellt werden. Physische NVIDIA-GPUs können mehrere virtuelle GPU-Geräte (vGPUs) unterstützen. Um diese Unterstützung bereitzustellen, muss die physische GPU unter der Kontrolle von NVIDIA Virtual GPU Manager stehen, der in der XenServer Control Domain (dom0) ausgeführt wird. Die vGPUs können direkt virtuellen Rechnern zugewiesen werden.

VMs verwenden virtuelle GPUs wie eine physische GPU, die der Hypervisor durchlaufen hat. Ein in die VM geladener NVIDIA-Treiber bietet direkten Zugriff auf die GPU für leistungskritische schnelle Pfade. Es bietet auch eine paravirtualisierte Schnittstelle zum virtuellen NVIDIA-GPU-Manager.

> **Wichtig:**
>
> Um sicherzustellen, dass Sie immer über die neuesten Sicherheits- und Funktionsupdates verfügen, stellen Sie sicher, dass Sie das neueste NVIDIA vGPU-Softwarepaket für XenServer (bestehend aus dem NVIDIA Virtual GPU Manager für XenServer und NVIDIA-Treibern) installieren und es auf die neueste von NVIDIA bereitgestellte Version aktualisieren. Weitere Informationen

> finden Sie in der NVIDIA-Dokumentation.
>
> Die neuesten NVIDIA-Treiber sind bei NVIDIA NVOnlineerhältlich.

NVIDIA vGPU ist mit der HDX 3D Pro-Funktion von Citrix Virtual Apps and Desktops oder Citrix DaaS kompatibel. Weitere Informationen finden Sie unter HDX 3D Pro.

Hinweis zur Lizenzierung

NVIDIA vGPU ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zu den XenServer-Editionen und zum Upgrade finden Sie auf der XenServer-Website. Weitere Informationen finden Sie unter Lizenzierung.

Abhängig von der verwendeten NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-Abonnement oder eine Lizenz.

Informationen zur Lizenzierung von NVIDIA-Karten finden Sie auf der NVIDIA-Website.

Verfügbare NVIDIA vGPU-Typen

NVIDIA GRID-Karten enthalten mehrere Graphics Processing Units (GPU). Zum Beispiel enthalten TESLA M10-Karten vier GM107GL-GPUs, und TESLA M60-Karten enthalten zwei GM204GL-GPUs. Jede physische GPU kann mehrere verschiedene Arten von virtueller GPU (vGPU) hosten. vGPU-Typen haben eine feste Menge an Bildpuffer, Anzahl unterstützter Displayköpfe und maximale Auflösungen und sind auf verschiedene Arbeitslastklassen ausgerichtet.

Eine Liste der zuletzt unterstützten NVIDIA-Karten finden Sie in der Hardwarekompatibilitätsliste und in den NVIDIA-Produktinformationen.

> **Hinweis:**
>
> Die vGPUs, die gleichzeitig auf einer physischen GPU gehostet werden, **müssen alle vom gleichen Typ sein**. Es gibt jedoch keine entsprechende Beschränkung für physische GPUs auf derselben Karte. Diese Einschränkung erfolgt automatisch und kann zu unerwarteten Problemen bei der Kapazitätsplanung führen.

NVIDIA vGPU Systemanforderungen

- NVIDIA GRID-Karte:
  - Eine Liste der zuletzt unterstützten NVIDIA-Karten finden Sie in der Hardwarekompatibilitätsliste und in den NVIDIA-Produktinformationen.

- Abhängig von der verwendeten NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-Abonnement oder eine Lizenz. Weitere Informationen finden Sie in den NVIDIA-Produktinformationen.
- Abhängig von der NVIDIA-Grafikkarte müssen Sie möglicherweise sicherstellen, dass die Karte auf den richtigen Modus eingestellt ist. Weitere Informationen finden Sie in der NVIDIA-Dokumentation.
- XenServer Premium-Ausgabe.
- Ein Host, der XenServer und die unterstützten NVIDIA-Karten hosten kann.
- NVIDIA vGPU-Softwarepaket für XenServer, bestehend aus dem NVIDIA Virtual GPU Manager für XenServer und NVIDIA-Treibern.

  > **Hinweis:**
  >
  > Lesen Sie die NVIDIA Virtual GPU-Softwaredokumentation, die auf der NVIDIA-Websiteverfügbar ist. Registriere dich bei NVIDIA um auf diese Komponenten zuzugreifen.

- Um Citrix Virtual Desktops mit VMs auszuführen, auf denen NVIDIA vGPU ausgeführt wird, benötigen Sie außerdem: Citrix Virtual Desktops 7.6 oder höher, vollständige Installation.
- Für NVIDIA Ampere vGPUs und alle zukünftigen Generationen müssen Sie SR-IOV in Ihrer Systemfirmware aktivieren.

vGPU Livemigration

XenServer ermöglicht die Verwendung von Live-Migration, Speicher-Livemigration und die Möglichkeit, für NVIDIA vGPU-fähige VMs anzuhalten und fortzufahren.

Um die vGPU-Livemigration, Speicher-Livemigration oder Suspend-Funktionen zu verwenden, müssen Sie die folgenden Anforderungen erfüllen:

- Eine NVIDIA GRID-Karte, Maxwell-Familie oder höher.
- Ein NVIDIA Virtual GPU Manager für XenServer mit aktivierter Live-Migration. Weitere Informationen finden Sie in der NVIDIA-Dokumentation.
- Eine Windows-VM, auf der livemigrationsfähige NVIDIA-vGPU-Treiber installiert sind.

vGPU-Livemigration ermöglicht die Verwendung von Livemigration innerhalb eines Pools, Livemigration zwischen Pools, Speicher-Livemigration und Aussetzen/Fortsetzen von vGPU-fähigen VMs.

Überblick über die Vorbereitung

1. Installieren Sie XenServer

2. Installieren Sie den NVIDIA Virtual GPU Manager für XenServer
3. Starten Sie den XenServer-Host neu

Installation auf XenServer

XenServer steht auf der XenServer-Downloadseite zum Download zur Verfügung.

Installieren Sie Folgendes:

- **ISO für die XenServer-Basisinstallation**
- **XenCenter Windows Managementkonsole**

Weitere Informationen finden Sie unter Installation.

Hinweis zur Lizenzierung

vGPU ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zu den XenServer-Editionen und zum Upgrade finden Sie auf der XenServer-Website. Weitere Informationen finden Sie unter Lizenzierung.

Abhängig von der verwendeten NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-Abonnement oder eine Lizenz. Weitere Informationen finden Sie unter NVIDIA-Produktinformationen.

Informationen zur Lizenzierung von NVIDIA-Karten finden Sie auf der NVIDIA-Website.

Installieren Sie den NVIDIA vGPU Manager für XenServer

Installieren Sie die virtuelle NVIDIA-GPU-Software, die von NVIDIAerhältlich ist. Die virtuelle NVIDIA-GPU-Software besteht aus:

- Virtueller NVIDIA-GPU-Manager
- Windows Displaytreiber (Der Windows Bildschirmtreiber hängt von der Windows-Version ab)

Der **NVIDIA Virtual GPU Manager** wird in der XenServer Control Domain (dom0) ausgeführt. Es wird entweder als zusätzliches Paket oder als RPM-Datei bereitgestellt. Weitere Informationen zur Installation finden Sie in der Dokumentation zur virtuellen NVIDIA-Software für Grafikprozessoren.

Das Update kann mit einer der folgenden Methoden installiert werden:

- Verwenden Sie XenCenter (**Tools** > **Update installieren** > **Wählen Sie ein Update oder ein zusätzliches Paket von dem Datenträger aus**)
- Verwenden Sie den xe-Befehl CLI-Befehl `xe-install-supplemental-pack`.

> **Hinweis:**
>
> Wenn Sie den NVIDIA Virtual GPU Manager mithilfe einer RPM-Datei installieren, müssen Sie die RPM-Datei nach dom0 kopieren und dann installieren.

1. Verwenden Sie den Befehl rpm, um das Paket zu installieren:

```
rpm -iv <vgpu_manager_rpm_filename>
<!--NeedCopy-->
```

2. Starten Sie den XenServer-Host neu:

```
shutdown -r now
<!--NeedCopy-->
```

3. Stellen Sie nach dem Neustart des XenServer-Hosts sicher, dass die Software korrekt installiert und geladen wurde, indem Sie den NVIDIA-Kerneltreiber überprüfen:

```
[root@xenserver ~]#lsmod |grep nvidia
    nvidia            8152994 0
<!--NeedCopy-->
```

4. Stellen Sie sicher, dass der NVIDIA-Kerneltreiber erfolgreich mit den physischen NVIDIA-GPUs in Ihrem Host kommunizieren kann Führen Sie den Befehl `nvidia-smi` aus, um eine Liste der GPUs in Ihrer Plattform zu erstellen, ähnlich wie:

```
[root@xenserver ~]# nvidia-smi

    Thu Jan 26 13:48:50 2017
    +-----------------------------------------------------------+|
    NVIDIA-SMI 367.64  Driver Version: 367.64                    |
    -------------------------------+----------------------+
     GPU Name    Persistence-M| Bus-Id   Disp.A | Volatile Uncorr.
         ECC|
    Fan Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util
       Compute M.|
    ===============================+======================+==================

    |  0 Tesla M60       On | 0000:05:00.0    Off|   Off |
    | N/A  33C  P8    24W / 150W |   7249MiB /  8191MiB |      0%
            Default  |
    +-------------------------------+----------------------+----------------

    |  1 Tesla M60       On | 0000:09:00.0    Off |  Off |
    | N/A  36C  P8    24W / 150W |   7249MiB /  8191MiB |      0%
            Default  |
    +-------------------------------+----------------------+----------------

    |  2 Tesla M60       On | 0000:85:00.0    Off |  Off |
    | N/A  36C  P8    23W / 150W |   19MiB /  8191MiB |        0%
            Default  |
```



```
+-------------------------------+----------------------+----------------------
|   3 Tesla M60       On | 0000:89:00.0     Off |  Off |
| N/A  37C    P8    23W / 150W |     14MiB /  8191MiB |     0%
        Default  |
+-------------------------------+----------------------+----------------------

+-----------------------------------------------------------------------------
| Processes:                  GPU Memory |
| GPU    PID  Type  Process name    Usage    |
|=============================================================================
| No running compute processes found |
+-----------------------------------------------------------------------------
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie NVIDIA vGPU mit XenServer-Servern verwenden, die über mehr als 768 GB RAM verfügen, fügen Sie den Parameter `iommu=dom0-passthrough` zur Xen-Befehlszeile hinzu:
>
> a) Führen Sie den folgenden Befehl in der Steuerdomäne (Dom0) aus:
>
> `/opt/xensource/libexec/xen-cmdline –-set-xen iommu=dom0-passthrough`
>
> b) Starten Sie den Host neu.

Intel GVT-D und GVT-G

XenServer unterstützt die virtuelle GPU (GVT-G) von Intel, eine Grafikbeschleunigungslösung, für die keine zusätzliche Hardware erforderlich ist. Es verwendet die Intel Iris Pro-Funktion, die in bestimmte Intel-Prozessoren eingebettet ist, und einen in der VM installierten Standard-Intel-GPU-Treiber.

Um sicherzustellen, dass Sie immer über die neuesten Sicherheits- und Funktionsupdates verfügen, stellen Sie sicher, dass Sie alle von Intel bereitgestellten Updates für die Treiber auf Ihren VMs und die Firmware auf Ihrem Host installieren.

Intel GVT-D und GVT-G sind mit den HDX 3D Pro-Funktionen von Citrix Virtual Apps and Desktops oder Citrix DaaS kompatibel. Weitere Informationen finden Sie unter HDX 3D Pro.

> **Hinweis:**
>
> Da die Intel Iris Pro-Grafikfunktion in die Prozessoren eingebettet ist, können CPU-intensive Anwendungen dazu führen, dass Strom von der GPU umgeleitet wird. Daher ist möglicherweise

> keine vollständige Grafikbeschleunigung wie bei rein GPU-intensiven Workloads möglich.

Intel GVT-G Systemanforderungen und Konfiguration (veraltet)

Um Intel GVT-G verwenden zu können, muss Ihr XenServer-Host über die folgende Hardware verfügen:

- Eine CPU mit Iris Pro-Grafik. Diese CPU muss in der Hardwarekompatibilitätslisteals unterstützt für Grafiken aufgeführt sein
- Ein Motherboard mit einem grafikfähigen Chipsatz. Zum Beispiel C226 für Xeon E3 v4-CPUs oder C236 für Xeon E3 v5-CPUs.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die Hosts neu starten, wenn Sie zwischen Intel GPU Passthrough (GVT-D) und Intel Virtual GPU (GVT-G) wechseln.

Bei der Konfiguration von Intel GVT-G hängt die Anzahl der virtuellen Intel-GPUs, die auf einem bestimmten XenServer-Host unterstützt werden, von dessen GPU-Balkengröße ab. Die GPU-Balkengröße wird in der Systemfirmware als „Aperturgröße“bezeichnet. Wir empfehlen, die Aperture-Größe auf 1.024 MB einzustellen, um maximal sieben virtuelle GPUs pro Host zu unterstützen.

Wenn Sie die Aperture-Größe auf 256 MB konfigurieren, kann nur eine VM auf dem Host starten. Eine Einstellung auf 512 MB kann dazu führen, dass nur drei VMs auf dem XenServer-Host gestartet werden. Eine Aperture-Größe über 1.024 MB wird nicht unterstützt und erhöht **nicht** die Anzahl der virtuellen Maschinen, die auf einem Host beginnen.

Intel GPU-Passthrough aktivieren

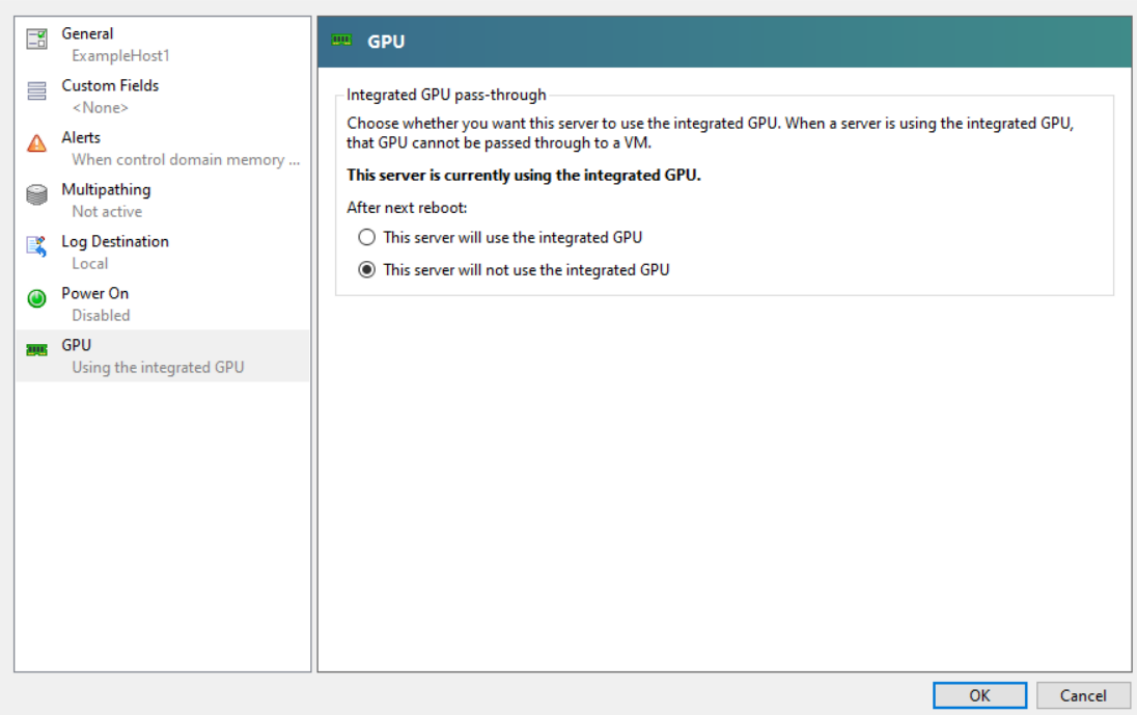
XenServer unterstützt die GPU-Passthrough-Funktion für Windows-VMs, die ein integriertes Intel-GPU-Gerät verwenden.

- Weitere Informationen zu Windows-Versionen, die mit Intel GPU-Passthrough unterstützt werden, finden Sie unter Grafik.
- Weitere Informationen zu unterstützter Hardware finden Sie in der Hardwarekompatibilitätsliste.

Bei Verwendung von Intel GPU auf Intel-Servern hat die Control Domain (dom0) des XenServer-Servers Zugriff auf das integrierte GPU-Gerät. In solchen Fällen ist die GPU für Pass-Through verfügbar. Um die Intel GPU-Pass-Through-Funktion auf Intel-Servern zu verwenden, deaktivieren Sie die Verbindung zwischen dom0 und der GPU, bevor Sie die GPU zur VM durchlaufen.

Führen Sie die folgenden Schritte aus, um diese Verbindung zu deaktivieren:

1. Wählen Sie im Bereich **Ressourcen** den XenServer-Host aus.
2. Klicken Sie auf der Registerkarte **Allgemein** auf **Eigenschaften**, und klicken Sie im linken Bereich auf **GPU**.
3. Wählen Sie im Abschnitt **Integrierte GPU-Passthroughdie Option Dieser Server verwendet die integrierte GPU nicht**.



   Dieser Schritt deaktiviert die Verbindung zwischen dom0 und dem integrierten Intel-GPU-Gerät.
4. Klicken Sie auf **OK**.
5. Starten Sie den XenServer-Host neu, damit die Änderungen wirksam werden.

   Die Intel-GPU ist jetzt während der Erstellung einer neuen VM in der GPU-Typliste und auf der Registerkarte **Eigenschaften** der VM sichtbar.

   > **Hinweis:**
   >
   > Der externe Konsolenausgang des XenServer-Hosts (z. B. VGA, HDMI, DP) ist nicht verfügbar, nachdem die Verbindung zwischen dom0 und der GPU deaktiviert wurde.

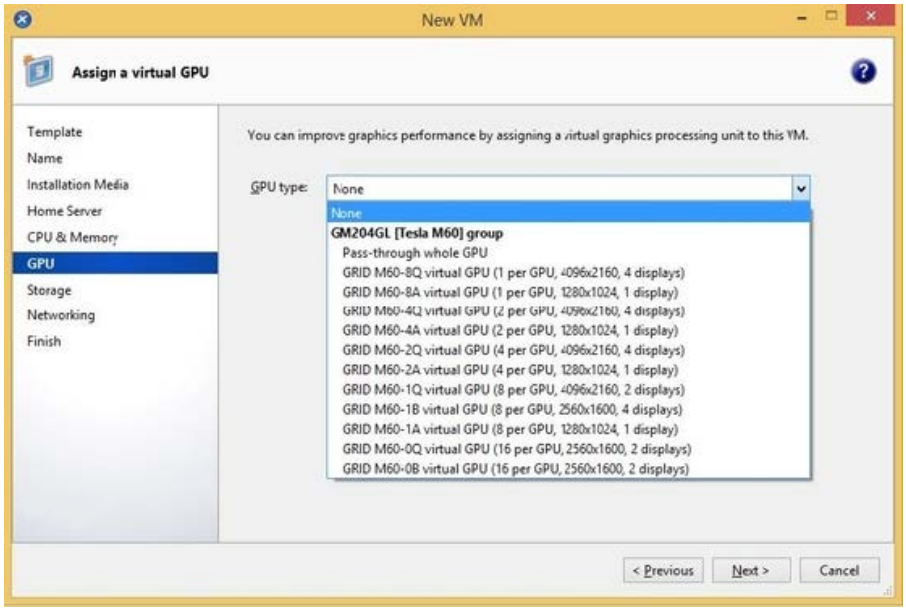
Erstellen vGPU-fähiger VMs

February 24, 2024

In diesem Abschnitt finden Sie schrittweise Anweisungen zum Erstellen einer virtuellen GPU- oder GPU-Passthrough-fähigen VM.

> **Hinweis:**
>
> Wenn Sie die Intel GPU-Pass-Through-Funktion verwenden, lesen Sie zunächst den Abschnitt *Intel GPU-Passthrough aktivieren* für weitere Konfiguration, und führen Sie dann die folgenden Schritte aus.

1. Erstellen Sie eine VM mit XenCenter. Wählen Sie den Host im Bereich Ressourcen aus und wählen Sie dann im VM-Menü **Neue VM** aus.
2. Befolgen Sie die Anweisungen in der Konfiguration für **neue VM** und wählen Sie das **Installationsmedium**, den **Homeserver**sowie **CPU und Speicher**aus.
3. GPU-fähige Hosts zeigen eine **GPU-Konfigurationsseite** an:



4. Klicken Sie auf **Hinzufügen**. Wählen Sie in der Liste **GPU-Typ** entweder **Ganze GPU durchleiten**oder einen virtuellen GPU-Typ aus.

   Nicht verfügbare virtuelle GPU-Typen sind ausgegraut.

   Wenn Sie Ihrer VM mehrere vGPUs zuweisen möchten, stellen Sie sicher, dass Sie einen vGPU-Typ auswählen, der mehrere vGPU unterstützt. Wiederholen Sie diesen Schritt, um weitere vGPUs desselben Typs hinzuzufügen.

5. Klicken Sie auf **Weiter**, um **Speicher** und dann auf **Netzwerk**zu konfigurieren
6. Nachdem Sie Ihre Konfiguration abgeschlossen haben, klicken Sie auf **Jetzt erstellen**.

Installieren Sie die XenServer VM Tools

Ohne die optimierten Netzwerk- und Speichertreiber, die von den XenServer VM Tools bereitgestellt werden, bieten Remote-Grafikanwendungen, die auf NVIDIA vGPU ausgeführt werden, **keine** maximale Leistung.

- Wenn es sich bei Ihrer VM um eine Windows-VM handelt, müssen Sie die XenServer VM Tools für Windows auf Ihrer VM installieren. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Windows.
- Wenn es sich bei Ihrer VM um eine Linux-VM handelt, können Sie die XenServer VM Tools für Linux auf Ihrer VM installieren. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Installieren Sie die Gasttreiber

Beim Anzeigen der VM-Konsole in XenCenter startet die VM normalerweise im VGA-Modus mit einer Auflösung von 800 x 600 auf dem Desktop. Die standardmäßigen Steuerelemente für die Windows-Bildschirmauflösung können verwendet werden, um die Auflösung auf andere Standardauflösungen zu erhöhen. (**Systemsteuerung> Display> Bildschirmauflösung**)

> **Hinweis:**
>
> Wenn Sie GPU-Passthrough verwenden, empfehlen wir, die In-Guest-Treiber über RDP oder VNC über das Netzwerk zu installieren. Das heißt, nicht über XenCenter.

Um sicherzustellen, dass Sie immer über die neuesten Sicherheits- und Funktionsverbesserungen verfügen, stellen Sie sicher, dass Sie immer die neuesten Updates für Ihre Gasttreiber verwenden.

Installieren Sie die NVIDIA-Treiber

Installieren Sie NVIDIA-Treiber in der VM, um den vGPU-Betrieb zu ermöglichen (wie bei einer physischen NVIDIA-GPU).

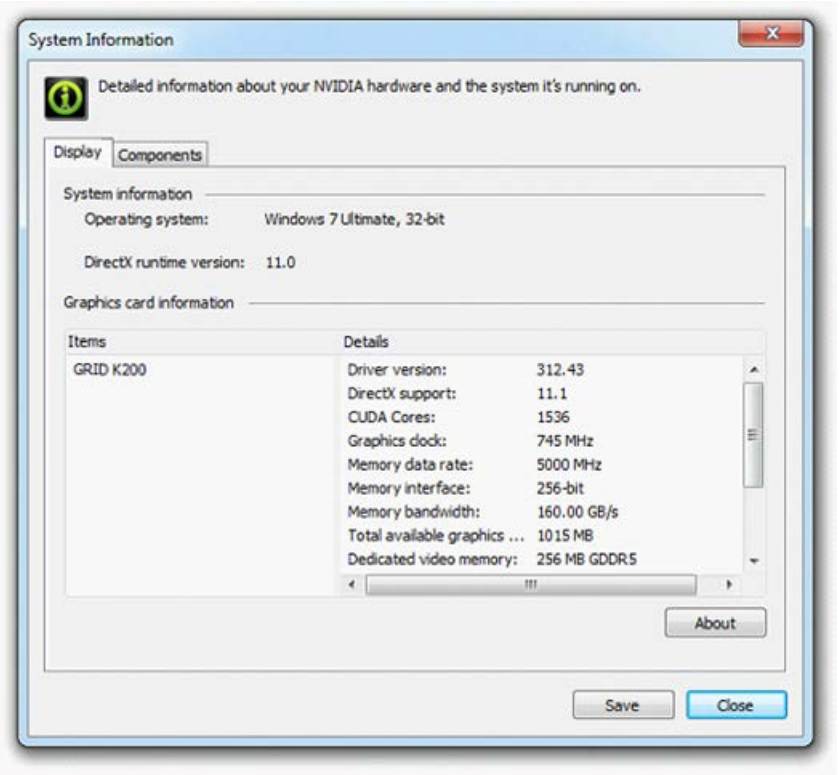
Der folgende Abschnitt gibt einen Überblick über das Verfahren. Eine ausführliche Anleitung finden Sie in der Dokumentation zur virtuellen NVIDIA-Software für Grafikprozessoren.

1. Starten Sie die VM. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf die VM, und klicken Sie auf **Start**.

   Während dieses Startvorgangs weist XenServer der VM dynamisch eine vGPU zu.

2. Folgen Sie den Installationsbildschirmen des Windows-Betriebssystems.
3. Nachdem die Installation des Betriebssystems abgeschlossen ist, starten Sie die VM neu.

4. Installieren Sie den entsprechenden Treiber für die GPU im Gast. Das folgende Beispiel zeigt den speziellen Fall für die Gastinstallation der NVIDIA GRID-Treiber.
5. Kopieren Sie das 64-Bit-NVIDIA-Windows-Treiberpaket auf die VM, öffnen Sie die ZIP-Datei und führen Sie setup.exe aus.
6. Befolgen Sie die Schritte des Installationsprogramms zur Installation des Treibers.
7. Nachdem die Treiberinstallation abgeschlossen ist, werden Sie möglicherweise aufgefordert, die VM neu zu starten. Wählen Sie **Jetzt neu starten**, um die VM sofort neu zu starten. Beenden Sie alternativ das Installationspaket und starten Sie die VM neu, wenn Sie bereit sind. Wenn die VM gestartet wird, bootet sie auf einem Windows-Desktop.
8. Um zu überprüfen, ob der NVIDIA-Treiber ausgeführt wird, klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie **NVIDIA-Bedienfeld**
9. Wählen Sie in der NVIDIA-Systemsteuerung **Systeminformationen**aus. Diese Schnittstelle zeigt den von der VM verwendeten GPU-Typ, seine Funktionen und die verwendete NVIDIA-Treiberversion an:



> **Hinweis:**
>
> Je nach verwendeter NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-Abonnement oder eine Lizenz. Weitere Informationen finden Sie in den NVIDIA-Produktinformationen.

Die VM ist jetzt bereit, die gesamte Palette der von der GPU unterstützten DirectX- und OpenGL-Grafikanwendungen auszuführen.

Für Linux-VMs

Installieren Sie den Treiber auf Ihrer Linux-VM gemäß den Anweisungen in den NVIDIA-Benutzerhandbüchern.

Wenn Ihre Linux-VM im UEFI Secure Boot-Modus startet, müssen Sie möglicherweise zusätzliche Schritte unternehmen, um den Treiber zu signieren. Weitere Informationen finden Sie unter Installieren von Treibern von Drittanbietern auf Ihrer Secure Boot Linux-VM.

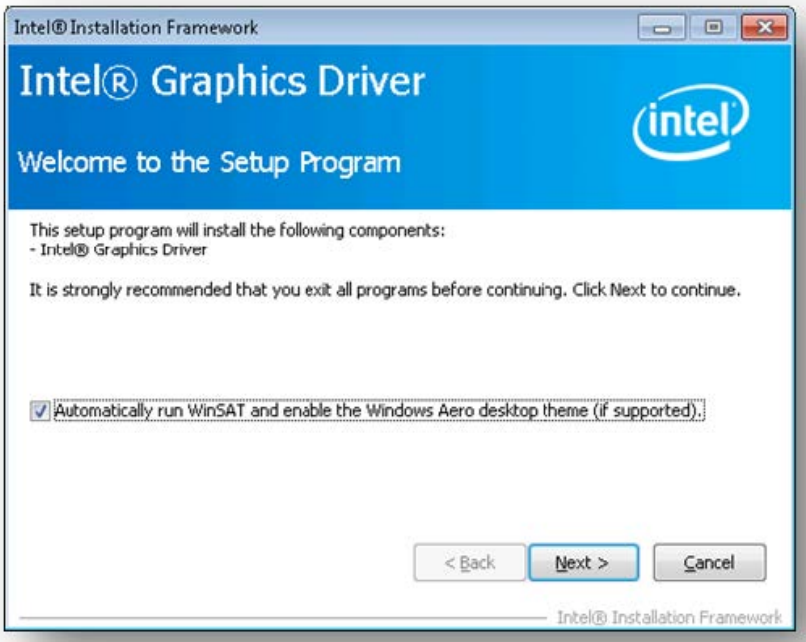
Installieren Sie die Intel-Treiber (veraltet)

Installieren Sie Intel-Treiber in der VM, um den GPU-Betrieb zu ermöglichen.

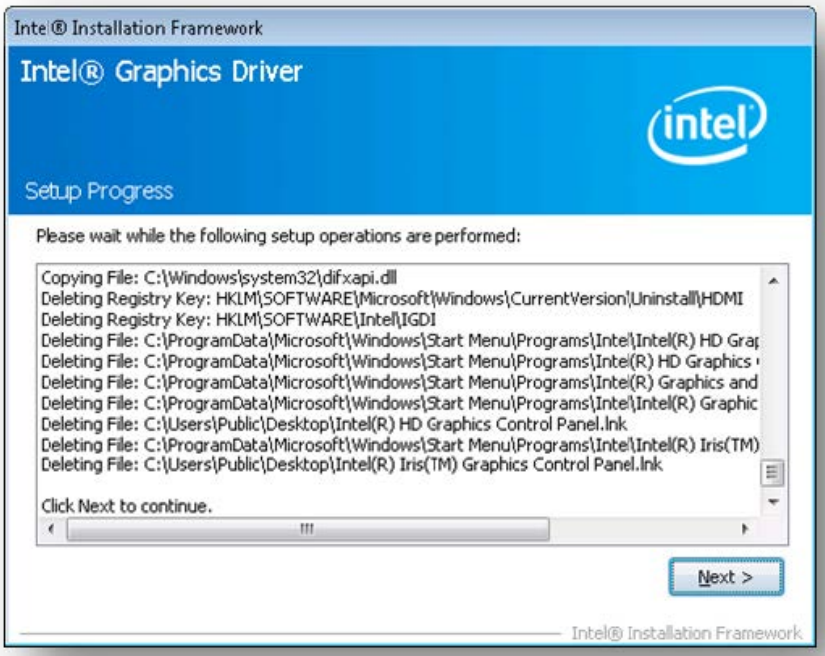
1. Starten Sie die **VM**. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf die VM, und klicken Sie auf **Start**.

   Während dieses Startvorgangs weist XenServer der VM dynamisch eine GPU zu.

2. Folgen Sie den Installationsbildschirmen des Windows-Betriebssystems.
3. Nachdem die Installation des Betriebssystems abgeschlossen ist, starten Sie die VM neu.
4. Kopieren Sie den 64-Bit-Intel-Windows-Treiber (Intel Graphics Driver) auf die VM.
5. Führen Sie das **Intel Grafiktreiber**-Setupprogramm aus
6. Wählen Sie **WinSAT automatisch ausführen** aus, und klicken Sie dann auf **Weiter**.



7. Um die Lizenzvereinbarung zu akzeptieren, klicken Sie auf **Ja**, und klicken Sie im Bildschirm Readmedateiinformationen auf **Weiter**.
8. Warten Sie, bis die Einrichtungsvorgänge abgeschlossen sind. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**.



9. Um die Installation abzuschließen, werden Sie aufgefordert, die VM neu zu starten. Wählen Sie **Ja**, ich möchte diesen Computer jetzt neu starten und klicken Sie auf **Fertig stellen**.
10. Stellen Sie nach dem Neustart der VM sicher, dass die Grafiken korrekt funktionieren. Öffnen Sie den Windows Geräte-Manager, erweitern Sie **Displayadapter**, und stellen Sie sicher, dass der Intel Graphics Adapter keine Warnsymbole enthält.

> **Hinweis:**
>
> Die neuesten Treiber erhalten Sie auf der Intel-Website.

---

layout: doc
description: Configure the amount of memory allocated to the control domain (dom0) of a XenServer host.—

Speichernutzung

Zwei Komponenten tragen zum Speicherbedarf des XenServer-Hosts bei. Erstens der vom Xen-Hypervisor selbst verbrauchte Speicher. Zweitens gibt es den Speicher, der von der *Control Domain* des Hosts verbraucht wird. Die Steuerdomäne, auch bekannt als “Domain0”oder “dom0”, ist eine

sichere, privilegierte Linux-VM, auf der der XenServer Management Toolstack (XAPI) ausgeführt wird. Neben den XenServer-Verwaltungsfunktionen führt die Steuerdomäne auch den Treiberstapel aus, der vom Benutzer erstellte VM-Zugriff auf physische Geräte ermöglicht.

Domänenspeicher steuern

Die Menge an Speicher, die der Steuerdomäne zugewiesen ist, wird automatisch angepasst und basiert auf der Größe des physikalischen Speichers auf dem physikalischen Host. Standardmäßig weist XenServer der Steuerdomäne **1 GiB plus 5% des gesamten physischen Speichers** zu, bis zu einem anfänglichen Maximum von 8 GiB.

> **Hinweis:**
>
> Die im XenServer-Abschnitt in XenCenter angegebene Menge beinhaltet den von der Steuerdomäne (dom0) verwendeten Speicher, den Xen-Hypervisor selbst und den Crash-Kernel. Daher kann die in XenCenter gemeldete Speichermenge diese Werte überschreiten. Der vom Hypervisor verwendete Arbeitsspeicher ist größer für Hosts, die mehr Speicher verwenden.

Ändern der Speichermenge, die der Steuerdomäne zugewiesen ist

Sie können die Speichermenge, die dom0 zugewiesen ist, mit XenCenter oder über die Befehlszeile ändern. Wenn Sie die Speichermenge, die der Steuerdomäne zugewiesen ist, über die standardmäßig zugewiesene Menge hinaus erhöhen, führt diese Aktion dazu, dass weniger Speicher für virtuelle Maschinen verfügbar ist.

In den folgenden Fällen müssen Sie möglicherweise die Speichermenge erhöhen, die der Steuerdomäne eines XenServer-Hosts zugewiesen ist:

- Sie führen viele VMs auf dem Host aus
- Sie verwenden den PVS-Accelerator
- Sie verwenden Lesecaching

> **Wichtig:**
>
> Wenn Sie einen GFS2 SR verwenden und einer dieser Fälle auch auf Ihre Umgebung zutrifft, müssen Sie den Speicherplatz der Steuerdomäne erhöhen. Ungenügender Steuerdomänenspeicher kann zu Netzwerkinstabilität und daraufhin zu Problemen bei geclusterten Pools mit GFS2-SRs führen.

Die Menge an Arbeitsspeicher, die der Steuerdomäne zugewiesen werden soll, hängt von Ihrer Umgebung und den Anforderungen Ihrer VMs ab.

Sie können die folgenden Metriken überwachen, um zu beurteilen, ob die Größe des Control-Domain-Speichers für Ihre Umgebung geeignet ist und welche Auswirkungen die von Ihnen vorgenommenen Änderungen haben:

- **Swap-Aktivität:** Wenn die Steuerdomäne tauscht, erhöhen Sie den Speicher der Steuerdomäne.
- **Tapdisk-Modus:** Sie können auf der Registerkarte XenCenter **Performance** für den Host überwachen, ob sich Ihre Tapdisks im Low-Memory-Modus befinden. Wählen Sie **Aktionen** > **Neues Diagramm** und wählen Sie die **Tapdisks im Low-Memory-Modus** aus. Wenn sich eine Tapdisk im Low-Memory-Modus befindet, erhöhen Sie den Speicher der Steuerdomäne.
- **Pagecache-Druck:** Verwenden Sie den Befehl `top` zur Überwachen der Metrik `buff/cache`. Wenn diese Zahl zu niedrig wird, sollten Sie möglicherweise den Speicher der Steuerdomäne erhöhen.

Ändern des dom0-Speichers mit XenCenter

Informationen zum Ändern des dom0-Speichers über XenCenter finden Sie unter Ändern des Control-Domänenspeichers in der XenCenter-Dokumentation.

> **Hinweis:**
>
> Sie können XenCenter nicht verwenden, um den dom0-Speicher unter den Wert zu reduzieren, der ursprünglich bei der XenServer-Installation festgelegt wurde. Um diese Änderung vorzunehmen, müssen Sie die Befehlszeile verwenden.

dom0-Speicher über die Befehlszeile ändern

> **Hinweis:**
>
> Auf Hosts mit kleinerem Speicher (weniger als 16 GiB) sollten Sie den der Control Domain zugewiesenen Speicher auf einen niedrigeren Wert als den Standardwert der Installation reduzieren. Sie können die Befehlszeile verwenden, um diese Änderung vorzunehmen. Wir empfehlen jedoch, **den dom0-Speicher nicht unter 1 GiB zu reduzieren** und diesen Vorgang unter Anleitung des Support-Teams durchzuführen.

1. Öffnen Sie auf dem XenServer-Host eine lokale Shell und melden Sie sich als Root an.
2. Geben Sie Folgendes ein:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<
   nn>M
<!--NeedCopy-->
```

   Wobei <nn> für die Speichermenge in MiB steht, die dom0 zugewiesen werden soll.

3. Starten Sie den XenServer-Host mit XenCenter oder dem `reboot` Befehl auf der XenServer-Konsole neu.

   Führen Sie beim Neustart des Hosts auf der XenServer-Konsole den `free` Befehl aus, um die neuen Speichereinstellungen zu überprüfen.

Wie viel Speicher steht virtuellen Rechnern zur Verfügung?

Um herauszufinden, wie viel Host-Speicher verfügbar ist, um VMs zugewiesen zu werden, ermitteln Sie den Wert des freien Speichers des Hosts, indem Sie ausführen `memory-free`. Geben Sie dann den Befehl ein `vm-compute-maximum-memory`, um die tatsächliche Menge an freiem Speicher abzurufen, die der VM zugewiesen werden kann. Beispiel:

```
xe host-list uuid=host_uuid params=memory-free
xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
<!--NeedCopy-->
```

---

layout: doc
description: Use performance metrics exposed through Round Robin Databases (RRDs) to monitor your XenServer environment.—

Überwachen und verwalten Sie Ihre Bereitstellung

XenServer bietet eine detaillierte Überwachung der Leistungsmetriken. Zu diesen Metriken gehören CPU-, Arbeitsspeicher-, Datenträger-, Netzwerk-, C-State/P-State-Informationen und Speicher. Gegebenenfalls sind diese Metriken pro Host und pro VM verfügbar. Diese Metriken sind direkt verfügbar oder können in XenCenter oder anderen Anwendungen von Drittanbietern abgerufen und grafisch angezeigt werden.

XenServer bietet auch System- und Leistungswarnungen. Warnungen sind Benachrichtigungen, die als Reaktion auf ausgewählte Systemereignisse auftreten. Diese Benachrichtigungen treten auch auf, wenn einer der folgenden Werte einen bestimmten Schwellenwert auf einem verwalteten Host, einer VM oder einem Speicherrepository überschreitet: CPU-Auslastung, Netzwerkauslastung, Speicherauslastung, Steuerung der Domänenspeicherauslastung, Speicherdurchsatz oder VM-Datenträgerauslastung. Sie können die Warnungen mit der Xe-Befehlszeilenschnittstelle oder mit XenCenter konfigurieren. Informationen zum Erstellen von Benachrichtigungen basierend auf einer der verfügbaren Host- oder VM-Leistungsmetriken finden Sie unter Leistungswarnungen.

Überwachen Sie die XenServer-Leistung

Kunden können die Leistung ihrer XenServer-Hosts und virtuellen Maschinen (VMs) anhand der über Round-Robin-Datenbanken (RRDs) bereitgestellten Metriken überwachen. Diese Metriken können über HTTP oder über das RRD2CSV-Tool abgefragt werden. Darüber hinaus verwendet XenCenter diese Daten, um Diagramme zur Systemleistung zu erstellen. Weitere Informationen finden Sie unter Analysieren und Visualisieren von Metriken.

In den folgenden Tabellen sind alle verfügbaren Host- und VM-Metriken aufgeführt.

> **Hinweise:**
>
> - Die Latenz über einen Zeitraum ist definiert als die durchschnittliche Latenz der Vorgänge während dieses Zeitraums.
> - Die Verfügbarkeit und der Nutzen bestimmter Metriken sind SR- und CPU-abhängig.
> - Leistungsmetriken sind für GFS2-SRs und Datenträger auf diesen SRs nicht verfügbar.

Verfügbare Host-Messwerte

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
`avgqu_sz_<sr-uuid-short>`	Durchschnittliche I/O-Warteschlangengröße (Anfragen).	Mindestens ein in SR `<sr-uuid-short>` eingesteckter VBD auf dem Host	`sr-uuid-short` Queue Size
`cpu<cpu>-C<cstate>`	Zeit, die CPU `cpu` im C-Status `cstate` verbracht hat, in Millisekunden.	C-state exists on CPU	CPU `cpu` C-state `cstate`
`cpu<cpu>-P<pstate>`	Zeit, die CPU `cpu` im P-Status `pstate` verbracht hat, in Millisekunden.	P-state exists on CPU	CPU `cpu` P-state `pstate`
`cpu<cpu>`	Nutzung der physischen CPU `cpu` (Bruch). Standardmäßig aktiviert.	CPU `cpu` existiert	CPU `cpu`

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
cpu_avg	Mittlere Auslastung physischer CPUs (Bruch). Standardmäßig aktiviert.	Ohne	Durchschnittliche CPU
hostload	Hostlast pro physischer CPU, wobei sich die Last auf die Anzahl der vCPUs in einem laufenden oder ausführbaren Zustand bezieht.	Ohne	Host-CPU-Last
inflight_<sr-uuid-**short**>	Anzahl der aktuell laufenden I/O-Anforderungen. Standardmäßig aktiviert.	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Inflight Requests
io_throughput_read_<sr-uuidshort>	Aus SR gelesene Daten (MiB/s).	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Read Throughput
io_throughput_write_<sr-uuidshort>	In den SR geschriebene Daten (MiB/s).	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Write Throughput
io_throughput_total_<sr-uuidshort>	Alle SR-I/O (MiB/s).	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Total Throughput
iops_read_<sr-uuid-**short**>	Requests pro Sekunde lesen.	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Read IOPS
iops_write_<sr-uuid-**short**>	Schreibanfragen pro Sekunde.	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Write IOPS
iops_total_<sr-uuid-**short**>	I/O-Anforderungen pro Sekunde.	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr Total IOPS
iowait_<sr-uuid-**short**>	Prozentsatz der Wartezeit auf I/O.	Mindestens ein in SR sr eingesteckter VBD auf dem Host	sr IO Wait

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
`latency_<sr-uuid-short>`	Durchschnittliche I/O-Latenz (Millisekunden).	Mindestens ein in SR `sr` eingesteckter VBD auf dem Host	`sr` Latency
`loadavg`	Durchschnitt der Domain0-Auslastung. Diese Option ist in der Standardeinstellung aktiviert.	Ohne	Domänenlast steuern
`memory_free_kib`	Gesamtmenge an freiem Speicher (KiB). Standardmäßig aktiviert.	Ohne	*In XenCenter nicht vorhanden. Ersetzt durch Used Memory.*
Nicht vom Toolstack gemeldet. Berechnet von XenCenter.	Gesamtmenge des verwendeten Speichers (KiB). Standardmäßig aktiviert.	Ohne	Benutzter Speicher
`memory_reclaimed`	Host-Speicher wird durch Squeeze (B) zurückgewonnen.	Ohne	Wiedergewonnener Speicher
`memory_reclaimed_max`	Host-Speicher zur Rückgewinnung mit Squeeze (B) verfügbar.	Ohne	Potenziell zurückgewonnener Speicher
`memory_total_kib`	Gesamtmenge des Speichers (KiB) im Host. Standardmäßig aktiviert.	Ohne	Gesamter Arbeitsspeicher
`network/latency`	Intervall in Sekunden zwischen den letzten beiden Herzschlägen, die vom lokalen Host an alle Online-Hosts übertragen wurden. Diese Funktion ist standardmäßig deaktiviert.	HA aktiviert	Netzwerk-Latenz

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
statefile/<vdi_uuid>/latency	Bearbeitungszeit in Sekunden des letzten State-File-Zugriffs vom lokalen Host. Diese Funktion ist standardmäßig deaktiviert.	HA aktiviert	HA State File Latency
pif_<pif>_rx	Bytes pro Sekunde, die auf der physikalischen Schnittstelle empfangen pifwerden. Standardmäßig aktiviert.	PIF ist vorhanden	XenCenter-pifname Empfangen (siehe Hinweis)
pif_<pif>_tx	Byte pro Sekunde, die über eine physische Schnittstelle gesendet pifwerden. Standardmäßig aktiviert.	PIF ist vorhanden	XenCenter-pifname Senden (siehe Hinweis)
pif_<pif>_rx_errors	Empfangen Sie Fehler pro Sekunde auf der physischen Schnittstelle pif. Diese Funktion ist standardmäßig deaktiviert.	PIF ist vorhanden	XenCenter-pifname Fehler erhalten (siehe Hinweis)
pif_<pif>_tx_errors	Übertragen Sie Fehler pro Sekunde auf der physischen Schnittstelle pif . Standardmäßig deaktiviert	PIF ist vorhanden	XenCenter-pifname Fehler senden (siehe Hinweis)

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
pif_aggr_rx	Bytes pro Sekunde, die auf allen physikalischen Schnittstellen empfangen werden. Standardmäßig aktiviert.	Ohne	NIC-Empfang insgesamt
pif_aggr_tx	Byte pro Sekunde, die auf allen physikalischen Schnittstellen gesendet werden. Standardmäßig aktiviert.	Ohne	Netzwerkkarte insgesamt gesendet
pvsaccelerator_evicted	Byte pro Sekunde werden aus dem Cache vertrieben	PVSAccelerator Enabled	PVS-Accelerator eviction rate
pvsaccelerator_readshits	Reads per second served from the cache	PVSAccelerator Enabled	PVS-Accelerator hit rate
pvsaccelerator_readsmisses	Lesevorgänge pro Sekunde, die nicht aus dem Cache bedient werden können	PVSAccelerator Enabled	PVS-Accelerator miss rate
pvsaccelerator_trafficoncache_sent	Byte pro Sekunde, gesendet von PVS-Clients im Cache	PVSAccelerator Enabled	PVS-Accelerator beobachtete Netzwerkverkehr von Clients
pvsaccelerator_trafficoncache_sent	Byte pro Sekunde, gesendet von PVS-Servern im Cache	PVSAccelerator Enabled	PVS-Accelerator beobachtete Netzwerkverkehr von Servern
pvsaccelerator_readstotal	Lesevorgänge pro Sekunde vom Cache beobachtet	PVSAccelerator Enabled	PVS-Accelerator observed read rate

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
pvsaccelerator_traffic_bytes_saved	Bytes pro Sekunde, gesendet von PvS-Accelerator anstelle des PVS-Servers	PVSAccelerator Enabled	Der PVS-Accelerator spart Netzwerkverkehr
pvsaccelerator_space_utilization	Prozentsatz des vom PVSAccelerator auf diesem Host belegten Speicherplatzes im Vergleich zur Gesamtgröße des Cachespeichers	PVSAccelerator Enabled	PVS-Accelerator Speicherplatznutzung
running_vcpus	Die Gesamtzahl der laufenden vCPUs	Ohne	Anzahl der laufenden vCPUs
running_domains	Die Gesamtzahl der laufenden Domänen einschließlich dom0 (die Steuerdomäne des Hosts)	Ohne	Anzahl der laufenden Domänen
sr_<sr>_cache_size	Größe des IntelliCache SRs in Byte. Standardmäßig aktiviert.	IntelliCache Enabled	IntelliCache Cache Size
sr_<sr>_cache_hits	Cache-Treffer pro Sekunde. Standardmäßig aktiviert.	IntelliCache Enabled	IntelliCache Cache Hits
sr_<sr>_cache_misses	Cache-Fehlschläge pro Sekunde. Standardmäßig aktiviert.	IntelliCache Enabled	IntelliCache Cache Misses
xapi_allocation_kib	Speicherzuweisung (KiB) erfolgt durch den XAPI-Daemon. Standardmäßig aktiviert.	Ohne	Agent Memory Allocation

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
xapi_free_memory_kib	Freier Speicher (KiB) für den XAPI-Daemon verfügbar. Standardmäßig aktiviert.	Ohne	Agent Memory Free
xapi_healthcheck/latency	Bearbeitungszeit in Sekunden des letzten XAPI-Statusüberwachungsaufrufs auf dem lokalen Host. Diese Funktion ist standardmäßig deaktiviert.	High availability Enabled	XenServer —Latenz bei hoher Verfügbarkeit
xapi_live_memory_kib	Live-Speicher (KiB), der vom XAPI-Daemon verwendet wird. Standardmäßig aktiviert.	Ohne	Agent Memory Live
xapi_memory_usage_kib	Gesamter Speicher (KiB), der vom XAPI-Daemon verwendet wird. Standardmäßig aktiviert.	Ohne	Agent Memory Usage

Verfügbare VM-Messwerte

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
cpu<cpu>	Utilization of vCPU cpu (fraction). Diese Option ist in der Standardeinstellung aktiviert.	vCPU cpu exists	CPU
cpu_usage	CPU-Auslastung der Domäne	Ohne	cpu_usage

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
memory	Derzeit VM zugewiesener Speicher (Byte). Standardmäßig aktiviert	Ohne	Gesamter Arbeitsspeicher
memory_target	Target of VM balloon driver (Bytes). Diese Option ist in der Standardeinstellung aktiviert.	Ohne	Memory target
memory_internal_free	Verwendeter Speicher, wie vom Gastagent gemeldet (KiB). Diese Option ist in der Standardeinstellung aktiviert.	Ohne	Freier Speicher
runstate_fullrun	Bruchteil der Zeit, in der alle vCPUs ausgeführt werden.	Ohne	vCPUs full run
runstate_full_contention	Bruchteil der Zeit, in der alle vCPUs ausgeführt werden können (d. h. auf die CPU warten)	Ohne	vCPUs full contention
runstate_concurrency_hazard	Bruchteil der Zeit, in der einige vCPUs ausgeführt werden und einige ausgeführt werden können	Ohne	vCPUs concurrency hazard
runstate_blocked	Bruchteil der Zeit, in der alle vCPUs blockiert oder offline sind	Ohne	vCPUs idle
runstate_partial_run	Bruchteil der Zeit, in der einige vCPUs ausgeführt werden und einige blockiert sind	Ohne	vCPUs partial run

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
runstate_partial_contention	Bruchteil der Zeit, in der einige vCPUs ausgeführt werden können und einige blockiert sind	Ohne	vCPUs partial contention
vbd_<vbd>_write	Writes to device vbd in bytes per second. Diese Option ist in der Standardeinstellung aktiviert.	VBD vbd exists	Disk vbd Write
vbd_<vbd>_read	Reads from device vbd in bytes per second. Standardmäßig aktiviert.	VBD vbd exists	Disk vbd Read
vbd_<vbd>_write_latency	Writes to device vbd in microseconds.	VBD vbd exists	Disk vbd Write Latency
vbd_<vbd>_read_latency	Reads from device vbd in microseconds.	VBD vbd exists	Disk vbd Read Latency
vbd <vbd>_iops_read	Requests pro Sekunde lesen.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd Read IOPs
vbd <vbd>_iops_write	Schreibanfragen pro Sekunde.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd Write IOPS
vbd <vbd>_iops_total	I/O-Anforderungen pro Sekunde.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd Total IOPS
vbd <vbd>_iowait	Prozentsatz der Wartezeit auf I/0.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd IO Wait
vbd <vbd>_inflight	Anzahl der aktuell laufenden I/O-Anforderungen.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd Inflight Requests

Name der Metrik	Beschreibung	Bedingung	XenCenter-Name
vbd <vbd> _avgqu_sz	Durchschnittliche I/O-Warteschlangengröße.	Mindestens eine angeschlossene VBD für Nicht-ISO-VDI auf dem Host	Disk vbd Queue Size
vif_<vif>_rx	Bytes pro Sekunde empfangen auf virtueller Schnittstellennummer vif. Standardmäßig aktiviert.	VIF vif exists	vif Receive
vif_<vif>_tx	Byte pro Sekunde werden auf der virtuellen Schnittstelle übertragen vif. Standardmäßig aktiviert.	VIF vif exists	vif Send
vif_<vif> _rx_errors	Empfangen Sie Fehler pro Sekunde auf der virtuellen Schnittstelle vif. Standardmäßig aktiviert.	VIF vif exists	vif Receive Errors
vif_<vif> _tx_errors	Fehler pro Sekunde auf der virtuellen Schnittstelle vif übertragen Standardmäßig aktiviert.	VIF vif exists	vif Send Errors

> **Hinweis:**
>
> Der Wert von <XenCenter-pif-name> kann einer der folgenden Werte sein:
>
> - NIC <pif> - if <pif> contains pif_eth#, where ## is 0–9
> - <pif> - if <pif> contains pif_eth#.## or pif_xenbr## or pif_bond##
> - <Internal> Network <pif> - if <pif> contains pif_xapi##, (note that <Internal> appears as is)
> - TAP <tap> - if <pif> contains pif_tap##
> - xapi Loopback - if <pif> contains pif_lo

Analysieren und Visualisieren von Metriken

Die Registerkarte Leistung in XenCenter bietet eine Echtzeitüberwachung von Leistungsstatistiken über Ressourcenpools hinweg sowie grafische Trends der Leistung virtueller und physischer Maschinen. Diagramme, die CPU, Speicher, Netzwerk und Datenträger-E/A zeigen, sind standardmäßig auf der Registerkarte Leistung enthalten. Sie können weitere Metriken hinzufügen, das Erscheinungsbild der vorhandenen Diagramme ändern oder zusätzliche erstellen. Weitere Informationen finden Sie im folgenden Abschnitt unter *Konfigurieren von Metriken*.

- Sie können Leistungsdaten von bis zu 12 Monaten anzeigen und vergrößern, um die Leistungsspitzen genauer zu betrachten.
- XenCenter kann Leistungswarnungen generieren, wenn die CPU-, Speicher-, Netzwerk-I/O-, Speicher-I/O- oder Datenträger-I/O-Auslastung einen bestimmten Schwellenwert auf einem Host, einer VM oder einer SR überschreitet. Weitere Informationen finden Sie im folgenden Abschnitt unter *Alerts*.

> **Hinweis:**
>
> Installieren Sie die XenServer VM Tools, um die vollständigen VM-Leistungsdaten zu sehen.

Konfigurieren von Leistungsdiagrammen So fügen Sie eine Grafik hinzu:

1. Klicken Sie auf der Registerkarte **Leistung** auf **Aktionen** und dann auf **Neues Diagramm**. Das Dialogfeld “Neues Diagramm “wird angezeigt.
2. Geben Sie im Feld **Name** einen Namen für das Diagramm ein.
3. Wählen Sie aus der Liste der **Datenquellen** die Kontrollkästchen für die Datenquellen aus, die Sie in das Diagramm aufnehmen möchten.
4. Klicken Sie auf **Speichern**.

So bearbeiten Sie ein vorhandenes Diagramm:

1. Navigieren Sie zur Registerkarte **Leistung** und wählen Sie das Diagramm aus, das Sie ändern möchten.
2. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Aktionen** oder klicken Sie auf die Schaltfläche **Aktionen**. Wählen Sie dann **Diagramm bearbeiten** aus.
3. Nehmen Sie im Fenster “Diagrammdetails”die erforderlichen Änderungen vor, und klicken Sie auf **OK**.

Konfigurieren des Diagrammtyps Daten in den Leistungsdiagrammen können als Linien oder als Bereiche angezeigt werden. So ändern Sie den Diagrammtyp:

1. Klicken Sie im Menü **Extras** auf **Optionen**, und wählen Sie **Diagramme**aus.
2. Um Leistungsdaten als Liniendiagramm anzuzeigen, klicken Sie auf die Option **Liniendiagramm** .
3. Um Leistungsdaten als Flächendiagramm anzuzeigen, klicken Sie auf die Option **Flächendiagramm** .
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Umfassende Details zum Konfigurieren und Anzeigen von XenCenter-Leistungsdiagrammen finden Sie in der XenCenter-Dokumentation im Abschnitt Überwachung der Systemleistung.

Metriken konfigurieren

> **Hinweis:**
>
> C-States und P-States sind Energieverwaltungsfunktionen einiger Prozessoren. Der Bereich der verfügbaren Zustände hängt von den physikalischen Fähigkeiten des Hosts sowie der Energieverwaltungskonfiguration ab.

Sowohl Host- als auch VM-Befehle geben Folgendes zurück:

- Eine vollständige Beschreibung der Datenquelle
- Die auf die Metrik angewendeten Einheiten
- Der Bereich der möglichen Werte, die verwendet werden können

Beispiel:

```
    name_label: cpu0-C1
    name_description: Proportion of time CPU 0 spent in C-state 1
    enabled: true
    standard: true
    min: 0.000
    max: 1.000
    units: Percent
<!--NeedCopy-->
```

Eine bestimmte Metrik aktivieren Die meisten Metriken sind standardmäßig aktiviert und erfasst. Um die Metriken zu aktivieren, die dies nicht sind, geben Sie Folgendes ein:

```
xe host-data-source-record data-source=metric name host=hostname
<!--NeedCopy-->
```


Deaktiviert eine bestimmte Metrik Möglicherweise möchten Sie bestimmte Metriken nicht regelmäßig sammeln. Um eine zuvor aktivierte Metrik zu deaktivieren, geben Sie Folgendes ein:

```
xe host-data-source-forget data-source=metric name host=hostname
<!--NeedCopy-->
```

Zeigt eine Liste der aktuell aktivierten Host-Metriken Um die aktuell erfassten Host-Metriken aufzulisten, geben Sie Folgendes ein:

```
xe host-data-source-list host=hostname
<!--NeedCopy-->
```

Zeigt eine Liste der aktuell aktivierten VM-Metriken Um die aktuell erfassten VM-Metriken zu hosten, geben Sie Folgendes ein:

```
xe vm-data-source-list vm=vm_name
<!--NeedCopy-->
```

Verwenden Sie RRDs

XenServer verwendet RRDs zum Speichern von Leistungsmetriken. Diese RRDs bestehen aus mehreren Round Robin Archives (RRAs) in einer Datenbank fester Größe.

Jedes Archiv in der Datenbank tastet seine bestimmte Metrik mit einer bestimmten Granularität ab:

- Alle 5 Sekunden für 10 Minuten
- Jede Minute der letzten zwei Stunden
- Jede Stunde der letzten Woche
- Jeden Tag des letzten Jahres

Die Stichprobe, die alle fünf Sekunden stattfindet, zeichnet tatsächliche Datenpunkte auf, die folgenden RRAs verwenden jedoch stattdessen Konsolidierungsfunktionen. Die von XenServer unterstützten Konsolidierungsfunktionen sind:

- AVERAGE
- MIN.
- MAX.

RRDs existieren für einzelne VMs (einschließlich dom0) und den XenServer-Host. VM-RRDs werden auf dem Host gespeichert, auf dem sie ausgeführt werden, oder auf dem Poolkoordinator, wenn sie nicht ausgeführt werden. Daher muss der Standort einer VM bekannt sein, um die zugehörigen Leistungsdaten abzurufen.

Ausführliche Informationen zur Verwendung von XenServer RRDs finden Sie im XenServer Software DevelopmentKit Guide.

Analysieren Sie RRDs mit HTTP

Sie können RRDs über HTTP von dem angegebenen XenServer-Host herunterladen, indem Sie den HTTP-Handler verwenden, der unter oder registriert ist. `/host_rrd`/`vm_rrd` Beide Adressen erfordern eine Authentifizierung entweder durch HTTP-Authentifizierung oder durch Angabe einer gültigen Verwaltungs-API-Sitzungsreferenz als Abfrageargument. Beispiel:

Laden Sie eine Host-RRD herunter.

```
wget http://server/host_rrd?session_id=OpaqueRef:SESSION HANDLE>
<!--NeedCopy-->
```

Laden Sie eine VM-RRD herunter.

```
wget http://server/vm_rrd?session_id=OpaqueRef:SESSION HANDLE>&uuid=VM
   UUID>
<!--NeedCopy-->
```

Beide Aufrufe laden XML in einem Format herunter, das zur Analyse in das `rrdtool` importiert oder direkt analysiert werden kann.

Analysieren Sie RRDs mit rrd2csv

Neben der Anzeige von Leistungsmetriken in XenCenter protokolliert das rrd2csv-Tool RRDs im Comma Separated Value (CSV) -Format. Man- und Hilfeseiten werden bereitgestellt. Führen Sie den folgenden Befehl aus, um die Benutzer- oder Hilfeseiten des rrd2csv-Werkzeugs anzuzeigen:

```
man rrd2csv
<!--NeedCopy-->
```

Oder

```
rrd2csv --help
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn mehrere Optionen verwendet werden, geben Sie diese einzeln an. Beispiel: Um sowohl die UUID als auch die Namensbezeichnung zurückzugeben, die mit einer VM oder einem Host verknüpft sind, rufen Sie rrd2csv auf, wie unten gezeigt:
>
> `rrd2csv -u -n`

> Die zurückgegebene UUID ist eindeutig und als Primärschlüssel geeignet, allerdings muss das Namenslabel einer Entität nicht unbedingt eindeutig sein.

Die Manpage (`rrd2csv --help`) ist der endgültige Hilfetext des Tools.

Warnungen

Sie können XenServer so konfigurieren, dass Warnungen auf der Grundlage der verfügbaren Host- oder VM-Metriken generiert werden. Darüber hinaus bietet XenServer vorkonfigurierte Warnungen, die ausgelöst werden, wenn Hosts bestimmten Bedingungen und Zuständen ausgesetzt sind. Sie können diese Warnungen mit XenCenter oder der xe CLI anzeigen.

Warnungen mit XenCenter anzeigen

Sie können verschiedene Arten von Warnungen in XenCenter anzeigen, indem Sie auf **Benachrichtigungen** und dann auf **Warnungen**klicken. In der Ansicht "Warnungen"werden verschiedene Arten von Warnungen angezeigt, darunter Leistungswarnungen, Systemwarnungen und Softwareupdate-Warnungen.

Performance-Warnungen

Leistungswarnungen können generiert werden, wenn einer der folgenden Werte einen bestimmten Schwellenwert auf einem verwalteten Host, einer VM oder einem Speicherrepository (SR) überschreitet: CPU-Auslastung, Netzwerkauslastung, Speicherauslastung, Steuerung der Domänenspeicherauslastung, Speicherdurchsatz oder VM-Datenträgerauslastung.

Standardmäßig ist das Wiederholungsintervall für Warnungen auf 60 Minuten festgelegt und kann bei Bedarf geändert werden. Warnungen werden auf der Seite "Warnungen"im Bereich "Benachrichtigungen"in XenCenter angezeigt. Sie können XenCenter auch so konfigurieren, dass eine E-Mail für angegebene Leistungswarnungen zusammen mit anderen schwerwiegenden Systemwarnungen gesendet wird.

Alle benutzerdefinierten Warnungen, die mit der xe CLI konfiguriert wurden, werden auch auf der Seite "Warnungen"in XenCenter angezeigt.

Jeder Alert hat eine entsprechende Priorität/Schweregrad. Sie können diese Stufen ändern und optional eine E-Mail erhalten, wenn die Warnung ausgelöst wird. Die standardmäßige Priorität/der Schweregrad der Warnung ist auf festgelegt 3.

Priorität	Name	Beschreibung	Standard-E-Mail-Warnung
1	Kritisch	Handeln Sie jetzt oder Daten sind möglicherweise dauerhaft verloren/beschädigt.	Ja
2	Hauptfach	Handeln Sie jetzt oder einige Dienste können fehlschlagen.	Ja
3	Warnung	Handeln Sie jetzt oder ein Dienst kann darunter leiden.	Ja
4	Minor	Beachten Sie, dass etwas gerade verbessert wurde.	Nein
5	Informationen	Tägliche Informationen (VM Start, Stopp, Fortsetzen usw.)	Nein
?	Unbekannt	Unbekannter Fehler	Nein

Konfigurieren von Leistungswarnungen

1. Wählen Sie im Bereich **Ressourcen** den entsprechenden Host, die VM oder das SR aus, und klicken Sie dann auf die Registerkarte **Allgemein** und dann auf **Eigenschaften**.
2. Wählen Sie die Registerkarte **Warnungen** aus. Die folgende Tabelle fasst zusammen, welche Warnungen für Hosts, VMs oder SRs verfügbar sind:

Name der Warnung	Host	VM	SR	Beschreibung
Warnungen zur CPU-Auslastung generieren	X	X		Legen Sie die CPU-Auslastung und den Zeitschwellen-wert fest, die die Warnung auslösen.

Name der Warnung	Host	VM	SR	Beschreibung
Warnungen zur CPU-Auslastung der Steuerdomäne generieren	X			Legen Sie die CPU-Auslastung und den Zeitschwellen-wert der Steuerdomäne fest, die die Warnung auslösen.
Warnungen zur Speichernutzung generieren	X			Legen Sie den Speicherver-brauch und den Zeitschwellen-wert fest, der die Warnung auslöst.
Warnungen zur Speichernutzung der Steuerdomäne generieren	X			Stellen Sie die Speichernutzung der Steuerdomäne und den Zeitschwellen-wert ein, der die Warnung auslöst.
Warnmeldungen über freien Speicher in der Steuerdomäne gemerierem	X			Legen Sie den freien Speicher der Steuerdomäne und den Zeitschwellen-wert fest, der die Warnung auslöst.

Name der Warnung	Host	VM	SR	Beschreibung
Warnmeldungen zur Datenträger-nutzung generieren		X		Festlegen der Da-tenträgernutzung und des Zeitschwellen-werts die Warnung auslösen.

Name der Warnung	Host	VM	SR	Beschreibung
Speicherdurchsatzwarnungen generieren			X	Legen Sie den Speicherdurchsatz und den Zeitschwellenwert fest, die die Warnung auslösen. Hinweis: Physical Block Devices (PBD) stellen die Schnittstelle zwischen einem bestimmten XenServer-Host und einem angeschlossenen SR dar. Wenn die gesamte SR-Durchsatzaktivität mit Lese-/Schreibzugriff auf einem PBD den angegebenen Schwellenwert überschreitet, werden Warnungen auf dem mit dem PBD verbundenen Host generiert. Im Gegensatz zu anderen XenServer-Host-Warnungen muss diese Warnung auf der SR konfiguriert werden.

Name der Warnung	Host	VM	SR	Beschreibung
Warnmeldungen zur Netzwerknutzung generieren	X	X		Legen Sie die Netzwerknutzung und den Zeitschwellen-wert fest, der die Warnung auslöst.

Um das Warnwiederholungsintervall zu ändern, geben Sie die Anzahl der Minuten in das Feld **Warnwiederholungsintervall** ein. Wenn ein Alarmschwellenwert erreicht und eine Warnung generiert wurde, wird erst nach Ablauf des Alert-Wiederholungsintervalls eine weitere Warnung generiert.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Umfassende Informationen zum Anzeigen, Filtern und Konfigurieren von Schweregraden von Leistungswarnungen finden Sie unter Konfigurieren von Leistungswarnungen in der XenCenter-Dokumentation.

Systemwarnungen

In der folgenden Tabelle werden die Systemereignisse/-bedingungen angezeigt, die eine Warnung auslösen, die auf der Seite “Warnungen”in XenCenter angezeigt wird.

Name	Priorität/Schweregrad	Beschreibung
license_expires_soon	2	Die XenServer-Lizenzvereinbarung läuft bald ab.
ha-statefile_lost	2	Haben Sie den Kontakt zum hochverfügbaren Speicherrepository verloren, handeln Sie bald.
ha-heartbeat_approaching_timeout	5	Hochverfügbarkeit nähert sich dem Timeout, Host wird möglicherweise neu gestartet, sofern keine Maßnahmen ergriffen werden

Name	Priorität/Schweregrad	Beschreibung
ha_statefile_approaching_timeout	5	Hochverfügbarkeit nähert sich dem Timeout, Host wird möglicherweise neu gestartet, sofern keine Maßnahmen ergriffen werden
haxapi_healthcheck_approaching_timeout	5	Hochverfügbarkeit nähert sich dem Timeout, Host wird möglicherweise neu gestartet, sofern keine Maßnahmen ergriffen werden
ha_network_bonding_error	3	Möglicher Verlust des Dienstes. Netzwerkverlust, der einen Heartbeat mit hoher Verfügbarkeit sendet.
ha_pool_overcommited	3	Möglicher Verlust des Dienstes. Hochverfügbarkeit kann keinen Schutz für konfigurierte VMs garantieren.
ha_poor_drop_in_plan_exists_for	3	Die Abdeckung mit hoher Verfügbarkeit ist gesunken, es ist wahrscheinlicher, dass sie scheitert, es ist noch kein Verlust
ha_protected_vm_restart_failed	2	Verlust des Dienstes. Hochverfügbarkeit konnte eine geschützte VM nicht neu starten.
ha_host_failed	3	Hochverfügbarkeit hat festgestellt, dass ein Host ausgefallen ist
ha_host_was_fenced	4	Bei hoher Verfügbarkeit wurde ein Host zum Schutz vor VM-Beschädigung neu gestartet.
redo_log_healthy	4	Das XAPI-Redo-Protokoll wurde von einem früheren Fehler wiederhergestellt.

Name	Priorität/Schweregrad	Beschreibung
redo_log_broken	3	Im XAPI-Redo-Logbuch ist ein Fehler aufgetreten.
ip_configured_pif_can_unplug	3	Eine IP-konfigurierte NIC kann bei Verwendung von Hochverfügbarkeit von XAPI getrennt werden, was möglicherweise zu einem Ausfall der Hochverfügbarkeit führen kann.
host_sync_data_failed	3	Die XenServer-Leistungsstatistiken konnten nicht synchronisiert werden.
host_clock_skew_detected	3	Die Host-Uhr ist nicht mit anderen Hosts im Pool synchronisiert.
host_clock_went_backwards	1	Die Host-Uhr ist beschädigt.
pool_master_transition	4	Ein neuer Host wurde als Poolkoordinator angegeben.
pbd_plug_failed_on_server_start	3	Der Host konnte beim Booten keine Verbindung zum Speicher herstellen.
auth_external_init_failed	2	Der Host konnte die externe AD-Authentifizierung nicht aktivieren.
auth_external_pool_non-homogeneous	2	Hosts in einem Pool haben eine andere Konfiguration für die AD-Authentifizierung.
multipath_period_alert	3	Ein Pfad zu einem SR ist ausgefallen oder hat sich erholt.
bond-status-changed	3	Eine Verbindung in einem Bond wurde getrennt oder wieder verbunden.

Warnungen zu Softwareupgrades

- **XenCenter alt:** XenServer erwartet eine neuere Version, kann aber trotzdem eine Verbindung zur aktuellen Version herstellen
- **XenCenter veraltet:** XenCenter ist zu alt, um eine Verbindung zu XenServer herzustellen
- **XenServer veraltet:** XenServer ist eine alte Version, zu der das aktuelle XenCenter keine Verbindung herstellen kann
- **Warnung "Lizenz abgelaufen":** Die XenServer-Lizenz ist abgelaufen
- **Fehlende IQN-Warnung:** XenServer verwendet iSCSI-Speicher, aber der Host-IQN ist leer
- **Warnung wegen doppelter IQN:** XenServer verwendet iSCSI-Speicher und es gibt doppelte Host-IQNs

Konfigurieren Sie Leistungswarnungen über die xe-CLI

> **Hinweis:**
>
> Auslöser für Alerts werden in einem Mindestintervall von fünf Minuten geprüft. Dieses Intervall vermeidet eine übermäßige Belastung des Systems, um nach diesen Bedingungen zu suchen und Fehlalarme zu melden. Wenn Sie ein Alert-Wiederholungsintervall von weniger als fünf Minuten festlegen, werden die Warnungen weiterhin im Mindestintervall von fünf Minuten generiert.

Das `perfmon` Tool zur Leistungsüberwachung wird alle fünf Minuten ausgeführt und fordert Updates von XenServer an, die durchschnittlich über eine Minute liegen. Diese Standardwerte können in `/etc/sysconfig/perfmon` geändert werden.

`perfmon` liest alle fünf Minuten Updates von Leistungsvariablen, die auf demselben Host ausgeführt werden. Diese Variablen sind in eine Gruppe unterteilt, die sich auf den Host selbst bezieht, und eine Gruppe für jede VM, die auf diesem Host ausgeführt wird. Für jede VM und jeden Host liest `perfmon` den Parameter `other-config:perfmon` und verwendet diese Zeichenfolge, um zu bestimmen, welche Variablen überwacht werden sollen und unter welchen Umständen eine Nachricht generiert werden soll.

Im folgenden Beispiel wird ein Beispiel für die Konfiguration einer VM-Warnung "CPU-Auslastung" gezeigt, indem eine XML-Zeichenfolge in den Parameter `other-config:perfmon` geschrieben wird:

```
xe vm-param-set uuid=vm_uuid other-config:perfmon=\

'<config>
    <variable>
        <name value="cpu_usage"/>
        <alarm_trigger_level value="0.5"/>
    </variable>
</config>'
<!--NeedCopy-->
```


> **Hinweis:**
>
> Sie können mehrere variable Knoten verwenden.

Nachdem Sie die neue Konfiguration festgelegt haben, verwenden Sie den folgenden Befehl, um `perfmon` für jeden Host zu aktualisieren:

```
xe host-call-plugin host=host_uuid plugin=perfmon fn=refresh
<!--NeedCopy-->
```

Wenn diese Aktualisierung nicht durchgeführt wird, gibt es eine Verzögerung, bis die neue Konfiguration wirksam wird, da standardmäßig `perfmon` alle 30 Minuten nach einer neuen Konfiguration sucht. Diese Standardeinstellung kann in `/etc/sysconfig/perfmon` geändert werden.

Gültige VM-Elemente

- `name`: Der Name der Variablen (kein Standard). Wenn der Namenswert entweder `cpu_usage`, `network_usage` oder `disk_usage` ist, sind die Parameter `alarm_trigger_sense` und `rrd_regex` nicht erforderlich, da Standardwerte für diese Werte verwendet werden.
- `alarm_priority`: Die Priorität der generierten Alerts (Standard 3).
- `alarm_trigger_level`: Die Wertebene, die eine Warnung auslöst (kein Standardwert).
- `alarm_trigger_sense`: Der Wert ist `high` wenn `alarm_trigger_level` ein Maximalwert ist, andernfalls `low`, wenn `alarm_trigger_level` ein Minimalwert ist (der Standardwert `high`).
- `alarm_trigger_period`: Die Anzahl der Sekunden, die Werte (über oder unter dem Alarmschwellenwert) empfangen werden können, bevor eine Warnung gesendet wird (der Standardwert ist `60`).
- `alarm_auto_inhibit_period`: Die Anzahl der Sekunden, in denen diese Warnung deaktiviert wird, nachdem eine Warnung gesendet wurde (der Standardwert ist `3600`).
- `consolidation_fn`: Kombiniert Variablen aus rrd_updates zu einem Wert. Die Standardeinstellung für `cpu-usage` ist `average`, für `fs_usage` ist die Standardeinstellung `get_percent_fs_usage` und für alle anderen - `sum`.
- `rrd_regex`: Entspricht den Namen der Variablen von `xe vm-data-sources-list uuid=vm_uuid`, um Leistungswerte zu berechnen. Dieser Parameter hat Standardwerte für die benannten Variablen:
  - cpu_usage
  - memory_internal_free
  - network_usage
  - disk_verwendung

Falls angegeben, werden die Werte aller zurückgegebenen Elemente `xe vm-data-source-list`, deren Namen mit dem angegebenen regulären Ausdruck übereinstimmen, mit der als angegebenen Methode konsolidiert `consolidation_fn`.

Gültige Host-Elemente

- `name`: Der Name der Variablen (kein Standard).
- `alarm_priority`: Die Priorität der generierten Alerts (Standard 3).
- `alarm_trigger_level`: Die Wertebene, die eine Warnung auslöst (kein Standardwert).
- `alarm_trigger_sense`: Der Wert ist `high`, wenn `alarm_trigger_level` ein Maximalwert ist, andernfalls `low`, wenn der ein Minimalwert `alarm_trigger_level` ist. (Standard `high`)
- `alarm_trigger_period`: Die Anzahl der Sekunden, die Werte (über oder unter dem Alarmschwellenwert) empfangen werden können, bevor eine Warnung gesendet wird (Standard `60`).
- `alarm_auto_inhibit_period`: Die Anzahl der Sekunden, für die die Warnung nach dem Senden einer Warnung deaktiviert ist. (Standard `3600`).
- `consolidation_fn`: Kombiniert Variablen aus `rrd_updates` in einem Wert (Standard `sum` - oder `average`)
- `rrd_regex`: Ein regulärer Ausdruck, der den Namen der Variablen entspricht, die vom Befehl `xe vm-data-source-list uuid=vm_uuid` zurückgegeben werden, zur Berechnung des statistischen Werts. Dieser Parameter hat Standardwerte für die folgenden benannten Variablen:
  - cpu_usage
  - network_usage
  - memory_free_kib
  - sr_io_throughput_total_xxxxxxxx (wo `xxxxxxxx` die ersten acht Zeichen der SR-UUID sind).

SR-Durchsatz: Warnungen zum Speicherdurchsatz müssen in dem SR und nicht auf dem Host konfiguriert werden. Beispiel:

```
xe sr-param-set uuid=sr_uuid other-config:perfmon=\
'<config>
    <variable>
        <name value="sr_io_throughput_total_per_host"/>
        <alarm_trigger_level value="0.01"/>
    </variable>
</config>'
<!--NeedCopy-->
```

Generische Beispielkonfiguration Das folgende Beispiel zeigt eine generische Konfiguration:


```
<config>
    <variable>
    <name value="NAME_CHOSEN_BY_USER"/>
    <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALERT"/>
    <alarm_trigger_period value="
       RAISE_ALERT_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
    <alarm_priority value="PRIORITY_LEVEL"/>
    <alarm_trigger_sense value="HIGH_OR_LOW"/>
    <alarm_auto_inhibit_period value="
       MINIMUM_TIME_BETWEEN_ALERT_FROM_THIS_MONITOR"/>
    <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
    <rrd_regex value="REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
    </variable>

    <variable>
    ...
    </variable>

    ...
</config>
<!--NeedCopy-->
```

Konfigurieren von E-Mail-Benachrichtigungen

Sie können XenServer so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, wenn XenServer-Hosts Warnungen generieren. Das Mail-Alarm-Hilfsprogramm in XenServer verwendet SSMTP, um diese E-Mail-Benachrichtigungen zu senden. Sie können grundlegende E-Mail-Benachrichtigungen mithilfe von XenCenter oder der XE-Befehlszeilenschnittstelle (CLI) aktivieren. Für die weitere Konfiguration von E-Mail-Benachrichtigungen können Sie die Konfigurationsdatei `mail-alarm.conf` ändern.

Verwenden Sie einen SMTP-Server, der keine Authentifizierung erfordert. E-Mails, die über SMTP-Server gesendet werden und für die eine Authentifizierung erforderlich ist, können nicht zugestellt werden.

Aktivieren von E-Mail-Warnungen über XenCenter

1. Klicken Sie im Bereich `Resources` mit der rechten Maustaste auf einen Pool und wählen Sie `Properties` aus.
2. Wählen Sie `Email Options` im Fenster `Properties`.
3. Markieren Sie das Kontrollkästchen `Send email alert notifications`. Geben Sie Ihre bevorzugte Zieladresse für die Benachrichtigungs-E-Mails und die SMTP-Serverdetails ein.

4. Wählen Sie Ihre bevorzugte Sprache aus der Liste `Mail language` aus. Die Standardsprache für E-Mails mit Leistungswarnungen ist Englisch.

Aktivieren Sie E-Mail-Benachrichtigungen mit der xe-CLI

Um E-Mail-Benachrichtigungen zu konfigurieren, geben Sie Ihre bevorzugte Zieladresse für die Benachrichtigungs-E-Mails und den SMTP-Server an:

```
xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.
   bloggs@example.com
xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
   example.com:<port>
<!--NeedCopy-->
```

XenServer konfiguriert die Absenderadresse automatisch als. `noreply@<hostname>` Sie können die Absenderadresse jedoch explizit festlegen:

```
xe pool-param-set uuid=pool_uuid other-config:mail-sender=
   serveralerts@example.com
<!--NeedCopy-->
```

Wenn Sie E-Mail-Benachrichtigungen aktivieren, erhalten Sie eine E-Mail-Benachrichtigung, wenn eine Warnung mit einer Priorität von 3 oder höher generiert wird. Daher lautet die standardmäßige Mindestprioritätsstufe 3. Sie können diese Standardeinstellung mit dem folgenden Befehl ändern:

```
xe pool-param-set uuid=pool_uuid other-config:mail-min-priority=level
<!--NeedCopy-->
```

> **Hinweis:**
>
> Manche SMTP-Server leiten nur E-Mails mit Adressen weiter, die FQDNs verwenden. Wenn Sie feststellen, dass E-Mails nicht weitergeleitet werden, kann dies aus diesem Grund geschehen. In diesem Fall können Sie den Serverhostnamen auf den FQDN festlegen, sodass diese Adresse verwendet wird, wenn Sie eine Verbindung zu Ihrem Mailserver herstellen.

Um die Sprache für die E-Mails mit Leistungswarnungen zu konfigurieren, gehen Sie wie folgt vor:

```
xe pool-param-set uuid=pool_uuid other-config:mail-language=ja-JP
<!--NeedCopy-->
```

Die Standardsprache für E-Mails mit Leistungswarnungen ist Englisch.

Weitere Konfiguration

Um das Mail-Alarm-Hilfsprogramm in XenServer weiter zu konfigurieren, erstellen Sie eine `/etc/mail-alarm.conf` Datei, die Folgendes enthält:


```
root=postmaster
authUser=<username>
authPass=<password>
mailhub=@MAILHUB@
<!--NeedCopy-->
```

/etc/mail-alarm.conf ist eine vom Benutzer bereitgestellte Vorlage für die SSMTP-Konfigurationsdatei ssmtp.conf und wird für alle von XenServer-Hosts generierten Warnungen verwendet. Sie besteht aus Schlüsseln, wobei key=@KEY@ und @KEY@ durch den entsprechenden Wert von ssmtp-key in pool.other_config ersetzt wird. Diese Werte werden dann an ssmtp übergeben, sodass Sie Aspekte der sSMTP-Konfiguration mithilfe von Werten von steuern können pool.other_config. Beachten Sie, wie @KEY@ (Großbuchstaben) sich zu ssmtp-key (Kleinbuchstaben, mit Präfix ssmtp-) verhält.

Wenn Sie beispielsweise den SMTP-Server wie folgt einrichten:

```
xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
   example.com
<!--NeedCopy-->
```

und Sie dann Folgendes zur Datei /etc/mail-alarm.conf hinzufügen:

```
mailhub=@MAILHUB@
<!--NeedCopy-->
```

wird mailhub=@MAILHUB@ zu mailhub=smtp.example.com.

Jeder SMTP-Server kann sich in seiner Einrichtung geringfügig unterscheiden und erfordert möglicherweise eine zusätzliche Konfiguration. Um sSMTP weiter zu konfigurieren, ändern Sie die Konfigurationsdatei ssmtp.conf. Indem Sie die entsprechenden Schlüssel in der Datei mail-alarm.conf speichern, können Sie die Werte in pool.other_config verwenden, um sSMTP zu konfigurieren. Der folgende Auszug aus der ssmtp.conf-Manpage zeigt die korrekte Syntax und die verfügbaren Optionen:

```
NAME
    ssmtp.conf - ssmtp configuration file

DESCRIPTION
    ssmtp reads configuration data from /etc/ssmtp/ssmtp.conf The file
       con-
    tains keyword-argument pairs, one per line. Lines starting with '#'
    and empty lines are interpreted as comments.

The possible keywords and their meanings are as follows (both are case-
insensitive):

    Root
    The user that gets all mail for userids less than 1000. If blank,
    address rewriting is disabled.
```



```
15
16      Mailhub
17          The host to send mail to, in the form host | IP_addr port :
18          <port>. The default port is 25.
19
20      RewriteDomain
21      The domain from which mail seems to come. For user authentication.
22
23      Hostname
24          The full qualified name of the host. If not specified, the host
25          is queried for its hostname.
26
27      FromLineOverride
28          Specifies whether the From header of an email, if any, may over
                -
29          ride the default domain. The default is "no".
30
31      UseTLS
32      Specifies whether ssmtp uses TLS to talk to the SMTP server.
33      The default is "no".
34
35      UseSTARTTLS
36          Specifies whether ssmtp does a EHLO/STARTTLS before starting
                TLS
37          negotiation. See RFC 2487.
38
39      TLSCert
40          The file name of an RSA certificate to use for TLS, if required
                .
41
42      AuthUser
43          The user name to use for SMTP AUTH. The default is blank, in
44          which case SMTP AUTH is not used.
45
46      AuthPass
47          The password to use for SMTP AUTH.
48
49      AuthMethod
50          The authorization method to use. If unset, plain text is used.
51          May also be set to "cram-md5".
52  <!--NeedCopy-->
```

Benutzerdefinierte Felder und Tags

XenCenter unterstützt das Erstellen von ags und benutzerdefinierten Feldern, die eine Organisation und schnelle Suche von VMs, Speicher usw. ermöglichen. Weitere Informationen finden Sie unter Überwachen der Systemleistung.

Benutzerdefinierte Suchen

XenCenter unterstützt die Erstellung von benutzerdefinierten Suchvorgängen. Suchen können exportiert und importiert werden, und die Ergebnisse einer Suche können im Navigationsbereich angezeigt werden. Weitere Informationen finden Sie unter Überwachen der Systemleistung.

Bestimmen des Durchsatzes von physikalischen Busadaptern

Für FC-, SAS- und iSCSI-HBAs können Sie den Netzwerkdurchsatz Ihrer PBDs mithilfe des folgenden Verfahrens ermitteln.

1. Listen Sie die PBDs auf einem Host auf.
2. Bestimmen Sie, welche LUNs über welche PBDs geroutet werden.
3. Listen Sie für jedes PBD und SR die VBDs auf, die auf VDIs in dem SR verweisen.
4. Berechnen Sie für alle aktiven VBDs, die an VMs auf dem Host angeschlossen sind, den kombinierten Durchsatz.

Überprüfen Sie für iSCSI- und NFS-Speicher Ihre Netzwerkstatistiken, um festzustellen, ob am Array ein Durchsatzengpass vorliegt oder ob die PBD überlastet ist.

Überwachen Sie Host- und Dom0-Ressourcen mit NRPE

> **Hinweis:**
>
> Die NRPE-Funktion ist für XenServer Premium- oder Trial Edition-Kunden verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.

Benutzer mit der Rolle Pool Admin können jedes Überwachungstool eines Drittanbieters verwenden, das den Nagios Remote Plugin Executor (NRPE) unterstützt, um die von Ihrem XenServer-Host und dom0 —der Steuerdomäne Ihres Hosts —verbrauchten Ressourcen zu überwachen.

Sie können die folgenden Check-Plugins verwenden, um Host- und dom0-Ressourcen zu überwachen:

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Host-CPU-Last	check_host_load	Ruft die aktuelle Last pro physischer CPU des Hosts ab und überprüft sie, wobei sich Last auf die Anzahl der vCPUs in einem laufenden oder ausführbaren Zustand bezieht.	3	4	Aktuelle Systemlast der CPU des Hosts (berechnet anhand der durchschnittlichen Auslastung der physischen CPU des Hosts).
CPU-Auslastung des Hosts (%)	check_host_cpu	Ruft die aktuelle durchschnittliche CPU-Gesamtauslastung des Hosts ab und überprüft sie.	80%	90%	Der Prozentsatz der Host-CPU, die derzeit frei ist, und der Prozentsatz, der verwendet wird.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Speicherauslastung des Hosts (%)	Hostspeicher überprüfen	Ruft die aktuelle Speichernutzung des Hosts ab und überprüft sie.	80%	90%	Der Prozentsatz des Hostspeichers, der derzeit frei ist, und der Prozentsatz, der verwendet wird.
Host-vGPU-Nutzung (%)	check_vgpu	Ruft die gesamte aktuell laufende Nvidia vGPU-Nutzung des Hosts ab und überprüft sie.	80%	90%	Der Prozentsatz der laufenden vGPU, die derzeit kostenlos ist, und der Prozentsatz, der verwendet wird.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Host-vGPU-Speicherauslastung (%)	check_vgpu_memory	Ruft die gesamte aktuell ausgeführte Nvidia vGPU-Speichernutzung (einschließlich des gemeinsam genutzten Speichers und des Grafikspeichers) des Hosts ab und überprüft sie.	80%	90%	Der Prozentsatz des laufenden vGPU-Speichers (einschließlich des gemeinsam genutzten Speichers und des Grafikspeichers), der derzeit frei ist, und der Prozentsatz, der verwendet wird.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Dom0 CPU-Last	check_load	Ruft den aktuellen Durchschnitt der Systemlast pro CPU von dom0 ab und überprüft ihn, wobei sich Last auf die Anzahl der Prozesse bezieht, die sich in einem laufenden oder ausführbaren Zustand befinden.	2.7,2.6,2.5	3.2,3.1,3	Die CPU-Lastdaten des Hosts wurden anhand des Durchschnitts der letzten 1, 5 und 15 Minuten berechnet.
Dom0 CPU-Auslastung (%)	check_cpu	Ruft die aktuelle durchschnittliche CPU-Gesamtauslastung von dom0 ab und überprüft sie.	80%	90%	Die durchschnittliche CPU-Gesamtauslastung von dom0 in Prozent.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Dom0 Speicherauslastung (%)	Speicher überprüfen	Ruft die aktuelle Speicherbelegung von dom0 ab und überprüft sie.	80%	90%	Der Prozentsatz des derzeit freien dom0-Speichers und der Prozentsatz, der verwendet wird.
Dom0 Kostenloser Swap (%)	check_swap	Ruft die aktuelle Swap-Nutzung von dom0 ab und überprüft sie.	20%	10%	Der Prozentsatz von MB auf dom0, der derzeit kostenlos ist.
Freier Speicherplatz der Dom0-Root-Partition (%)	check_disk_root	Ruft die aktuelle Root-Partitionsnutzung von dom0 ab und überprüft sie.	20%	10%	Der Prozentsatz von MB auf der dom0-Root-Partition, die derzeit frei ist.
Freier Speicherplatz der Dom0-Log-Partition (%)	check_disk_log	Ruft die aktuelle Logpartitionsnutzung von dom0 ab und überprüft sie.	20%	10%	Der Prozentsatz von MB auf der dom0-Logpartition, die derzeit frei ist.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Toolstack-Status	check_xapi	Ruft den Status des XenServer Management Toolstack (auch bekannt als XAPI) ab und überprüft ihn.			Die Betriebszeit von XAPI ist in Sekunden abgelaufen.

Metrik	NRPE-Prüfname	Beschreibung	Standardwarnschwelle	Standardmäßiger kritischer Schwellenwert	Rückgegebene Leistungsdaten
Multipath-Status	check_multipath	Ruft den Status der Speicherpfade ab und überprüft ihn.			Der Status der Speicherpfade. `OK` gibt an, dass alle Pfade aktiv sind, `WARNING` zeigt an, dass einige Pfade ausgefallen sind, aber mehr als ein Pfad aktiv ist, `CRITICAL` zeigt an, dass nur ein Pfad aktiv ist oder dass alle Pfade ausgefallen sind, `UNKNOWN` gibt an, dass Host-Multipathing deaktiviert ist und dass der Status der Pfade nicht abgerufen werden kann.

NRPE ist ein on-premises Dienst, der in dom0 ausgeführt wird und am TCP-Port (Standard) 5666 auf Anfragen zur Prüfausführung von einem Überwachungstool wartet. Nachdem eine Anfrage eingetroffen ist, analysiert NRPE sie, findet den entsprechenden Prüfbefehl einschließlich der Parameterdetails aus der Konfigurationsdatei und führt ihn dann aus. Das Ergebnis der Prüfung wird an das Monitoring-

Tool gesendet, das die Ergebnisse vergangener Prüfungen speichert und ein Diagramm mit den historischen Leistungsdaten bereitstellt.

Voraussetzungen

Um NRPE zur Überwachung von Host- und Dom0-Ressourcen verwenden zu können, muss das von Ihnen verwendete Überwachungstool die folgenden Voraussetzungen erfüllen:

- Das Monitoring-Tool muss mit der NRPE-Version 4.1.0 kompatibel sein.
- Um die Kommunikation zwischen NRPE und dem Überwachungstool zu ermöglichen, muss das Überwachungstool TLS 1.2 mit den Chiffren `ECDHE-RSA-AES256-GCM-SHA384` und `ECDHE-RSA-AES128-GCM-SHA256` unterstützen, und die EC-Kurve muss `secp384r1` sein.

Einschränkungen

- Sie können NRPE-Einstellungen für einen gesamten Pool oder für einen eigenständigen Host konfigurieren, der nicht Teil eines Pools ist. Derzeit können Sie keine NRPE-Einstellungen für einen einzelnen Host in einem Pool konfigurieren.
- Wenn Sie einem Pool einen Host hinzufügen, auf dem NRPE bereits aktiviert und konfiguriert ist, wendet XenCenter die NRPE-Einstellungen des Pools nicht automatisch auf den neuen Host an. Sie müssen die NRPE-Einstellungen im Pool neu konfigurieren, nachdem Sie den neuen Host hinzugefügt haben, oder den neuen Host mit denselben NRPE-Einstellungen konfigurieren, bevor Sie ihn zum Pool hinzufügen.

  > **Hinweis:**
  >
  > Wenn Sie die NRPE-Einstellungen in einem Pool nach dem Hinzufügen eines neuen Hosts neu konfigurieren, stellen Sie sicher, dass der Host betriebsbereit ist.

- Wenn ein Host aus einem Pool entfernt wird, auf dem NRPE aktiviert und konfiguriert ist, ändert XenCenter die NPRE-Einstellungen auf dem Host oder Pool nicht.

Konfigurieren Sie NRPE mithilfe der Xe-CLI

Sie können NRPE mithilfe der Xe-CLI oder XenCenter konfigurieren. Weitere Informationen zur Konfiguration von NRPE mithilfe von XenCenter finden Sie unter Überwachen von Host- und Dom0-Ressourcenmit NRPE.

Nachdem Sie die Konfiguration von NRPE geändert haben, starten Sie den NRPE-Dienst neu, indem Sie:


```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=restart
<!--NeedCopy-->
```

NRPE aktivieren NRPE ist in XenServer standardmäßig deaktiviert. Führen Sie die folgenden Befehle in der XE-CLI aus, um NRPE in der Steuerdomäne eines Hosts (dom0) zu aktivieren:

1. Ermitteln Sie die Host-UUID des Hosts, den Sie überwachen möchten:

   ```
   xe host-list
   ```

2. Aktivieren Sie NRPE auf dem Host:

   ```
   xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=enable
   ```

   Wenn der Vorgang erfolgreich ausgeführt wird, wird dieser Befehl ausgegeben `Success`. Wenn XenServer neu gestartet wird, wird NRPE automatisch gestartet.

Um NRPE zu beenden, zu starten, neu zu starten oder zu deaktivieren:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=<operation>
<!--NeedCopy-->
```

wo **Operation**`stop`, `startrestart`, oder ist `disable`.

Server überwachen Dies ist eine kommagetrennte Liste von IP-Adressen oder Hostnamen, die mit dem NRPE-Daemon kommunizieren dürfen. Netzwerkadressen mit einer Bitmaske (zum Beispiel `192.168.1.0/24`) werden ebenfalls unterstützt.

Sehen Sie sich die aktuelle Liste der Überwachungsserver an:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:allowed_hosts
<!--NeedCopy-->
```

Erlauben Sie dem Monitoring-Tool, Prüfungen auszuführen:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:allowed_hosts=<IP address or hostname>
<!--NeedCopy-->
```

Alle NRPE-Einstellungen abfragen:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
<!--NeedCopy-->
```

Konfigurieren Sie mehrere NRPE-Einstellungen:


```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:allowed_hosts=<IP address or hostname> args:ssl_logging=<SSL
   log level> args:debug=<debug log level>
<!--NeedCopy-->
```

Protokolle

Protokollierung debuggen Die Debug-Protokollierung ist standardmäßig deaktiviert.

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Debug-Protokollierung aktiviert ist:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:debug
<!--NeedCopy-->
```

Wenn `debug: 0` zurückgegeben wird, ist die Debug-Protokollierung deaktiviert.

So aktivieren Sie die Debug-Protokollierung:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:debug=1
<!--NeedCopy-->
```

SSL-Protokollierung Standardmäßig ist die SSL-Protokollierung deaktiviert:

```
ssl_logging=0x00
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die SSL-Protokollierung aktiviert ist:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-config
   args:ssl_logging
<!--NeedCopy-->
```

So aktivieren Sie die SSL-Protokollierung:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-config
   args:ssl_logging=0x2f
<!--NeedCopy-->
```

Warnung und kritische Schwellenwerte Für einige dieser Check-Plugins können Sie Warn- und kritische Schwellenwerte festlegen, sodass eine Warnung generiert wird, wenn der von einem Check-Plugin zurückgegebene Wert die Schwellenwerte überschreitet. Der Warnschwellenwert weist auf ein potenzielles Problem hin, und der kritische Schwellenwert weist auf ein schwerwiegenderes Problem hin, das sofortige Aufmerksamkeit erfordert. Obwohl Standardwerte für die Warnung und die kritischen Schwellenwerte festgelegt sind, können Sie die Schwellenwerte anpassen.

Um die Standardwarnungs- und kritischen Schwellenwerte für alle Prüfungen abzufragen, führen Sie den folgenden xe-CLI-Befehl aus, der eine Liste aller Prüfungen und der zugehörigen Warn- und kritischen Schwellenwerte zurückgibt:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-threshold
<!--NeedCopy-->
```

Sie können auch die Schwellenwerte für eine bestimmte Prüfung abfragen. Um beispielsweise die Warn- und kritischen Schwellenwerte für das Check-Plug-In `check_memory` abzurufen, führen Sie den folgenden xe-CLI-Befehl aus:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=get-threshold
   args:check_memory
<!--NeedCopy-->
```

Sie können auch den Standardwert eines Schwellenwerts ändern. Um beispielsweise die Standardschwellenwerte für das Check-Plug-In `check_memory` zu ändern, führen Sie den folgenden xe-CLI-Befehl aus:

```
xe host-call-plugin host-uuid=<host uuid> plugin=nrpe fn=set-threshold
   args:check_memory args:w=75 args:c=85
<!--NeedCopy-->
```

Überwachen Sie Host- und Dom0-Ressourcen mit SNMP

> **Hinweis:**
>
> Die SNMP-Funktion ist für XenServer Premium- oder Trial Edition-Kunden verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.

Mit der Pool-Admin-Rolle können Sie SNMP verwenden, um Ressourcen, die von Ihrem XenServer-Host und dom0, der Steuerdomäne Ihres Hosts, verbraucht werden, remote zu überwachen. Ein SNMP-Manager, auch bekannt als Netzwerkmanagementsystem (NMS), sendet Abfrageanforderungen an einen SNMP-Agenten, der auf einem XenServer-Host ausgeführt wird. Der SNMP-Agent beantwortet diese Abfrageanforderungen, indem er Daten, die auf verschiedenen Metriken gesammelt wurden, zurück an das NMS sendet. Die Daten, die gesammelt werden können, werden durch Objektkennungen (OIDs) in einer Textdatei definiert, die als Management Information Base (MIB) bezeichnet wird. Eine OID steht für eine bestimmte messbare Information über ein Netzwerkgerät, z. B. die CPU- oder Speicherauslastung.

Sie können auch Traps konfigurieren. Dabei handelt es sich um vom Agenten initiierte Meldungen, die den NMS darauf hinweisen, dass ein bestimmtes Ereignis in XenServer eingetreten ist. Sowohl Abfrageanforderungen als auch Traps können verwendet werden, um den Status Ihrer XenServer-Pools zu überwachen. Diese sind als Metrik- und Trap-Objekte definiert und werden durch OIDs in

der MIB-Datei `XENSERVER-MIB.txt` identifiziert, die von der XenServer-Downloadseite heruntergeladen werden kann. Die folgenden Tabellen enthalten Informationen zu diesen Metrik- und Trap-Objekten.

Metrische Objekte

Sie können mithilfe der in der folgenden Tabelle aufgeführten Metriken bestimmte Informationen über Ihre XenServer-Hosts anfordern. Diese Metriken werden vom SNMP-Manager verwendet, wenn er Abfrageanforderungen an einen SNMP-Agenten sendet, sodass Sie diese Daten in Ihrem NMS anzeigen können.

Sie können die von diesen Metrikobjekten zurückgegebenen Daten in Ihrem NMS oder in der xe-CLI anzeigen. Um die Metrikobjekte über die XE-CLI abzufragen, führen Sie `host-data-source-query` oder `vm-data-source-query` aus und geben Sie die RRDD-Datenquelle als Wert für den Parameter `data-source` an. Beispiel:

```
xe host-data-source-query data-source=cpu_avg host=<host UUID>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Standardmäßig sendet das NMS OID-Abfrageanforderungen über Port 161 an SNMP-Agents.

Objektbezeichner (OID)	RRDD-Datenquelle	Zurückgegebene Daten	Typ
.1.3.6.1.4.1.60953.1.1.1.1	`memory`	Dom0 Gesamtspeicher in MB	Unsigniert 32
.1.3.6.1.4.1.60953.1.1.1.2	`memory_internal_free`	Dom0 freier Speicher in MB	Unsigniert 32
.1.3.6.1.4.1.60953.1.1.1.3	`cpu_usage`	Dom0 CPU-Auslastung in Prozent	Gleitkomma
.1.3.6.1.4.1.60953.1.1.1.4	`memory_total_kib`	Gesamtspeicher des Hosts in MB	Unsigniert 32
.1.3.6.1.4.1.60953.1.1.1.5	`memory_free_kib`	Freier Host-Speicher in MB	Unsigniert 32
.1.3.6.1.4.1.60953.1.1.1.6	`cpu_avg`	CPU-Auslastung des Hosts in Prozent	Gleitkomma
.1.3.6.1.4.1.60953.1.1.1.7	(siehe Hinweis 1)	Anzahl der PCPUs	Unsigniert 32
.1.3.6.1.4.1.60953.1.1.1.8	`running_vcpus`	Laufende vCPU-Nummer	Unsigniert 32

Objektbezeichner (OID)	RRDD-Datenquelle	Zurückgegebene Daten	Typ
.1.3.6.1.4.1.60953.1.1.1.9	`running_domains`	Nummer laufender VMs	Unsigniert 32

Hinweise:

1. Der Name einer pCPU hat das Format `cpu` gefolgt von einer Zahl. Führen Sie den folgenden Befehl aus, um die Anzahl der PCPUs über die xe-CLI abzufragen:

   ```
   xe host-data-source-list host=<host UUID> | grep -E 'cpu[0-9]+$'
   ```

   This returns a list of the CPU metrics that match the regular expression `cpu[0-9]+`.

Traps

Traps sind Warnungen, die vom SNMP-Agenten gesendet werden, um den SNMP-Manager zu benachrichtigen, wenn bestimmte Ereignisse eintreten. So können Sie Ihre XenServer-Hosts überwachen und Probleme frühzeitig erkennen. Sie können Ihre SNMP-Einstellungen so konfigurieren, dass ein Trap generiert wird, wenn ein Limit erreicht wird (z. B. wenn die Host-CPU-Auslastung zu hoch ist). Wenn ein Trap generiert wird, wird er an Ihr NMS gesendet und die folgenden Felder werden als Teil des Trapobjekts zurückgegeben.

Hinweis:

Standardmäßig sendet der SNMP-Agent auf dem Poolkoordinatorhost Traps über den UPD-Port 162 an den NMS.

Objektbezeichner (OID)	Feldname	Typ	Beschreibung
.1.3.6.1.4.1.60953.1.10.1.1	`operation`	Zeichenfolge	Kann einer der folgenden Werte sein: `add` oder `del`. `operation` ist `add`, wenn ein Trap von XenServer generiert und an Ihr NMS gesendet wird (eine Warnung wird auch in XenCenter erstellt) oder `del`, wenn eine Warnung zerstört wird (z. B. wenn Sie eine Warnung verwerfen).
.1.3.6.1.4.1.60953.1.10.1.2	`ref`	Zeichenfolge	Die Referenz für das Trapobjekt.
.1.3.6.1.4.1.60953.1.10.1.3	`uuid`	Zeichenfolge	Die UUID des Trapobjekts.
.1.3.6.1.4.1.60953.1.10.1.4	`name`	Zeichenfolge	Der Name des Trapobjekts.
.1.3.6.1.4.1.60953.1.10.1.5	`priority`	Ganzzahl	Der Schweregrad des Traps. Kann einer der folgenden Werte sein: 1: Kritisch, 2: Schwer, 3: Warnung, 4: Leicht, 5: Information, `others`: Unbekannt.
.1.3.6.1.4.1.60953.1.10.1.6	**`class`**	Zeichenfolge	Die Kategorie des generierten Traps. Kann einen der folgenden Werte haben: `VM`, `Host`, `SR`, `Pool`, `VMPP`, `VMSS`, `PVS_proxy`, `VDI` oder `Certificate`.

Objektbezeichner (OID)	Feldname	Typ	Beschreibung
.1.3.6.1.4.1.60953.1.10.1.7	`obj-uuid`	Zeichenfolge	Die Xapi-Objekt-UUID der verschiedenen Klassen des Felds **`class`**.
.1.3.6.1.4.1.60953.1.10.1.8	`timestamp`	Zeichenfolge	Der Zeitpunkt, zu dem der Trap generiert wird.
.1.3.6.1.4.1.60953.1.10.1.9	`body`	Zeichenfolge	Detaillierte Informationen über das Feld `name`.

Voraussetzungen

- Auf allen Hosts in einem Pool muss dieselbe XenServer-Version ausgeführt werden, und diese Version muss das SNMP-Plugin enthalten.

  > **Hinweis:**
  >
  > Wenn Sie die Registerkarte **SNMP** in XenCenter nicht sehen können, liegt dies möglicherweise daran, dass der Host oder ein Mitglied des Pools keine Version von XenServer ausführt, die SNMP unterstützt. Aktualisieren Sie den Host oder Pool auf die neueste Version von XenServer.

- Das von Ihnen verwendete NMS muss SNMPv2c oder SNMPv3 unterstützen.
- Ihr NMS und XenServer müssen mit dem Netzwerk verbunden sein.

Einschränkungen

- Sie können SNMP-Einstellungen für einen gesamten Pool oder für einen eigenständigen Host konfigurieren, der nicht Teil eines Pools ist. Derzeit können Sie keine SNMP-Einstellungen für einen einzelnen Host in einem Pool konfigurieren.
- Wenn Sie einen Host zu einem Pool hinzufügen, auf dem SNMP bereits aktiviert und konfiguriert ist, wendet XenCenter die SNMP-Einstellungen des Pools nicht automatisch auf den neuen Host an. Sie müssen die SNMP-Einstellungen im Pool neu konfigurieren, nachdem Sie den neuen Host hinzugefügt haben, oder den neuen Host mit denselben SNMP-Einstellungen konfigurieren, bevor Sie ihn dem Pool hinzufügen.

> **Hinweis:**
>
> Wenn Sie die SNMP-Einstellungen in einem Pool nach dem Hinzufügen eines neuen Hosts neu konfigurieren, stellen Sie sicher, dass der Host betriebsbereit ist und sich nicht im Wartungsmodus befindet.

- Bevor Sie ein Rolling-Pool-Upgrade von Citrix Hypervisor 8.2 CU1 auf XenServer 8 durchführen oder Updates auf Ihre XenServer-Hosts und -Pools anwenden, sichern Sie die folgenden Konfigurationsdateien, falls Sie sie zuvor manuell geändert haben und benötigen:
  - `/etc/snmp/snmpd.xs.conf`
  - `/etc/sysconfig/snmp`
  - `/var/lib/net-snmp/snmpd.conf`
- Wenn der SNMP-Agent offline ist, können keine Traps generiert werden. Zum Beispiel, wenn der SNMP-Agent neu gestartet oder der Poolkoordinator neu gestartet oder neu benannt wird.

SNMP mit der xe-CLI konfigurieren

Sie können SNMP mit der xe-CLI oder XenCenter konfigurieren. Weitere Informationen zur Konfiguration von SNMP mit XenCenter finden Sie unter Host- und Dom0-Ressourcen mit SNMP überwachen.

`result` Objekte Bei der Konfiguration von SNMP werden alle Antworten im JSON-Format zurückgegeben. Wenn ein Befehl erfolgreich ausgeführt wird, gibt er das Schlüssel-Wert-Paar `"code": 0` zurück. Einige Befehle (wie der Befehl `get-config`) geben ein verschachteltes JSON-Objekt mit dem Namen `result`zurück. Das JSON-Objekt `result` ist auch für den Befehl `set-config` erforderlich, der zum Aktualisieren der SNMP-Konfiguration verwendet wird.

Das JSON-Objekt `result` besteht aus den folgenden Objekten `common`, `agent` und `nmss`.

`common`

Feld	Zulässige Werte	Standardwert
`enabled`	`no` (SNMP-Dienst deaktivieren) oder `yes` (SNMP-Dienst aktivieren)	`no`
`debug_log`	`no` (Debug-Logging deaktivieren) oder `yes` (Debug-Logging aktivieren)	`no`

Feld	Zulässige Werte	Standardwert
max_nmss	N/A (Dieses Feld ist schreibgeschützt und gibt die maximale Anzahl unterstützter NMS an)	1

agent

Feld	Zulässige Werte	Standardwert
v2c	no (SNMPv2C deaktivieren) oder yes (SNMPv2C aktivieren)	yes
community	COMMON_STRING_TYPE (siehe Hinweis 1)	**public**
v3	no (v3 deaktivieren) oder yes (v3 aktivieren)	no
user_name	COMMON_STRING_TYPE (siehe Hinweis 1)	
authentication_password	COMMON_STRING_TYPE wo Länge >= 8 (siehe Anmerkung 1)	
authentication_protocol	MD5 oder SHA	
privacy_password	COMMON_STRING_TYPE wo Länge >= 8 (siehe Anmerkung 1)	
privacy_protocol	DES oder AES	
engine_id	N/A (Dieses Feld ist schreibgeschützt und wird generiert, wenn der SNMP-Agent zum ersten Mal gestartet wird)	

nmss

Feld	Zulässige Werte	Standardwert
`uuid`	NMS UUID (Sie legen dies fest, wenn Sie den NMS-Trap-Empfänger konfigurieren, und dieser Wert sollte auf allen Hosts in einem Pool konsistent sein)	
`address`	NMS-IPv4-Adresse oder Hostname (FQDN)	
`port`	1 bis 65535	162
`v2c`	`no` (SNMPv2c deaktivieren), `yes` (SNMPv2c aktivieren) oder unterstützen Sie entweder SNMPv2c oder v3.	`yes`
`community`	COMMON_STRING_TYPE (siehe Hinweis 1)	**`public`**
`v3`	`no` (v3 deaktivieren), `yes` (v3 aktivieren) oder entweder SNMPv2c oder SNMPv3 unterstützen.	`no`
`user_name`	COMMON_STRING_TYPE (siehe Hinweis 1)	
`authentication_password`	COMMON_STRING_TYPE wo Länge >= 8 (siehe Anmerkung 1)	
`authentication_protocol`	`MD5` oder `SHA`	
`privacy_password`	COMMON_STRING_TYPE wo Länge >= 8 (siehe Anmerkung 1)	
`privacy_protocol`	`DES` oder `AES`	

> **Hinweise:**
>
> 1. COMMON_STRING_TYPE bezieht sich auf eine Zeichenfolge, die die folgenden Anforderungen erfüllt:
>   - Jede Kombination aus Buchstaben, Zahlen, Bindestrich (-), Punkt (.), Pfund (#), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) oder Unterstrich (_).

- Länge zwischen 6 und einschließlich 32.

2. Kennwörter werden in keiner Konfigurationsdatei in XenServer im Klartext gespeichert. Sie werden in einen lokalisierten Schlüssel umgewandelt und gespeichert. Der Befehl `get-config` zeigt das Kennwort als versteckte Konstante an, die aus Sternchen (*) besteht.

Konfigurieren Sie den SNMP-Dienst Rufen Sie den Status des SNMP-Dienstes ab:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=status
<!--NeedCopy-->
```

Starten, beenden oder starten Sie den SNMP-Dienst neu:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=<operation>
<!--NeedCopy-->
```

Dabei gilt: **operaiton** ist `start`, `stop` oder `restart`.

Rufen Sie die SNMP-Konfigurationsdetails ab:

```
xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=get-config
<!--NeedCopy-->
```

Bei Erfolg gibt dieser Befehl das Schlüsselwertpaar `"code": 0` und das JSON-Objekt `result` zurück, das die Konfigurationsdetails des SNMP-Dienstes enthält. Beispiel:

```
"code": 0,
  "result": {

    "common": {

      "enabled": "no",
      "debug_log": "no",
      "max_nmss": 1
     }
 ,
    "agent": {

      "v2c": "yes",
      "v3": "no",
      "community": "public",
      "user_name": "",
      "authentication_password": "",
      "authentication_protocol": "",
      "privacy_password": "",
      "privacy_protocol": "",
      "engine_id": "<engine_id>"
     }
 ,
    "nmss": []
   }
```



```
26
27 <!--NeedCopy-->
```

Kopieren Sie das JSON-Objekt `result` in Ihren bevorzugten Texteditor und entfernen Sie alle Zeilenumbrüche (**\n**) aus der Datei. Aktualisieren Sie die Felder mit Ihren SNMP-Konfigurationsdetails. Konfigurieren Sie Ihr NMS, indem Sie auf Ihre NMS-Dokumentation verweisen und Werte für die Felder angeben, die für das Objekt `nmss` erforderlich sind. Weitere Informationen finden Sie in den oben aufgeführten Objekten.

Um den SNMP-Dienst zu konfigurieren, führen Sie den Befehl `set-config` aus und geben Sie das bearbeitete JSON-Objekt `result` als Parameterwert für den Parameter `args:config` an.

Stellen Sie die SNMP-Konfiguration ein:

```
1 xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=set-config
     args:config='<result>'
2 <!--NeedCopy-->
```

Dabei gilt: **result** ist das JSON-Objekt `result`, das von dem Befehl `get-config` zurückgegeben wurde, den Sie kopiert und bearbeitet haben.

> **Hinweis:**
>
> Um SNMP für einen gesamten Pool zu konfigurieren, müssen Sie den Befehl `set-config` für jeden Host im Pool ausführen.

Wenn die Konfigurationsänderungen erfolgreich sind, gibt der Befehl das Schlüssel-Wert-Paar `"code": 0` zurück. Wenn die Konfigurationsänderungen nicht erfolgreich sind, gibt der Befehl `set-config` eines der folgenden Schlüssel-Wert-Paare zurück, die darauf hinweisen, dass ein Fehler aufgetreten ist:

- `"code":` 1: Häufige Fehlerzeichenfolge. Zum Beispiel eine unbekannte Ausnahme.
- `"code":` 2: Fehlerstring (Parameter fehlt).
- `"code":` 3: Gibt das Objekt `message` als Liste zurück, in der jedes Element das Format von `[field_path, key, value, error string]` hat.

Sie können auch einen Test-SNMP-Trap an Ihren NMS senden, um zu überprüfen, ob die angegebenen Trap-Empfängerinformationen korrekt sind.

Senden Sie einen Test-SNMP-Trap:

```
1 xe host-call-plugin host-uuid=<host-uuid> plugin=snmp fn=send-test-trap
     args:config='{
2  "nmss":[{
3  "uuid":"<uuid>","address":"<address>","port":162,"v2c":"yes","v3":"no
     ","community":"public","user_name":"<user_name>","
     authentication_password":"<authentication_password>","
     authentication_protocol":"<authentication_protocol>","
```



```
        privacy_password":"<privacy_password>","privacy_protocol":"<
        privacy_protocol>" }
  ] }
  '
<!--NeedCopy-->
```

Dieser Befehl sendet einen Testtrap an Ihr NMS mit `TEST_TRAP`als `msg_name` und `This is a test trap from XenServer pool "<pool name>"to verify the NMS Trap Receiver configuration.` als `msg_body`.

Wenn Sie den Testtrap nicht erhalten, überprüfen Sie Ihre SNMP-Konfiguration erneut. Wenn der Befehl nicht erfolgreich ist, gibt der Befehl `send-test-trap` auch eines der folgenden Schlüssel-Wert-Paare zurück, die darauf hinweisen, dass ein Fehler aufgetreten ist:

- `"code":` 1: Häufige Fehlerzeichenfolge. Zum Beispiel eine unbekannte Ausnahme.
- `"code":` 2: Fehlerstring (Parameter fehlt).
- `"code":` 3: Gibt das Objekt `message` als Liste zurück, in der jedes Element das Format von `[field_path, key, value, error string]` hat.
- `"code":` 4: Gibt das Objekt `message` als Liste zurück, in der jedes Element das Format `[nms address, nms port, error string]` hat.

CPU-Auslastung überwachen

December 6, 2023

Die optimale Anzahl von vCPUs pro pCPU auf einem Host hängt von Ihrem Anwendungsfall ab. Stellen Sie während des Betriebs sicher, dass Sie die Leistung Ihrer XenServer-Umgebung überwachen und Ihre Konfiguration entsprechend anpassen.

Begriff

In diesem Bereich gibt es verschiedene Begriffe, die manchmal synonym verwendet werden. In diesem Artikel verwenden wir die folgenden Begriffe und Bedeutungen:

- **CPU (physische CPU):** Die physische Hardware, die an einen Prozessorsockel angeschlossen ist.
- **Kern:** Eine physische Verarbeitungseinheit, die in der Lage ist, einen unabhängigen Ausführungsthread auszuführen, der alle Funktionseinheiten enthält, die zur Unterstützung dieser Ausführung erforderlich sind.

- **Hyperthread:** Eine physische Verarbeitungseinheit, die in der Lage ist, einen unabhängigen Ausführungsthread auszuführen, der einige Funktionseinheiten mit einem anderen Hyperthread teilt (auch bekannt als sein "Geschwisterthread").
- **Logische CPU (pCPU):** Eine Einheit, die einen unabhängigen Ausführungsthread ausführen kann, der eine Reihe von Registern und einen Befehlszeiger enthält. In einem System mit aktivierten Hyperthreads ist dies ein Hyperthread. In anderen Fällen ist es ein Kern.
- **Host-pCPUs**: Die Gesamtzahl der logischen CPUs auf dem Host.
- **vCPU (Virtual CPU)**: Eine virtualisierte logische CPU. Dies ist eine logische Einheit, die einen unabhängigen Ausführungsthread ausführen kann und den VMs zur Verfügung gestellt wird. In XenServer können vCPUs sich pCPUs zeitweise teilen, indem sie mithilfe eines Schedulers ermitteln, welche vCPU zu einem bestimmten Zeitpunkt auf welcher pCPU läuft.
- **Gast-vCPUs**: Die vCPUs, die einem Gastbetriebssystem innerhalb einer VM präsentiert werden.
- **Dom0-vCPUs**: Die vCPUs, die für die XenServer-Steuerdomäne (dom0) sichtbar sind.
- **Gesamtanzahl der Host-vCPUs**: Die Summe der dom0-vCPUs und aller Gast-vCPUs auf dem Host.

Allgemeines Verhalten

Die Gesamtzahl der vCPUs auf einem Host ist die Anzahl der von dom0 verwendeten vCPUs, addiert zur Gesamtzahl der vCPUs, die allen VMs auf dem Host zugewiesen sind. Wenn Sie die Anzahl der vCPUs auf einem Host erhöhen, kann das folgende Verhalten auftreten:

- Wenn die Gesamtzahl der vCPUs auf dem Host *kleiner oder gleich der Anzahl der PCPUs auf* dem Host ist, stellt der Host immer so viel CPU bereit, wie von den VMs angefordert wird.
- Wenn die Gesamtzahl der vCPUs auf dem Host *größer ist als* die Anzahl der PCPUs auf dem Host, teilt der Host die Zeit der Host-PCPUs mit den VMs auf. Dieses Verhalten wirkt sich im Allgemeinen nicht auf die VMs aus, da ihre vCPUs normalerweise eine gewisse Zeit im Leerlauf sind und der Host in den meisten Fällen keine 100-prozentige pCPU-Auslastung erreicht.
- Wenn die Gesamtzahl der vCPUs auf dem Host *größer ist als* die Anzahl der PCPUs auf dem Host und der Host *manchmal* eine 100-prozentige Host-pCPU-Auslastung erreicht, erhalten die vCPUs der VMs während der Spitzenwerte nicht so viel pCPU, wie sie anfordern. Stattdessen werden die VMs während dieser Spitzen langsamer, um einen Teil der verfügbaren pCPU auf dem Host zu erhalten.
- Wenn die Gesamtzahl der vCPUs auf dem Host *größer ist als* die Anzahl der PCPUs auf dem Host und der Host *häufig* eine Host-PCPU-Auslastung von 100% erreicht, werden die vCPUs der VMs kontinuierlich verlangsamt, um einen Teil der verfügbaren CPUs auf dem Host zu erhalten. Wenn die VMs Echtzeitanforderungen haben, ist diese Situation nicht ideal. Sie können sie beheben, indem Sie die Anzahl der vCPUs auf dem Host reduzieren.

Die optimale Anzahl von vCPUs auf einem Host kann davon abhängen, wie die VM-Benutzer die Geschwindigkeit ihrer VMs wahrnehmen, insbesondere wenn die VMs Echtzeitanforderungen haben.

Informationen über Ihre CPUs abrufen

Führen Sie den folgenden Befehl aus, um die Gesamtzahl der PCPUs auf Ihrem Host zu ermitteln:

```
xe host-cpu-info --minimal
```

Führen Sie den folgenden Befehl aus, um die Gesamtzahl der derzeit auf Ihrem Host vorhandenen vCPUs (guest und dom0) zu ermitteln:

```
xl vcpu-list | grep -v VCPU | wc -l
```

Überwachung der CPU-Auslastung mit RRD-Metriken

XenServer bietet RRD-Metriken, die beschreiben, wie die vCPUs auf Ihren VMs funktionieren.

Wenn die pCPU-Auslastung des Hosts 100% beträgt

Wenn ein Host 100% der pCPU-Auslastung des Hosts erreicht, verwenden Sie diese VM-Metriken, um zu entscheiden, ob die VM auf einen anderen Host verschoben werden soll:

runstate_concurrency_hazard

- **runstate_concurrency_hazard > 0%** bedeutet, dass manchmal mindestens eine vCPU läuft, während mindestens eine andere vCPU laufen möchte, aber keine pCPU-Zeit abrufen kann. Wenn die vCPUs koordiniert werden müssen, führt dieses Verhalten zu Leistungsproblemen.
- **runstate_concurrency_hazard nähert sich** 100%, ist eine Situation, die es zu vermeiden gilt.

  > **Vorgeschlagene Maßnahmen:**
  >
  > Wenn Leistungsprobleme auftreten, ergreifen Sie eine der folgenden Maßnahmen:
  >
  > - Verringern Sie die Anzahl der vCPUs in der VM.
  > - Verschieben Sie die VM auf einen anderen Host.
  > - Verringern Sie die Gesamtzahl der vCPUs auf dem Host, indem Sie andere VMs migrieren oder deren Anzahl an vCPUs verringern.

runstate_partial_contention

- **runstate_partial_contention > 0%** bedeutet sowohl, dass mindestens eine vCPU ausgeführt werden möchte, aber keine pCPU-Zeit abrufen kann, als auch, dass mindestens eine andere vCPU blockiert ist (entweder weil nichts zu tun ist oder sie auf den Abschluss der I/O wartet).
- **runstate_concurrency_hazard nähert sich** 100%, ist eine Situation, die es zu vermeiden gilt.

  > **Vorgeschlagene Maßnahme:**
  >
  > Prüfen Sie, ob die Back-End-I/O-Speicherserver überlastet sind, indem Sie sich die von Ihrem Speicheranbieter bereitgestellten Backend-Metriken ansehen. Wenn die Speicherserver nicht überlastet sind und Leistungsprobleme auftreten, ergreifen Sie eine der folgenden Maßnahmen:
  >
  > - Verringern Sie die Anzahl der vCPUs in der VM.
  > - Verschieben Sie die VM auf einen anderen Host.
  > - Verringern Sie die Gesamtzahl der vCPUs auf dem Host, indem Sie andere VMs migrieren oder deren Anzahl an vCPUs verringern.

runstate_full_contention

- **runstate_full_contention > 0%** bedeutet, dass die vCPUs manchmal alle gleichzeitig ausführen möchten, aber keiner kann pCPU-Zeit abrufen.
- **runstate_full_contention nähert sich 100%**, ist eine Situation, die es zu vermeiden gilt.

  > **Vorgeschlagene Maßnahmen:**
  >
  > Wenn Leistungsprobleme auftreten, ergreifen Sie eine der folgenden Maßnahmen:
  >
  > - Verringern Sie die Anzahl der vCPUs in der VM.
  > - Verschieben Sie die VM auf einen anderen Host.
  > - Verringern Sie die Gesamtzahl der vCPUs auf dem Host, indem Sie andere VMs migrieren oder deren Anzahl an vCPUs verringern.

Wenn die pCPU-Auslastung des Hosts weniger als 100% beträgt

Wenn ein Host nicht 100% der Host-pCPU-Auslastung erreicht, verwenden Sie diese VM-Metriken, um zu entscheiden, ob eine VM über die richtige Anzahl an vCPUs verfügt:

runstate_fullrun

- **runstate_fullrun = 0%** bedeutet, dass die vCPUs niemals alle gleichzeitig verwendet werden.

> **Vorgeschlagene Maßnahme:**
>
> Verringern Sie die Anzahl der vCPUs in dieser VM.

- **0% < runstate_fullrun < 100%** bedeutet, dass die vCPUs manchmal alle gleichzeitig verwendet werden.
- **runstate_fullrun = 100%** gibt an, dass die vCPUs immer alle gleichzeitig verwendet werden.

> **Vorgeschlagene Maßnahme:**
>
> Sie können die Anzahl der vCPUs in dieser VM erhöhen, bis runstate_fullrun < 100% ist. Erhöhen Sie die Anzahl der vCPUs nicht weiter, da dies sonst die Wahrscheinlichkeit einer Parallelitätsgefahr erhöhen kann, wenn der Host 100% der pCPU-Auslastung erreicht.

runstate_partial_run

- **runstate_partial_run = 0%** gibt an, dass entweder immer alle vCPUs verwendet werden (full-run= 100%) oder keine vCPUs verwendet werden (idle= 100%).
- **0% < runstate_partial_run < 100%** bedeutet, dass manchmal mindestens eine vCPU blockiert ist, entweder weil sie nichts zu tun hat oder weil sie auf den Abschluss der I/O wartet.
- **runstate_partial_run= 100%** gibt an, dass immer mindestens eine vCPU blockiert ist.

> **Vorgeschlagene Maßnahme**:
>
> Überprüfen Sie, ob die Back-End-I/O-Speicherserver überlastet sind. Ist dies nicht der Fall, verfügt die VM wahrscheinlich über zu viele vCPUs, und Sie können die Anzahl der vCPUs in dieser VM verringern. Zu viele vCPUs in einer VM können das Risiko erhöhen, dass die VM in den Parallelitätszustand gerät, wenn die Host-CPU-Auslastung 100% erreicht.

---

layout: doc
description: Create virtual machines (VMs) from templates, by cloning, or by importing existing VMs.
—

Verwalten virtueller Maschinen

Dieser Abschnitt bietet einen Überblick über das Erstellen virtueller Maschinen (VMs) mithilfe von Vorlagen. Es werden auch andere Vorbereitungsmethoden erläutert, darunter das Klonen von Vorlagen und das Importieren zuvor exportierter VMs.

Was ist eine virtuelle Maschine?

Eine virtuelle Maschine (VM) ist ein Softwarecomputer, der wie ein physischer Computer ein Betriebssystem und Anwendungen ausführt. Die VM umfasst eine Reihe von Spezifikations- und Konfigurationsdateien, die von den physischen Ressourcen eines Hosts unterstützt werden. Jede VM verfügt über virtuelle Geräte, die dieselben Funktionen wie physische Hardware bieten. VMs können den Vorteil bieten, dass sie portabler, verwaltbarer und sicherer sind. Darüber hinaus können Sie das Startverhalten jeder VM an Ihre spezifischen Anforderungen anpassen. Weitere Informationen finden Sie unter VM-Startverhalten.

XenServer unterstützt Gäste mit einer beliebigen Kombination von IPv4- oder IPv6-konfigurierten Adressen.

In XenServer können VMs im vollständig virtualisierten Modus betrieben werden. Spezifische Prozessorfunktionen werden verwendet, um privilegierte Befehle, die von der virtuellen Maschine ausgeführt werden, zu "fangen". Mit dieser Funktion können Sie ein unverändertes Betriebssystem verwenden. Für den Netzwerk- und Speicherzugriff werden emulierte Geräte der virtuellen Maschine präsentiert. Alternativ können PV-Treiber aus Gründen der Leistung und Zuverlässigkeit verwendet werden.

Erstellen von virtuellen Rechnern

Verwenden Sie VM-Vorlagen

Virtuelle Rechner werden aus Vorlagen vorbereitet. Eine Vorlage ist ein *Gold-Image*, das alle verschiedenen Konfigurationseinstellungen zum Erstellen einer Instanz einer bestimmten VM enthält. XenServer wird mit einem Basissatz von Vorlagen geliefert, bei denen es sich um *rohe* VMs handelt, auf denen Sie ein Betriebssystem installieren können. Verschiedene Betriebssysteme benötigen unterschiedliche Einstellungen, um optimal zu funktionieren. XenServer-Vorlagen sind auf die Maximierung der Betriebssystemleistung abgestimmt.

Es gibt zwei grundlegende Methoden, mit denen Sie VMs aus Vorlagen erstellen können:

- Verwendung einer vollständigen vorkonfigurierten Vorlage.
- Installieren eines Betriebssystems von einer CD, einem ISO-Image oder einem Netzwerk-Repository auf der entsprechenden bereitgestellten Vorlage.

Windows VMs beschreibt, wie Windows-Betriebssysteme auf virtuellen Rechnern installiert werden.

Linux-VMs beschreiben, wie Linux-Betriebssysteme auf virtuellen Rechnern installiert werden.

> **Hinweis:**
>
> Vorlagen, die mit älteren Versionen von XenServer erstellt wurden, können in neueren Versionen von XenServer verwendet werden. Vorlagen, die in neueren Versionen von XenServer erstellt wurden, sind jedoch nicht mit älteren Versionen von XenServer kompatibel. Wenn Sie eine VM-Vorlage mit Citrix Hypervisor 8.2 erstellt haben, exportieren Sie die VDIs separat, und erstellen Sie die VM erneut, um sie mit einer früheren Version zu verwenden.

Andere Methoden der VM-Erstellung

Sie können nicht nur virtuelle Maschinen aus den bereitgestellten Vorlagen erstellen, sondern auch die folgenden Methoden verwenden, um VMs zu erstellen.

Klonen einer vorhandenen VM Sie können eine Kopie einer vorhandenen VM erstellen, indem Sie aus einer Vorlage *klonen* . Vorlagen sind normale VMs, die als Originalkopien verwendet werden sollen, um daraus Instanzen von VMs zu erstellen. Eine VM kann angepasst und in eine Vorlage umgewandelt werden. Stellen Sie sicher, dass Sie das entsprechende Vorbereitungsverfahren für die VM befolgen. Weitere Informationen finden Sie unter Vorbereiten des Klonens einer Windows-VM mit Sysprep und Vorbereiten des Klonens einer Linux-VM.

> **Hinweis:**
>
> Vorlagen können nicht als normale virtuelle Maschinen verwendet werden.

XenServer verfügt über zwei Mechanismen zum Klonen von VMs:

- Eine vollständige Kopie
- Kopieren-bei-Schreiben

  Der schnellere Copy-on-Write-Modus schreibt nur *modifizierte* Blöcke auf den Datenträger. Copy-on-Write wurde entwickelt, um Speicherplatz zu sparen und schnelle Klone zu ermöglichen, verlangsamt jedoch die normale Datenträgerleistung geringfügig. Eine Vorlage kann ohne Verlangsamung mehrfach schnell geklont werden.

  > **Hinweis:**
  >
  > Wenn Sie eine Vorlage in eine VM klonen und dann den Klon in eine Vorlage konvertieren, kann die Datenträgerleistung sinken. Das Ausmaß der Abnahme steht in linearem Zusammenhang mit der Häufigkeit, mit der dieser Prozess stattgefunden hat. In diesem Fall kann der CLI-Befehl `vm-copy` verwendet werden, um eine vollständige Kopie der Datenträger durchzuführen und die erwartete Datenträgerleistung wiederherzustellen.

Hinweise für Ressourcenpools Wenn Sie eine Vorlage aus virtuellen VM-Laufwerken auf einer gemeinsam genutzten SR erstellen, wird der Vorgang zum Klonen von Vorlagen an jeden Host im Pool weitergeleitet, der auf die gemeinsam genutzten SRs zugreifen kann. Wenn Sie die Vorlage jedoch von einem virtuellen VM-Laufwerk erstellen, das nur über eine lokale SR verfügt, kann der Vorlagenklonvorgang nur auf dem Host ausgeführt werden, der auf diese SR zugreifen kann.

Importieren einer exportierten VM Sie können eine VM erstellen, indem Sie eine vorhandene exportierte VM *importieren* . Wie beim Klonen ist das Exportieren und Importieren einer VM eine schnelle Möglichkeit, mehr VMs einer bestimmten Konfiguration zu erstellen. Mit dieser Methode können Sie die Geschwindigkeit Ihrer Bereitstellung erhöhen. Möglicherweise verfügen Sie beispielsweise über eine spezielle Host-Konfiguration, die Sie häufig verwenden. Nachdem Sie eine VM wie erforderlich eingerichtet haben, exportieren Sie sie und importieren Sie sie später, um eine weitere Kopie Ihrer speziell konfigurierten VM zu erstellen. Sie können auch Export und Import verwenden, um eine VM auf den XenServer-Host zu verschieben, der sich in einem anderen Ressourcenpool befindet.

Einzelheiten und Verfahren zum Importieren und Exportieren von VMs finden Sie unter Importieren und Exportieren von VMs.

XenServer VM-Tools

XenServer VM Tools bieten leistungsstarke I/O-Dienste ohne den Aufwand herkömmlicher Geräteemulation.

XenServer VM-Tools für Windows

XenServer VM Tools für Windows bestehen aus I/O-Treibern (auch bekannt als paravirtualisierte Treiber oder PV-Treiber) und dem Management Agent.

Die E/A-Treiber enthalten Speicher- und Netzwerktreiber sowie Low-Level-Management-Schnittstellen. Diese Treiber ersetzen die emulierten Geräte und ermöglichen den High-Speed-Transport zwischen Windows und der XenServer-Produktfamilie. Bei der Installation eines Windows-Betriebssystems verwendet XenServer die herkömmliche Geräteemulation, um der VM einen Standard-IDE-Controller und eine Standard-Netzwerkkarte zu präsentieren. Diese Emulation ermöglicht es der Windows-Installation, integrierte Treiber zu verwenden, jedoch mit reduzierter Leistung aufgrund des Overheads, der mit der Emulation der Controller-Treiber verbunden ist.

Der Management Agent, auch bekannt als Guest Agent, ist für allgemeine Verwaltungsfunktionen für virtuelle Maschinen verantwortlich und bietet XenCenter einen vollständigen Funktionsumfang.

Installieren Sie XenServer VM Tools für Windows auf jeder Windows-VM, damit diese VM eine vollständig unterstützte Konfiguration hat und die Xe-CLI oder XenCenter verwenden kann. Eine VM funk-

tioniert ohne die XenServer VM Tools für Windows, aber die Leistung wird beeinträchtigt, wenn die I/O-Treiber (PV-Treiber) nicht installiert sind. Sie müssen XenServer VM Tools für Windows auf Windows-VMs installieren, um die folgenden Vorgänge ausführen zu können:

- Sauberes Herunterfahren, Neustarten oder Anhalten einer virtuellen Maschine
- Anzeigen von VM-Leistungsdaten in XenCenter
- Migrieren einer laufenden VM (mithilfe von Live-Migration oder Speicher-Live-Migration)
- Erstellen von Snapshots mit Speicher (Checkpoints) oder Wiederherstellen von Snapshots

Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Windows.

XenServer VM Tools für Linux

Die XenServer VM Tools für Linux enthalten einen Gast-Agent, der dem Host zusätzliche Informationen über die VM zur Verfügung stellt.

Sie müssen die XenServer VM Tools für Linux auf Linux-VMs installieren, um die folgenden Vorgänge ausführen zu können:

- Anzeigen von VM-Leistungsdaten in XenCenter
- Passen Sie die Anzahl der vCPUs auf einer laufenden Linux-VM an
- Dynamische Speichersteuerung aktivieren

> **Hinweis:**
>
> Sie können die Funktion Dynamic Memory Control (DMC) nicht auf Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 oder CentOS Stream 9 VMs verwenden, da diese Betriebssysteme kein Memory Ballooning mit dem Xen-Hypervisor unterstützen.

Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Finden Sie den Virtualisierungsstatus einer VM heraus

XenCenter meldet den Virtualisierungsstatus einer VM auf der Registerkarte **Allgemein** der VM. Sie können herausfinden, ob die XenServer VM Tools installiert sind oder nicht. Auf dieser Registerkarte wird auch angezeigt, ob die VM Updates von Windows Update installieren und empfangen kann. Im folgenden Abschnitt werden die Meldungen aufgeführt, die in XenCenter angezeigt werden:

I/O-optimiert (nicht optimiert): In diesem Feld wird angezeigt, ob die I/O-Treiber auf der VM installiert sind oder nicht.

Management Agent installiert (nicht installiert): In diesem Feld wird angezeigt, ob der Management Agent auf der VM installiert ist oder nicht.

Kann (nicht in der Lage) Updates von Windows Update empfangen: gibt an, ob die VM I/O-Treiber von Windows Update empfangen kann.

> **Hinweis:**
>
> Windows Server Core 2016 unterstützt nicht die Verwendung von Windows Update zum Installieren oder Aktualisieren der E/A-Treiber. Verwenden Sie stattdessen das Installationsprogramm für XenServer VM Tools für Windows, das auf der XenServer-Downloadseitebereitgestellt wird.

I/O-Treiber und Management Agent installieren: Diese Meldung wird angezeigt, wenn auf der VM die I/O-Treiber oder der Management Agent nicht installiert sind.

UEFI-Gaststart und Secure Boot

XenServer ermöglicht den Start der folgenden Gastbetriebssysteme im UEFI-Modus:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9 (Vorschau)
- Ubuntu 20.04
- Ubuntu 22.04

UEFI-Boot bietet eine umfangreichere Schnittstelle für die Interaktion der Gastbetriebssysteme mit der Hardware, wodurch die Startzeiten der virtuellen Maschinen erheblich reduziert werden können. Wenn XenServer UEFI-Boot für Ihr Gastbetriebssystem unterstützt, empfehlen wir, diesen Startmodus anstelle des BIOS zu wählen.

Für diese Betriebssysteme unterstützt XenServer auch Secure Boot. Secure Boot verhindert, dass unsignierte, falsch signierte oder modifizierte Binärdateien während des Startvorgangs ausgeführt werden. Auf einer UEFI-fähigen VM, die Secure Boot erzwingt, müssen alle Treiber signiert sein. Diese Anforderung kann den Einsatzbereich der VM einschränken, bietet jedoch die Sicherheit, unsignierte/geänderte Treiber zu blockieren. Wenn Sie einen unsignierten Treiber verwenden, schlägt der sichere Start fehl und in XenCenter wird eine Warnung angezeigt. Secure Boot reduziert auch das Risiko, dass Malware im Gast die Startdateien manipulieren oder während des Startvorgangs ausgeführt werden kann.

Sie müssen den Startmodus angeben, wenn Sie eine VM erstellen. Es ist nicht möglich, den Startmodus einer VM zwischen BIOS und UEFI (oder UEFI Secure Boot) zu ändern, nachdem die VM zum ersten Mal gestartet wurde. Sie können jedoch den Startmodus zwischen UEFI und UEFI Secure Boot ändern, nachdem die VM zur Behebung potenzieller Secure Boot-Probleme verwendet wurde. Weitere Informationen finden Sie unter Problembehandlung.

Beachten Sie Folgendes, wenn Sie UEFI-Boot auf VMs aktivieren:

- Stellen Sie sicher, dass eine UEFI-fähige Windows-VM über mindestens zwei vCPUs verfügt. UEFI-fähige Linux-VMs haben diese Einschränkung nicht.
- Sie können eine auf XenServer erstellte UEFI-fähige VM als OVA-, OVF- oder XVA-Datei importieren oder exportieren. Das Importieren einer UEFI-fähigen VM aus OVA- oder OVF-Paketen, die auf anderen Hypervisors erstellt wurden, wird nicht unterstützt
- Um den PVS-Accelerator mit UEFI-fähigen VMs zu verwenden, stellen Sie sicher, dass Sie Citrix Provisioning 1906 oder höher verwenden.
- Verwenden Sie für Windows-VMs das UEFI-Einstellungsmenü, um die Bildschirmauflösung der XenCenter Konsole zu ändern. Ausführliche Anweisungen finden Sie unter Fehlerbehebung.

> **Hinweis**
>
> UEFI-fähige VMs verwenden NVME und E1000 für emulierte Geräte. In den Emulationsinformationen werden diese Werte erst angezeigt, nachdem Sie die XenServer VM Tools für Windows auf der VM installiert haben.
> UEFI-fähige VMs werden auch so angezeigt, dass sie nur über 2 NICs verfügen, bis Sie die XenServer VM Tools für Windows installiert haben.

UEFI-Boot oder UEFI Secure Boot aktivieren

Sie können XenCenter oder die xe CLI verwenden, um UEFI-Boot oder UEFI Secure Boot für Ihre VM zu aktivieren.

Informationen zum Erstellen einer UEFI-fähigen VM in XenCenter finden Sie unter Erstellen einer Windows-VM mit XenCenter oder [Erstellen einer Linux-VM](/de-de/xenserver/8/vms/linux.html#create-a-linux-vm-by-using-xencenter) mit XenCenter.

Verwenden der xe CLI zum Aktivieren von UEFI-Boot oder UEFI Secure Boot Wenn Sie eine VM erstellen, führen Sie den folgenden Befehl aus, bevor Sie die VM zum ersten Mal starten:

```
1     xe vm-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
2     xe vm-param-set uuid=<UUID> platform:device-model=qemu-upstream-
         uefi
3     xe vm-param-set uuid=<UUID> platform:secureboot=<OPTION>
4 <!--NeedCopy-->
```


Wobei, UUID die UUID der VM ist, MODE entweder BIOS oder uefi und OPTION ist entweder "wahr"oder "falsch". Wenn Sie den Modus nicht angeben, wird für diese Option standardmäßig uefi eingestellt, wenn Ihr VM-Betriebssystem dies unterstützt. Andernfalls ist der Standardmodus BIOS. Wenn Sie die secureboot-Option nicht angeben, wird standardmäßig "auto"verwendet. Bei UEFI-fähigen VMs besteht das "automatische"Verhalten darin, Secure Boot für die VM zu aktivieren.

Führen Sie den folgenden Befehl aus, um eine UEFI-fähige VM aus einer im Lieferumfang von XenServer enthaltenen Vorlage zu erstellen:

```
1     UUID=$(xe vm-clone name-label='Windows 10 (64-bit)' new-name-label=
          'Windows 10 (64-bit)(UEFI)')
2     xe template-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
          platform:secureboot=<OPTION>
3 <!--NeedCopy-->
```

Führen Sie diesen Befehl nicht für Vorlagen aus, auf denen etwas installiert ist, oder für Vorlagen, die Sie aus einem Snapshot erstellt haben. Der Startmodus dieser Snapshots kann nicht geändert werden, und wenn Sie versuchen, den Startmodus zu ändern, startet die VM nicht.

Wenn Sie die UEFI-fähige VM zum ersten Mal starten, werden Sie auf der VM-Konsole aufgefordert, eine beliebige Taste zu drücken, um die Installation zu starten. Wenn Sie die Betriebssysteminstallation nicht starten, wechselt die VM-Konsole zur UEFI-Shell.

Um den Installationsvorgang neu zu starten, geben Sie in der UEFI-Konsole die folgenden Befehle ein.

```
1 EFI:
2 EFI\BOOT\BOOTX64
```

Wenn der Installationsvorgang neu gestartet wird, achten Sie in der VM-Konsole auf die Installationsaufforderung. Wenn die Eingabeaufforderung erscheint, drücken Sie eine beliebige Taste.

Deaktivierung des sicheren Starts

Möglicherweise möchten Sie Secure Boot gelegentlich deaktivieren. Beispielsweise können einige Debugging-Arten auf einer VM, die sich im Secure Boot-Benutzermodus befindet, nicht aktiviert werden. Um Secure Boot zu deaktivieren, ändern Sie die VM in den Secure Boot-Einrichtungsmodus. Führen Sie auf Ihrem XenServer-Host den folgenden Befehl aus:

```
1 varstore-sb-state <VM_UUID> setup
```

Kinderklavier

Für Windows-VMs:

UEFI-fähige Windows-VMs werden mit einer PK aus einem kurzlebigen privaten Schlüssel, dem Microsoft KEK, dem Microsoft Windows Production PCA und Microsoft-Schlüsseln von Drittanbietern bereitgestellt. Die VMs erhalten außerdem eine aktuelle Sperrliste aus dem UEFI-Forum. Diese Konfiguration ermöglicht es Windows-VMs, mit aktiviertem Secure Boot zu starten und automatische Updates der Schlüssel und der Sperrliste von Microsoft zu erhalten.

Für Linux-VMs:

Um Treiber von Drittanbietern auf einer Linux-VM zu installieren, auf der Secure Boot aktiviert ist, müssen Sie einen Signaturschlüssel erstellen, ihn der VM als Maschinenbesitzerschlüssel (MOK) hinzufügen und diesen Schlüssel verwenden, um den Treiber zu signieren. Weitere Informationen finden Sie unter Installieren von Treibern von Drittanbietern auf Ihrer Secure Boot Linux-VM.

Problembehandlung bei Ihren UEFI- und UEFI Secure Boot-VMs

Informationen zur Problembehandlung Ihrer UEFI- oder UEFI Secure Boot-VMs finden Sie unter Beheben von UEFI- undSecure Boot-Problemen.

Unterstützte Gäste und Zuweisung von Ressourcen

Eine Liste der unterstützten Gastbetriebssysteme finden Sie unter Unterstützte Gäste, virtueller Speicher und Datenträgergrößenbeschränkungen

In diesem Abschnitt werden die Unterschiede bei der Unterstützung virtueller Geräte für die Mitglieder der XenServer-Produktfamilie beschrieben.

Unterstützung für virtuelle Geräte der XenServer-Produktfamilie

Die aktuelle Version der XenServer-Produktfamilie hat einige allgemeine Beschränkungen für virtuelle Geräte für VMs. Für bestimmte Gastbetriebssysteme gelten möglicherweise niedrigere Grenzwerte für bestimmte Funktionen. Der Abschnitt für einzelne Gastinstallationen weist auf die Einschränkungen hin. Ausführliche Informationen zu den Beschränkungen der Konfiguration finden Sie unter Configuration Limits.

Faktoren wie Hardware und Umgebung können die Beschränkungen beeinflussen. Informationen zu unterstützter Hardware finden Sie in der XenServer-Hardwarekompatibilitätsliste.

VM-Block-Geräte XenServer emuliert einen IDE-Bus in Form eines hd⋆ Geräts. Wenn Sie Windows verwenden, wird bei der Installation der XenServer VM Tools ein spezieller I/O-Treiber installiert, der ähnlich wie Linux funktioniert, außer in einer vollständig virtualisierten Umgebung.

CPU-Funktionen

Der CPU-Funktionsumfang eines Pools kann sich ändern, während eine VM läuft, z. B. wenn ein neuer Host zu einem vorhandenen Pool hinzugefügt wird oder wenn die VM auf einen Host in einem anderen Pool migriert wird. Wenn sich der CPU-Funktionsumfang eines Pools ändert, verwendet die VM weiterhin den Funktionsumfang, der beim Start angewendet wurde. Um die VM so zu aktualisieren, dass sie den neuen Funktionsumfang des Pools verwendet, müssen Sie die VM neu starten.

Windows-VMs

April 12, 2024

Für die Installation von Windows-VMs auf dem XenServer-Host ist Unterstützung für Hardwarevirtualisierung (Intel VT oder AMD-V) erforderlich.

> **Hinweis:**
>
> Verschachtelte Virtualisierung wird für Windows-VMs, die auf XenServer gehostet werden, nicht unterstützt.

Grundlegendes Verfahren zum Erstellen einer Windows-VM

Das Installieren eines Windows auf einer VM umfasst die folgenden Schritte:

1. Auswahl der entsprechenden Windows-Vorlage
2. Auswahl des entsprechenden Startmodus
3. Installieren des Windows-Betriebssystems
4. Installation der XenServer VM Tools für Windows (*I/O-Treiber* und *Management Agent*)

> **Warnung:**
>
> Windows-VMs werden nur unterstützt, wenn auf den VMs die XenServer VM Tools für Windows installiert sind.

Windows VM-Vorlagen

Windows-Betriebssysteme werden auf VMs installiert, indem eine entsprechende Vorlage mit XenCenter oder der xe-CLI geklont und anschließend das Betriebssystem installiert wird. In den Vorlagen für einzelne Gäste sind vordefinierte Plattformflags gesetzt, die die Konfiguration der virtuellen

Hardware definieren. Beispielsweise werden alle Windows-VMs mit aktiviertem ACPI-Hardware-Abstraktionslayer-Modus (HAL) installiert. Wenn Sie später eine dieser VMs so ändern, dass sie über mehrere virtuelle CPUs verfügt, schaltet Windows die HAL automatisch in den Multiprozessormodus um.

Die verfügbaren Windows-Vorlagen sind in der folgenden Tabelle aufgeführt:

Vorlagenname	Unterstützte Startmodi	Beschreibung
Windows 10 (64-Bit)	BIOS, UEFI, UEFI-Sicherer Start	Wird zur Installation von Windows 10 (64 Bit) verwendet
Windows 11 (64 Bit)	UEFI, UEFI Secure Boot	Wird zur Installation von Windows 11 (64-Bit) verwendet
Windows Server 2016 (64-Bit)	BIOS, UEFI, UEFI-Sicherer Start	Wird zur Installation von Windows Server 2016 oder Windows Server Core 2016 (64 Bit) verwendet
Windows Server 2019 (64-Bit)	BIOS, UEFI, UEFI-Sicherer Start	Wird zur Installation von Windows Server 2019 oder Windows Server Core 2019 (64 Bit) verwendet
Windows Server 2022 (64 Bit)	BIOS, UEFI, UEFI-Sicherer Start	Wird zur Installation von Windows Server 2022 oder Windows Server Core 2022 (64 Bit) verwendet

XenServer unterstützt alle SKUs (Editionen) für die aufgelisteten Versionen von Windows.

Anhängen einer ISO-Image-Bibliothek

Das Windows-Betriebssystem kann entweder von einer Installations-CD in einem physischen CD-ROM-Laufwerk auf dem XenServer-Host oder von einem ISO-Image installiert werden. Informationen dazu, wie Sie ein ISO-Image von einer Windows-Installations-CD erstellen und zur Verwendung bereitstellen, finden Sie unter Erstellen von ISO-Images .

Erstellen einer VM mit XenCenter

So erstellen Sie eine Windows VM:

1. Klicken Sie auf der XenCenter -Symbolleiste auf die Schaltfläche **Neue VM**, um den Assistenten für neue VM zu öffnen.

   Mit dem Assistenten für neue VM können Sie die neue VM konfigurieren und verschiedene Parameter für CPU-, Speicher- und Netzwerkressourcen anpassen.

2. Wählen Sie eine VM-Vorlage und klicken Sie auf **Weiter**.

   Jede Vorlage enthält die Setup-Informationen, die erforderlich sind, um eine VM mit einem bestimmten Gastbetriebssystem (OS) und mit optimalem Speicher zu erstellen. Diese Liste spiegelt die Vorlagen wider, die XenServer derzeit unterstützt.

   > **Hinweis:**
   >
   > Wenn das Betriebssystem, das Sie auf Ihrer VM installieren, nur mit der Originalhardware kompatibel ist, aktivieren Sie das Kästchen **Host-BIOS-Zeichenfolgen auf VM kopieren** . Sie könnten diese Option beispielsweise für eine Betriebssystem-Installations-CD verwenden, die mit einem bestimmten Computer verpackt wurde.
   >
   > Nachdem Sie eine VM zum ersten Mal gestartet haben, können Sie ihre BIOS-Zeichenfolgen nicht ändern. Stellen Sie sicher, dass die BIOS-Zeichenfolgen korrekt sind, bevor Sie die VM zum ersten Mal starten.

   Informationen zum Kopieren von BIOS-Zeichenfolgen mit der CLI finden Sie unter Installieren von VMs von Reseller Option Kit-Medien (BIOS-gesperrt).

   Fortgeschrittene Benutzer können benutzerdefinierte BIOS-Strings festlegen. Weitere Informationen finden Sie unter Benutzerdefinierte BIOS-Zeichenketten.

3. Geben Sie einen Namen und eine optionale Beschreibung für die neue VM ein.

4. Wählen Sie die Quelle der Betriebssystemmedien aus, die auf der neuen VM installiert werden sollen.

   Die Installation von einer CD/DVD ist die einfachste Option für den Einstieg.

   a) Wählen Sie die Standardoption für die Installationsquelle (DVD-Laufwerk)
   b) Legen Sie den Datenträger in das DVD-Laufwerk des XenServer-Hosts ein

   Mit XenServer können Sie auch Betriebssysteminstallationsmedien aus einer Reihe von Quellen abrufen, einschließlich einer bereits vorhandenen ISO-Bibliothek. Ein ISO-Image ist eine Datei, die alle Informationen enthält, die eine optische Disc (CD, DVD usw.) enthalten würde. In diesem Fall würde ein ISO-Image dieselben Betriebssystemdaten wie eine Windows-Installations-CD enthalten.

   Um eine bereits vorhandene ISO-Bibliothek anzuhängen, klicken Sie auf **Neue ISO-Bibliothek** und geben Sie den Speicherort und den Typ der ISO-Bibliothek an. Sie können dann das spezifische ISO-Medium des Betriebssystems aus der Liste auswählen.

5. Auf der Registerkarte **Installationsmedien** können Sie einen Startmodus für die VM auswählen. Standardmäßig wählt XenCenter den sichersten Startmodus aus, der für die VM-Betriebssystemversion verfügbar ist.

   > **Hinweise:**
   >
   > - Die **UEFI-Boot** - und **UEFI-Secure-Bootoptionen** werden abgeblendet angezeigt, wenn die von Ihnen gewählte VM-Vorlage den UEFI-Start nicht unterstützt.
   > - Sie können den Startmodus nicht ändern, nachdem Sie die VM zum ersten Mal gestartet haben.
   >
   > Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.

6. Ändern Sie bei Bedarf die Option **Neues vTPM erstellen und anhängen**.

   - Für VM-Betriebssysteme, die ein vTPM benötigen, ist die Option ausgewählt und kann nicht abgewählt werden.
   - Für VM-Betriebssysteme, die kein vTPM unterstützen, ist die Option ausgegraut und kann nicht ausgewählt werden.
   - Wählen Sie für VM-Betriebssysteme, die vTPM unterstützen, es aber nicht benötigen, aus, ob ein vTPM an die VM angehängt werden soll.

   Weitere Informationen finden Sie unter vTPM.

7. Wählen Sie einen Homeserver für die VM aus.

   Ein Homeserver ist der Host, der die Ressourcen für eine VM in einem Pool bereitstellt. Wenn Sie einen Homeserver für eine VM nominieren, versucht XenServer, die VM auf diesem Host zu starten. Wenn diese Aktion nicht möglich ist, wird automatisch ein alternativer Host innerhalb desselben Pools ausgewählt. Um einen Home-Server auszuwählen, klicken Sie **auf VM auf diesem Server platzieren** und wählen Sie einen Host aus der Liste aus.

   > **Hinweise:**
   >
   > - In WLB-fähigen Pools wird der nominierte Homeserver nicht zum Starten, Neustarten, Fortsetzen oder Migrieren der VM verwendet. Stattdessen nominiert Workload Balancing den besten Host für die VM, indem es die XenServer-Ressourcenpool-Metriken analysiert und Optimierungen empfiehlt.
   > - Wenn einer VM eine oder mehrere virtuelle GPUs zugewiesen sind, wird die Nominierung des Homeservers nicht wirksam. Stattdessen basiert die Hostnominierung auf der vom Benutzer festgelegten Richtlinie zur Platzierung virtueller GPU.
   > - Beim Rolling Pool-Upgrade wird der Homeserver bei der Migration der VM nicht berücksichtigt. Stattdessen wird die VM zurück auf den Host migriert, auf dem sie sich vor dem Upgrade befand.

Wenn Sie keinen Homeserver nominieren möchten, klicken Sie auf **Dieser VM keinen Homeserver zuweisen**. Die VM wird auf einem beliebigen Host mit den erforderlichen Ressourcen gestartet.

Klicken Sie zum Fortfahren auf **Weiter**.

8. Weisen Sie Prozessor- und Speicherressourcen für die VM zu. Für eine Windows 10-VM (64 Bit) sind die Standardeinstellungen 2 virtuelle CPUs und 4 GB RAM. Sie können auch die Standardeinstellungen ändern. Klicken Sie zum Fortfahren auf **Weiter**.
9. Weisen Sie eine virtuelle GPU zu. Der Assistent für neue VM fordert Sie auf, der VM eine dedizierte GPU oder eine oder mehrere virtuelle GPUs zuzuweisen. Mit dieser Option kann die VM die Rechenleistung der GPU nutzen. Mit dieser Funktion haben Sie eine bessere Unterstützung für professionelle High-End-3D-Grafikanwendungen wie CAD/CAM, GIS und medizinische Bildgebungsanwendungen.
10. Weisen Sie Speicher für die neue VM zu und konfigurieren Sie ihn.

    Klicken Sie auf **Weiter**, um die Standardzuweisung (32 GB) und Konfiguration auszuwählen, oder Sie möchten möglicherweise die folgende zusätzliche Konfiguration durchführen:

    - Ändern Sie den Namen, die Beschreibung oder die Größe Ihres virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.
    - Fügen Sie einen neuen virtuellen Datenträger hinzu, indem Sie **Hinzufügen**auswählen.
11. Konfigurieren Sie das Netzwerk auf der neuen VM.

    Klicken Sie auf **Weiter**, um die Standard-Netzwerkkarte und -konfigurationen auszuwählen, einschließlich einer automatisch erstellten eindeutigen MAC-Adresse für jede Netzwerkkarte. Alternativ möchten Sie möglicherweise die folgende zusätzliche Konfiguration vornehmen:

    - Ändern Sie das physische Netzwerk, die MAC-Adresse oder die Quality of Service (QoS) -Priorität des virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.
    - Fügen Sie eine neue virtuelle Netzwerkkarte hinzu, indem **Sie Hinzufügen**auswählen
12. (Optional) Wenn diese VM als Vorlage mit Citrix Provisioning oder mit gesetztem Flag `reset-on-boot` verwendet werden soll, stellen Sie sicher, dass die Option **Neue VM automatisch starten** nicht ausgewählt ist. Auf diese Weise können Sie vor der Installation von Windows einige erforderliche Konfigurationen vornehmen.
13. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Jetzt erstellen**, um die VM zu erstellen und zur Registerkarte **Suchen** zurückzukehren.

    Ein Symbol für Ihre neue VM wird unter dem Host im Bereich **Ressourcen** angezeigt.
14. (Optional) Wenn diese VM als Vorlage mit Citrix Provisioning verwendet werden soll oder das Flag `reset-on-boot` gesetzt ist, konfigurieren Sie die VM vor der Installation von Windows.

Geben Sie in der Host-Konsole den folgenden Befehl ein:

```
xe vm-param-set uuid=<uuid> has-vendor-device=false
```

Das Flag `has-vendor-device=false` stellt sicher, dass Windows Update nicht versucht, die in den XenServer VM Tools enthaltenen I/O-Treiber zu installieren oder zu aktualisieren. Weitere Informationen finden Sie unter Einstellungen für Citrix Provisioning Provisioning-Ziele oder beim Booten zurückgesetzte Maschinen.

15. Wählen Sie im Bereich **Ressourcen** die VM aus, und klicken Sie dann auf die Registerkarte **Konsole**, um die VM-Konsole anzuzeigen.
16. (Optional) Wenn Sie die VM klonen möchten, empfehlen wir, die Windows-Erstinstallation, die sogenannte Out-Of-Box-Experience (OOBE), nicht auszuführen. Wenn die OOBE stattdessen auf der Seite startet, die nach Regionsinformationen fragt, drücken Sie **Strg + Shift + F3, um in den Auditmodus** zu wechseln.

    Sie können dann Sysprep verwenden, um die VM zu generalisieren. Weitere Informationen finden Sie unter Vorbereiten des Klonens einer Windows-VM mithilfe von Sysprep.

    Wenn Sie nicht beabsichtigen, die VM zu klonen, fahren Sie mit den folgenden Schritten in diesem Verfahren fort.
17. Folgen Sie dem Betriebssystem-Installationsbildschirm und treffen Sie Ihre Auswahl.
18. Installieren Sie XenServer VM Tools für Windows, nachdem die Betriebssysteminstallation abgeschlossen ist und die VM neu gestartet wurde.

Erstellen einer Windows-VM mit der Befehlszeilenschnittstelle

So erstellen Sie eine Windows-VM aus einem ISO-Repository mithilfe der xe CLI:

> **Hinweis:**
>
> Für Windows 10- und Windows 11-VMs wird die Anforderung für ein vTPM durch die Vorlage angegeben. Sie müssen den xe CLI-Befehlen nichts hinzufügen, um das vTPM einzurichten.

1. Erstellen Sie eine VM aus einer Vorlage:

    ```
    xe vm-install new-name-label=<vm_name> template=<template_name>
    <!--NeedCopy-->
    ```

    Dieser Befehl gibt die UUID der neuen VM zurück.
2. (Optional) Ändern Sie den Startmodus der VM.

    ```
    xe vm-param-set uuid=<uuid> HVM-boot-params:firmware=<mode>
    xe vm-param-set uuid=<uuid> platform:secureboot=<option>
    <!--NeedCopy-->
    ```


Der Wert von `mode` kann entweder `BIOS` oder `uefi` sein und ist standardmäßig `uefi`, wenn diese Option für Ihr VM-Betriebssystem unterstützt wird. Andernfalls ist der Standardmodus `BIOS`. Der Wert von `option` kann entweder auf **`true`** oder gesetzt werden **`false`**. Wenn Sie die Option Secure Boot nicht angeben, ist sie standardmäßig auf `auto`eingestellt.

Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.

3. (Optional) Wenn diese VM als Vorlage mit Citrix Provisioning verwendet werden soll oder das Flag `reset-on-boot` gesetzt ist, konfigurieren Sie die VM vor der Installation von Windows.

```
xe vm-param-set uuid=<uuid> has-vendor-device=false
<!--NeedCopy-->
```

Das Flag `has-vendor-device=`**`false`** stellt sicher, dass Windows Update nicht versucht, die in den XenServer VM Tools enthaltenen I/O-Treiber zu installieren oder zu aktualisieren. Weitere Informationen finden Sie unter Einstellungen für Citrix Provisioning Provisioning-Ziele oder beim Booten zurückgesetzte Maschinen.

4. Erstellen Sie ein ISO-Speicher-Repository:

```
xe-mount-iso-sr <path_to_iso_sr>
<!--NeedCopy-->
```

5. Listen Sie alle verfügbaren ISOs auf:

```
xe cd-list
<!--NeedCopy-->
```

6. Legen Sie das angegebene ISO-Image in das virtuelle CD-Laufwerk der angegebenen VM ein:

```
xe vm-cd-add vm=<vm_name> cd-name=<iso_name> device=3
<!--NeedCopy-->
```

7. Starten Sie die VM und installieren Sie das Betriebssystem:

```
xe vm-start vm=<vm_name>
<!--NeedCopy-->
```

Zu diesem Zeitpunkt ist die VM-Konsole in XenCenter sichtbar.

8. Wählen Sie in XenCenter im Bereich **Resources** die VM aus und klicken Sie dann auf die Registerkarte **Konsole**, um die VM-Konsole anzuzeigen.

9. (Optional) Wenn Sie die VM klonen möchten, empfehlen wir, die Windows-Erstinstallation, die sogenannte Out-Of-Box-Experience (OOBE), nicht auszuführen. Wenn die OOBE stattdessen auf der Seite startet, die nach Regionsinformationen fragt, drücken Sie **Strg + Shift + F3, um in den Auditmodus** zu wechseln.

Sie können dann Sysprep verwenden, um die VM zu generalisieren. Weitere Informationen finden Sie unter Vorbereiten des Klonens einer Windows-VM mithilfe von Sysprep.

Wenn Sie nicht beabsichtigen, die VM zu klonen, fahren Sie mit den folgenden Schritten in diesem Verfahren fort.

10. Folgen Sie dem Betriebssystem-Installationsbildschirm und treffen Sie Ihre Auswahl.
11. Nachdem die Betriebssysteminstallation abgeschlossen und die VM neu gestartet wurde, installieren Sie die XenServer VM Tools für Windows.

Weitere Informationen zur Verwendung der CLI finden Sie unter Befehlszeilenschnittstelle.

Installieren Sie die XenServer VM Tools für Windows

XenServer VM Tools für Windows bieten leistungsstarke I/O-Dienste ohne den Aufwand herkömmlicher Geräteemulation. Weitere Informationen zu den XenServer VM Tools für Windows und zur erweiterten Verwendung finden Sie unter XenServer VM Tools fürWindows.

> **Hinweis:**
>
> Um XenServer VM Tools für Windows auf einer Windows-VM zu installieren, muss auf der VM Microsoft.NET Framework Version 4.0 oder höher ausgeführt werden.

Stellen Sie vor der Installation der XenServer VM Tools für Windows sicher, dass Ihre VM so konfiguriert ist, dass sie die I/O-Treiber von Windows Update empfängt. Windows Update ist die empfohlene Methode, um Updates für die I/O-Treiber zu erhalten. Wenn Windows Update jedoch keine verfügbare Option für Ihre VM ist, können Sie Updates für die I/O-Treiber auch auf andere Weise erhalten. Weitere Informationen finden Sie unter XenServer VM Tools für Windows.

So installieren Sie die XenServer VM Tools für Windows:

1. Wir empfehlen, dass Sie einen Snapshot Ihrer VM erstellen, bevor Sie die XenServer VM Tools installieren oder aktualisieren.
2. Laden Sie die Datei XenServer VM Tools für Windows von der XenServer-Downloadseiteherunter.
3. Überprüfen Sie Ihren Download anhand des angegebenen SHA256-Werts.
4. Kopieren Sie die Datei auf Ihre Windows-VM oder auf ein freigegebenes Laufwerk, auf das die Windows-VM zugreifen kann.
5. Führen Sie die `managementagentxXX.msi` Datei aus, um mit der Installation der XenServer VM Tools zu beginnen.

   ```
   1 Msiexec.exe /package managementagentxXX.msi
   ```

6. Befolgen Sie die Anweisungen im Installationsprogramm.

   a) Folgen Sie den Anweisungen des Assistenten, um die Lizenzvereinbarung zu akzeptieren, und wählen Sie einen Zielordner aus.

b) Der Assistent zeigt die empfohlenen Einstellungen auf der Seite mit den **Installations- und Update einstellungen** an. Informationen zum Anpassen dieser Einstellungen finden Sie unter XenServer VM Tools für Windows.

c) Klicken Sie auf **Weiter** und dann auf **Installieren**, um mit der Installation der XenServer VM Tools für Windows zu beginnen.

7. Starten Sie die VM neu, wenn Sie aufgefordert werden, den Installationsvorgang abzuschließen.

vTPM

Mit XenServer können Sie ein virtuelles Trusted Platform Module (vTPM) erstellen und es an Ihre Windows 10- oder Windows 11-VM anhängen.

Windows 11-VMs erfordern das Vorhandensein eines verknüpften vTPM. Dieses vTPM wird automatisch erstellt, wenn die Windows 11-VM aus der bereitgestellten Vorlage erstellt wird. Für Windows 10-VMs ist das vTPM optional.

Eine VM hat eine Eins-zu-Eins-Beziehung zu ihrem verknüpften vTPM. Eine VM kann nur ein vTPM haben und ein vTPM kann nur einer einzelnen VM zugeordnet werden. Benutzer mit den Rollen VM Admin und höher können vTPM-Instanzen erstellen und löschen.

Anwendungen, die auf der VM ausgeführt werden, können über die TPM 2.0-kompatible API auf das vTPM zugreifen. TPM 1.2 wird nicht unterstützt. Benutzer mit den Rollen VM Operator und höher können über die VM auf das vTPM zugreifen.

Um zu überprüfen, ob Ihre VM über ein verknüpftes vTPM verfügt, wechseln Sie in XenCenter zur Registerkarte **Allgemein** und suchen Sie im Abschnitt **Gerätesicherheit** nach.

Einschränkungen

Die folgenden Einschränkungen gelten derzeit für VMs, die mit einem angehängten vTPM erstellt wurden:

- Sie können Ihre VMs zwar in das OVF/OVA-Format exportieren, aber alle Daten in Ihrem vTPM gehen dabei verloren. Diese verlorenen Daten können dazu führen, dass die VM unerwartetes Verhalten zeigt oder dass sie nicht gestartet werden kann. Wenn Sie vTPM-Funktionen in der VM verwenden, exportieren Sie Ihre VMs nicht in diesem Format.
- BitLocker wird derzeit nicht für VMs mit angehängtem vTPM unterstützt.
- HA wird derzeit nicht für VMs unterstützt, an die ein vTPM angehängt ist.
- Sie können keine Snapshots oder Checkpoints für eine unterbrochene VM erstellen, an die ein vTPM angehängt ist.

Bekannte Probleme

- Wenn Sie viele VMs mit einem vTPM haben, kann es zu den folgenden Verhaltensweisen kommen:
  - Die XAPI-Datenbank wird groß und verbraucht viel Speicher.
  - VM-Schreibvorgänge in das vTPM können zu einem Engpass im Toolstack führen.
- vTPM-Operationen, die vom Benutzer oder von Windows im Hintergrund ausgeführt werden, können in den folgenden Situationen fehlschlagen:
  - Wenn der Toolstack oder der XenServer-Host abstürzt, bevor der Vorgang mit der Datenträger synchronisiert wird. Fehler beim Schreiben auf den Datenträger werden ignoriert.

  Bei einem solchen Fehler gibt das vTPM einen Fehler an das Betriebssystem zurück. Windows protokolliert diese Fehler im Systemereignisprotokoll.

Hängen Sie ein vTPM an eine Windows-VM an

Für neue Windows 11-VMs und Windows 10-VMs kann das vTPM während der VM-Erstellung hinzugefügt werden. Weitere Informationen finden Sie in der Dokumentation zu Ihrer bevorzugten VM-Erstellungsmethode.

Wenn Sie eine vorhandene UEFI- oder UEFI Secure Boot Windows 10-VM haben, zu der Sie ein vTPM hinzufügen möchten, können Sie dies mithilfe von XenCenter oder mithilfe der xe-CLI tun. Wenn Sie das Betriebssystem der VM auf ein Betriebssystem aktualisieren möchten, das ein vTPM erfordert, müssen Sie das vTPM an die VM anhängen, *bevor* Sie Ihr VM-Betriebssystem aktualisieren.

Durch die Verwendung von XenCenter

1. Fahren Sie die Windows 10-VM herunter.
2. Fügen Sie der VM ein vTPM hinzu.
   a) Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **vTPMs verwalten**aus. Oder gehen Sie in der Hauptmenüleiste zu **VM > Manage vTPMs**. Das Dialogfeld **TPM Manager** wird geöffnet.
   b) Fügen Sie im Dialogfeld **TPM Manager** ein vTPM hinzu.
3. Um zu überprüfen, ob die VM über ein verknüpftes vTPM verfügt, wählen Sie die VM aus, wechseln Sie zur Registerkarte **Allgemein** und suchen Sie im Abschnitt **Gerätesicherheit** nach.
4. Starten Sie die Windows 10-VM.

Mit der Xe-CLI

1. Fahren Sie die VM herunter:

```
xe vm-shutdown uuid=<vm_uuid>
<!--NeedCopy-->
```

2. Erstellen Sie ein vTPM und hängen Sie es an die VM an:

```
xe vtpm-create vm-uuid=<vm_uuid>
<!--NeedCopy-->
```

3. Starten Sie die VM:

```
xe vm-start uuid=<vm_uuid>
<!--NeedCopy-->
```

Aktualisieren Sie das Windows-Betriebssystem in Ihrer VM

Upgrades auf VMs sind normalerweise erforderlich, wenn Sie auf eine neuere Version von XenServer umsteigen.

Bevor Sie Ihre Windows-VM aktualisieren

1. Wenn Sie Ihr Betriebssystem auf eine Version von Windows aktualisieren, für die ein vTPM erforderlich ist (z. B. Windows 11), müssen Sie ein vTPM an Ihre VM anhängen, bevor Sie das Betriebssystem aktualisieren. Weitere Informationen finden Sie unter Anhängen eines vTPM an eine Windows-VM.
2. Aktualisieren Sie XenServer VM Tools für Windows auf die neueste Version auf der VM. Weitere Informationen finden Sie unter XenServer VM Tools für Windows.

   Wir empfehlen, dass Sie die XenServer VM Tools nicht von Ihrer Windows-VM entfernen, bevor Sie die Version von Windows auf der VM automatisch aktualisieren.

Aktualisieren Sie das Windows-Betriebssystem

Sie können Ihre Windows-VMs auf eine der folgenden Arten aktualisieren:

- Verwenden Sie Windows Update, um die Version des Windows-Betriebssystems auf Ihren Windows-VMs zu aktualisieren. Wenn Sie Windows Update verwenden, um Ihre XenServer VM Tools zu aktualisieren, empfehlen wir Ihnen, diese Methode zu verwenden.
- Verwenden Sie das Windows-Installations-ISO für die neueren Versionen. Windows-Installationsdatenträger bieten normalerweise eine Upgrade-Option, wenn Sie sie auf einem Server starten, auf dem bereits eine frühere Version von Windows installiert ist.

Folgen Sie in Ihrer Windows-VM-Konsole den Upgrade-Anweisungen von Windows.

Vorbereiten des Klonens einer Windows-VM mithilfe von Sysprep

Die einzige unterstützte Methode zum Klonen einer Windows-VM ist die Verwendung des Windows-Hilfsprogramms `sysprep` zur Vorbereitung der VM.

Das `sysprep`-Hilfsprogramm ändert die SID des lokalen Computers, sodass sie für jeden Computer eindeutig ist. Die `sysprep`-Binärdateien sind im Ordner `C:\Windows\System32\Sysprep`.

Weitere Informationen zur Verwendung von Sysprep finden Sie unter Sysprep (Generalisieren) einer Windows-Installation.

So führen Sie Sysprep auf einer Windows-VM aus:

> **Hinweis:**
>
> Unter Windows 10 und 11 installiert Windows bei der Ersteinrichtung oder mit Out-Of-Box-Experience (OOBE) Anwendungen (wie AppX), die den Prozess `sysprep` stören können. Aufgrund dieses Verhaltens empfehlen wir, beim Erstellen einer klonbaren VM die Erstinstallation zu überspringen und Windows stattdessen im Überwachungsmodus zu starten.

1. Erstellen Sie eine Windows-VM.
2. Installieren Sie Windows.
3. (Optional) Wenn die Out-Of-Box-Experience (OOBE) auf der Seite startet, die nach Regionsinformationen fragt, drücken Sie **Strg**+ Shift + F3. Windows wird im Überwachungsmodus gestartet. Weitere Informationen finden Sie unter Starten von Windows im Überwachungsmodus oder OOBE.

   Es ist zwar nicht erforderlich, wir empfehlen jedoch, OOBE zu beenden, um zu vermeiden, dass ein unnötiges Benutzerkonto auf dem Image erstellt wird und Probleme mit der Kompatibilität von Drittanbieter-Anwendungen vermieden werden. Wenn Sie mit OOBE fortfahren, verhindern einige Anwendungen oder Windows-Updates, die während OOBE installiert werden, möglicherweise den ordnungsgemäßen Betrieb von Sysprep.
4. Installieren Sie die neueste Version von XenServer VM Tools für Windows.
5. Installieren Sie alle Anwendungen und führen Sie alle anderen erforderlichen Konfigurationen durch.
6. Führen Sie den Befehl `sysprep` aus, um die VM zu generalisieren. Dieses Hilfsprogramm fährt die VM herunter, wenn sie abgeschlossen ist.

> **Hinweis:**
>
> Starten Sie die ursprüngliche, generalisierte VM (die Quell-VM) nach der `sysprep`-Phase nicht erneut. Konvertieren Sie es anschließend sofort in eine Vorlage, um Neustarts zu verhindern. Wenn die Quell-VM neu gestartet wird, muss `sysprep` neu ausgeführt werden, bevor sie sicher zum Erstellen weiterer Klone verwendet werden kann.

So klonen Sie eine generalisierte Windows-VM:

1. Konvertieren Sie mit XenCenter die VM in eine Vorlage.
2. Klonen Sie die neu erstellte Vorlage nach Bedarf in neue VMs.
3. Wenn die geklonte VM gestartet wird, führt sie die folgenden Aktionen aus, bevor sie verwendet werden kann:
    - Es erhält eine neue SID und einen neuen Namen
    - Es führt ein Setup aus, um bei Bedarf zur Eingabe von Konfigurationswerten aufzufordern
    - Schließlich wird es neu gestartet

Windows VM Versionshinweise

Es gibt viele Versionen und Varianten von Windows mit unterschiedlicher Unterstützung für die von XenServer bereitgestellten Funktionen. In diesem Abschnitt werden Hinweise und Errata für die bekannten Unterschiede aufgeführt.

Allgemeine Windows Probleme

- Beginnen Sie bei der Installation von Windows-VMs mit nicht mehr als drei virtuellen Datenträgern. Nachdem die VM und die XenServer VM Tools für Windows installiert wurden, können Sie zusätzliche virtuelle Datenträger hinzufügen. Stellen Sie sicher, dass das Startgerät immer einer der ersten Datenträger ist, damit die VM ohne die XenServer VM Tools für Windows erfolgreich gestartet werden kann.
- Wenn der Startmodus für eine Windows-VM das BIOS-Boot ist, formatiert Windows den primäre Datenträger mit einem Master Boot Record (MBR). MBR begrenzt den maximal adressierbaren Speicherplatz einem Datenträger auf 2 TiB. Um einen Datenträger, der größer als 2 TiB ist, mit einer Windows-VM zu verwenden, führen Sie eine der folgenden Aktionen aus:
    - Wenn UEFI-Start für die Version von Windows unterstützt wird, stellen Sie sicher, dass Sie UEFI als Startmodus für die Windows-VM verwenden.
    - Erstellen Sie den großen Datenträger als sekundären Datenträger für die VM und wählen Sie das Format GUID Partition Table (GPT) aus.

- Mehrere vCPUs sind als CPU-Sockets für Windows-Gäste verfügbar und unterliegen den in der VM vorhandenen Lizenzbeschränkungen. Die Anzahl der im Gast vorhandenen CPUs kann im Geräte-Manager überprüft werden. Die Anzahl der CPUs, die tatsächlich von Windows verwendet werden, kann im Task-Manager angezeigt werden.
- Die Reihenfolge der Datenträgerenumerierung in einem Windows-Gast kann sich von der Reihenfolge unterscheiden, in der sie ursprünglich hinzugefügt wurden. Dieses Verhalten ist auf die Interaktion zwischen den I/O-Treibern und dem Plug-and-Play-Subsystem in Windows zurückzuführen. Beispielsweise könnte der erste Datenträger als `Disk 1` angezeigt werden, der nächste Datenträger im laufenden Betrieb als `Disk 0`, ein späterer Datenträger als `Disk 2` und dann weiter wie erwartet.
- Ein Fehler im DirectX-Backend des VLC-Players ersetzt während der Videowiedergabe Gelb durch Blau, wenn die Windows-Anzeigeeigenschaften auf 24-Bit-Farbe eingestellt sind. VLC, der OpenGL als Back-End verwendet, funktioniert korrekt, und jeder andere DirectX- oder OpenGL-basierte Videoplayer funktioniert ebenfalls. Es ist kein Problem, wenn der Gast eher 16-Bit-Farbe als 24 verwendet.
- Der PV-Ethernet-Adapter meldet eine Geschwindigkeit von 100 Gbit/s in Windows-VMs. Diese Geschwindigkeit ist ein künstlicher fest codierter Wert und in einer virtuellen Umgebung nicht relevant, da die virtuelle Netzwerkkarte mit einem virtuellen Switch verbunden ist. Die Windows-VM verwendet die volle Geschwindigkeit, die verfügbar ist, aber das Netzwerk kann möglicherweise nicht die vollen 100 Gbit/s erreichen.
- Wenn Sie versuchen, eine unsichere RDP-Verbindung zu einer Windows-VM herzustellen, schlägt diese Aktion möglicherweise mit der folgenden Fehlermeldung fehl: “Dies könnte auf die Oracle-Wiederherstellung der CredSSP-Verschlüsselung zurückzuführen sein. “Dieser Fehler tritt auf, wenn das Update des Credential Security Support Provider-Protokolls (CredSSP) nur auf einen der Clients und Server in der RDP-Verbindung angewendet wird. Weitere Informationen finden Sie unter https://support.microsoft.com/en-gb/help/4295591/credssp-encryption-oracle-remediation-error-when-to-rdp-to-azure-vm.

XenServer VM-Tools für Windows

April 13, 2024

XenServer VM Tools (früher Citrix VM Tools oder XenServer PV Tools) für Windows bieten leistungsstarke I/O-Dienste ohne den Aufwand herkömmlicher Geräteemulation. XenServer VM Tools für Windows bestehen aus I/O-Treibern (auch bekannt als paravirtualisierte Treiber oder PV-Treiber) und dem Management Agent.

XenServer VM Tools für Windows müssen auf jeder Windows-VM installiert sein, damit die VM eine vollständig unterstützte Konfiguration hat. Eine VM funktioniert ohne sie, aber die Leistung wird beeinträchtigt.

Die Version der XenServer VM Tools für Windows wird unabhängig von der Version von XenServer aktualisiert. Stellen Sie sicher, dass Ihre XenServer VM Tools für Windows regelmäßig auf die neueste Version aktualisiert werden, sowohl in Ihren VMs als auch in allen Vorlagen, die Sie zum Erstellen Ihrer VMs verwenden. Weitere Informationen zur neuesten Version der Tools finden Sie unter Neuigkeiten.

Installieren Sie die XenServer VM Tools

> **Hinweis:**
>
> Um XenServer VM Tools für Windows auf einer Windows-VM zu installieren, muss auf der VM Microsoft.NET Framework Version 4.0 oder höher ausgeführt werden.

Die XenServer VM Tools für Windows werden standardmäßig im `C:\Program Files\XenServer\XenTools` Verzeichnis auf der VM installiert.

So installieren Sie die XenServer VM Tools für Windows:

1. Wir empfehlen, dass Sie einen Snapshot Ihrer VM erstellen, bevor Sie die XenServer VM Tools installieren oder aktualisieren.
2. Laden Sie die Datei XenServer VM Tools für Windows von der XenServer-Downloadseiteherunter.
3. Überprüfen Sie Ihren Download anhand des angegebenen SHA256-Werts.
4. Kopieren Sie die Datei auf Ihre Windows-VM oder auf ein freigegebenes Laufwerk, auf das die Windows-VM zugreifen kann.
5. Führen Sie die `managementagentx64.msi` Datei aus, um mit der Installation der XenServer VM Tools zu beginnen.

   ```
   1 Msiexec.exe /package managementagentx64.msi
   ```

6. Befolgen Sie die Anweisungen im Installationsprogramm.

   - Folgen Sie den Anweisungen des Assistenten, um die Lizenzvereinbarung zu akzeptieren, und wählen Sie einen Zielordner aus.
   - Passen Sie die Einstellungen auf der Seite **Einstellungen für Installation und Updates** an.

     Standardmäßig zeigt der Assistent die folgenden empfohlenen Einstellungen an:

     - Installieren Sie jetzt I/O-Treiber

    * Wenn für die VM `has-vendor-device=true` eingestellt ist, ist diese Option nicht ausgewählt, da die I/O-Treiber bereits von Windows Update installiert wurden.
    * WENN für die VM `has-vendor-device=false` eingestellt ist, ist diese Option ausgewählt.
  - Automatische Management Agent-Updates zulassen
  - Automatische I/O-Treiberupdates durch den Management Agent verbieten
  - Senden Sie anonyme Nutzungsinformationen an Cloud Software Group, Inc.

  Für einige Anwendungsfälle werden unterschiedliche Update einstellungen empfohlen. Weitere Informationen finden Sie unter Aktualisieren der XenServer VM Tools.

  Um das Update seinstellungen zu konfigurieren, können Sie die folgenden Änderungen vornehmen:

  - Wenn Sie die automatische Aktualisierung des Management Agents nicht zulassen möchten, wählen Sie in der Liste die Option **Automatische Management Agent-Updates** verbieten aus.
  - Wenn Sie dem Management Agent erlauben möchten, die I/O-Treiber automatisch zu aktualisieren, wählen Sie **Automatische I/O-Treiberupdates durch den Management Agent zulassen** aus. Wir empfehlen jedoch, dass Sie Windows Update verwenden, um die I/O-Treiber zu aktualisieren, nicht den Management Agent. Wenn Sie ausgewählt haben, I/O-Treiberupdates über den Windows Update-Mechanismus zu erhalten, erlauben Sie dem Management Agent nicht, die E/A-Treiber automatisch zu aktualisieren.
  - Wenn Sie keine anonymen Nutzungsinformationen mit uns teilen möchten, deaktivieren Sie das Kontrollkästchen **Anonyme Nutzungsinformationen an Cloud Software Group, Inc. senden.** Ankreuzfeld. Die an die Cloud Software Group übermittelten Informationen enthalten die ersten vier Zeichen der UUID der VM, die das Update anfordert. Es werden keine weiteren Informationen über die VM gesammelt oder übertragen.

- Klicken Sie auf **Weiter** und dann auf **Installieren**, um mit der Installation der XenServer VM Tools für Windows zu beginnen.

7. Starten Sie die VM neu, wenn Sie aufgefordert werden, den Installationsvorgang abzuschließen.

   Kunden, die die XenServer VM Tools für Windows oder den Management Agent über RDP installieren, sehen die Neustartaufforderung möglicherweise nicht, da sie nur in der Windows-Konsolensitzung angezeigt wird. Um sicherzustellen, dass Sie Ihre VM neu starten (falls erforderlich) und um Ihre VM in einen optimierten Zustand zu versetzen, geben Sie die Option Neustart erzwingen in RDP an. Die Option Neustart erzwingen startet die VM nur dann neu, wenn sie erforderlich ist, um die VM in einen optimierten Zustand zu versetzen.

> **Warnung:**
>
> Die Installation oder Aktualisierung der XenServer VM Tools für Windows kann dazu führen, dass sich der Anzeigename und die ID einiger Netzwerkadapter ändern. Jede Software, die für die Verwendung eines bestimmten Adapters konfiguriert ist, muss möglicherweise nach der Installation oder dem Upgrade von XenServer VM Tools für Windows neu konfiguriert werden.

Automatische Installation

Führen Sie einen der folgenden Befehle aus, um die XenServer VM Tools für Windows im Hintergrund zu installieren und zu verhindern, dass das System neu gestartet wird:

```
Msiexec.exe /package managementagentx64.msi /quiet /norestart
<!--NeedCopy-->
```

Oder

```
Setup.exe /quiet /norestart
<!--NeedCopy-->
```

Eine nicht interaktive, aber nicht stille Installation kann erhalten werden, indem Sie Folgendes ausführen:

```
Msiexec.exe managementagentx64.msi /passive
<!--NeedCopy-->
```

Oder

```
Setup.exe /passive
<!--NeedCopy-->
```

> **Hinweise:**
>
> - Der Parameter `/quiet` gilt nur für die Installationsdialoge, aber nicht für die Installation des Gerätetreibers. Wenn der Parameter `/quiet` angegeben ist, fordert die Gerätetreiberinstallation bei Bedarf die Berechtigung zum Neustart an.
>   - Wenn `/quiet /norestart` angegeben ist, wird das System nicht neu gestartet, nachdem die gesamte Tools-Installation abgeschlossen ist. Dieses Verhalten ist unabhängig davon, was der Benutzer im Reboot-Dialog angibt.
>   - Wenn `/quiet /forcerestart` angegeben ist, kann der Upgrade- oder Installationsvorgang mehrere Neustarts auslösen. Dieses Verhalten ist unabhängig davon, was der Benutzer im Reboot-Dialog angibt.
>   - Wenn die Gerätetreiberinstallation die Berechtigung zum Neustart anfordert, kann eine Tools-Installation mit dem angegebenen Parameter `quiet` weiterhin ausgeführt

> werden. Verwenden Sie den Task-Manager, um zu überprüfen, ob das Installationsprogramm noch läuft.

Um die Installationseinstellungen anzupassen, verwenden Sie die folgenden Parameter mit den Befehlen für die unbeaufsichtigte Installation:

Parameter	Zulässige Werte	Standard	Beschreibung
ALLOWAUTOUPDATE	JA oder NEIN	JA	Automatische Management Agent-Updates zulassen
ALLOWDRIVERINSTALL	JA oder NEIN	JA	Installieren Sie jetzt die I/O-Treiber
ALLOWDRIVERUPDATE	JA oder NEIN	NEIN	Erlauben Sie den automatischen Management Agent-Updates, aktualisierte Treiber zu installieren
IDENTIFYAUTOUPDATE	JA oder NEIN	JA	Senden Sie uns anonyme Nutzungsinformationen

Um beispielsweise eine automatische Installation der Tools durchzuführen, die keine zukünftigen automatischen Management Agent-Updates zulässt und keine anonymen Informationen an Cloud Software Group, Inc. sendet, führen Sie einen der folgenden Befehle aus:

```
1 Msiexec.exe /package managementagentx64.msi ALLOWAUTOUPDATE=NO
     IDENTIFYAUTOUPDATE=NO /quiet /norestart
2 <!--NeedCopy-->
```

Bei interaktiven, unbeaufsichtigten und passiven Installationen kann es nach dem nächsten Systemneustart zu mehreren automatisierten Neustarts kommen, bevor die XenServer VM Tools für Windows vollständig installiert sind. Dieses Verhalten ist auch bei Installationen mit dem angegebenen Flag `/norestart` der Fall. Bei Installationen, bei denen das Flag `/norestart` bereitgestellt wird, kann der erste Neustart jedoch manuell eingeleitet werden.

Aktualisieren Sie die XenServer VM Tools

Stellen Sie sicher, dass Ihre XenServer VM Tools für Windows regelmäßig auf die neueste Version aktualisiert werden, sowohl in Ihren VMs als auch in allen Vorlagen, die Sie zum Erstellen Ihrer VMs ver-

wenden. Wir empfehlen, dass Sie einen Snapshot Ihrer VM erstellen, bevor Sie die XenServer VM Tools aktualisieren. Weitere Informationen zur neuesten Version der Tools finden Sie unter Neuigkeiten.

> **Wichtig:**
>
> Stellen Sie sicher, dass alle angeforderten VM-Neustarts im Rahmen des Updates abgeschlossen sind. Möglicherweise sind mehrere Neustarts erforderlich. Wenn nicht alle angeforderten Neustarts abgeschlossen sind, zeigt die VM möglicherweise ein unerwartetes Verhalten.

XenServer bietet automatische Updatemechanismen für jede seiner Komponenten:

- Der Management Agent kann sich automatisch selbst aktualisieren
- Die I/O-Treiber können entweder vom Management Agent oder über Windows Update aktualisiert werden.

Alternativ können Sie eine oder beide dieser Komponenten manuell aktualisieren.

das Update smethode, die für jede Komponente der Tools ausgewählt werden muss, kann von Ihrer Umgebung abhängen.

Empfohlene Update einstellungen

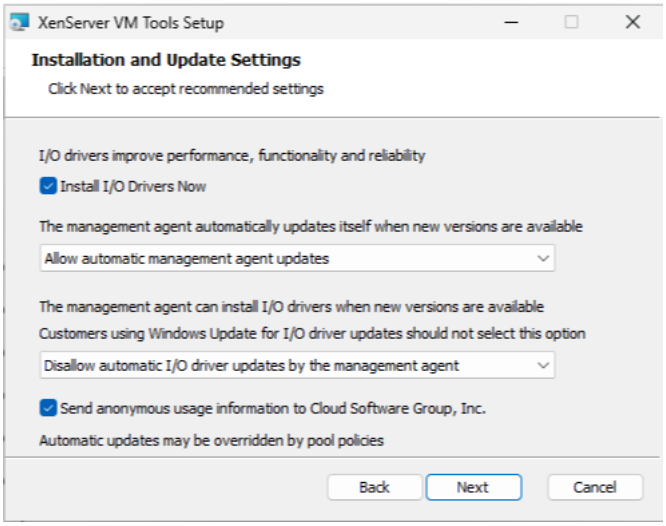
Für die meisten Anwendungsfälle empfehlen wir, die folgenden Einstellungen für das Update der verschiedenen Komponenten der XenServer VM Tools für Windows zu verwenden:

1. Aktivieren Sie Management Agent-Updates.
2. Halten Sie den Management Agent davon ab, die I/O-Treiber zu aktualisieren.
3. Setzen Sie den Wert des folgenden Registrierungsschlüssels auf einen REG_DWORD-Wert von ‘3’:. `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`

   Weitere Informationen finden Sie unter ### Automatische Neustarts.
4. Stellen Sie die I/O-Treiber so ein, dass sie über Windows Update aktualisiert werden.

Während der Installation:

Die ersten beiden Einstellungen sind die Standardeinstellungen, wenn Sie das Installationsprogramm ausführen:



Einstellungen für Citrix Provisioning Provisioning-Ziele oder beim Booten zurückgesetzte Maschinen

Wenn Sie beabsichtigen, Ihre Windows-VM als Citrix Provisioning Provisioning-Ziel zu verwenden oder wenn das Reset-On-Boot-Flag gesetzt ist, können Sie keinen der automatisierten Update mechanismen verwenden. Wir empfehlen, dass Sie die folgende Konfiguration in der Master-Vorlage festlegen, die Sie zum Erstellen dieser VMs verwenden:

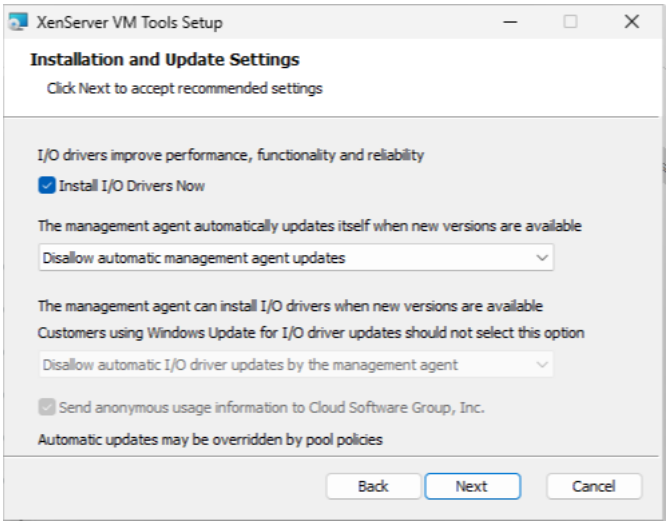
1. Stellen Sie bei der Erstellung Ihrer VM sicher, dass das Flag `has-vendor-device` auf **`false`** gesetzt ist.

   Weitere Informationen finden Sie unter Erstellen einer Windows-VM mithilfe der CLI.

2. Deaktivieren Sie Management Agent-Updates.

Während der Installation:

Geben Sie diese Konfiguration an, wenn Sie die XenServer VM Tools zum ersten Mal installieren:



Einstellungen für automatische Updates nur durch den Management Agent

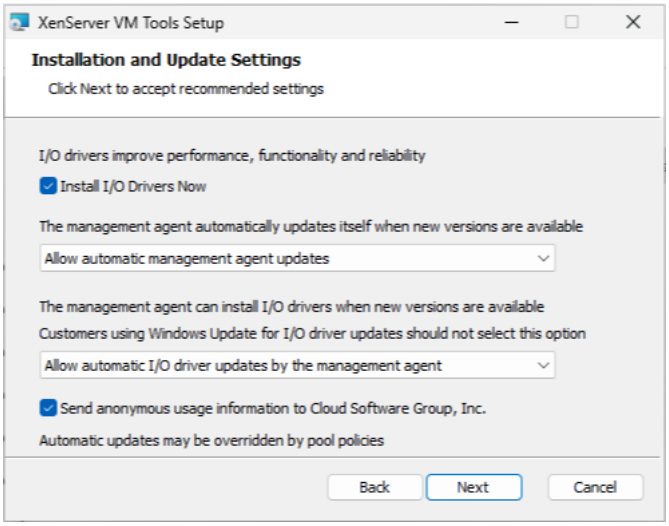
Sie können den Management Agent so konfigurieren, dass er sowohl sich selbst als auch die I/O-Treiber aktualisiert. Wenn Sie diese Konfiguration verwenden, stellen Sie sicher, dass die VMs daran gehindert werden, die I/O-Treiber über Windows Update zu aktualisieren. Wenn beide Mechanismen versuchen, die I/O-Treiber zu aktualisieren, kann dies zu unnötigen Updates führen.

Wählen Sie diesen Ansatz, wenn Ihre Organisation verlangt, dass Sie alle Updates überprüfen, bevor Sie sie auf Ihre Windows-VMs anwenden. In diesem Fall müssen Sie auch den Management Agent umleiten, um seine Updates von einem internen Server abzurufen.

1. Deaktivieren Sie das Update der I/O-Treiber über Windows Update.
2. Stellen Sie den Management Agent so ein, dass er die I/O-Treiber aktualisiert.
3. (Optional) Leiten Sie die Management Agent-Updatesum.

Während der Installation:

Geben Sie diese Konfiguration an, wenn Sie die XenServer VM Tools zum ersten Mal installieren:



Aktualisieren des Management-Agenten

Mit XenServer können Sie den Management Agent sowohl auf neuen als auch auf vorhandenen Windows-VMs automatisch aktualisieren. XenServer ermöglicht standardmäßig die automatische Aktualisierung des Management Agents. Allerdings erlaubt es dem Management Agent nicht, die E/A-Treiber automatisch zu aktualisieren. Sie können die Einstellungen für das Management Agent-Update während der Installation von XenServer VM Tools für Windows anpassen. Die automatische Aktualisierung des Management Agents erfolgt nahtlos und startet die VM nicht neu. In Szenarien, in denen ein Neustart der VM erforderlich ist, wird auf der Registerkarte Konsole der VM eine Meldung angezeigt, die Benutzer über die erforderliche Aktion informiert.

Sie können die Management Agent-Updates automatisch abrufen, sofern die Windows-VM Zugriff auf das Internet hat.

Verwalten automatischer Updates über die CLI Mit XenServer können Sie die Befehlszeile verwenden, um die automatische Aktualisierung der I/O-Treiber und des Management Agents zu verwalten. Sie können `msiexec.exe` mit den in der folgenden Tabelle aufgeführten Argumenten ausführen, um anzugeben, ob die I/O-Treiber und der Management Agent automatisch aktualisiert werden. Informationen zur Installation von XenServer VM Tools für Windows mithilfe von `msiexec.exe` finden Sie unter Automatische Installation.

> **Hinweis:**
>
> Bei VMs, die entweder mit PVS oder MCS verwaltet werden, werden automatisierte Updates automatisch ausgeschaltet, wenn der Citrix Virtual Desktops VDA vorhanden ist und meldet, dass die Maschine nicht persistent ist.

Argument	Werte	Beschreibung
ALLOWAUTOUPDATE	JA/NEIN	Zulassen/Verbieten der automatischen Aktualisierung des Management Agents
ALLOWDRIVERINSTALL	JA/NEIN	Erlauben/verbieten Sie dem XenServer VM Tools for Windows-Installationsprogramm die Installation von I/O-Treibern
ALLOWDRIVERUPDATE	JA/NEIN	Erlauben/verbieten dem Management Agent, die I/O-Treiber automatisch zu aktualisieren
IDENTIFYAUTOUPDATE	JA/NEIN	Erlauben/verbieten Sie, dass der automatische Update mechanismus anonyme Nutzungsinformationen an uns sendet

Beispiel:

```
setup.exe  /passive /forcerestart ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
     ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
<!--NeedCopy-->
```

Management Agent-Updates aktivieren Gehen Sie wie folgt vor, um die automatische Aktualisierung des Management Agents auf VM-Basis zu aktivieren:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.
2. Führen Sie den folgenden Befehl aus:

   ```
   reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t
      REG_DWORD /v DisableAutoUpdate /d 0
   <!--NeedCopy-->
   ```

3. Stellen Sie sicher, dass Management Agent-Updates von Ihrem Pool zugelassen werden. Führen Sie in der Host-Konsole den folgenden Befehl aus:

   ```
   xe pool-param-set uuid=pooluuid guest-agent-config:
      auto_update_enabled=true
   <!--NeedCopy-->
   ```


Management Agent-Updates deaktivieren So deaktivieren Sie die automatische Aktualisierung des Management Agents pro VM:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t
   REG_DWORD /v DisableAutoUpdate /d 1
<!--NeedCopy-->
```

Um die automatische Aktualisierung des Management Agents auf Pool-Basis zu deaktivieren, führen Sie den folgenden Befehl in der Host-Konsole aus:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=
   false
<!--NeedCopy-->
```

Umleiten der Management Agent-Updates XenServer ermöglicht es Kunden, Management Agent-Updates vor der Installation auf einen internen Webserver umzuleiten. Mit dieser Umleitung können Kunden die Updates überprüfen, bevor sie automatisch auf der VM installiert werden.

Der Management Agent verwendet ein Updatesdatei, um Informationen über die verfügbaren Updates abzurufen. Der Name dieser Update-Datei hängt von der Version des Management Agents ab, die Sie verwenden:

- Verwenden Sie für Management Agent 9.2.1.35 und höher https://pvupdates.vmd.citrix.com/autoupdate.v1.json.
- Für Management Agent 9.0.0.0 bis 9.2.0.27 https://pvupdates.vmd.citrix.com/updates.v9.json.

Führen Sie die folgenden Schritte aus, um die Management Agent-Updates umzuleiten:

1. Laden Sie die Update-Datei herunter.
2. Laden Sie die Management Agent MSI-Dateien herunter, auf die in der Update-Datei
3. Laden Sie die MSI-Dateien auf einen internen Webserver hoch, auf den Ihre virtuellen Maschinen zugreifen können.
4. Aktualisieren Sie die Update-Datei, sodass sie auf die MSI-Dateien auf dem internen Webserver verweist.
5. Laden Sie die Update-Datei auf den Webserver hoch.

Automatische Updates können auch pro VM oder pro Pool umgeleitet werden. So leiten Sie Updates auf einer Pro-VM-Basis um:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.

2. Führen Sie den Befehl aus

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools /t REG_SZ /v
   update_url /d \
    url of the update file on the web server
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um die automatische Aktualisierung des Management Agents pro Pool umzuleiten:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url
   of the update file on the web server
<!--NeedCopy-->
```

Aktualisieren Sie die I/O-Treiber

Sie können die I/O-Treiber über Windows Update oder mithilfe des Management Agents aktualisieren. Sie können automatische Updates auch deaktivieren und Updates für die I/O-Treiber manuell verwalten.

Jeder der I/O-Treiber (xennet, xenvif, xenvbd, xeniface und xenbus) hat seine eigene Version. Informationen zu den neuesten Versionen finden Sie unter Was ist neu.

Stellen Sie die I/O-Treiber so ein, dass sie über Windows Update aktualisiert werden Sie können I/O-Treiber-Updates automatisch von Microsoft Windows Update erhalten, vorausgesetzt:

- Windows Update ist innerhalb der VM aktiviert
- Die VM hat Zugriff auf das Internet oder kann eine Verbindung zu einem WSUS-Proxyserver herstellen.
- Sie verwenden nicht die Core-Version von Windows Server. Windows Server Core unterstützt nicht die Verwendung von Windows Update zum Installieren oder Aktualisieren der I/O-Treiber.

Der Abschnitt **Virtualisierungsstatus** auf der Registerkarte **Allgemein** einer VM in XenCenter gibt an, ob die VM Updates von Windows Update empfangen kann. Der Mechanismus zum Empfangen von E/A-Treiberupdates von Windows Update ist standardmäßig aktiviert. Wenn Sie keine I/O-Treiberupdates von Windows Update erhalten möchten, deaktivieren Sie Windows Update auf Ihrer VM oder geben Sie eine Gruppenrichtlinie an.

Deaktivieren Sie das Update der I/O-Treiber über Windows Update Der Abschnitt **Virtualisierungsstatus** auf der Registerkarte **Allgemein** einer VM in XenCenter gibt an, ob die VM Updates von Windows Update empfangen kann. Der Mechanismus zum Empfangen von E/A-Treiberupdates von Windows Update ist standardmäßig aktiviert.

Geben Sie für bereits vorhandene Windows-VMs eine Gruppenrichtlinie an, wenn Sie keine I/O-Treiberupdates von Windows Update erhalten möchten.

Für neue Windows-VMs können Sie während der VM-Erstellung ein Flag in der VM setzen, um I/O-Treiberupdates von Windows Update zu verhindern. Weitere Informationen finden Sie unter Einstellungen für Citrix Provisioning Provisioning-Ziele oder Reset-On-Boot-Maschinen und Erstellen einer Windows-VM mithilfeder CLI.

Stellen Sie den Management Agent so ein, dass er die I/O-Treiber aktualisiert Während der Installation von XenServer VM Tools für Windows können Sie angeben, dass der Management Agent die I/O-Treiber automatisch aktualisiert. Wenn Sie diese Einstellung lieber nach Abschluss des Installationsvorgangs für XenServer VM Tools für Windows aktualisieren möchten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t REG_SZ
   /v \
    InstallDrivers /d YES
<!--NeedCopy-->
```

Halten Sie den Management Agent davon ab, die I/O-Treiber zu aktualisieren Gehen Sie wie folgt vor, um zu verhindern, dass der Management Agent die I/O-Treiber aktualisiert:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate /t REG_SZ
   /v \
    InstallDrivers /d NO
<!--NeedCopy-->
```

Automatischer Neustart

Stellen Sie sicher, dass alle angeforderten VM-Neustarts im Rahmen des Updates abgeschlossen sind. Möglicherweise sind mehrere Neustarts erforderlich. Wenn alle angeforderten Neustarts nicht abgeschlossen sind, tritt möglicherweise ein unerwartetes Verhalten auf.

Sie können einen Registrierungsschlüssel festlegen, der die maximale Anzahl automatischer Neustarts angibt, die bei der Installation der Treiber über den Geräte-Manager oder Windows Update durchgeführt werden. Nachdem Sie den Xenbus-Treiber Version 9.1.1.8 oder höher installiert haben, verwenden die XenServer VM Tools für Windows die Anweisungen dieses Registrierungsschlüssels.

Um diese Funktion zu nutzen, Wir empfehlen, dass Sie so schnell wie möglich den folgenden Registrierungsschlüssel festlegen: `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`. Der Wert des Registrierungsschlüssels muss eine positive Ganzzahl sein. Es wird empfohlen, die Anzahl der Neustarts im Registrierungsschlüssel auf 3 festzulegen.

Wenn dieser Registrierungsschlüssel festgelegt ist, führen die XenServer VM Tools für Windows so viele Neustarts durch, wie erforderlich sind, um die Updates abzuschließen, oder die im Registrierungsschlüssel angegebene Anzahl von Neustarts —je nachdem, welcher Wert niedriger ist.

Vor jedem Neustart kann Windows 60 Sekunden lang eine Warnung anzeigen, die vor dem bevorstehenden Neustart warnt. Sie können die Warnung verwerfen, aber diese Aktion bricht den Neustart nicht ab. Warten Sie aufgrund dieser Verzögerung zwischen den Neustarts einige Minuten nach dem ersten Neustart, bis der Neustartzyklus abgeschlossen ist.

> **Hinweise:**
>
> Diese Einstellung ist für Headless-Server mit statischen IP-Adressen erforderlich.
>
> Diese automatische Neustartfunktion gilt nur für Updates der Windows I/O-Treiber über den Geräte-Manager oder Windows Update. Wenn Sie das Management Agent-Installationsprogramm zum Bereitstellen Ihrer Treiber verwenden, ignoriert das Installationsprogramm diesen Registrierungsschlüssel und verwaltet die Neustarts der VM gemäß seinen eigenen Einstellungen.

Andere Konfigurationen und Abfragen

Finden der I/O-Treiberversion

Um die Version der auf der VM installierten I/O-Treiber herauszufinden:

1. Navigieren Sie zu `C:\Windows\System32\drivers`.
2. Suchen Sie den Treiber aus der Liste.
3. Rechtsklicken Sie auf den Treiber und wählen Sie **Eigenschaften** und dann **Details**.

   Im Feld **Dateiversion** wird die Version des auf der VM installierten Treibers angezeigt.

Finden Sie die Version des Management Agents

So ermitteln Sie die Version des Management Agents, der auf der VM installiert ist:

1. Navigieren Sie zu `C:\Program Files\XenServer\XenTools`.
2. Klicken Sie mit der rechten Maustaste auf `XenGuestAgent` aus der Liste und klicken Sie auf **Eigenschaften** und dann **Details**.

Im Feld **Dateiversion** wird die Version des Management Agents angezeigt, der auf der VM installiert ist.

Anonyme Nutzungsinformationen konfigurieren

Während der Installation von XenServer VM Tools für Windows können Sie angeben, ob Sie anonyme Nutzungsinformationen an Cloud Software Group, Inc. senden möchten. Wenn Sie diese Einstellung lieber nach Abschluss des Installationsvorgangs von XenServer VM Tools für Windows aktualisieren möchten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf der VM als Administrator eine Eingabeaufforderung.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\XenServer\XenTools\AutoUpdate REG_SZ /v
    \
    IDENTIFYAUTOUPDATE /d YES/NO
<!--NeedCopy-->
```

Deinstallieren Sie die XenServer VM Tools

Es wird nicht empfohlen, die XenServer VM Tools von Ihren Windows-VMs zu entfernen. Diese Tools sind erforderlich, damit Ihre Windows-VMs vollständig unterstützt werden. Wenn Sie sie entfernen, kann dies zu unerwartetem Verhalten führen. Deinstallieren Sie Ihre XenServer VM Tools nur als letzten Ausweg manuell.

Standarddeinstallation

Für eine Standarddeinstallation der XenServer VM Tools können Sie die Windows-Funktion zum **Hinzufügen oder Entfernen von Programmen** verwenden:

1. Erstellen Sie einen Snapshot der VM, bevor Sie beginnen.
2. Gehen Sie in der Windows-VM zu **Programme hinzufügen oder entfernen**.
3. Wählen Sie **XenServer VM Tools** und klicken Sie auf **Deinstallieren**.
4. Starten Sie die VM neu.

Der Befehl `uninstall.exe`

Bei der Deinstallation der XenServer VM Tools mithilfe der Windows-Funktion zum **Hinzufügen oder Entfernen von Programmen** wird die `<tools-install-directory>\uninstall.exe` Datei aufgerufen, um die Deinstallationsaktionen auszuführen. Sie können diesen Befehl stattdessen von einem PowerShell-Terminal oder einer Befehlszeile mit Administratorrechten aufrufen.

1. Erstellen Sie einen Snapshot der VM, bevor Sie beginnen.
2. Öffnen Sie als Administrator eine Eingabeaufforderung oder ein PowerShell-Terminal.
3. Führen Sie den Befehl `<tools-install-directory>\uninstall.exe` aus.
4. Starten Sie die VM neu.

Befehlsoptionen Der Befehl `uninstall.exe` akzeptiert die folgenden Parameter:

- `help` - Zeigt Verwendungsinformationen für den Befehl an.
- `log` - Generiert eine Protokolldatei, die angibt, was der Befehl getan hat.
- `verbose` - Druckt auf die Konsole, was der Befehl bewirkt hat.
- `disable` - Deaktiviert Treiber, die vom Installationsprogramm MSI installiert wurden.
- `force-disable` - Deaktiviert die Treiber in allen Situationen.
- `hidden` - Löscht versteckte Geräte. Diese Geräte sind unbenutzt und wurden ersetzt, haben aber möglicherweise veraltete Registrierungseinträge hinterlassen.
- `cleanup` - Entfernt alte Deinstallationsprogramme aus dem Bereich **Programme hinzufügen oder entfernen**. Diese Deinstallationsprogramme können doppelte Einträge aus älteren Versionen der Tools enthalten.
- `purge` - (9.3.1 und höher) Setzt die VM auf einen sauberen Zustand zurück, wie sie vor der Installation eines Teils der XenServer VM Tools war. Weitere Informationen finden Sie unter Vollständige Deinstallation aller XenServer VM Tools-Komponenten.
- `install` - (9.3.1 und höher) Installiert den aktuellen Satz von I/O-Treibern und fordert bei Bedarf einen VM-Neustart auf.
- `reboot`- Startet die VM neu, nachdem alle anderen Befehlsoperationen abgeschlossen sind.

Vollständige Deinstallation aller XenServer VM Tools-Komponenten

Die neueste Version von XenServer VM Tools für Windows (9.3.1 und höher) enthält den Befehl. `uninstall.exe purge` Die Option `purge` in der Anwendung `uninstall.exe` setzt eine VM auf den Zustand zurück, bevor einer der I/O-Treiber installiert wurde. Wenn beim Upgrade Ihrer Tools auf eine neuere Version Probleme auftreten oder wenn Sie einen sauberen Status benötigen, um einen späteren Satz von Tools auf Ihrer VM zu installieren, verwenden Sie dieses Tool.

1. Erstellen Sie einen Snapshot der VM, bevor Sie beginnen.
2. Öffnen Sie als Administrator eine Eingabeaufforderung oder ein PowerShell-Terminal.
3. Führen Sie den Befehl `<tools-install-directory>\uninstall.exe purge verbose` aus.
4. Starten Sie die VM neu.

Nachdem Sie diesen Befehl verwendet haben, müssen Sie keine manuellen Bereinigungsschritte wie bei früheren Versionen der XenServer VM Tools ausführen. Alle Änderungen im Zusammenhang mit den XenServer VM Tools wurden entfernt.

Was entfernt die Option purge? Wenn Sie den Befehl verwenden `uninstall.exe purge`, werden alle Spuren der XenServer VM Tools von Ihrer Windows-VM entfernt. Die Liste der mit diesem Befehl ausgeführten Aktionen lautet wie folgt:

- Dienstleistungen:
  - Deaktiviert alle XenServer VM Tools-Dienste, wodurch verhindert wird, dass installierte Treiber und Dienste beim Neustart gestartet werden.
  - Stoppt alle laufenden XenServer VM Tools-Dienste.
- Treiber:
  - Deinstalliert I/O-Treiber von allen Geräteknoten.
  - Deinstalliert versteckte Geräte. Diese Aktion entspricht der Aktion, die die Befehlszeilenoption `hidden` ausgeführt hat.
  - Deinstalliert zwischengespeicherte Treiberpakete, wodurch sie aus dem Treiberspeicher entfernt werden. Daher werden die I/O-Treiber nicht automatisch neu installiert.
- Registrierung:
  - Entfernt veraltete Registrierungsinformationen, die von Versionen der Treiber verwendet wurden, die nicht mehr unterstützt werden.
  - Löscht Schlüssel, die sich auf Tools beziehen, aus `HKLM\System\CurrentControlSet\Control\Class\...`
  - Löscht Schlüssel, die sich auf Werkzeuge beziehen, von `HKLM\System\CurrentControlSet\Services`.
  - Löscht Schlüssel, die sich auf Tools beziehen, aus `HKLM\System\CurrentControlSet\Enum\...`
- Dateien:
  - Löscht alle XenServer VM Tools-Treiberdateien aus `C:\Windows\System32` und. `C:\Windows\System32\drivers`
  - Löscht XenServer VM `INF` Tools-Dateien von. `C:\Windows\INF`
  - Löscht alle veralteten Dateien von Versionen der Tools, die nicht mehr unterstützt werden, aus `C:\Program Files\Citrix\XenTools` und `C:\Program Files\XenServer\XenTools`.
- Andere:
  - Löscht alte Einträge unter **Programme hinzufügen oder entfernen**. Diese Aktion entspricht der Aktion, die die Befehlszeilenoption `cleanup` ausgeführt hat.
  - Löscht einige der veralteten Statusinformationen des InstallAgents.
  - Entfernt `xenfilt.sys` aus den oberen Filtern. Diese Änderung verhindert, dass `xenfilt.sys` auf Treiberknoten geladen wird.

- Entfernt die `unplug`-Schlüssel, wodurch die VM beim Neustart zu emulierten Geräten zurückkehrt.
- Entfernt StartOverride von StorNvME. Diese Änderung erzwingt den Start von `stornvme.sys` beim Booten und ermöglicht die Funktion emulierter NVMe-Startgeräte (UEFI).

Was ist neu

Die Version der XenServer VM Tools für Windows wird unabhängig von der Version von XenServer aktualisiert. Stellen Sie sicher, dass Ihre XenServer VM Tools für Windows regelmäßig auf die neueste Version aktualisiert werden, sowohl in Ihren VMs als auch in allen Vorlagen, die Sie zum Erstellen Ihrer VMs verwenden.

Die neueste Version der XenServer VM Tools für Windows ist auf der XenServer-Downloadseite verfügbar.

XenServer VM-Tools für Windows 9.3.2

Veröffentlicht am 27. November 2023

In dieser Version werden die Citrix VM Tools in XenServer VM Tools umgetauft.

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installer: 9.3.2
- Management-Agent: 9.2.2.435
- xenbus: 9.1.7.80
- xeniface: 9.1.8.69
- xennet: 9.1.5.51
- xenvbd: 9.1.6.58
- xenvif: 9.1.10.83

Verbesserungen in 9.3.2 Diese Version enthält auch die folgenden Verbesserungen:

- Verbesserungen des Befehls `uninstall.exe`.
- Änderungen, die es einigen Windows-VMs ermöglichen, bis zu 64 vCPUs zu verwenden, sofern Ihre Version von XenServer und das Windows-Betriebssystem dies unterstützen.

Probleme in 9.3.2 behoben Diese Version enthält eine Lösung für das folgende Problem:

- Manchmal kann bei der Installation der XenServer VM Tools ein nicht schwerwiegender Fehler dazu führen, dass die Installation fehlschlägt.

Frühere Releases

9.3.1 Veröffentlicht am 25. Januar 2023

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installationsprogramm: 9.3.1
- Verwaltungsagent: 9.2.1.35
- xenbus: 9.1.5.54
- xeniface: 9.1.5.42
- xennet: 9.1.3.34
- xenvbd: 9.1.4.37
- xenvif: 9.1.8.58

Diese Version beinhaltet die folgenden Verbesserungen:

- Verbesserungen des Hilfsprogramms `uninstall.exe`, einschließlich des Parameters `purge`. Weitere Informationen finden Sie unter XenServer VM Tools deinstallieren.
- Allgemeine Verbesserungen am XenServer VM Tools-Installationsprogramm.
- Allgemeine Verbesserungen der Zeichenkettenbehandlung von Registrierungsschlüsseln.

Diese Version enthält Korrekturen für die folgenden Probleme:

- Wenn die XenServer VM Tools über Windows Update aktualisiert werden, gehen manchmal die statischen IP-Einstellungen verloren und die Netzwerkeinstellungen ändern sich, um DHCP zu verwenden.
- Auf Windows-VMs können die Grant-Tabellen leicht erschöpft sein. In diesem Fall können Lese- und Schreibanforderungen fehlschlagen oder zusätzliche VIFs werden nicht richtig aktiviert und können nicht gestartet werden.
- In seltenen Fällen kann es vorkommen, dass der vorhandene Management Agent beim Upgrade der XenServer VM Tools für Windows nicht heruntergefahren wird und das Upgrade nicht erfolgreich ist.
- Auf einer Windows-VM sehen Sie möglicherweise sowohl die vorherige als auch eine neuere Version der Tools oder des Management Agents, die in Ihren installierten Programmen aufgeführt sind.

  - (VORHERIGE) Citrix XenServer Windows Management-Agent
  - (SPÄTER) Citrix Hypervisor PV-Tools.

  Nachdem Sie die Tools auf die neueste Version aktualisiert haben, wird keiner dieser früheren Namen aufgeführt. Nur die XenServer VM Tools sind in Ihren installierten Programmen aufgeführt.

9.3.0 Veröffentlicht am 26. Juli 2022

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installationsprogramm: 9.3.0
- Management-Agent: 9.2.0.27
- xenbus: 9.1.4.49
- xeniface: 9.1.4.34
- xennet: 9.1.3.34
- xenvbd: 9.1.3.33
- xenvif: 9.1.6.52

Diese Version beinhaltet die folgenden Verbesserungen:

- Allgemeine Verbesserungen am XenServer VM Tools-Installationsprogramm.

Diese Version enthält Korrekturen für die folgenden Probleme:

- Sicherheitssoftware blockierte sekundäre Datenträger, die als austauschbar gekennzeichnet sind, daran, dem Betriebssystem ausgesetzt zu werden, um die Datenexfiltration zu verhindern. Mit diesem Update können Sie eine VBD als nicht entfernbar kennzeichnen und diese über das Betriebssystem korrekt verfügbar machen.
- Auf einer Windows-VM ist manchmal die IP-Adresse eines SR-IOV-VIF in XenCenter nicht sichtbar.

9.2.3 Veröffentlicht am 28. April 2022

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installationsprogramm: 9.2.3
- Management-Agent: 9.1.1.13
- xenbus: 9.1.3.30
- xeniface: 9.1.4.34
- xennet:
  - 9.1.1.8 (für Windows Server 2012 und Windows Server 2012 R2)
  - 9.1.2.23 (für alle anderen unterstützten Windows-Betriebssysteme)
- xenvbd: 9.1.2.20
- xenvif: 9.1.5.48

Diese Version enthält Korrekturen für die folgenden Probleme:

- In XenServer VM Tools für Windows Version 9.2.2 sind Zeitsynchronisierungsoptionen nicht verfügbar.
- Eine Rennbedingung kann dazu führen, dass Windows-VMs nach der Live-Migration auf Citrix Hypervisor 8.2 Cumulative Update 1 einen Bluescreen-Fehler anzeigen.

- Windows-VMs, auf denen Version 9.2.1 oder 9.2.2 der XenServer VM Tools installiert ist und die PVS-Ziele sind, können manchmal mit einem schwarzen Bildschirm einfrieren. Die Meldung "Guest Rx stalled"ist in den dom0-Kernelprotokollen enthalten. Dieses Problem tritt häufiger bei Poolkoordinatoren auf als bei anderen Poolmitgliedern.
- Auf Windows-VMs mit mehr als 8 vCPUs funktioniert Receive Side Scaling möglicherweise nicht, da der Xenvif-Treiber die Indirektionstabelle nicht einrichten kann.

9.2.2 Veröffentlicht am 14. Januar 2022

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installationsprogramm: 9.2.2
- Management-Agent: 9.1.1.13
- xenbus: 9.1.3.30
- xeniface: 9.1.2.22
- xennet:
  - 9.1.1.8 (für Windows Server 2012 und Windows Server 2012 R2)
  - 9.1.2.23 (für alle anderen unterstützten Windows-Betriebssysteme)
- xenvbd: 9.1.2.20
- xenvif: 9.1.3.31

Diese Version enthält Korrekturen für die folgenden Probleme:

- Während eines Updates der Tools kann der Xenbus-Treiber einen Neustart veranlassen, bevor die Treiberinstallation abgeschlossen ist. Das Akzeptieren des Neustarts kann zu einem Bluescreen-Fehler in Ihrer Windows-VM führen.
- Beim Komprimieren gesammelter Diagnoseinformationen läuft das xt-bugtool-Diagnosetool nach 20 Sekunden ab. Dieses Verhalten kann dazu führen, dass die Diagnose-ZIP-Datei nicht korrekt erstellt wird.
- Das Teilen der VNC-Zwischenablage funktioniert nicht.
- Die vorherigen Versionen der Treiber wurden nicht über Windows Update veröffentlicht.

9.2.1 Veröffentlicht am 24. Juni 2021

Dieses Toolset enthält die folgenden Komponentenversionen:

- Installationsprogramm: 9.2.1
- Management-Agent: 9.1.0.10
- xenbus: 9.1.2.14
- xeniface: 9.1.1.11
- xennet: 9.1.1.8

- xenvbd: 9.1.1.8
- xenvif: 9.1.2.16

> **Hinweis:**
>
> Dieser Treibersatz wurde nicht über Windows Update bereitgestellt.

Diese Version enthält Korrekturen für die folgenden Probleme:

- In einigen Fällen kann der Laptop/Slate-Status der VM nicht geändert werden.
- Nach dem Neustart einer VM kann es manchmal vorkommen, dass übermäßig viele Protokollmeldungen an die Datei daemon.log gesendet werden.
- Ein Race Condition in den Treiberlastabhängigkeiten nach einem Betriebssystemupgrade kann verhindern, dass die XenServer VM Tools aktualisiert werden.
- Ein Speicherfehler kann zum Absturz von Windows-VMs führen.
- Manchmal ist die IP-Adresse eines SR-IOV-VIF in XenCenter nicht sichtbar. Um das Problem zu beheben, starten Sie den Management Agent über den Service Manager der VM neu.
- Bei hoher Netzwerk- und Systemlast und niedrigen Ressourcen kann es bei virtuellen Maschinen zu Bugchecks sowohl in Citrix als auch in Treibern von Drittanbietern kommen, typischerweise mit dem Code IRQL_NOT_LESS_OR_EQUAL. Dieser Fix verbessert die Netzwerkpufferung, um diese Bugchecks zu verhindern.
- Ein Upgrade der Windows-I/O-Treiber kann dazu führen, dass UEFI-VMs nicht gestartet werden und “0xC000000E”gemeldet werden. Ein erforderliches Gerät ist nicht angeschlossen oder es kann nicht darauf zugegriffen werden.’”’
- Bei der Installation der XenServer VM Tools nach der Deinstallation einer früheren Version der XenServer VM Tools kann ein Problem auftreten, das die folgende Fehlermeldung zurückgibt: “Dieses Gerät kann nicht gestartet werden (Code 10) (Operation failed) The requested operation was failed”.

---

layout: doc
description: Create a Linux VM from a template for the operating system you want to run on the VM. You can create the VM from either XenCenter or the CLI.—

Linux-VMs

Wenn Sie eine Linux-VM erstellen möchten, erstellen Sie die VM mithilfe einer Vorlage für das Betriebssystem, das Sie auf der VM ausführen möchten. Sie können eine Vorlage verwenden, die XenServer für Ihr Betriebssystem bereitstellt, oder eine, die Sie zuvor erstellt haben. Sie können die VM entweder

über XenCenter oder über die CLI erstellen. Dieser Abschnitt konzentriert sich auf die Verwendung der CLI.

> **Hinweis:**
>
> Gehen Sie wie folgt vor, um eine VM mit einem neueren kleineren Update einer RHEL-Version zu erstellen, das für die Installation von XenServer unterstützt wird:
>
> - Installieren Sie von den neuesten unterstützten Medien
> - Verwenden Sie `yum update`, um die VM auf den neuesten Stand zu bringen
>
> Dieser Prozess gilt auch für RHEL-Derivate wie CentOS und Oracle Linux.

Wir empfehlen, die XenServer VM Tools für Linux unmittelbar nach der Installation des Betriebssystems zu installieren. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Die Übersicht zum Erstellen einer Linux-VM lautet wie folgt:

1. Erstellen Sie die VM für Ihr Zielbetriebssystem mit XenCenter oder der CLI.
2. Installieren Sie das Betriebssystem mithilfe des Installationsmediums des Anbieters.
3. Installieren Sie die XenServer VM Tools für Linux (empfohlen).
4. Konfigurieren Sie die richtige Zeit und Zeitzone auf der VM und VNC wie in einer normalen, nicht virtuellen Umgebung.

XenServer unterstützt die Installation vieler Linux-Distributionen als virtuelle Rechner.

> **Warnung:**
>
> Die Vorlage **Andere Installationsmedien** richtet sich an fortgeschrittene Benutzer, die versuchen möchten, VMs mit nicht unterstützten Betriebssystemen zu installieren. XenServer wurde nur mit den unterstützten Distributionen und spezifischen Versionen getestet, die von den mitgelieferten Standardvorlagen abgedeckt werden. Alle VMs, die mit der Vorlage "**Andere Installationsmedien** "installiert wurden, werden *nicht* unterstützt.

Informationen zu bestimmten Linux-Distributionen finden Sie unter Hinweise zur Installation für Linux-Distributionen

Unterstützte Linux-Distributionen

Eine Liste der unterstützten Linux-Distributionen finden Sie unter Unterstützung für Gastbetriebssysteme.

Andere Linux-Distributionen werden **nicht** unterstützt. Distributionen, die denselben Installationsmechanismus wie Red Hat Enterprise Linux verwenden (z. B. Fedora Core), können jedoch erfolgreich mit derselben Vorlage installiert werden.

Erstellen einer Linux-VM

Dieser Abschnitt enthält Verfahren zum Erstellen einer Linux-VM durch Installieren des Betriebssystems von einer physischen CD/DVD oder von einer ISO, auf die über das Netzwerk zugegriffen werden kann.

Erstellen Sie eine Linux-VM über die xe-CLI

Dieser Abschnitt zeigt das CLI-Verfahren zum Erstellen einer Linux-VM durch Installieren des Betriebssystems von einer physischen CD/DVD oder von einem über das Netzwerk zugänglichen ISO-Image.

1. Erstellen Sie eine VM aus der entsprechenden Vorlage. Die UUID der VM wird zurückgegeben:

   ```
   xe vm-install template=template-name new-name-label=vm-name
   <!--NeedCopy-->
   ```

2. (Optional) Ändern Sie den Startmodus der VM.

   ```
   xe vm-param-set uuid=<uuid> HVM-boot-params:firmware=<mode>
   xe vm-param-set uuid=<UUID> platform:device-model=qemu-upstream-
      uefi
   xe vm-param-set uuid=<uuid> platform:secureboot=<option>
   <!--NeedCopy-->
   ```

   Dieser Wert von `mode` kann entweder `BIOS` oder sein `uefi` und ist standardmäßig auf, `uefi` wenn diese Option für Ihr VM-Betriebssystem unterstützt wird. Andernfalls ist der Standardmodus `BIOS`. Der Wert von `option` kann entweder auf **`true`** oder gesetzt werden **`false`**. Wenn Sie die Option Secure Boot nicht angeben, ist sie standardmäßig auf `auto`eingestellt.

   Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.

3. Fügen Sie der neuen VM eine virtuelle CD-ROM hinzu:

   - Wenn Sie von einer CD oder DVD installieren, rufen Sie den Namen des physischen CD-Laufwerks auf dem XenServer-Host ab:

     ```
     xe cd-list
     <!--NeedCopy-->
     ```

     Das Ergebnis dieses Befehls gibt Ihnen so etwas wie SCSI 0:0:0:0 für das Feld `name-`**`label`**.

Verwenden Sie diesen Wertparameter als Parameter `cd-name`:

```
xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label"
   device=3
<!--NeedCopy-->
```

- Wenn Sie von einem über das Netzwerk zugänglichen ISO installieren, verwenden Sie den Namen der ISO aus dem ISO-Bibliothekslabel als Wert für den Parameter `cd-name`:

```
xe vm-cd-add vm=vm_name cd-name="iso_name.iso" device=3
<!--NeedCopy-->
```

4. Legen Sie die Betriebssystem-Installations-CD in das CD-Laufwerk auf dem XenServer-Host ein.
5. Öffnen Sie eine Konsole für die VM mit XenCenter oder einem SSH-Terminal und befolgen Sie die Schritte, um die Betriebssysteminstallation durchzuführen.
6. Starten Sie die VM. Es bootet direkt in das Betriebssystem-Installationsprogramm:

```
xe vm-start uuid=UUID
<!--NeedCopy-->
```

7. Installieren Sie die Gasthilfsprogramme und konfigurieren Sie die grafische Anzeige. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Erstellen Sie eine Linux-VM mit XenCenter

1. Klicken Sie auf der XenCenter -Symbolleiste auf die Schaltfläche **Neue VM**, um den Assistenten für neue VM zu öffnen.

   Mit dem Assistenten für neue VM können Sie die neue VM konfigurieren und verschiedene Parameter für CPU-, Speicher- und Netzwerkressourcen anpassen.

2. Wählen Sie eine VM-Vorlage und klicken Sie auf **Weiter**.

   Jede Vorlage enthält die Setup-Informationen, die erforderlich sind, um eine VM mit einem bestimmten Gastbetriebssystem (OS) und mit optimalem Speicher zu erstellen. Diese Liste spiegelt die Vorlagen wider, die XenServer derzeit unterstützt.

   > **Hinweis:**
   >
   > Wenn das Betriebssystem, das Sie auf Ihrer VM installieren, nur mit der Originalhardware kompatibel ist, aktivieren Sie das Kästchen **Host-BIOS-Zeichenfolgen auf VM kopieren** . Sie könnten diese Option beispielsweise für eine Betriebssystem-Installations-CD verwenden, die mit einem bestimmten Computer verpackt wurde.
   >
   > Nachdem Sie eine VM zum ersten Mal gestartet haben, können Sie ihre BIOS-Zeichenfolgen nicht ändern. Stellen Sie sicher, dass die BIOS-Zeichenfolgen korrekt sind, bevor Sie die VM

> zum ersten Mal starten.

Informationen zum Kopieren von BIOS-Zeichenfolgen mit der CLI finden Sie unter Installieren von VMs von Reseller Option Kit-Medien (BIOS-gesperrt).

Fortgeschrittene Benutzer können benutzerdefinierte BIOS-Strings festlegen. Weitere Informationen finden Sie unter Benutzerdefinierte BIOS-Zeichenketten.

3. Geben Sie einen Namen und eine optionale Beschreibung für die neue VM ein.
4. Wählen Sie die Quelle der Betriebssystemmedien aus, die auf der neuen VM installiert werden sollen.

   Die Installation von einer CD/DVD ist die einfachste Option für den Einstieg.

   a) Wählen Sie die Standardoption für die Installationsquelle (DVD-Laufwerk)
   b) Legen Sie den Datenträger in das DVD-Laufwerk des XenServer-Hosts ein

   Mit XenServer können Sie auch Betriebssysteminstallationsmedien aus einer Reihe von Quellen abrufen, einschließlich einer bereits vorhandenen ISO-Bibliothek.

   Um eine bereits vorhandene ISO-Bibliothek anzuhängen, klicken Sie auf **Neue ISO-Bibliothek** und geben Sie den Speicherort und den Typ der ISO-Bibliothek an. Sie können dann das spezifische ISO-Medium des Betriebssystems aus der Liste auswählen.
5. Auf der Registerkarte **Installationsmedien** können Sie einen Startmodus für die VM auswählen. Standardmäßig wählt XenCenter den sichersten Startmodus aus, der für die VM-Betriebssystemversion verfügbar ist.

   > **Hinweise:**
   >
   > - Die **UEFI-Boot** - und **UEFI-Secure-Bootoptionen** werden abgeblendet angezeigt, wenn die von Ihnen gewählte VM-Vorlage den UEFI-Start nicht unterstützt.
   > - Sie können den Startmodus nicht ändern, nachdem Sie die VM zum ersten Mal gestartet haben.
   >
   > Weitere Informationen finden Sie unter UEFI-Gaststart und Sicherer Start.
6. Wählen Sie einen Homeserver für die VM aus.

   Ein Homeserver ist der Host, der die Ressourcen für eine VM in einem Pool bereitstellt. Wenn Sie einen Homeserver für eine VM nominieren, versucht XenServer, die VM auf diesem Host zu starten. Wenn diese Aktion nicht möglich ist, wird automatisch ein alternativer Host innerhalb desselben Pools ausgewählt. Um einen Home-Server auszuwählen, klicken Sie **auf VM auf diesem Server platzieren** und wählen Sie einen Host aus der Liste aus.

Hinweise:

- In WLB-fähigen Pools wird der nominierte Homeserver nicht zum Starten, Neustarten, Fortsetzen oder Migrieren der VM verwendet. Stattdessen nominiert Workload Balancing den besten Host für die VM, indem es die XenServer-Ressourcenpool-Metriken analysiert und Optimierungen empfiehlt.
- Wenn einer VM eine oder mehrere virtuelle GPUs zugewiesen sind, wird die Nominierung des Homeservers nicht wirksam. Stattdessen basiert die Hostnominierung auf der vom Benutzer festgelegten Richtlinie zur Platzierung virtueller GPU.
- Beim Rolling Pool-Upgrade wird der Homeserver bei der Migration der VM nicht berücksichtigt. Stattdessen wird die VM zurück auf den Host migriert, auf dem sie sich vor dem Upgrade befand.

  Wenn Sie keinen Homeserver nominieren möchten, klicken Sie auf **Dieser VM keinen Homeserver zuweisen**. Die VM wird auf einem beliebigen Host mit den erforderlichen Ressourcen gestartet.

Klicken Sie zum Fortfahren auf **Weiter**.

7. Weisen Sie Prozessor- und Speicherressourcen für die VM zu. Klicken Sie zum Fortfahren auf **Weiter**.
8. Weisen Sie eine virtuelle GPU zu.

   Wenn vGPU unterstützt wird, fordert der Assistent für neue VM Sie auf, der VM eine dedizierte GPU oder eine oder mehrere virtuelle GPUs zuzuweisen. Mit dieser Option kann die VM die Rechenleistung der GPU nutzen. Mit dieser Funktion haben Sie eine bessere Unterstützung für professionelle High-End-3D-Grafikanwendungen wie CAD/CAM, GIS und medizinische Bildgebungsanwendungen.
9. Weisen Sie Speicher für die neue VM zu und konfigurieren Sie ihn.

   Klicken Sie auf **Weiter**, um die Standardzuweisung (24 GB) und Konfiguration auszuwählen, oder Sie möchten möglicherweise die folgende zusätzliche Konfiguration durchführen:

   - Ändern Sie den Namen, die Beschreibung oder die Größe Ihres virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.
   - Fügen Sie einen neuen virtuellen Datenträger hinzu, indem Sie **Hinzufügen**auswählen.
10. Konfigurieren Sie das Netzwerk auf der neuen VM.

    Klicken Sie auf **Weiter**, um die Standard-Netzwerkkarte und -konfigurationen auszuwählen, einschließlich einer automatisch erstellten eindeutigen MAC-Adresse für jede Netzwerkkarte. Alternativ möchten Sie möglicherweise die folgende zusätzliche Konfiguration vornehmen:

    - Ändern Sie das physische Netzwerk, die MAC-Adresse oder die Quality of Service (QoS) -Priorität des virtuellen Laufwerks, indem Sie auf **Bearbeiten** klicken.

- Fügen Sie eine neue virtuelle Netzwerkkarte hinzu, indem **Sie Hinzufügen**auswählen

11. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Jetzt erstellen**, um die VM zu erstellen und zur Registerkarte **Suchen** zurückzukehren.

    Ein Symbol für Ihre neue VM wird unter dem Host im Bereich **Ressourcen** angezeigt.

    Wählen Sie im Bereich **Ressourcen** die VM aus, und klicken Sie dann auf die Registerkarte **Konsole**, um die VM-Konsole anzuzeigen.

12. Folgen Sie den Installationsbildschirmen des Betriebssystems und treffen Sie Ihre Auswahl.
13. Nachdem die Betriebssysteminstallation abgeschlossen und die VM neu gestartet wurde, installieren Sie die XenServer VM Tools für Linux.

Erstellen einer Linux-VM mithilfe von PXE-Boot

Sie können PXE-Boot verwenden, um das Betriebssystem Ihrer Linux-VM zu installieren. Dieser Ansatz kann nützlich sein, wenn Sie viele Linux-VMs erstellen müssen.

Um mithilfe von PXE-Boot zu installieren, richten Sie die folgenden Voraussetzungen in dem Netzwerk ein, in dem sich Ihre Linux-VMs befinden:

- DHCP-Server, der konfiguriert ist, um alle PXE-Startinstallationsanforderungen an den TFTP-Server weiterzuleiten
- TFTP-Server, der die Installationsdateien für das Linux-Betriebssystem hostet

Führen Sie beim Erstellen der Linux-VM die folgenden Befehle aus:

1. Erstellen Sie eine VM aus der entsprechenden Vorlage. Die UUID der VM wird zurückgegeben:

```
xe vm-install template=template-name new-name-label=vm-name
<!--NeedCopy-->
```

2. Legen Sie die Startreihenfolge fest, um von dem Datenträger und dann vom Netzwerk zu booten:

```
xe vm-param-set uuid=<UUID> HVM-boot-params:order=cn
<!--NeedCopy-->
```

3. Starten Sie die VM, um mit der PXE-Startinstallation zu beginnen:

```
xe vm-start uuid=<UUID>
<!--NeedCopy-->
```

4. Installieren Sie die Gasthilfsprogramme und konfigurieren Sie die grafische Anzeige. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Weitere Informationen zur Verwendung von PXE-Boot zur Installation von Linux-Betriebssystemen finden Sie in der Betriebssystemdokumentation:

- Debian: Debian mit dem Booten über das Netzwerk installieren
- Red Hat: Automatisches Starten einer Kickstart-Installation mit PXE
- CentOS: PXE-Einrichtung
- SLES: Vorbereitung der Netzwerk-Boot-Umgebung
- Ubuntu: Netboot des Server-Installers auf amd64

Installieren Sie die XenServer VM Tools für Linux

Obwohl alle unterstützten Linux-Distributionen nativ paravirtualisiert sind (und keine speziellen Treiber für die volle Leistung benötigen), bieten XenServer VM Tools für Linux einen Gast-Agent. Dieser Gastagent stellt dem Host zusätzliche Informationen über die VM zur Verfügung. Installieren Sie den Gast-Agent auf jeder Linux-VM, um von den folgenden Funktionen zu profitieren:

- Zeigen Sie VM-Leistungsdaten in XenCenter an.

  Beispielsweise sind die folgenden Speicherleistungswerte in XenCenter nur sichtbar, wenn die XenServer VM Tools installiert sind: “Verwendeter Speicher”, “Datenträger”, “Netzwerk”und “Adresse”.

- Sehen Sie sich in XenCenter die Informationen zum Linux-Gastbetriebssystem an.
- Sehen Sie sich auf der Registerkarte XenCenter **Networking** die IP-Adresse der VM an.
- Starten Sie von XenCenter aus eine SSH-Konsole für die VM.
- Anpassen der Anzahl der vCPUs auf einer laufenden Linux-VM.
- Aktivieren Sie Dynamic Memory Control (DMC).

  > **Hinweis:**
  >
  > Sie können die Funktion Dynamic Memory Control (DMC) nicht auf Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 oder CentOS Stream 9 VMs verwenden, da diese Betriebssysteme kein Memory Ballooning mit dem Xen-Hypervisor unterstützen.

Es ist wichtig, den Linux-Gast-Agent auf dem neuesten Stand zu halten, wenn Sie Ihren XenServer-Host aktualisieren. Weitere Informationen finden Sie unter Update von Linux-Kerneln und Gasthilfsprogrammen.

> **Hinweis:**
>
> Stellen Sie vor der Installation des Gastagenten auf einem SUSE Linux Enterprise Desktop- oder Server 15-Gast sicher, dass `insserv-compat-0.1-2.15.noarch.rpm` auf dem Gast installiert ist.

So installieren Sie die XenServer VM Tools für Linux:

1. Laden Sie die Datei XenServer VM Tools für Linux von der XenServer-Downloadseiteherunter.
2. Kopieren Sie die Datei `LinuxGuestTools-xxx.tar.gz` auf Ihre Linux-VM oder auf ein freigegebenes Laufwerk, auf das die Linux-VM zugreifen kann.
3. Entpacken Sie den Inhalt der TAR-Datei: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Führen Sie das Installationsskript als root-Benutzer aus:

```
/<extract-directory>/install.sh
<!--NeedCopy-->
```

5. Wenn der Kernel aktualisiert wurde oder die VM von einer früheren Version aktualisiert wurde, starten Sie die VM jetzt neu.

Deinstallieren Sie die XenServer VM Tools für Linux

Ab Version 8.4.0-1 können Sie das Skript `install.sh` verwenden, um XenServer VM Tools for Linux zu deinstallieren. Um die Tools zu deinstallieren, führen Sie den folgenden Befehl als Root-Benutzer aus:

```
/<extract-directory>/install.sh -u
<!--NeedCopy-->
```

Installieren Sie Treiber von Drittanbietern auf Ihrer Secure Boot Linux-VM

Um Treiber von Drittanbietern auf einer Linux-VM zu installieren, auf der UEFI Secure Boot aktiviert ist, müssen Sie einen Signaturschlüssel erstellen, ihn der VM als Maschinenbesitzerschlüssel (MOK) hinzufügen und diesen Schlüssel verwenden, um den Treiber zu signieren. Wenn Sie beispielsweise die XenServer-Grafikfunktionen mit Ihrer Linux-VM verwenden, müssen Sie möglicherweise den NVIDIA-Grafiktreiber auf Ihrer VM installieren.

Gehen Sie wie folgt vor, um einen Schlüssel zu erstellen und ihn zur Installation eines Drittanbietertreibers zu verwenden:

1. Generieren Sie ein Paar aus öffentlichem und privatem Schlüssel.
2. Registriere den öffentlichen Schlüssel in MOK.
3. Legen Sie die Schlüssel, die Sie erstellt haben, als Modulsignaturschlüssel für den Treiber fest.

Das folgende Beispiel zeigt dieses Verfahren im Detail für einen NVIDIA-Grafiktreiber auf einer Ubuntu-VM mit Secure-Boot-Fähigkeit:

1. Laden Sie den NVIDIA-Treiber auf Ihre VM herunter.
2. Erstellen Sie ein Verzeichnis (zum Beispiel `/root/module-signing`) für die Schlüssel:


```
mkdir -p /root/module-signing
```

3. Erstellen Sie einen öffentlichen und einen privaten Schlüssel, mit dem Sie den Treiber signieren können:

```
openssl req -new -x509 -newkey rsa:2048 -keyout /root/module-
    signing/Nvidia.key -outform DER -out /root/module-signing/
    Nvidia.der -nodes -days 36500 -subj "/CN=Graphics Drivers"
```

4. Importieren Sie den öffentlichen Schlüssel in MOK, indem Sie `mokutil` verwenden:

```
mokutil --import /root/module-signing/Nvidia.der
```

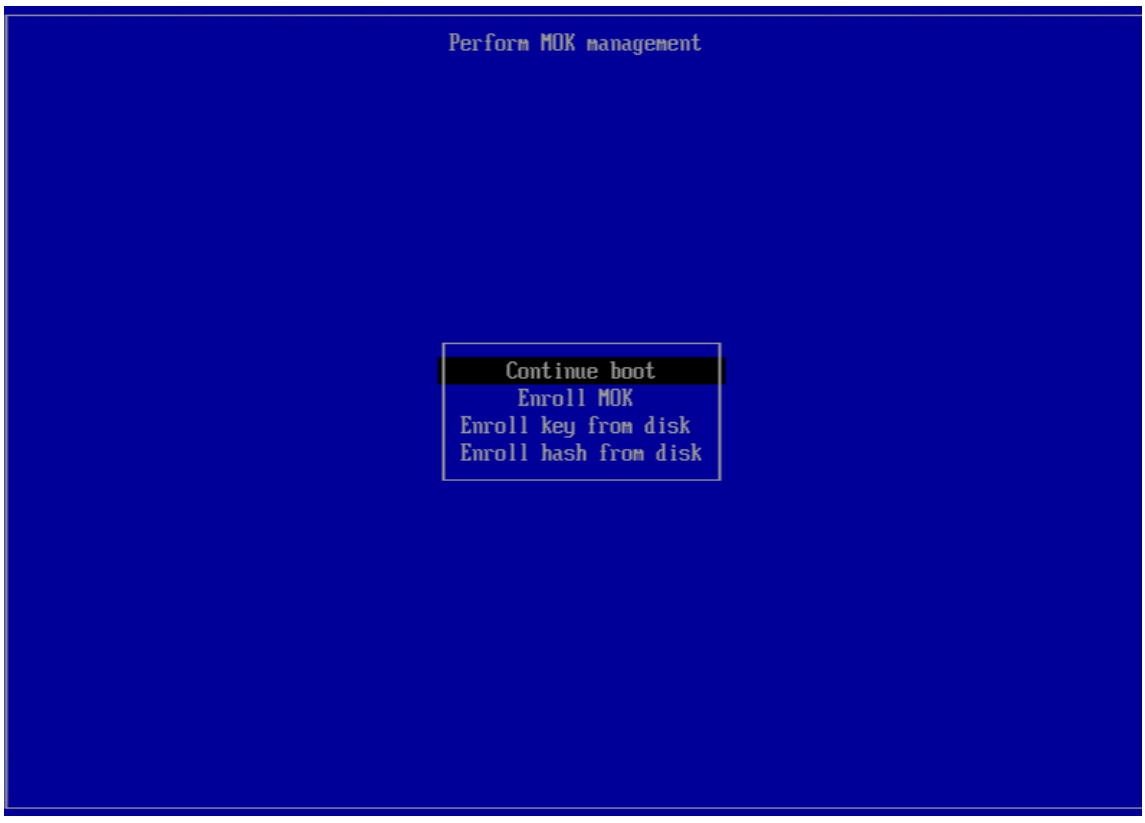
   In diesem Schritt werden Sie aufgefordert, ein Kennwort zu erstellen. Beim nächsten Start werden Sie aufgefordert, das Kennwort einzugeben, das Sie hier erstellen.

5. Stellen Sie sicher, dass das VM-Bootziel auf grafisch eingestellt ist:

```
systemctl set-default graphical.target
```

6. Starten Sie die VM neu.

7. Während des Startvorgangs wird die **Perform MOK Management-GUI** angezeigt.



   Führen Sie in dieser Oberfläche die folgenden Schritte aus:

a) **Wählen Sie**MOK registrieren > Fortfahren**.**
b) Wenn Sie gefragt werden, **Enroll the key(s)?**, wählen Sie **Ja**.
c) Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein, das Sie beim Import des öffentlichen Schlüssels erstellt haben (Schritt 4).

8. Installieren Sie das Paket `libglvnd-dev`:

```
apt install pkg-config libglvnd-dev
```

9. Installieren Sie den NVIDIA-Treiber und geben Sie die Schlüssel an, die Sie als Modulsignaturschlüssel erstellt haben:

```
bash ./NVIDIA-Linux-x86_64-535.129.03-grid.run --module-signing-
    secret-key=/root/module-signing/Nvidia.key --module-signing-
    public-key=/root/module-signing/Nvidia.der
```

Hinweise zur Installation von Linux-Distributionen

In diesem Abschnitt werden herstellerspezifische Konfigurationsinformationen aufgeführt, die vor der Erstellung der angegebenen Linux-VMs zu berücksichtigen sind.

Ausführlichere Versionshinweise zu allen Distributionen finden Sie unter Linux VM Release Notes.

RedHat Enterprise Linux* 7 (32-/64-bit)

Die neue Vorlage für diese Gäste legt 2 GB RAM fest. Diese Menge an RAM ist eine Voraussetzung für eine erfolgreiche Installation von Version 7.4 und höher. Für v7.0 - v7.3 gibt die Vorlage 2 GB RAM an, aber wie bei früheren Versionen von XenServer ist 1 GB RAM ausreichend.

> **Hinweis:**
>
> Diese Informationen gelten sowohl für Red Hat- als auch für Red Hat-Derivate.

Apt-Repositorys (Debian)

Für seltene oder einmalige Installationen ist es sinnvoll, direkt einen Debian-Spiegel zu verwenden. Wenn Sie jedoch mehrere VM-Installationen durchführen möchten, empfehlen wir Ihnen, einen Caching-Proxy oder einen lokalen Spiegel zu verwenden. Eines der folgenden Tools kann in einer VM installiert werden.

- `Apt-cacher`: Eine Implementierung eines Proxyservers, der einen lokalen Cache von Paketen führt
- `debmirror`: Ein Tool, das einen Teil- oder Vollspiegel eines Debian-Repositorys erstellt

Vorbereitung zum Klonen einer Linux-VM

Wenn Sie eine VM oder einen Computer klonen, werden die für diesen Computer eindeutigen Attribute normalerweise in Ihren Umgebungen dupliziert, sofern Sie das geklonte Image nicht verallgemeinern. Einige der eindeutigen Attribute, die beim Klonen dupliziert werden, sind die IP-Adresse, SID oder MAC-Adresse.

Daher ändert XenServer automatisch einige virtuelle Hardwareparameter, wenn Sie eine Linux-VM klonen. Wenn Sie die VM mit XenCenter kopieren, ändert XenCenter automatisch die MAC-Adresse und die IP-Adresse für Sie. Wenn diese Schnittstellen in Ihrer Umgebung dynamisch konfiguriert sind, müssen Sie die geklonte VM möglicherweise nicht ändern. Wenn die Schnittstellen jedoch statisch konfiguriert sind, müssen Sie möglicherweise ihre Netzwerkkonfigurationen ändern.

Die VM muss möglicherweise angepasst werden, um auf diese Änderungen aufmerksam gemacht zu werden. Anweisungen für bestimmte unterstützte Linux-Distributionen finden Sie unter Versionshinweise zu Linux VM.

Maschinenname

Eine geklonte VM ist ein weiterer Computer, und wie jeder neue Computer in einem Netzwerk muss er einen eindeutigen Namen innerhalb der Netzwerkdomäne haben.

IP-Adresse

Eine geklonte VM muss eine eindeutige IP-Adresse innerhalb der Netzwerkdomäne haben, zu der sie gehört. Im Allgemeinen ist diese Anforderung kein Problem, wenn DHCP zum Zuweisen von Adressen verwendet wird. Wenn die VM startet, weist der DHCP-Server ihr eine IP-Adresse zu. Wenn die geklonte VM eine statische IP-Adresse hatte, muss dem Klon vor dem Booten eine unbenutzte IP-Adresse zugewiesen werden.

MAC-Adresse

Es gibt zwei Situationen, in denen wir empfehlen, die MAC-Adressregeln vor dem Klonen zu deaktivieren:

1. In einigen Linux-Distributionen wird die MAC-Adresse für die virtuelle Netzwerkschnittstelle einer geklonten VM in den Netzwerkkonfigurationsdateien aufgezeichnet. Wenn Sie jedoch eine VM klonen, weist XenCenter der neuen geklonten VM eine andere MAC-Adresse zu. Wenn die neue VM zum ersten Mal gestartet wird, erkennt das Netzwerk daher die neue VM und wird nicht automatisch hochgefahren.

2. Einige Linux-Distributionen verwenden udev-Regeln, um sich die MAC-Adresse jeder Netzwerkschnittstelle zu merken und einen Namen für diese Schnittstelle beizubehalten. Dieses Verhalten ist dafür gedacht, dass dieselbe physische Netzwerkkarte immer derselben `eth`*n*-*Schnittstelle* zugeordnet wird, was bei austauschbaren NICs (wie Laptops) nützlich ist. Dieses Verhalten ist jedoch im Zusammenhang mit virtuellen Rechnern problematisch.

   Betrachten Sie beispielsweise das Verhalten im folgenden Fall:

   ```
   1.  Configure two virtual NICs when installing a VM
   1.  Shut down the VM
   1.  Remove the first NIC
   ```

   Wenn die VM neu gestartet wird, zeigt XenCenter nur eine Netzwerkkarte an, ruft sie jedoch auf `eth0`. In der Zwischenzeit zwingt die VM absichtlich diese Netzwerkkarte `eth1`. Das Ergebnis ist, dass das Networking nicht funktioniert.

Deaktivieren Sie für VMs, die persistente Namen verwenden, diese Regeln vor dem Klonen. Wenn Sie keine persistenten Namen ausschalten möchten, müssen Sie das Netzwerk innerhalb der VM neu konfigurieren (auf die übliche Weise). Die in XenCenter angezeigten Informationen stimmen jedoch nicht mit den Adressen in Ihrem Netzwerk überein.

Aktualisieren Sie Linux-Kernel und Gasthilfsprogramme

Die Linux-Gastdienstprogramme können aktualisiert werden, indem das `install.sh` Skript von den XenServer VM Tools für Linux erneut ausgeführt wird (siehe Installieren der XenServer VM Toolsfür Linux).

Für `yum`-fähige Distributionen, CentOS und RHEL, installiert `xe-guest-utilities` eine `yum`-Konfigurationsdatei, damit nachfolgende Updates mit `yum` auf standardmäßige Weise durchgeführt werden können.

Für Debian wird `/etc/apt/sources.list` standardmäßig aufgefüllt, um Updates mit APT zu ermöglichen.

Beim Upgrade empfehlen wir, dass Sie `install.sh` immer noch einmal ausführen. Dieses Skript ermittelt automatisch, ob Ihre VM irgendwelche Updates benötigt und installiert, falls erforderlich.

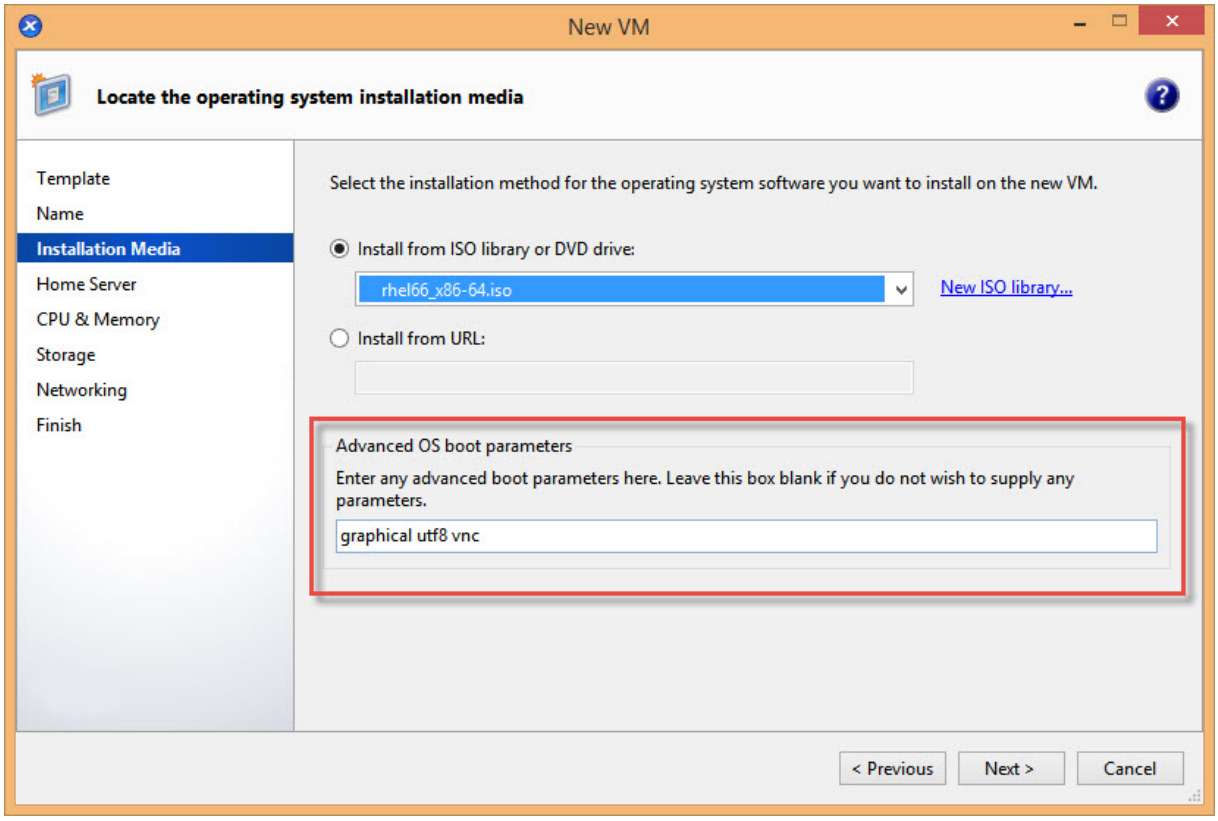
Versionshinweise zu Linux

Die meisten modernen Linux-Distributionen unterstützen die Xen-Paravirtualisierung direkt, haben jedoch unterschiedliche Installationsmechanismen und einige Kernel-Einschränkungen.

Unterstützung für grafische RHEL-Installationen

Um das grafische Installationsprogramm zu verwenden, führen Sie in XenCenter den Assistenten für **neue VM** durch. Fügen Sie auf der Seite **Installationsmedien** im Abschnitt **Erweiterte Betriebssystemstartparameter**vnc der Liste Parameter hinzu:

```
graphical utf8 vnc
<!--NeedCopy-->
```



Sie werden aufgefordert, die Netzwerkkonfiguration für die neue VM anzugeben, um die VNC-Kommunikation zu ermöglichen. Arbeiten Sie den Rest des Assistenten für neue VM durch. Wenn der Assistent abgeschlossen ist, wählen Sie in der **Infrastrukturansicht** die VM aus und klicken Sie auf **Konsole**, um eine Konsolensitzung der VM anzuzeigen. An dieser Stelle wird das Standardinstallationsprogramm verwendet. Die VM-Installation beginnt zunächst im Textmodus und fordert möglicherweise die Netzwerkkonfiguration an. Nach der Bereitstellung wird die Schaltfläche **Zur grafischen Konsole wechseln** in der oberen rechten Ecke des XenCenter-Fensters angezeigt.

Red Hat Enterprise Linux 7

Nach der Migration oder dem Aussetzen der VM frieren RHEL 7-Gäste möglicherweise während der Fortsetzung ein. Weitere Informationen finden Sie in RedHat Ausgabe 1141249.

Red Hat Enterprise Linux 8

Sie können die Funktion Dynamic Memory Control (DMC) nicht auf Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 9, Rocky Linux 8, Rocky Linux 9 oder CentOS Stream 9 VMs verwenden, da diese Betriebssysteme kein Memory Ballooning mit dem Xen-Hypervisor unterstützen.

CentOS 7

Eine Liste der CentOS 7-Versionshinweise finden Sie unter Red Hat Enterprise Linux 7.

Oracle Linux 7

Eine Liste der Versionshinweise zu Oracle Linux 7 finden Sie unter Red Hat Enterprise Linux 7.

Wissenschaftliches Linux 7

Eine Liste der Versionshinweise zu Scientific Linux 7 finden Sie unter Red Hat Enterprise Linux 7.

Debian 10

Wenn Sie Debian 10 (Buster) über PXE-Netzwerkstarts installieren, fügen Sie den Bootparametern nicht `console=tty0` hinzu. Dieser Parameter kann zu Problemen beim Installationsvorgang führen. Verwenden Sie nur `console=hvc0` in den Bootparametern.

Weitere Informationen finden Sie in den Debian-Ausgaben 944106 und 944125.

SUSE Linux Enterprise 12

Bereiten Sie einen SLES-Gast für das Klonen vor

> **Hinweis:**
>
> Bevor Sie einen SLES-Gast für das Klonen vorbereiten, müssen Sie die udev-Konfiguration für Netzwerkgeräte wie folgt löschen:

```
cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
```

So bereiten Sie einen SLES-Gast für das Klonen vor:

1. Öffne die Datei `/etc/sysconfig/network/config`
2. Bearbeiten Sie die Zeile mit der Aufschrift:


```
FORCE_PERSISTENT_NAMES=yes
<!--NeedCopy-->
```

Ziel

```
FORCE_PERSISTENT_NAMES=no
<!--NeedCopy-->
```

3. Speichern Sie die Änderungen und starten Sie die VM neu.
   Weitere Informationen finden Sie unter Vorbereiten des Klonens einer Linux-VM.

Ubuntu 18.04 (veraltet)

Ubuntu 18.04 bietet die folgenden Kerneltypen:

- Der General Availability (GA) -Kernel, der bei Point-Releases nicht aktualisiert wird
- Der Hardware Enablement (HWE) -Kernel, der bei Point-Releases aktualisiert wird

Einige Nebenversionen von Ubuntu 18.04 (zum Beispiel 18.04.2 und 18.04.3) verwenden standardmäßig einen HWE-Kernel, bei dem beim Ausführen der grafischen Konsole Probleme auftreten können. Um diese Probleme zu umgehen, können Sie diese Nebenversionen von Ubuntu 18.04 mit dem GA-Kernel ausführen oder einige der Grafikeinstellungen ändern. Weitere Informationen finden Sie unter CTX265663 - Ubuntu 18.04.2 VMskönnen auf XenServer nicht gestartet werden.

VM-Arbeitsspeicher

November 9, 2023

Wenn Sie eine VM erstellen, wird der VM eine feste Menge an Arbeitsspeicher zugewiesen. Sie können Dynamic Memory Control (DMC) verwenden, um die Auslastung des physischen Speichers in Ihrer XenServer-Umgebung zu verbessern. DMC ist eine Speicherverwaltungsfunktion, die eine dynamische Neuzuweisung von Speicher zwischen VMs ermöglicht.

XenCenter bietet eine grafische Anzeige der Speicherauslastung auf der Registerkarte “**Speicher** “. Weitere Informationen finden Sie in der XenCenter-Dokumentation.

Die Dynamic Memory Control (DMC) bietet folgende Vorteile:

- Sie können Speicher hinzufügen oder löschen, ohne die VMs neu zu starten, was dem Benutzer ein nahtloses Erlebnis bietet.
- Wenn die Hosts voll sind, können Sie mit DMC mehr VMs auf diesen Hosts starten, wodurch die Menge an Arbeitsspeicher, die den laufenden VMs zugewiesen wird, proportional reduziert wird.

Was ist Dynamic Memory Control (DMC)?

XenServer DMC passt den Arbeitsspeicher laufender VMs automatisch an, wobei die jeder VM zugewiesene Speichermenge zwischen den angegebenen Mindest- und Höchstspeicherwerten bleibt, was die Leistung garantiert und eine höhere Dichte von VMs pro Host ermöglicht.

Ohne DMC schlägt das Starten zusätzlicher VMs fehl, wenn ein Host voll ist, und es treten Fehler auf, dass nicht genügend Arbeitsspeicher zur Verfügung steht. Um die vorhandene VM-Speicherzuweisung zu reduzieren und Platz für mehr VMs zu schaffen, bearbeiten Sie die Speicherzuweisung jeder VM und starten Sie dann die VM neu. Bei Verwendung von DMC versucht XenServer, Speicher zurückzugewinnen, indem die aktuelle Speicherzuweisung laufender VMs innerhalb ihrer definierten Speicherbereiche automatisch reduziert wird. XenServer versucht, Speicher zurückzugewinnen, auch wenn der Host voll ist.

> **Hinweise:**
>
> Dynamic Memory Control wird bei virtuellen Rechnern mit virtueller GPU nicht unterstützt.

Das Konzept des Dynamikbereichs

Für jede VM kann der Administrator einen dynamischen Speicherbereich festlegen. Der dynamische Speicherbereich ist der Bereich, in dem Speicher der VM hinzugefügt/entfernt werden kann, ohne dass ein Neustart erforderlich ist. Wenn eine VM ausgeführt wird, kann der Administrator den Dynamikbereich anpassen. XenServer garantiert immer, dass die der VM zugewiesene Speichermenge innerhalb des dynamischen Bereichs bleibt. Daher kann eine Anpassung bei laufender VM dazu führen, dass XenServer die der VM zugewiesene Speichermenge anpasst. Im Extremfall setzt der Administrator das dynamische Min/Max auf denselben Wert und zwingt XenServer, sicherzustellen, dass diese Speichermenge der VM zugewiesen wird. Wenn neue VMs auf „vollen“Hosts gestartet werden müssen, wird bei laufenden VMs der Arbeitsspeicher „gequetscht“, um neue zu starten. Der erforderliche zusätzliche Speicher wird erhalten, indem die vorhandenen laufenden VMs proportional innerhalb ihrer vordefinierten Dynamikbereiche zusammengedrückt werden.

Mit DMC können Sie dynamische minimale und maximale Speicherpegel konfigurieren und so einen Dynamic Memory Range (DMR) erstellen, in dem die VM arbeitet.

- Dynamischer Mindestspeicher: Ein niedrigeres Speicherlimit, das Sie der VM zuweisen.
- Dynamisches höheres Limit: Ein oberes Speicherlimit, das Sie der VM zuweisen.

Wenn beispielsweise der dynamische Mindestspeicher auf 512 MB und der dynamische maximale Speicher auf 1.024 MB festgelegt wurde, wird der VM ein Dynamic Memory Range (DMR) von 512—1024 MB zugewiesen, innerhalb dessen sie arbeitet. XenServer *garantiert*, dass bei Verwendung von DMC immer jeder VM-Speicher innerhalb des angegebenen DMR zugewiesen wird.

Das Konzept der statischen Reichweite

Viele Betriebssysteme, die XenServer unterstützt, „verstehen“den Begriff des dynamischen Hinzufügens oder Löschens von Speicher nicht vollständig. Daher muss XenServer die maximale Speichermenge angeben, die eine VM beim Neustart verbrauchen soll. Durch die Angabe der maximalen Speichermenge kann das Gastbetriebssystem seine Seitentabellen und andere Speicherverwaltungsstrukturen entsprechend dimensionieren. Dies führt das Konzept eines statischen Speicherbereichs in XenServer ein. Der statische Speicherbereich kann nicht angepasst werden, wenn die VM läuft. Für einen bestimmten Start ist der Dynamikbereich so eingeschränkt, dass er immer in diesem statischen Bereich enthalten ist. Das statische Minimum (die Untergrenze des statischen Bereichs) schützt den Administrator und ist auf die niedrigste Speichermenge festgelegt, die das Betriebssystem mit XenServer ausführen kann.

> **Hinweis:**
>
> Es wird empfohlen, den statischen Mindestpegel nicht zu ändern, da der statische Mindestpegel auf der unterstützten Ebene pro Betriebssystem festgelegt ist. Weitere Informationen finden Sie in der Tabelle mit Speicherbeschränkungen.
>
> Wenn Sie einen statischen Maximalpegel höher als ein dynamisches Maximum festlegen, können Sie einer VM in Zukunft mehr Speicher zuweisen, ohne die VM neu zu starten.

DMC-Verhalten

Automatisches VM-Quetschen

- Wenn DMC nicht aktiviert ist und die Hosts voll sind, schlagen neue VM-Starts mit Fehlern “Out of Memory”fehl.
- Wenn DMC aktiviert ist, versucht XenServer, auch wenn die Hosts voll sind, Speicher zurückzugewinnen, indem die Speicherzuweisung laufender VMs innerhalb ihrer definierten Dynamikbereiche reduziert wird. Auf diese Weise werden laufende VMs proportional auf demselben Abstand zwischen dem dynamischen Minimum und dem dynamischen Maximum für alle VMs auf dem Host gequetscht.

Wenn DMC aktiviert ist

- Wenn der Arbeitsspeicher des Hosts reichlich vorhanden ist, erhalten alle laufenden VMs ihren dynamischen maximalen Speicherpegel
- Wenn der Arbeitsspeicher des Hosts knapp ist, erhalten alle laufenden VMs ihren dynamischen Mindestspeicherpegel.

Denken Sie bei der Konfiguration von DMC daran, dass die Zuweisung nur einer geringen Speichermenge zu einer VM diese negativ beeinflussen kann. Zum Beispiel zu wenig Speicher zuweisen:

- Die Verwendung von Dynamic Memory Control zur Reduzierung des für eine VM verfügbaren physischen Speichers kann dazu führen, dass sie langsam neu gestartet wird. Wenn Sie einer VM zu wenig Speicher zuweisen, kann sie ebenfalls langsam beginnen.
- Wenn Sie das dynamische Speicherminimum für eine VM zu niedrig festlegen, kann dies zu schlechten Leistungs- oder Stabilitätsproblemen führen, wenn die VM gestartet wird.

Wie funktioniert die DMC?

Mit DMC ist es möglich, eine virtuelle Gastmaschine in einem von zwei Modi zu betreiben:

1. **Zielmodus:** Der Administrator gibt ein Speicherziel für den Gast an. XenServer passt die Speicherzuweisung des Gastes an das Ziel an. Die Angabe eines Ziels ist in virtuellen Serverumgebungen nützlich und in Situationen, in denen Sie genau wissen, wie viel Speicher ein Gast verwenden soll. XenServer passt die Speicherzuweisung des Gastes an das von Ihnen angegebene Ziel an.
2. **Dynamikbereichsmodus:** Der Administrator gibt einen dynamischen Speicherbereich für den Gast an. XenServer wählt ein Ziel aus dem Bereich aus und passt die Speicherzuweisung des Gastes an das Ziel an. Die Angabe eines Dynamikbereichs ist in virtuellen Desktopumgebungen und in allen Situationen nützlich, in denen XenServer den Hostspeicher dynamisch neu partitionieren soll, um auf eine sich ändernde Anzahl von Gästen oder einen sich ändernden Hostspeicherdruck zu reagieren. XenServer wählt ein Ziel aus dem Bereich aus und passt die Speicherzuweisung des Gastes an das Ziel an.

> **Hinweis:**
>
> Es ist für jeden laufenden Gast möglich, jederzeit zwischen dem Zielmodus und dem Dynamikbereichsmodus zu wechseln. Geben Sie ein neues Ziel oder einen neuen Dynamikbereich an, und XenServer kümmert sich um den Rest.

Einschränkungen des Speichers

Mit XenServer können Administratoren alle Speichersteuerungsvorgänge mit jedem Gastbetriebssystem verwenden. XenServer erzwingt jedoch die folgende Einschränkung der Reihenfolge der Speichereigenschaften für alle Gäste:

```
0 < memory-static-min <= memory-dynamic-min <= memory-dynamic-max <=
memory-static-max
```

XenServer ermöglicht es Administratoren, die Eigenschaften des Gastspeichers auf alle Werte zu ändern, die diese Einschränkung erfüllen, sofern Validierungsprüfungen durchgeführt werden.

Zusätzlich zur vorherigen Einschränkung unterstützen wir jedoch nur bestimmte Gastspeicherkonfigurationen für jedes unterstützte Betriebssystem. Der Umfang der unterstützten Konfigurationen hängt vom verwendeten Gastbetriebssystem ab. XenServer verhindert nicht, dass Administratoren Gäste so konfigurieren, dass sie das unterstützte Limit überschreiten. Kunden wird jedoch empfohlen, die Speichereigenschaften innerhalb der unterstützten Grenzwerte zu halten, um Leistungs- oder Stabilitätsprobleme zu vermeiden. Ausführliche Richtlinien zu den minimalen und maximalen Speicherbeschränkungen für jedes unterstützte Betriebssystem finden Sie unter Unterstützung für Gastbetriebssysteme.

> **Warnung:**
>
> Bei der Konfiguration des Gastspeichers empfehlen wir, die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, NICHT zu überschreiten. Das Festlegen eines Speichermaximums, das über dem vom Betriebssystem unterstützten Limit liegt, kann zu Stabilitätsproblemen innerhalb Ihres Gastes führen.
>
> Das dynamische Minimum muss größer oder gleich einem Viertel des statischen Maximums für alle unterstützten Betriebssysteme sein. Eine Reduzierung der Untergrenze unter das dynamische Minimum kann ebenfalls zu Stabilitätsproblemen führen. Administratoren werden aufgefordert, die Größe ihrer VMs sorgfältig zu kalibrieren und sicherzustellen, dass ihre Arbeitsanwendungen bei minimaler Dynamik zuverlässig funktionieren.
>
> Das dynamische Minimum muss mindestens 75 % des statischen Maximums betragen. Ein niedrigerer Betrag kann zu Ausfällen bei Gästen führen und wird nicht unterstützt.

xe CLI-Befehle

Zeigen Sie die statischen Speichereigenschaften einer VM an

1. Suchen Sie die UUID der erforderlichen VM:

```
xe vm-list
<!--NeedCopy-->
```

2. Notieren Sie sich die UUID und führen Sie dann den Befehl aus `param-name=memory-static`

```
xe vm-param-get uuid=uuid param-name=memory-static-{
 min,max }

<!--NeedCopy-->
```

   Im Folgenden werden beispielsweise die statischen maximalen Speichereigenschaften für die VM angezeigt, wobei die UUID ec77 beginnt:


```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-static-max;
    268435456
<!--NeedCopy-->
```

Das Beispiel zeigt, dass der statische maximale Speicher für diese VM 268.435.456 Byte (256 MB) beträgt.

Zeigen Sie die dynamischen Speichereigenschaften einer VM an

Um die Eigenschaften des dynamischen Speichers anzuzeigen, gehen Sie wie oben beschrieben vor, aber verwenden Sie den Befehl `param-name=memory-dynamic`:

1. Suchen Sie die UUID der erforderlichen VM:

   ```
   xe vm-list
   <!--NeedCopy-->
   ```

2. Notieren Sie sich die uuid, und führen Sie dann den Befehl `param-name=memory-dynamic` aus :

   ```
   xe vm-param-get uuid=uuid param-name=memory-dynamic-{
    min,max }

   <!--NeedCopy-->
   ```

   Im Folgenden werden beispielsweise die dynamischen maximalen Speichereigenschaften für die VM mit der UUID beginnend mit ec77 angezeigt.

   ```
   xe vm-param-get uuid= \
       ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
       param-name=memory-dynamic-max;
       134217728
   <!--NeedCopy-->
   ```

   Das Beispiel zeigt, dass der dynamische maximale Arbeitsspeicher für diese VM 134.217.728 Byte (128 MB) beträgt.

Aktualisieren der Speichereigenschaften

> **Warnung:**
>
> Verwenden Sie die richtige Reihenfolge, wenn Sie die statischen/dynamischen Minimum/Maximum-Parameter einstellen. Darüber hinaus dürfen Sie die folgende Einschränkung nicht ungültig machen:


```
0 < memory-static-min <= memory-dynamic-min <= memory-dynamic-max
 <= memory-static-max
```

Aktualisieren Sie den statischen Speicherbereich einer virtuellen Maschine:

```
xe vm-memory-static-range-set uuid=uuid min=value max=value
<!--NeedCopy-->
```

Aktualisieren Sie den dynamischen Speicherbereich einer virtuellen Maschine:

```
xe vm-memory-dynamic-range-set \
      uuid=uuid min=value \
      max=value
<!--NeedCopy-->
```

Die Angabe eines Ziels ist in virtuellen Serverumgebungen nützlich und in jeder Situation, in der Sie genau wissen, wie viel Speicher ein Gast verwenden soll. XenServer passt die Speicherzuweisung des Gastes an das von Ihnen angegebene Ziel an. Beispiel:

```
xe vm-memory-target-set target=value vm=vm-name
<!--NeedCopy-->
```

Aktualisieren Sie alle Speicherbeschränkungen (statisch und dynamisch) einer virtuellen Maschine:

```
xe vm-memory-limits-set \
      uuid=uuid \
      static-min=value \
      dynamic-min=value \
      dynamic-max=value static-max=value
<!--NeedCopy-->
```

> **Hinweise:**
>
> - Um einer VM, die sich nicht ändert, eine bestimmte Speichermenge zuzuweisen, legen Sie das dynamische Maximum und das dynamische Minimum auf denselben Wert fest.
> - Sie können den dynamischen Speicher einer VM nicht über das statische Maximum hinaus erhöhen.
> - Um das statische Maximum einer VM zu ändern, müssen Sie die VM herunterfahren.

Aktualisieren einzelner Speichereigenschaften

> **Warnung:**
>
> Ändern Sie nicht die statische Mindeststufe, da sie auf der unterstützten Ebene pro Betriebssystem festgelegt ist. Weitere Informationen finden Sie unter Speicherbeschränkungen.

Aktualisieren Sie die dynamischen Speichereigenschaften einer VM.

1. Suchen Sie die UUID der erforderlichen VM:

```
xe vm-list
<!--NeedCopy-->
```

2. Notieren Sie sich die UUID und verwenden Sie dann den Befehl `memory-dynamic-{ min, max } =value`

```
xe vm-param-set uuid=uuid memory-dynamic-{
 min,max }
 =value
<!--NeedCopy-->
```

Im folgenden Beispiel wird das dynamische Maximum auf 128 MB geändert:

```
xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-
   dynamic-max=128MiB
<!--NeedCopy-->
```

VMs migrieren

April 12, 2024

Sie können eine laufende VM migrieren, indem Sie Livemigration oder Speicher-Livemigration verwenden, um das Virtual Disk Image (VDI) einer VM ohne VM-Ausfallzeiten zu verschieben.

Livemigration und Speicher-Livemigration

In den folgenden Abschnitten werden die Kompatibilitätsanforderungen und Einschränkungen der Livemigration und der Speicher-Livemigration

Livemigration

Live-Migration ist in allen Versionen von XenServer verfügbar. Mit dieser Funktion können Sie eine laufende VM von einem Host auf einen anderen Host verschieben, wenn sich die Datenträger (VDIs) der VM auf einem von beiden Hosts gemeinsam genutzten Speicher befinden. Poolwartungsfunktionen wie Hochverfügbarkeit und Rolling Pool Upgrade (RPU) können virtuelle Maschinen mit der Livemigration automatisch verschieben. Diese Funktionen ermöglichen den Workloadausgleich, die Ausfallsicherheit der Infrastruktur und das Upgrade der Serversoftware ohne Ausfallzeiten der VM.

Während der Live-Migration einer VM wird ihr Speicher als Datenstrom zwischen zwei Hosts über das Netzwerk übertragen. Die Komprimierungsfunktion für Migrationsströme komprimiert diesen Datenstrom und beschleunigt so die Speicherübertragung in langsamen Netzwerken. Diese Funktion ist

standardmäßig deaktiviert, kann jedoch mithilfe von XenCenter oder der Xe-CLI geändert werden. Weitere Informationen finden Sie unter Pooleigenschaften —Erweitert und Poolparameter. Alternativ können Sie die Komprimierung bei der Migration einer VM über die Befehlszeile aktivieren. Weitere Informationen finden Sie unter dem `vm-migrate` Befehl unter VM-Befehle.

Die Funktion zur parallelen Host-Evakuierung beschleunigt die Host-Evakuierung (während Hostupdates), indem VMs parallel statt sequentiell von einem Host verschoben werden. Standardmäßig ist diese Funktion aktiviert und die VMs werden in Batches von 10 parallel migriert. Sie können die Standardstapelgröße in der `/etc/xapi.conf` Datei ändern.

> **Hinweis:**
>
> Speicher kann nur zwischen Hosts im selben Pool freigegeben werden. Daher können virtuelle Maschinen nur auf Hosts im selben Pool migriert werden.
>
> Intel GVT-G ist nicht mit Livemigration, Speicher-Livemigration oder VM Suspend kompatibel. Weitere Informationen finden Sie unter Grafik.

Live-Speichermigration

> **Hinweise:**
>
> - Verwenden Sie keine Speicher-Livemigration in Citrix Virtual Desktops-Bereitstellungen.
> - Die Speicherlivemigration kann nicht auf VMs verwendet werden, bei denen das Tracking geänderter Blocks aktiviert ist. Deaktivieren Sie das Tracking geänderter Blocks, bevor Sie versuchen, die Speicherlivemigration durchzuführen.
> - Die Livemigration des Speichers kann nicht auf VMs verwendet werden, deren VDIs sich auf einem GFS2-SR befinden.

Mit der Speicher-Livemigration kann eine VM von einem Host auf einen anderen verschoben werden, wenn sich die Datenträger der VM nicht auf dem von den beiden Hosts gemeinsam genutzten Speicher befinden. Infolgedessen können im lokalen Speicher gespeicherte VMs ohne Ausfallzeiten migriert werden, und virtuelle Maschinen können von einem Pool in einen anderen verschoben werden. Mit dieser Funktion können Systemadministratoren:

- Rebalancing von VMs zwischen XenServer-Pools (z. B. von einer Entwicklungsumgebung zu einer Produktionsumgebung).
- Aktualisieren und aktualisieren Sie eigenständige XenServer-Hosts ohne VM-Ausfallzeiten.
- Aktualisieren Sie die XenServer-Serverhardware.

> **Hinweis:**
>
> - Bei der Migration einer VM von einem Host auf einen anderen bleibt der *VM-Status* erhal-

> ten. Zu den Statusinformationen gehören Informationen, die die VM und die historischen Leistungsmetriken wie CPU- und Netzwerknutzung definieren und identifizieren.
>
> • Um die Sicherheit zu verbessern, können Sie den TCP-Port 80 auf der Verwaltungsschnittstelle Ihrer XenServer-Hosts schließen. Sie können eine VM jedoch nicht von einem Citrix Hypervisor 8.2 CU1-Pool ohne installierten Hotfix XS82ECU1033 zu einem XenServer-Pool mit geschlossenem Port 80 migrieren. Installieren Sie dazu XS82ECU1033 auf Ihrem Citrix Hypervisor 8.2 CU1-Pool oder öffnen Sie vorübergehend Port 80 in Ihrem XenServer-Pool. Weitere Informationen zum Schließen von Port 80 finden Sie unter Verwendung von Port 80 einschränken.

Kompatibilitätsanforderungen

Bei der Migration einer VM mit Live-Migration oder Speicher-Live-Migration müssen die neue VM und der Server die folgenden Kompatibilitätsanforderungen erfüllen:

- Auf dem Zielhost muss dieselbe oder eine neuere Version von XenServer als Quellhost installiert sein.
- XenServer VM Tools für Windows müssen auf jeder Windows-VM installiert sein, die Sie migrieren möchten.
- Wenn die CPUs auf dem Quell- und Zielhost unterschiedlich sind, muss der Zielhost mindestens so leistungsfähig sein wie der Quellhost. Im Allgemeinen bedeutet dies, dass das Ziel dieselbe oder eine neuere CPU hat.
  - Wenn Sie innerhalb desselben Pools migrieren, versucht der Pool automatisch, eine VM kompatibel zu machen.
  - Wenn Sie zwischen Pools migrieren, müssen Sie sicherstellen, dass die VM mit dem Funktionsumfang im Zielpool kompatibel ist.
- Sie können eine VM nicht live zwischen AMD- und Intel-Prozessoren migrieren.
- Sie können nicht mehr als 3 VMs gleichzeitig migrieren, deren Quellspeicherort sich im selben Pool befindet.
- Der Zielhost muss über ausreichende freie Speicherkapazität verfügen oder mit Dynamic Memory Control ausreichend Kapazität freigeben können. Wenn nicht genügend Speicher vorhanden ist, kann die Migration nicht abgeschlossen werden.
- Nur Speichermigration: Ein Host im Quellpool muss über ausreichend freie Speicherkapazität verfügen, um eine angehaltene VM auszuführen, die gerade migriert wird. Diese Anforderung ermöglicht es, die angehaltene VM zu einem beliebigen Zeitpunkt während des Migrationsprozesses zu starten.

- Nur Live-Speichermigration: Der Zielspeicher muss über ausreichend freien Speicherplatz für die eingehenden VMs verfügen. Der erforderliche freie Speicherplatz kann die dreifache VDI-Größe haben (ohne Snapshots). Wenn nicht genügend Speicherplatz vorhanden ist, kann die Migration nicht abgeschlossen werden.
- Sie können die Speicherlivemigration nicht verwenden, um VMs zu migrieren, bei denen das Tracking geänderter Blocks aktiviert ist. Deaktivieren Sie das Tracking geänderter Blocks, bevor Sie versuchen, die Speicherlivemigration durchzuführen. Weitere Informationen finden Sie unter Tracking geänderter Blocks.

Einschränkungen und Hinweise

Livemigration und Speicher-Livemigration unterliegen den folgenden Einschränkungen und Vorbehalte:

- Die Speicher-Livemigration kann nicht mit von Machine Creation Services erstellten VMs verwendet werden.
- VMs, die PCI-Passthrough-Geräte verwenden, können nicht migriert werden (außer im Fall von NVIDIA SR-IOV-GPUs). Weitere Informationen finden Sie unter Verwenden von SR-IOV-fähigen NICs.
- VMs mit angeschlossenen VUSBs können nicht migriert werden.
- VMs mit dem `no-migrate` Parametersatz können nicht migriert werden.
- Intel GVT-G ist nicht mit Livemigration und Speicher-Livemigration kompatibel. Weitere Informationen finden Sie unter Grafikübersicht.
- VMs, bei denen die Option `on-boot` auf `reset` eingestellt ist, können nicht migriert werden. Weitere Informationen finden Sie unter Intellicache.
- Wenn Sie die Hochverfügbarkeitsfunktion verwenden und die zu migrierende VM als geschützt markiert ist, erhalten Sie während der Livemigration möglicherweise eine Warnung, wenn der Vorgang dazu führt, dass die HA-Einschränkungen nicht eingehalten werden.
- Die VM-Leistung wird während der Migration reduziert.
- Die Zeit bis zum Abschluss der VM-Migration hängt vom Speicherbedarf der VM und ihrer Aktivität ab. Darüber hinaus können sich die Größe des VDI und die Speicheraktivität des VDI auf VMs auswirken, die mit der Livemigration des Speichers migriert werden. VMs mit angeschlossenen vGPUs migrieren den gesamten vGPU-Status, während die VM angehalten ist. Es wird empfohlen, im Verwaltungsnetzwerk eine schnelle Netzwerkkarte zu verwenden, um Ausfallzeiten zu reduzieren, insbesondere bei vGPUs mit großem Arbeitsspeicher.
- Wenn die Live-Migration fehlschlägt, z. B. im Fall eines Netzwerkfehlers, kann die VM auf dem Quellhost sofort in einen angehaltenen Zustand übergehen.

Migrieren einer VM mit XenCenter

1. Wählen Sie im Bereich Ressourcen die VM aus, und führen Sie eine der folgenden Aktionen aus:

    - Um eine laufende oder angehaltene VM mit Livemigration oder Speicherlivemigration zu migrieren, klicken Sie im Menü **VM** auf **Auf Server migrieren** und dann auf den Assistenten **VM migrieren**. Diese Aktion öffnet den Assistenten zum **Migrieren einer VM**.
    - So verschieben Sie eine gestoppte VM: Wählen Sie im Menü **VM** die Option **VM verschieben** aus. Diese Aktion öffnet den Assistenten zum **Verschieben einer VM**

2. Wählen Sie aus der **Zielliste** einen eigenständigen Host oder einen Pool aus.
3. Wählen Sie aus der **Home-Server-Liste** einen Host aus, der als Home-Server für die VM zugewiesen werden soll, und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Speicher** das Speicherrepository an, in dem Sie die virtuellen Datenträger der migrierten VM platzieren möchten, und klicken Sie dann auf **Weiter**.

    - Das Optionsfeld **Alle migrierten virtuellen Datenträger auf dasselbe SR platzieren** ist standardmäßig ausgewählt und zeigt das standardmäßig freigegebene SR im Zielpool an.
    - Klicken Sie auf **Migrierte virtuellen Datenträger auf angegebenen SRs platzieren**, um ein SR aus der Liste **Speicherrepository** anzugeben. Mit dieser Option können Sie für jeden virtuellen Datenträger auf der migrierten VM unterschiedliche SRs auswählen.

5. Wählen Sie in der Liste **Speichernetzwerk** ein Netzwerk im Zielpool aus, das für die Livemigration der virtuellen Datenträger der VM verwendet wird. Klicken Sie auf **Weiter**.

    > **Hinweis:**
    >
    > Aus Leistungsgründen wird empfohlen, dass Sie Ihr Verwaltungsnetzwerk nicht für die Livemigration verwenden.

6. Überprüfen Sie die Konfigurationseinstellungen und klicken Sie auf **Fertigstellen**, um die Migration der VM zu starten.

Wenn Sie ein Upgrade von 7.1 CU2 auf 8.2 CU1 durchführen, müssen Sie nach der Migration Ihrer VMs möglicherweise alle VMs herunterfahren und starten, um sicherzustellen, dass neue Virtualisierungsfunktionen genutzt werden.

Live-VDI-Migration

Die Live-VDI-Migration ermöglicht es dem Administrator, das Virtual Disk Image (VDI) der virtuellen Maschine zu verlagern, ohne die VM herunterzufahren. Diese Funktion ermöglicht administrative Vorgänge wie:

- Verschieben einer VM vom günstigen lokalen Speicher zu einem schnellen, stabilen, Array-gestützten Speicher.
- Verschieben einer VM von einer Entwicklungs- in eine Produktionsumgebung.
- Wechseln zwischen Speicherebenen, wenn eine VM durch Speicherkapazität begrenzt ist.
- Durchführung von Speicher-Array-Upgrades.

Einschränkungen und Hinweise

Die Live-VDI-Migration unterliegt den folgenden Einschränkungen und Vorbehalte:

- Verwenden Sie keine Speicher-Livemigration in Citrix Virtual Desktops-Bereitstellungen.
- IPv6 Linux-VMs benötigen einen Linux-Kernel mit mehr als 3,0.
- Wenn Sie eine Live-VDI-Migration auf einer VM durchführen, die über eine vGPU verfügt, wird die vGPU-Livemigration verwendet. Der Host muss über ausreichend vGPU-Speicherplatz verfügen, um eine Kopie der vGPU-Instanz auf dem Host zu erstellen. Wenn die PGPUs voll ausgelastet sind, ist eine VDI-Migration möglicherweise nicht möglich.
- Wenn Sie eine VDI-Livemigration für eine VM durchführen, die auf demselben Host verbleibt, benötigt diese VM vorübergehend die doppelte Menge an RAM.

So verschieben Sie virtuelle Datenträger

1. Wählen Sie im Bereich **Ressourcen** das SR aus, in dem der virtuelle Datenträger gespeichert ist, und klicken Sie dann auf die Registerkarte **Speicher**.
2. Wählen Sie in der Liste **Virtuelle Laufwerke** das virtuelle Laufwerk aus, das Sie verschieben möchten, und klicken Sie dann auf **Verschieben**.
3. Wählen Sie im Dialogfeld **Virtuellen Datenträger verschieben** das Ziel-SR aus, auf das Sie den VDI verschieben möchten.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass das SR ausreichend Speicherplatz für einen anderen virtueller Datenträger hat: Der verfügbare Speicherplatz wird in der Liste der verfügbaren SRs angezeigt.

4. Klicken Sie auf **Verschieben**, um das virtuelle Laufwerk zu verschieben.

VMs importieren und exportieren

February 24, 2024

XenServer ermöglicht es Ihnen, VMs aus verschiedenen Formaten zu importieren und in verschiedene Formate zu exportieren. Mit dem XenCenter Importassistenten können Sie VMs aus Disk-Images (VHD und VMDK), Open Virtualization Format (OVF und OVA) und XenServer XVA-Format importieren. Sie können sogar VMs importieren, die auf anderen Virtualisierungsplattformen wie den von VMware und Microsoft angebotenen erstellt wurden.

> **Hinweis:**
>
> Wenn Sie VMs importieren, die mit anderen Virtualisierungsplattformen erstellt wurden, konfigurieren oder *reparieren* Sie das Gastbetriebssystem, um sicherzustellen, dass es auf XenServer startet. Die Funktion zur Betriebssystemfixierung in XenCenter soll dieses grundlegende Maß an Interoperabilität bieten. Weitere Informationen finden Sie unter Betriebssystem-Update.

Mit dem XenCenter **Exportassistenten** können Sie VMs in das Open Virtualization Format (OVF und OVA) und das XenServer XVA-Format exportieren.

Sie können auch die xe-CLI verwenden, um VMs aus dem XenServer XVA-Format zu importieren und in das XenServer XVA-Format zu exportieren.

Unterstützte Formate

Format	Beschreibung
Offenes Virtualisierungsformat (OVF und OVA)	OVF ist ein offener Standard zum Verpacken und Verteilen einer virtuellen Appliance, die aus einer oder mehreren VMs besteht.
Disk-Image-Formate (VHD und VMDK)	Disk-Image-Dateien im Format Virtual Hard Disk (VHD) und Virtual Machine Disk (VMDK) können mit dem Importassistenten importiert werden. Das Importieren eines Datenträgerimages ist möglicherweise sinnvoll, wenn ein virtuelles Datenträgerimage verfügbar ist, ohne dass OVF-Metadaten verknüpft sind.

Format	Beschreibung
XenServer XVA-Format	XVA ist ein für Xen-basierte Hypervisoren spezifisches Format zum Verpacken einer einzelnen VM als einzelnes Dateiarchiv, einschließlich eines Deskriptors und Disk-Images. Die Dateinamenerweiterung ist `.xva`.

Welches Format soll verwendet werden?

Erwägen Sie die Verwendung von OVF/OVA-Format für

- Teilen Sie XenServer-vApps und VMs mit anderen Virtualisierungsplattformen, die OVF unterstützen
- Speichern Sie mehr als eine VM
- Schützen Sie eine vApp oder VM vor Beschädigung und Manipulation
- Fügen Sie eine Lizenzvereinbarung hinzu
- Vereinfachen der vApp-Verteilung durch Speichern eines OVF-Pakets in einer OVA-Datei

Erwägen Sie die Verwendung des XVA-Formats für

- Importieren und Exportieren von VMs aus einem Skript mit einer CLI

Offenes Virtualisierungsformat (OVF und OVA)

OVF ist ein offener Standard, der von der Distributed Management Task Force festgelegt wird, zum Verpacken und Verteilen einer virtuellen Appliance, die aus einer oder mehreren VMs besteht. Weitere Informationen zu OVF- und OVA-Formaten finden Sie in den folgenden Informationen:

- Knowledge Base-Artikel CTX121652: Überblick über das Open Virtualization Format
- Open Virtualization Format-Spezifikation

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu importieren oder zu exportieren, müssen Sie als Root angemeldet sein oder die Rolle Pool-Administrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.

Ein **OVF-Paket** ist der Satz von Dateien, der die virtuelle Appliance umfasst. Es enthält immer eine Deskriptordatei und alle anderen Dateien, die die folgenden Attribute des Pakets darstellen:

Attribute Deskriptor (`.ovf`): Der Deskriptor gibt immer die virtuellen Hardwareanforderungen des Pakets an. Es kann auch andere Informationen angeben, darunter:

- Beschreibungen der virtuellen Datenträger, des Pakets selbst und der Gastbetriebssysteme
- Eine Lizenzvereinbarung
- Anweisungen zum Starten und Stoppen von virtuellen Rechnern in der Appliance
- Anweisungen zum Installieren des Pakets

Signatur (`.cert`): Die Signatur ist die digitale Signatur, die von einem Public-Key-Zertifikat im X.509-Format verwendet wird, um den Autor des Pakets zu authentifizieren.

Manifest (`.mf`): Mit dem Manifest können Sie die Integrität des Paketinhalts überprüfen. Es enthält die SHA-1-Digests jeder Datei im Paket.

Virtuelle Datenträger: OVF gibt kein Datenträgerimageformat an. Ein OVF-Paket enthält Dateien, die virtuelle Laufwerke in dem Format enthalten, das durch das Virtualisierungsprodukt definiert wurde, das die virtuellen Laufwerke exportiert hat. XenServer produziert OVF-Pakete mit Disk-Images im Dynamic VHD-Format; VMware-Produkte und Virtual Box erstellen OVF-Pakete mit virtuellen Datenträger im Stream-optimierten VMDK-Format.

OVF-Pakete unterstützen auch andere nicht mit Metadaten verbundene Funktionen wie Komprimierung, Archivierung, EULA-Anlage und Anmerkungen.

> **Hinweis:**
>
> Wenn Sie ein OVF-Paket importieren, das komprimiert wurde oder komprimierte Dateien enthält, müssen Sie möglicherweise zusätzlichen Speicherplatz auf dem XenServer-Host freigeben, um es ordnungsgemäß importieren zu können.

Ein **Open Virtual Appliance (OVA) -Paket** ist eine einzelne Archivdatei im Format Tape Archive (.tar), die die Dateien enthält, aus denen ein OVF-Paket besteht.

Wählen Sie OVF oder OVA-Format OVF-Pakete enthalten eine Reihe unkomprimierter Dateien, was den Zugriff auf einzelne Disk-Images in der Datei erleichtert. Ein OVA-Paket enthält eine große Datei, und obwohl Sie diese Datei komprimieren können, bietet es Ihnen nicht die Flexibilität einer Reihe von Dateien.

Die Verwendung des OVA-Formats ist für bestimmte Anwendungen nützlich, für die es vorteilhaft ist, nur eine Datei zu haben, z. B. das Erstellen von Paketen für Web-Downloads. Erwägen Sie, OVA nur als Option zu verwenden, um die Handhabung des Pakets zu vereinfachen. Die Verwendung dieses Formats verlängert sowohl den Export- als auch den Importvorgang.

Disk-Image-Formate (VHD und VMDK)

Mit XenCenter können Sie Datenträgerimages in den Formaten Virtual Hard Disk (VHD) und Virtual Machine Disk (VMDK) importieren. Das Exportieren eigenständiger Datenträgerimages wird nicht unterstützt.

> **Hinweis:**
>
> Um Disk-Images zu importieren, stellen Sie sicher, dass Sie als root angemeldet sind oder dass Ihrem Benutzerkonto die RBAC-Rolle Pooladministrator zugeordnet ist.

Sie können ein Datenträgerimage importieren, wenn ein virtuelles Datenträgerimage ohne zugehörige OVF-Metadaten verfügbar ist. Diese Option kann in den folgenden Situationen auftreten:

- Es ist möglich, ein Disk-Image zu importieren, aber die zugehörigen OVF-Metadaten sind nicht lesbar
- Ein virtuelles Laufwerk ist nicht in einem OVF-Paket definiert
- Sie bewegen sich von einer Plattform, auf der Sie kein OVF-Paket erstellen können (z. B. ältere Plattformen oder Images)
- Sie möchten eine ältere VMware-Appliance importieren, die keine OVF-Informationen enthält.
- Sie möchten eine eigenständige VM importieren, die keine OVF-Informationen enthält

Sofern verfügbar, empfehlen wir, Appliance-Pakete zu importieren, die OVF-Metadaten anstelle eines einzelnen Disk-Images enthalten. Die OVF-Daten enthalten Informationen, die der Importassistent benötigt, um eine VM von seinem Datenträgerimage neu zu erstellen. Diese Informationen umfassen die Anzahl der Datenträgerimages, die mit der VM verknüpft sind, den Prozessor, den Speicher, das Netzwerk, den Speicherbedarf usw. Ohne diese Informationen kann es viel komplexer und fehleranfälliger sein, die VM neu zu erstellen.

XVA-Format

XVA ist ein für XenServer spezifisches virtuelles Appliance-Format, das eine einzelne VM als einen einzigen Satz von Dateien packt, einschließlich eines Deskriptors und Disk-Images. Die Dateinamenerweiterung lautet `.xva`.

Der Deskriptor (Dateinamenerweiterung `ova.xml`) gibt die virtuelle Hardware einer einzelnen VM an.

Das Disk-Image-Format ist ein Verzeichnis von Dateien. Der Verzeichnisname entspricht einem Referenznamen im Deskriptor und enthält zwei Dateien für jeden 1-MB-Block des Disk-Images. Der Basisname jeder Datei ist die Blocknummer in Dezimalzahl. Die erste Datei enthält einen Block des Disk-Images im Roh-Binärformat und hat keine Erweiterung. Die zweite Datei ist eine Prüfsumme der ersten Datei. Wenn die VM aus Citrix Hypervisor 8.0 oder früher exportiert wurde, hat diese Datei die

Erweiterung `.checksum`. Wenn die VM aus Citrix Hypervisor 8.1 oder höher exportiert wurde, hat diese Datei die Erweiterung `.xxhash`.

> **Wichtig:**
>
> Wenn eine VM vom XenServer-Host exportiert und dann in einen anderen XenServer-Host mit einem anderen CPU-Typ importiert wird, läuft sie möglicherweise nicht richtig. Beispielsweise läuft eine Windows-VM, die von einem Host mit einer Intel® VT-fähigen CPU exportiert wurde, möglicherweise nicht, wenn sie in einen Host mit einer AMD-VTM-CPU importiert wird.

Betriebssystem-Update

Wenn Sie ein virtuelles Gerät oder ein Festplatten-Image importieren, das von einer anderen Virtualisierungsplattform als XenServer erstellt und exportiert wurde, müssen Sie die VM möglicherweise konfigurieren, bevor sie ordnungsgemäß auf dem XenServer-Host gestartet wird.

XenCenter enthält eine erweiterte Hypervisor-Interoperabilitätsfunktion —Operating System Fixup —, die darauf abzielt, ein grundlegendes Maß an Interoperabilität für VMs sicherzustellen, die Sie in XenServer importieren. Verwenden Sie Operating System Fixup, wenn Sie VMs aus OVF/OVA-Paketen und Datenträgerimages importieren, die auf anderen Virtualisierungsplattformen erstellt wurden.

Der Betriebssystem-Fixup-Prozess behebt die Geräte- und Treiberprobleme des Betriebssystems, die beim Wechsel von einem Hypervisor zum anderen auftreten. Der Prozess versucht, Probleme mit dem Startgerät mit der importierten VM zu reparieren, die das darin enthaltene Betriebssystem möglicherweise daran hindern, in der XenServer-Umgebung zu booten. Diese Funktion ist nicht für Konvertierungen von einer Plattform zur anderen ausgelegt.

> **Hinweis:**
>
> Für diese Funktion ist ein ISO-Speicherrepository mit 40 MB freiem Speicherplatz und 256 MB virtuellem Speicher erforderlich.

Das Betriebssystem-Fixup wird als automatisch startendes ISO-Image geliefert, das an das DVD-Laufwerk der importierten VM angeschlossen ist. Es führt die erforderlichen Reparaturvorgänge durch, wenn die VM zum ersten Mal gestartet wird, und fährt dann die VM herunter. Beim nächsten Start der neuen VM wird das Startgerät zurückgesetzt und die VM wird normal gestartet.

Um Operating System Fixup auf importierten Disk-Images oder OVF/OVA-Paketen zu verwenden, aktivieren Sie das Feature auf der Seite Erweiterte Optionen des XenCenter Import-Assistenten. Geben Sie einen Speicherort an, an den das Fixup-ISO kopiert wird, damit XenServer es verwenden kann.

Was macht das Betriebssystem-Fixup mit der VM?

Die Option Betriebssystemfixup wurde entwickelt, um minimale Änderungen zu ermöglichen, damit ein virtuelles System gestartet werden kann. Je nach Gastbetriebssystem und Hypervisor des ursprünglichen Hosts sind nach der Verwendung von Operating System Fixup möglicherweise weitere Aktionen erforderlich. Zu diesen Aktionen können Konfigurationsänderungen und Treiberinstallationen gehören.

Während des Fixup-Vorgangs wird ein ISO auf ein ISO-SR kopiert. Das ISO-Image ist an eine VM angeschlossen. Die Startreihenfolge wird vom virtuellen DVD-Laufwerk gestartet, und die VM startet in das ISO-Image. Die Umgebung innerhalb des ISO überprüft dann jeden Datenträger der VM, um festzustellen, ob es sich um ein Linux- oder ein Windows-System handelt.

Wenn ein Linux-System erkannt wird, wird der Speicherort der GRUB-Konfigurationsdatei bestimmt. Alle Zeiger auf SCSI-Disk-Boot-Geräte werden so geändert, dass sie auf IDE-Datenträger verweisen. Wenn GRUB beispielsweise einen Eintrag `/dev/sda1` enthält, der den ersten Datenträger auf dem ersten SCSI-Controller darstellt, wird dieser Eintrag in `/dev/hda1` geändert. was den ersten Datenträger auf dem ersten IDE-Controller darstellt.

Wenn ein Windows-System erkannt wird, wird ein generischer kritischer Startgerätetreiber aus der Treiberdatenbank des installierten Betriebssystems extrahiert und beim Betriebssystem registriert. Dieser Vorgang ist besonders wichtig für ältere Windows-Betriebssysteme, wenn das Startgerät zwischen einer SCSI- und einer IDE-Schnittstelle gewechselt wird.

Wenn bestimmte Virtualisierungs-Toolsets in der VM erkannt werden, sind sie deaktiviert, um Leistungsprobleme und unnötige Ereignismeldungen zu verhindern.

Importieren von virtuellen Rechnern

Wenn Sie eine VM importieren, erstellen Sie effektiv eine VM und verwenden dabei viele der gleichen Schritte, die zum Bereitstellen einer neuen VM erforderlich sind. Zu diesen Schritten gehören das Nominieren eines Hosts sowie das Konfigurieren von Speicher und Netzwerk.

Sie können OVF/OVA-, Disk-Image-, XVA- und XVA Version 1-Dateien mit dem XenCenter Importassistenten importieren. Sie können XVA-Dateien auch über die xe CLI importieren.

VMs aus OVF/OVA importieren

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu importieren, müssen Sie als Root angemeldet sein oder die Rolle Pool-Administrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.

Mit dem XenCenter Importassistenten können Sie VMs importieren, die als OVF-/OVA-Dateien gespeichert wurden. Der Importassistent führt Sie durch die üblichen Schritte zum Erstellen einer VM in XenCenter: Nominieren eines Hosts und anschließendes Konfigurieren von Speicher und Netzwerk für die neue VM. Beim Importieren von OVF- und OVA-Dateien sind möglicherweise zusätzliche Schritte erforderlich, z. B.:

- Führen Sie beim Importieren von VMs, die mit anderen Virtualisierungsplattformen erstellt wurden, die Funktion zur Betriebssystemfixierung aus, um ein grundlegendes Maß an Interoperabilität für die VM sicherzustellen. Weitere Informationen finden Sie unter Betriebssystem-Update.

> **Tipp:**
>
> Stellen Sie sicher, dass der Zielhost über ausreichend RAM verfügt, um die zu importierenden virtuellen Maschinen zu unterstützen. Ein Mangel an verfügbarem RAM führt zu einem fehlgeschlagenen Import. Weitere Informationen zur Behebung dieses Problems finden Sie unter CTX125120 —Appliance-Import-Assistent schlägt wegen fehlendem Arbeitsspeicher fehl.

Importierte OVF-Pakete werden beim Importieren mit XenCenter als vApps angezeigt. Wenn der Import abgeschlossen ist, werden die neuen VMs im Bereich XenCenter **Resources** angezeigt, und die neue vApp wird im Dialogfeld **vApps verwalten** angezeigt.

Importieren von VMs aus OVF/OVA mit XenCenter:

1. Öffnen Sie den Importassistenten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü die Option **Importieren** aus.
   - Wählen Sie im Menü **Datei** die Option **Importieren**aus.
2. Suchen Sie auf der ersten Seite des Assistenten nach der Datei, die Sie importieren möchten, und klicken Sie dann auf **Weiter**, um fortzufahren.
3. Prüfen und akzeptieren Sie gegebenenfalls die EULAs.

   Wenn das Paket, das Sie importieren, EULAs enthält, akzeptieren Sie diese und klicken Sie auf **Weiter**, um fortzufahren. Wenn keine EULAs im Paket enthalten sind, überspringt der Assistent diesen Schritt und geht direkt zur nächsten Seite über.
4. Geben Sie den Pool oder Host an, in den Sie die VMs importieren möchten, und weisen Sie die VMs dann (optional) einem Home-Server zu.

   Um einen Host oder Pool auszuwählen, wählen Sie aus der Liste Zu **importierende VM (s)** aus.

   Um jeder VM einen Home-Server zuzuweisen, wählen Sie einen Host aus der Liste auf dem **Home Server**aus. Wenn Sie keinen Homeserver zuweisen möchten, wählen Sie **Keinen Homeserver zuweisen**aus.

   Klicken Sie zum Fortfahren auf **Weiter**.

5. Konfigurieren des Speichers für die importierten VMs: Wählen Sie ein oder mehrere Speicherrepositories aus, auf denen die importierten virtuellen Datenträger abgelegt werden sollen, und klicken Sie dann auf **Weiter**, um fortzufahren.

   Um alle importierten virtuellen Datenträger auf demselben SR zu platzieren, wählen Sie **Alle importierten VMs auf diesem Ziel-SR platzieren** aus. Wählen Sie ein SR aus der Liste aus.

   Um die virtuellen Laufwerke eingehender VMs auf verschiedenen SRs zu **platzieren, wählen Sie Importierte VMs auf den angegebenen Ziel-SRs**platzieren aus. Wählen Sie für jede VM das Ziel-SR aus der Liste in der SR-Spalte aus.

6. Konfigurieren des Netzwerks für die importierten VMs: Ordnen Sie die virtuellen Netzwerkschnittstellen in den VMs, die Sie importieren, den Zielnetzwerken im Zielpool zu. Das Netzwerk und die MAC-Adresse, die in der Liste der eingehenden VMs angezeigt werden, werden als Teil der Definition der ursprünglichen (exportierten) VM in der Exportdatei gespeichert. Um eine eingehende virtuelle Netzwerkschnittstelle einem Zielnetzwerk zuzuordnen, wählen Sie ein Netzwerk aus der Liste in der Spalte Zielnetzwerk aus. Klicken Sie zum Fortfahren auf **Weiter**.

7. Sicherheitseinstellungen angeben: Wenn das ausgewählte OVF-/OVA-Paket mit Sicherheitsfunktionen wie Zertifikaten oder einem Manifest konfiguriert ist, geben Sie die erforderlichen Informationen an, und klicken Sie dann auf **Weiter**, um fortzufahren.

   Auf der Seite Sicherheit werden verschiedene Optionen angezeigt, je nachdem, welche Sicherheitsfunktionen auf der OVF-Appliance konfiguriert wurden:

   - Wenn die Appliance signiert ist, wird das Kontrollkästchen **Digitale Signatur** überprüfen angezeigt, das automatisch aktiviert ist. Klicken Sie auf **Zertifikat anzeigen**, um das Zertifikat anzuzeigen, mit dem das Paket signiert wurde. Wenn das Zertifikat als nicht vertrauenswürdig erscheint, ist es wahrscheinlich, dass entweder dem Stammzertifikat oder der ausstellenden Zertifizierungsstelle auf dem lokalen Computer nicht vertraut wird. Deaktivieren Sie das Kontrollkästchen **Digitale Signatur überprüfen**, wenn Sie die Signatur nicht überprüfen möchten.
   - Wenn die Appliance ein Manifest enthält, wird das Kontrollkästchen **Manifestinhalt** überprüfen angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit der Assistent die Liste der Dateien im Paket überprüft.

   Wenn Pakete digital signiert werden, wird das zugehörige Manifest automatisch überprüft, sodass das Kontrollkästchen **Manifestinhalt** überprüfen auf der Seite Sicherheit nicht angezeigt wird.

   > **Hinweis:**
   >
   > VMware Workstation 7.1.x OVF-Dateien können nicht importiert werden, wenn Sie das Man-

> ifest überprüfen möchten. Dieser Fehler tritt auf, weil VMware Workstation 7.1.x eine OVF-Datei mit einem Manifest erzeugt, das ungültige SHA-1-Hashes enthält. Wenn Sie das Manifest nicht überprüfen möchten, ist der Import erfolgreich.

8. Betriebssystemfixup aktivieren: Wenn die VMs in dem Paket, das Sie importieren, auf einer anderen Virtualisierungsplattform als XenServer erstellt wurden, aktivieren Sie das Kontrollkästchen **Betriebssystemfixup verwenden** . Wählen Sie eine ISO-SR aus, in die die Fixup-ISO kopiert werden kann, damit XenServer darauf zugreifen kann. Weitere Informationen zu dieser Funktion finden Sie unter Betriebssystem-Update.

   Klicken Sie zum Fortfahren auf **Weiter**.

9. Überprüfen Sie die Importeinstellungen und klicken Sie dann auf **Fertig stellen**, um den Importvorgang zu starten und den Assistenten zu schließen.

   > **Hinweis:**
   >
   > Das Importieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Der Importfortschritt wird in der Statusleiste am unteren Rand des XenCenter-Fensters und auf der Registerkarte **Protokolle** angezeigt. Wenn die neu importierte VM verfügbar ist, wird sie im Bereich **Ressourcen** angezeigt, und die neue vApp wird im Dialogfeld **vApps verwalten** angezeigt.

> **Hinweis:**
>
> Nachdem Sie XenCenter zum Importieren eines OVF-Pakets verwendet haben, das Windows-Betriebssysteme enthält, müssen Sie den Parameter `platform` festlegen.
>
> 1. Setzen Sie den Parameter `platform` auf `device_id=0002`. Beispiel:
>
>    ```
>    xe vm-param-set uuid=VM uuid platform:device_id=0002
>    ```
>
> 2. Setzen Sie den Parameter `platform` auf `viridian=true`. Beispiel:
>
>    ```
>    xe vm-param-set uuid=VM uuid platform:viridian=true
>    ```

Importieren von Datenträgerimages

Mit dem XenCenter Importassistenten können Sie ein Disk-Image als VM in einen Pool oder einen bestimmten Host importieren. Der Importassistent führt Sie durch die üblichen Schritte zum Erstellen einer VM in XenCenter: Nominieren eines Hosts und anschließendes Konfigurieren von Speicher und Netzwerk für die neue VM.

Anforderungen

- Sie müssen als root angemeldet sein oder die Rolle Pooladministrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.
- Stellen Sie sicher, dass DHCP auf dem Verwaltungsnetzwerk ausgeführt wird, das XenServer verwendet.
- Der Import-Assistent benötigt lokalen Speicher auf dem Server, auf dem Sie ihn ausführen.

So importieren Sie VMs mit XenCenter aus einem Disk-Image:

1. Öffnen Sie den Importassistenten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü die Option **Importieren** aus.
   - Wählen Sie im Menü **Datei** die Option **Importieren**aus.
2. Suchen Sie auf der ersten Seite des Assistenten nach der Datei, die Sie importieren möchten, und klicken Sie dann auf **Weiter**, um fortzufahren.
3. Geben Sie den VM-Namen an und weisen Sie CPU- und Speicherressourcen zu

   Geben Sie einen Namen für die neue VM ein, die aus dem importierten Disk-Image erstellt werden soll, und weisen Sie dann die Anzahl der CPUs und die Menge an Arbeitsspeicher zu. Klicken Sie zum Fortfahren auf **Weiter**.
4. Geben Sie den Pool oder Host an, in den Sie die VMs importieren möchten, und weisen Sie die VMs dann (optional) einem Home-Server zu.

   Um einen Host oder Pool auszuwählen, wählen Sie aus der Liste Zu **importierende VM (s)** aus.

   Um jeder VM einen Home-Server zuzuweisen, wählen Sie einen Host aus der Liste auf dem **Home Server**aus. Wenn Sie keinen Homeserver zuweisen möchten, wählen Sie **Keinen Homeserver zuweisen**aus.

   Klicken Sie zum Fortfahren auf **Weiter**.
5. Konfigurieren des Speichers für die importierten VMs: Wählen Sie ein oder mehrere Speicherrepositories aus, auf denen die importierten virtuellen Datenträger abgelegt werden sollen, und klicken Sie dann auf **Weiter**, um fortzufahren.

   Um alle importierten virtuellen Datenträger auf demselben SR zu platzieren, wählen Sie **Alle importierten VMs auf diesem Ziel-SR platzieren** aus. Wählen Sie ein SR aus der Liste aus.

   Um die virtuellen Laufwerke eingehender VMs auf verschiedenen SRs zu **platzieren, wählen Sie Importierte VMs auf den angegebenen Ziel-SRs**platzieren aus. Wählen Sie für jede VM das Ziel-SR aus der Liste in der SR-Spalte aus.

6. Konfigurieren des Netzwerks für die importierten VMs: Ordnen Sie die virtuellen Netzwerkschnittstellen in den VMs, die Sie importieren, den Zielnetzwerken im Zielpool zu. Das Netzwerk und die MAC-Adresse, die in der Liste der eingehenden VMs angezeigt werden, werden als Teil der Definition der ursprünglichen (exportierten) VM in der Exportdatei gespeichert. Um eine eingehende virtuelle Netzwerkschnittstelle einem Zielnetzwerk zuzuordnen, wählen Sie ein Netzwerk aus der Liste in der Spalte Zielnetzwerk aus. Klicken Sie zum Fortfahren auf **Weiter**.

7. Betriebssystemfixup aktivieren: Wenn die Disk-Images, die Sie importieren, auf einer anderen Virtualisierungsplattform als XenServer erstellt wurden, aktivieren Sie das Kontrollkästchen Betriebssystemfixup verwenden. Wählen Sie eine ISO-SR aus, in die die Fixup-ISO kopiert werden kann, damit XenServer darauf zugreifen kann. Weitere Informationen zu dieser Funktion finden Sie unter Betriebssystem-Update.

   Klicken Sie zum Fortfahren auf **Weiter**.

8. Überprüfen Sie die Importeinstellungen und klicken Sie dann auf **Fertig stellen**, um den Importvorgang zu starten und den Assistenten zu schließen.

   > **Hinweis:**
   >
   > Das Importieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Der Importfortschritt wird in der Statusleiste am unteren Rand des XenCenter-Fensters und auf der Registerkarte **Protokolle** angezeigt. Wenn die neu importierte VM verfügbar ist, wird sie im Bereich **Ressourcen** angezeigt.

> **Hinweis:**
>
> Nachdem Sie XenCenter zum Importieren eines Datenträgerimages verwendet haben, das Windows-Betriebssysteme enthält, müssen Sie den Parameter `platform` festlegen. Der Wert dieses Parameters hängt von der Version von Windows ab, die im Disk-Image enthalten ist:

- Stellen Sie für Windows Server 2016 und höher den Parameter `platform` auf `device_id=0002` ein. Beispiel:

```
xe vm-param-set uuid=VM uuid platform:device_id=0002
<!--NeedCopy-->
```

- Stellen Sie für alle anderen Versionen von Windows den Parameter `platform` auf `viridian=true` ein. Beispiel:

```
xe vm-param-set uuid=VM uuid platform:viridian=true
<!--NeedCopy-->
```


VMs aus XVA importieren

Sie können VMs, Vorlagen und Snapshots importieren, die zuvor exportiert und lokal im XVA-Format (`.xva`) gespeichert wurden. Um dies zu tun, führen Sie die üblichen Schritte zum Erstellen einer VM aus: Nominieren eines Hosts und anschließendes Konfigurieren von Speicher und Netzwerk für die neue VM.

> **Warnung:**
>
> Es ist möglicherweise nicht immer möglich, eine importierte VM auszuführen, die von einem anderen Host mit einem anderen CPU-Typ exportiert wurde. Beispielsweise kann eine Windows-VM, die von einem Host mit einer Intel VT-fähigen CPU exportiert wurde, möglicherweise nicht ausgeführt werden, wenn sie auf einen Host mit einer AMD-VTM-CPU importiert wird.

So importieren Sie VMs aus XVA mit XenCenter:

1. Öffnen Sie den Importassistenten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü die Option **Importieren** aus.
   - Wählen Sie im Menü **Datei** die Option **Importieren**aus.
2. Suchen Sie auf der ersten Seite des Assistenten die Datei, die Sie importieren möchten (`.xva` oder `ova.xml`), und klicken Sie dann auf **Weiter**, um fortzufahren.

   Wenn Sie einen URL-Speicherort (`http`, `httpsfile`, oder `ftp`) in das Feld **Dateiname** eingeben. Klicken Sie auf **Weiter**, ein Dialogfeld zum Herunterladen des Pakets wird geöffnet, und Sie müssen einen Ordner auf Ihrem XenCenter Host angeben, in den die Datei kopiert wird.
3. Wählen Sie einen Pool oder Host aus, auf dem die importierte VM gestartet werden soll, und wählen Sie dann **Weiter**, um fortzufahren.
4. Wählen Sie die Speicher-Repositorys aus, auf denen das importierte virtuelle Laufwerk platziert werden soll, und klicken Sie dann auf **Weiter**, um fortzufahren.
5. Konfigurieren des Netzwerks für die importierte VM: Ordnen Sie die virtuelle Netzwerkschnittstelle in der VM zu, die Sie importieren, um ein Netzwerk im Zielpool anzuvisieren. Das Netzwerk und die MAC-Adresse, die in der Liste der eingehenden VMs angezeigt werden, werden als Teil der Definition der ursprünglichen (exportierten) VM in der Exportdatei gespeichert. Um eine eingehende virtuelle Netzwerkschnittstelle einem Zielnetzwerk zuzuordnen, wählen Sie ein Netzwerk aus der Liste in der Spalte Zielnetzwerk aus. Klicken Sie zum Fortfahren auf **Weiter**.
6. Überprüfen Sie die Importeinstellungen und klicken Sie dann auf **Fertig stellen**, um den Importvorgang zu starten und den Assistenten zu schließen.

> **Hinweis:**
>
> Das Importieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Der Importfortschritt wird in der Statusleiste am unteren Rand des XenCenter-Fensters und auf der Registerkarte **Protokolle** angezeigt. Wenn die neu importierte VM verfügbar ist, wird sie im Bereich **Ressourcen** angezeigt.

So importieren Sie eine VM aus XVA über die xe-CLI :

Um die VM in die Standard-SR auf dem XenServer-Zielhost zu importieren, geben Sie Folgendes ein:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file
<!--NeedCopy-->
```

Um die VM in eine andere SR auf dem XenServer-Zielhost zu importieren, fügen Sie den optionalen Parameter `sr-uuid` hinzu:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
<!--NeedCopy-->
```

Wenn Sie die MAC-Adresse der ursprünglichen VM beibehalten möchten, fügen Sie den optionalen Parameter `preserve` hinzu und setzen Sie ihn auf **`true`**:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file preserve=true
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Importieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Nachdem die VM importiert wurde, gibt die Eingabeaufforderung die UUID der neu importierten VM zurück.

Exportieren von virtuellen Rechnern

Sie können OVF/OVA- und XVA-Dateien mit dem XenCenter Export-Assistenten exportieren. Sie können XVA-Dateien auch über die xe-CLI exportieren.

VMs als OVF/OVA exportieren

Mit dem XenCenter Exportassistenten können Sie eine oder mehrere virtuelle Maschinen als OVF-/OVA-Paket exportieren. Wenn Sie VMs als OVF-/OVA-Paket exportieren, werden die Konfigurationsdaten zusammen mit den virtuellen Datenträgern jeder VM exportiert.

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu exportieren, müssen Sie als Root angemeldet sein oder die Rolle Pool-Administrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.

So exportieren Sie VMs mit XenCenter als OVF/OVA:

1. Fahren Sie die zu exportierenden VMs herunter oder setzen Sie sie aus.
2. Öffnen Sie den Export-Assistenten: Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf den Pool oder Host, der die zu exportierenden VMs enthält, und wählen Sie dann **Exportieren**aus.
3. Auf der ersten Seite des Assistenten:
   - Geben Sie den Namen der Exportdatei ein
   - Geben Sie den Ordner an, in dem die Dateien gespeichert werden sollen
   - Wählen Sie **OVF/OVA-Paket (*.ovf, *.ova)** aus der Liste **Format** aus
   - Klicken Sie auf **Weiter**, um fortzufahren
4. Wählen Sie aus der Liste der verfügbaren VMs die VMs aus, die Sie in das OVF-/OVA-Paket aufnehmen möchten, und klicken Sie dann auf **Weiter**, um fortzufahren.
5. Falls erforderlich, können Sie dem Paket ein zuvor vorbereitetes Dokument der Endbenutzer-Lizenzvereinbarung (EULA) (.rtf, .txt) hinzufügen.

   Um eine EULA hinzuzufügen, klicken Sie auf **Hinzufügen** und navigieren Sie zu der Datei, die Sie hinzufügen möchten. Nachdem Sie die Datei hinzugefügt haben, können Sie das Dokument anzeigen, indem Sie es aus der Liste der **EULA-Dateien** auswählen und dann auf **Ansicht**klicken.

   EULAs können die rechtlichen Bedingungen für die Nutzung des Geräts und der in der Appliance gelieferten Anwendungen enthalten.

   Durch die Möglichkeit, eine oder mehrere EULAs einzubeziehen, können Sie die Software auf der Appliance rechtlich schützen. Wenn Ihre Appliance beispielsweise ein proprietäres Betriebssystem in ihren VMs enthält, möchten Sie möglicherweise den Text der Endbenutzer-Lizenzvereinbarung von diesem Betriebssystem aufnehmen. Der Text wird angezeigt und die Person, die das Gerät importiert, muss ihn akzeptieren.

> **Hinweis:**
>
> Der Versuch, EULA-Dateien hinzuzufügen, die nicht in unterstützten Formaten vorliegen, einschließlich XML- oder Binärdateien, kann dazu führen, dass der Import der EULA fehlschlägt.

Wählen Sie **Weiter**, um fortzufahren.

6. Geben Sie auf der Seite **Erweiterte Optionen** ein Manifest, eine Signatur und Optionen für die Ausgabedatei an, oder klicken Sie einfach auf **Weiter**, um fortzufahren.

   a) Um ein Manifest für das Paket zu **erstellen, aktivieren Sie das Kontrollkästchen Manifest** erstellen.

   Das Manifest enthält eine Bestandsaufnahme oder eine Liste der anderen Dateien in einem Paket. Das Manifest wird verwendet, um sicherzustellen, dass die ursprünglich bei der Paketerstellung enthaltenen Dateien dieselben Dateien sind, die beim Eintreffen des Pakets vorhanden waren. Beim Importieren der Dateien wird eine Prüfsumme verwendet, um zu überprüfen, ob sich die Dateien seit dem Erstellen des Pakets nicht geändert haben.

   b) So fügen Sie dem Paket eine digitale Signatur hinzu

      i. Wählen Sie **OVF-Paket signieren**aus.

      Die digitale Signatur (`.cert`) enthält die Signatur der Manifestdatei und das Zertifikat, mit dem diese Signatur erstellt wurde. Wenn ein signiertes Paket importiert wird, kann der Benutzer die Identität des Paketerstellers überprüfen, indem er den öffentlichen Schlüssel des Zertifikats verwendet, um die digitale Signatur zu validieren.

      ii. Suchen Sie nach einem Zertifikat.

      Verwenden Sie ein X.509-Zertifikat, das Sie bereits von einer Trusted Authority erstellt und als `.pfx`-Datei exportiert haben. Für Zertifikate mit SHA-256-Digest exportieren Sie den “Microsoft Enhanced RSA and AES Cryptographic Provider”als CSP.

      iii. Geben Sie **unter Kennwort für privaten Schlüssel** das Exportkennwort (PFX) oder, falls kein Exportkennwort angegeben wurde, den privaten Schlüssel ein, der dem Zertifikat zugeordnet ist.

   c) Um die ausgewählten VMs als einzelne (TAR-) Datei im OVA-Format auszugeben, aktivieren Sie das Kontrollkästchen **OVA-Paket erstellen (einzelne OVA-Exportdatei)** . Weitere Informationen zu den verschiedenen Dateiformaten finden Sie unter Virtualisierungsformat öffnen.

   d) Um virtuelle Festplattenimages (VHD-Dateien) zu komprimieren, die im Paket enthalten sind, aktivieren Sie das Kontrollkästchen OVF-Dateien komprimieren.

Wenn Sie ein OVF-Paket erstellen, wird den virtuellen Datenträgerimages standardmäßig der gleiche Speicherplatz zugewiesen wie der exportierten VM. Beispielsweise verfügt eine VM, der 26 GB Speicherplatz zugewiesen sind, über ein Festplattenimage, das 26 GB Speicherplatz belegt. Das Festplattenimage nutzt diesen Speicherplatz unabhängig davon, ob die VM ihn tatsächlich benötigt oder nicht.

> **Hinweis:**
>
> Durch das Komprimieren der VHD-Dateien dauert der Exportvorgang länger. Das Importieren eines Pakets mit komprimierten VHD-Dateien dauert ebenfalls länger, da der Importassistent beim Importieren alle VHD-Images extrahieren muss.

Wenn sowohl **OVA-Paket erstellen (einzelne OVA-Exportdatei)** als auch **OVF-Dateien komprimieren** aktiviert sind, ist das Ergebnis eine komprimierte OVA-Datei mit der Erweiterung `.ova.gz`.

7. Prüfen Sie die Exporteinstellungen.

   Um den Assistenten das exportierte Paket überprüfen zu lassen, aktivieren Sie das Kontrollkästchen **Export nach Abschluss** überprüfen. Klicken Sie auf **Fertig stellen**, um den Exportvorgang zu starten und den Assistenten zu schließen.

   > **Hinweis:**
   >
   > Das Exportieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Der Exportfortschritt wird in der Statusleiste am unteren Rand des XenCenter-Fensters und auf der Registerkarte **Protokolle** angezeigt. Um einen laufenden Export abzubrechen, klicken Sie auf die Registerkarte **Protokolle**, suchen Sie den Export in der Liste der Ereignisse und klicken Sie auf die Schaltfläche **Abbrechen**.

VMs als XVA exportieren Sie können eine vorhandene VM mit dem XenCenter Export-Assistenten oder der xe-CLI als XVA-Datei exportieren. Wir empfehlen, eine VM auf einen anderen Computer als den XenServer-Host zu exportieren, auf dem Sie eine Bibliothek mit Exportdateien verwalten können. Sie können die VM beispielsweise auf den Computer exportieren, auf dem XenCenter ausgeführt wird.

> **Warnung:**
>
> Es ist möglicherweise nicht immer möglich, eine importierte VM auszuführen, die von einem anderen Host mit einem anderen CPU-Typ exportiert wurde. Beispielsweise kann eine Windows-

> VM, die von einem Host mit einer Intel VT-fähigen CPU exportiert wurde, möglicherweise nicht ausgeführt werden, wenn sie auf einen Host mit einer AMD-VTM-CPU importiert wird.

Exportieren von VMs als XVA-Dateien mit XenCenter:

1. Fahren Sie die VM, die Sie exportieren möchten, herunter oder setzen Sie sie aus.
2. Öffnen Sie den Export-Assistenten: Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf die VM, die Sie exportieren möchten, und wählen Sie dann **Exportieren**aus.
3. Auf der ersten Seite des Assistenten:
   - Geben Sie den Namen der Exportdatei ein
   - Geben Sie den Ordner an, in dem die Dateien gespeichert werden sollen
   - Wählen Sie die **XVA-Datei (*.xva)** aus der Liste "**Format** "
   - Klicken Sie auf **Weiter**, um fortzufahren
4. Wählen Sie aus der Liste der verfügbaren VMs die VM aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**, um fortzufahren.
5. Prüfen Sie die Exporteinstellungen.

   Um den Assistenten das exportierte Paket überprüfen zu lassen, aktivieren Sie das Kontrollkästchen **Export nach Abschluss** überprüfen. Klicken Sie auf Fertig stellen, um den Exportvorgang zu starten und den Assistenten zu schließen.

   > **Hinweis:**
   >
   > Das Exportieren einer VM kann einige Zeit dauern, abhängig von der Größe der VM und der Geschwindigkeit und Bandbreite der Netzwerkverbindung.

Der Exportfortschritt wird in der Statusleiste am unteren Rand des XenCenter-Fensters und auf der Registerkarte **Protokolle** angezeigt. Um einen laufenden Export abzubrechen, klicken Sie auf die Registerkarte **Protokolle**, suchen Sie den Export in der Liste der Ereignisse und klicken Sie auf die Schaltfläche **Abbrechen**.

So exportieren Sie VMs als XVA-Dateien mit der xe-CLI:

1. Fahren Sie die VM herunter, die Sie exportieren möchten.
2. Exportieren Sie die VM, indem Sie Folgendes ausführen:

```
xe vm-export -h hostname -u root -pw password vm=vm_name \
    filename=pathname_of_file
<!--NeedCopy-->
```


> **Hinweis:**
>
> Achten Sie darauf, die Erweiterung `.xva` bei der Angabe des Exportdateinamens anzugeben. Wenn die exportierte VM diese Erweiterung nicht hat, erkennt XenCenter die Datei möglicherweise nicht als gültige XVA-Datei, wenn Sie versuchen, sie zu importieren.

VMs löschen

September 19, 2023

Sie können VMs über die xe-CLI oder XenCenter löschen.

Durch das Löschen einer virtuellen Maschine (VM) werden ihre Konfiguration und ihr Dateisystem vom Host entfernt. Wenn Sie eine VM löschen, können Sie festlegen, ob alle virtuellen Laufwerke, die an die VM angeschlossen sind, gelöscht oder beibehalten werden sollen, zusätzlich zu allen Snapshots der VM.

Löschen einer VM mit der xe CLI

So löschen Sie eine VM:

1. Suchen Sie die VM-UUID:

   ```
   xe vm-list
   ```

2. Fahren Sie die VM herunter:

   ```
   xe vm-shutdown uuid=<uuid>
   ```

3. (Optional) Sie können die angeschlossenen virtuellen Datenträger löschen:

   a) Suchen Sie die UUIDs des virtuellen Datenträgers:

   ```
   xe vm-disk-list vm=<uuid>
   ```

   b) Löschen Sie das virtuelle Laufwerk:

   ```
   xe vdi-destroy uuid=<uuid>
   ```

   > **Wichtig:**
   >
   > Alle Daten, die in den virtuellen Laufwerken der VM gespeichert sind, gehen verloren.

4. (Optional) Sie können die mit der VM verknüpften Snapshots löschen:

a) Finde die UUIDs der Snapshots:

```
xe snapshot-list snapshot-of=<uuid>
```

b) Suchen Sie für jeden zu löschenden Snapshot die UUIDs der virtuellen Datenträger für diesen Snapshot:

```
xe snapshot-disk-list snapshot-uuid=<uuid>
```

c) Löschen Sie jedes Snapshot-Laufwerk:

```
xe vdi-destroy uuid=<uuid>
```

d) Löschen Sie den Snapshot:

```
xe snapshot-destroy uuid=<uuid>
```

5. Löschen Sie die VM:

```
xe vm-destroy uuid=<uuid>
```

Löschen einer VM über XenCenter

So löschen Sie eine VM:

1. Fahren Sie die VM herunter.
2. Wählen Sie die gestoppte VM im Bereich **Ressourcen** aus, klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü **Löschen** aus. Wählen Sie alternativ im Menü **VM** die Option **Löschen**aus.
3. Um ein angeschlossenes virtuelles Laufwerk zu löschen, aktivieren Sie das entsprechende Kontrollkästchen.

   > **Wichtig:**
   >
   > Alle Daten, die in den virtuellen Laufwerken der VM gespeichert sind, gehen verloren.

4. Um einen Snapshot der VM zu löschen, aktivieren Sie das entsprechende Kontrollkästchen.
5. Klicken Sie auf **Löschen**.

   Wenn der Löschvorgang abgeschlossen ist, wird die VM aus dem Bereich **Ressourcen** entfernt.

> **Hinweis:**
>
> VM-Snapshots, deren übergeordnete VM gelöscht wurde (*verwaiste Snapshots*), können weiterhin über den Bereich **Ressourcen** aufgerufen werden. Diese Snapshots können exportiert, gelöscht oder zum Erstellen von VMs und Vorlagen verwendet werden. Um Snapshots im

> **Ressourcenbereich** anzuzeigen, wählen Sie im Navigationsbereich **Objekte** aus und erweitern Sie dann die Gruppe **Snapshots** im Ressourcenbereich.

vApps

September 19, 2023

Eine vApp ist eine logische Gruppe aus einer oder mehreren verwandten virtuellen Maschinen (VMs), die als eine Einheit gestartet werden können. Wenn eine vApp gestartet wird, werden die in der vApp enthaltenen VMs in einer vom Benutzer vordefinierten Reihenfolge gestartet. Mit dieser Funktion können virtuelle Maschinen, die voneinander abhängen, automatisch sequenziert werden. Ein Administrator muss den Start abhängiger VMs nicht mehr manuell sequenzieren, wenn ein ganzer Dienst einen Neustart erfordert (z. B. für ein Softwareupdate). Die VMs innerhalb der vApp müssen sich nicht auf einem Host befinden und können mithilfe der normalen Regeln innerhalb eines Pools verteilt werden.

Die vApp-Funktion ist in der Notfallwiederherstellungssituation nützlich. Sie können alle VMs gruppieren, die sich im selben Speicherrepository befinden, oder alle VMs, die sich auf dasselbe Service Level Agreement (SLA) beziehen.

> **Hinweis:**
>
> vApps können sowohl mit XenCenter als auch mit der xe CLI erstellt und geändert werden. Informationen zum Arbeiten mit vApps über die CLI finden Sie unter Befehlszeilenschnittstelle.

Verwalten von vApps in XenCenter

Im Dialogfeld **vApps verwalten** können Sie vApps erstellen, löschen, ändern, starten und herunterfahren sowie vApps innerhalb des ausgewählten Pools importieren und exportieren. Wenn Sie in der Liste eine vApp auswählen, werden die darin enthaltenen VMs im Detailbereich auf der rechten Seite aufgeführt.

Mit **"vApps verwalten"** können Sie die folgenden Aktionen ausführen:

- So ändern Sie den Namen oder die Beschreibung einer vApp
- So fügen Sie der vApp virtuelle Computer hinzu oder entfernen sie aus
- So ändern Sie die Startreihenfolge der VMs in der vApp

So ändern Sie vApps:

1. Wählen Sie den Pool aus, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus.

Sie können auch mit der rechten Maustaste in den Bereich **Ressourcen** klicken und im Kontextmenü **vApps verwalten** auswählen.

2. Wählen Sie die vApp aus und wählen Sie **Eigenschaften**, um das Eigenschaften-Dialogfeld zu öffnen.
3. Wählen Sie die Registerkarte **Allgemein**, um den Namen oder die Beschreibung der vApp zu ändern.
4. Wählen Sie die Registerkarte **Virtuelle Maschinen** aus, um VMs zur vApp hinzuzufügen oder daraus zu entfernen.
5. Wählen Sie die Registerkarte **VM-Startsequenz** aus, um die Startreihenfolge und die Verzögerungsintervallwerte für einzelne VMs in der vApp zu ändern.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und **Eigenschaften**zu schließen.

vApps erstellen

Gehen Sie folgendermaßen vor, um VMs in einer vApp zu gruppieren:

1. Wählen Sie den Pool aus, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus.
2. Geben Sie einen Namen für die vApp und optional eine Beschreibung ein. Klicken Sie auf **Weiter**.

   Sie können einen beliebigen Namen wählen, aber ein Name, der die vApp beschreibt, ist am besten. Obwohl es ratsam ist, zu vermeiden, mehrere vApps mit demselben Namen zu erstellen, ist dies nicht erforderlich. XenCenter erzwingt nicht, dass vApp-Namen eindeutig sind. Es ist nicht notwendig, Anführungszeichen für Namen zu verwenden, die Leerzeichen enthalten.
3. Wählen Sie aus, welche VMs in die neue vApp aufgenommen werden sollen. Klicken Sie auf **Weiter**.

   Sie können das Suchfeld verwenden, um nur VMs aufzulisten, die Namen haben, die die angegebene Textzeichenfolge enthalten.
4. Geben Sie die Startsequenz für die VMs in der vApp an. Klicken Sie auf **Weiter**.

Wert	Beschreibung
Bestellung starten	Gibt die Reihenfolge an, in der einzelne VMs innerhalb der vApp gestartet werden, sodass bestimmte VMs vor anderen neu gestartet werden können. VMs mit einem Startreihenfolgenwert von 0 (Null) werden zuerst gestartet. Virtuelle Rechner mit einem Startreihenfolgenwert von 1 werden als Nächstes gestartet. Dann werden VMs mit einem Startreihenfolgenwert von 2 gestartet und so weiter.
Versuch, die nächste VM danach zu starten	Gibt an, wie lange nach dem Start der VM gewartet werden soll, bevor versucht wird, die nächste Gruppe von VMs in der Startsequenz zu starten. Bei dieser nächsten Gruppe handelt es sich um die Gruppe von VMs mit einer niedrigeren Startreihenfolge.

1. Auf der letzten Seite von **vApps verwalten**können Sie die vApp-Konfiguration überprüfen. Klicken Sie auf **Zurück**, um zurückzugehen und Einstellungen zu ändern, oder auf **Fertig stellen**, um die vApp zu erstellen und **vApps verwalten**zu schließen.

> **Hinweis:**
>
> Eine vApp kann sich über mehrere Hosts in einem einzigen Pool erstrecken, kann sich jedoch nicht über mehrere Pools erstrecken.

vApps löschen

Gehen Sie wie folgt vor, um eine vApp zu löschen:

1. Wählen Sie den Pool aus, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus.
2. Wählen Sie die vApp, die Sie löschen möchten, aus der Liste aus. Klicken Sie auf **Löschen**.

> **Hinweis:**
>
> Die virtuellen Maschinen in der vApp werden **nicht** gelöscht.

Starten und Herunterfahren von vApps mit XenCenter

Um eine vApp zu starten oder herunterzufahren, verwenden Sie **vApps verwalten**, auf die Sie über das **Pool**-Menü zugreifen können. Wenn Sie eine vApp starten, werden alle darin enthaltenen VMs automatisch nacheinander gestartet. Die für jede einzelne VM angegebenen Werte für die Startreihenfolge und das Verzögerungsintervall steuern die Startsequenz. Diese Werte können festgelegt werden, wenn Sie die vApp zum ersten Mal erstellen. Sie können diese Werte jederzeit im Dialogfeld vApp-Eigenschaften oder im Eigenschaftendialogfeld der einzelnen VM ändern.

So starten Sie eine vApp:

1. Öffnen Sie **vApps verwalten**: Wählen Sie den Pool aus, in dem sich die VMs in der vApp befinden, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus. Sie können auch mit der rechten Maustaste in den Bereich **Ressourcen** klicken und im Kontextmenü **vApps verwalten** auswählen.
2. Wählen Sie die vApp aus und klicken Sie auf **Start**, um alle darin enthaltenen VMs zu starten.

So fahren Sie eine vApp herunter:

1. Öffnen Sie **vApps verwalten**: Wählen Sie den Pool aus, in dem sich die VMs in der vApp befinden, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus. Sie können auch mit der rechten Maustaste in den Bereich **Ressourcen** klicken und im Kontextmenü **vApps verwalten** auswählen.
2. Wählen Sie die vApp aus und klicken Sie auf **Herunterfahren**, um alle VMs in der vApp herunterzufahren.

   Ein Soft-Shutdown wird auf allen VMs versucht. Wenn ein Soft-Shutdown nicht möglich ist, wird ein erzwungenes Herunterfahren durchgeführt.

> **Hinweis:**
>
> Ein weiches Herunterfahren führt ein ordnungsgemäßes Herunterfahren der VM durch, und alle laufenden Prozesse werden einzeln angehalten.
>
> Ein erzwungenes Herunterfahren führt ein hartes Herunterfahren durch und entspricht dem Trennen eines physischen Servers. Es werden möglicherweise nicht immer alle laufenden Prozesse heruntergefahren. Wenn Sie eine VM auf diese Weise herunterfahren, riskieren Sie Datenverlust. Verwenden Sie ein erzwungenes Herunterfahren nur, wenn ein Soft Shutdown nicht möglich ist

Importieren und exportieren Sie vApps

vApps können als OVF/OVA-Pakete importiert und exportiert werden. Weitere Informationen finden Sie unter Importieren und Exportieren von VMs.

So exportieren Sie eine vApp:

1. Öffnen **Sie vApps verwalten**: Wählen Sie im Menü **Pool** die Option **vApps verwalten**aus.
2. Wählen Sie in der Liste die vApp aus, die Sie exportieren möchten. Klicken Sie auf **Exportieren**.
3. Befolgen Sie das unter Exportieren von VMs als OVF/OVAbeschriebene Verfahren.

Das Exportieren einer vApp kann einige Zeit in Anspruch nehmen.

So importieren Sie eine vApp:

1. Öffnen **Sie vApps verwalten**: Wählen Sie im Menü **Pool** die Option **vApps verwalten**aus.
2. Klicken Sie auf **Importieren**, um das Dialogfeld **Importieren** zu öffnen.
3. Befolgen Sie das unter Importieren von VMs als OVF/OVAbeschriebene Verfahren.

Nachdem der Import abgeschlossen ist, wird die neue vApp in der Liste der vApps unter “vApps **verwalten**”angezeigt.

Fortgeschrittene Hinweise für virtuelle Maschinen

January 19, 2024

Dieser Abschnitt enthält einige erweiterte Hinweise für virtuelle Maschinen.

VM-Startverhalten

Es gibt zwei Optionen für das Verhalten des VDI einer virtuellen Maschine beim Booten der VM:

> **Hinweis:**
>
> Die VM muss heruntergefahren werden, bevor Sie ihre Einstellung für das Startverhalten ändern können.

Persist

> **Tipp:**
>
> Verwenden Sie dieses Startverhalten, wenn Sie Citrix Virtual Desktops hosten, die statische oder dedizierte Maschinen sind.

Dieses Verhalten ist die Standardeinstellung beim Booten der VM. Der VDI befindet sich in dem Zustand, in dem er sich beim letzten Herunterfahren befand.

Wählen Sie diese Option aus, wenn Sie Benutzern erlauben möchten, dauerhafte Änderungen an ihren Desktops vorzunehmen. Um "Persistieren"auszuwählen, fahren Sie die VM herunter und geben Sie dann den folgenden Befehl ein:

```
xe vdi-param-set uuid=vdi_uuid on-boot=persist
<!--NeedCopy-->
```

Zurücksetzen

> **Tipp:**
>
> Verwenden Sie dieses Startverhalten, wenn Sie Citrix Virtual Desktops hosten, bei denen es sich um gemeinsam genutzte oder zufällig zugewiesene Maschinen handelt.

Beim Start der VM wird der VDI in den Zustand zurückgesetzt, in dem er sich beim vorherigen Start befand. Alle während der Ausführung der VM vorgenommenen Änderungen gehen verloren, wenn die VM das nächste Mal gestartet wird.

Wählen Sie diese Option, wenn Sie standardisierte Desktops bereitstellen möchten, die Benutzer nicht dauerhaft ändern können. Um Reset auszuwählen, fahren Sie die VM herunter und geben Sie dann den folgenden Befehl ein:

> **Warnung:**
>
> Nach der Änderung `on-boot=reset`werden alle im VDI gespeicherten Daten nach dem nächsten Herunterfahren/Start oder Neustart verworfen.

Stellen Sie die ISO-Bibliothek für XenServer-Hosts zur Verfügung

Um eine ISO-Bibliothek für XenServer-Hosts verfügbar zu machen, erstellen Sie ein externes NFS- oder SMB/CIFS-Freigabeverzeichnis. Der NFS- oder SMB/CIFS-Server muss Root-Zugriff auf die Freigabe ermöglichen. Ermöglichen Sie für NFS-Freigaben den Zugriff, indem Sie das Flag `no_root_squash` setzen, wenn Sie den Freigabeeintrag in `/etc/exports` auf dem NFS-Server erstellen.

Verwenden Sie dann entweder XenCenter, um die ISO-Bibliothek anzuhängen, oder stellen Sie eine Verbindung zur Hostkonsole her und führen Sie den folgenden Befehl aus:

```
xe-mount-iso-sr host:/volume
<!--NeedCopy-->
```

Für erweiterte Verwendung können Sie zusätzliche Argumente an den Mount-Befehl übergeben.

Um eine Windows SMB/CIFS-Freigabe für den Host verfügbar zu machen, verwenden Sie entweder XenCenter, oder stellen Sie eine Verbindung zur Hostkonsole her und führen Sie den folgenden Befehl aus:


```
xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
<!--NeedCopy-->
```

Ersetzen Sie die Rückstriche im Argument `unc_path` durch Schrägstriche. Beispiel:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
<!--NeedCopy-->
```

Nach dem Mounten der Freigabe sind alle verfügbaren ISOs in der Liste **Von ISO-Bibliothek installieren oder DVD-Laufwerk** in XenCenter verfügbar. Diese ISOs sind auch als CD-Images aus den CLI-Befehlen verfügbar.

Hängen Sie das ISO-Image an eine geeignete Windows-Vorlage an.

Verbinden mit einer Windows-VM mithilfe von Remotedesktop

Sie können eine der folgenden Möglichkeiten zum Anzeigen einer Windows VM-Konsole verwenden, die beide die vollständige Verwendung von Tastatur und Maus unterstützen.

- XenCenter verwenden. Diese Methode bietet eine grafische Standardkonsole und verwendet die in XenServer integrierte VNC-Technologie, um den Fernzugriff auf die Konsole Ihrer virtuellen Maschine zu ermöglichen.
- Herstellen einer Verbindung mit Windows Remote Desktop. Bei dieser Methode wird die Remote Desktop Protocol-Technologie verwendet.

In XenCenter auf der Registerkarte **Konsole** befindet sich die Schaltfläche **Switch to Remote Desktop** . Diese Schaltfläche deaktiviert die standardmäßige grafische Konsole in XenCenter und wechselt zur Verwendung von Remote Desktop.

Wenn Sie Remote Desktop in der VM nicht aktiviert haben, ist diese Schaltfläche deaktiviert. Um es zu aktivieren, installieren Sie die XenServer VM Tools für Windows. Befolgen Sie das nachstehende Verfahren, um es in jeder VM zu aktivieren, die Sie mit Remotedesktop verbinden möchten.

So aktivieren Sie Remotedesktop auf einer Windows-VM:

1. Öffnen Sie **System**, indem Sie auf die Schaltfläche **Start** klicken, mit der rechten Maustaste auf **Computer**klicken und dann **Eigenschaften**auswählen.
2. Klicken Sie auf **Remote-Einstellungen**. Wenn Sie nach einem Administratorkennwort gefragt werden, geben Sie das Kennwort ein, das Sie während des VM-Setups erstellt haben.
3. Klicken Sie im Bereich **Remotedesktop** auf das Kontrollkästchen **Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remote Desktop ausgeführt**wird.
4. Um Benutzer ohne Administratorrechte auszuwählen, die eine Verbindung zu dieser Windows-VM herstellen können, klicken Sie auf die Schaltfläche **Remotebenutzer auswählen** und geben

Sie die Benutzernamen an. Benutzer mit Administratorrechten in der Windows-Domäne können standardmäßig eine Verbindung herstellen.

Sie können jetzt über Remotedesktop eine Verbindung zu dieser VM herstellen. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel Verbinden mit einem anderen Computer mithilfe der Remotedesktopverbindung.

> **Hinweis:**
>
> Sie können keine Verbindung zu einer VM herstellen, die im Ruhezustand oder im Ruhezustand ist. Stellen Sie die Einstellungen für den Schlaf- und Ruhezustand auf dem Remotecomputer auf **Nie**ein.

Umgang mit der Zeit in Windows-VMs

Für Windows-Gäste steuert zunächst die Steuerdomänenuhr die Uhrzeit. Die Zeitaktualisierung während VM-Lebenszyklusvorgängen wie Suspendieren und Neustart.Wir empfehlen, einen zuverlässigen NTP-Dienst in der Steuerdomäne und allen Windows-VMs auszuführen.

Wenn Sie eine VM manuell so einstellen, dass sie der Steuerdomäne zwei Stunden voraus ist, bleibt sie bestehen. Sie können die VM voraussetzen, indem Sie einen Zeitzonen-Offset innerhalb der VM verwenden. Wenn Sie später die Steuerdomänenzeit ändern (entweder manuell oder per NTP), verschiebt sich die VM entsprechend, behält jedoch den Zwei-Stunden-Offset bei. Das Ändern der Zeitzone der Steuerdomäne wirkt sich nicht auf VM-Zeitzonen oder Offset aus. XenServer verwendet die Hardwareuhreinstellung der VM, um die VM zu synchronisieren. XenServer verwendet nicht die Systemuhreinstellung der VM.

Stellen Sie sicher, dass Sie die aktuellen XenServer VM Tools für Windows installiert haben, wenn Sie Vorgänge unterbrechen und fortsetzen oder die Livemigration verwenden. XenServer VM Tools für Windows benachrichtigen den Windows-Kernel, dass nach der Wiederaufnahme (möglicherweise auf einem anderen physischen Host) eine Zeitsynchronisierung erforderlich ist.

> **Hinweis:**
>
> Wenn Sie Windows-VMs in einer Citrix Virtual Desktops-Umgebung ausführen, müssen Sie sicherstellen, dass die Host-Uhr dieselbe Quelle wie die Active Directory-Domäne (AD) hat. Wenn die Uhren nicht synchronisiert werden, können die VMs eine falsche Uhrzeit anzeigen und die Windows PV-Treiber zum Absturz bringen.

Zeitmanagement bei Linux-VMs

Zusätzlich zu dem von XenServer definierten Verhalten können Betriebssystemeinstellungen und -verhalten das Zeitverarbeitungsverhalten Ihrer Linux-VMs beeinflussen. Einige Linux-Betriebssysteme synchronisieren möglicherweise regelmäßig ihre Systemuhr und Hardwareuhr,

oder das Betriebssystem verwendet standardmäßig seinen eigenen NTP-Dienst. Weitere Informationen finden Sie in der Dokumentation für das Betriebssystem Ihrer Linux-VM.

> **Hinweis:**
>
> Stellen Sie bei der Installation einer neuen Linux-VM sicher, dass Sie die Zeitzone von der Standard-UTC auf Ihren lokalen Wert ändern. Spezifische Verteilungsanweisungen finden Sie unter Linux-Versionshinweise

Hardwareuhren in Linux-VMs sind **nicht** mit der Uhr synchronisiert, die in der Steuerdomäne ausgeführt wird, und können geändert werden. Wenn die VM zum ersten Mal gestartet wird, wird die Steuerdomänenzeit verwendet, um die Anfangszeit der Hardwareuhr und der Systemuhr einzustellen.

Wenn Sie die Uhrzeit auf der Hardwareuhr ändern, wird diese Änderung beim Neustart der VM beibehalten.

Das Verhalten der Systemuhr hängt vom Betriebssystem der VM ab. Weitere Informationen finden Sie in der Dokumentation Ihres VM-Betriebssystems.

Sie können dieses Zeitverarbeitungsverhalten von XenServer nicht ändern.

Installieren von virtuellen Rechnern von Reseller Option Kit-Medien (BIOS-gesperrt)

Es gibt zwei Arten von virtuellen Rechnern: BIOS-Generic und BIOS-Customized. Um die Installation von Reseller Option Kit (mit BIOS gesperrten) OEM-Versionen von Windows auf einer VM zu ermöglichen, kopieren Sie die BIOS-Zeichenfolgen der VM von dem Host, mit dem das Medium geliefert wurde. Fortgeschrittene Benutzer können auch benutzerdefinierte Werte für die BIOS-Zeichenfolgen festlegen.

BIOS-Generikum

Die VM hat generische XenServer-BIOS-Zeichenfolgen.

> **Hinweis:**
>
> Wenn für eine VM beim Start keine BIOS-Zeichenfolgen festgelegt sind, werden die standardmäßigen XenServer-BIOS-Zeichenfolgen eingefügt und die VM wird BIOS-generisch.

Bios-kundenspezifisch

Sie können das BIOS auf zwei Arten anpassen: Copy-Host-BIOS-Zeichenfolgen und benutzerdefinierte BIOS-Zeichenfolgen.

> **Hinweis:**
>
> Nachdem Sie eine VM zum ersten Mal gestartet haben, können Sie ihre BIOS-Zeichenfolgen nicht ändern. Stellen Sie sicher, dass die BIOS-Zeichenfolgen korrekt sind, bevor Sie die VM zum ersten Mal starten.

Kopieren-Host-BIOS-Zeichenfolgen Die VM hat eine Kopie der BIOS-Strings eines bestimmten Hosts im Pool. Befolgen Sie die unten angegebenen Verfahren, um die mit Ihrem Host gelieferten BIOS-gesperrten Medien zu installieren.

XenCenter verwenden:

1. Klicken Sie im Assistenten für neue virtuelle Maschinen auf das Kontrollkästchen **Host-BIOS-Strings auf VM kopieren**.

Verwenden der Befehlszeilenschnittstelle:

1. Führen Sie den Befehl `vm-install copy-bios-strings-from` aus. Geben Sie `host-uuid` als den Host an, von dem die Zeichenfolgen kopiert werden (d. h. den Host, mit dem das Medium geliefert wurde):

   ```
   xe vm-install copy-bios-strings-from=host uuid \
       template=template name sr-name-label=name of sr \
       new-name-label=name for new VM
   <!--NeedCopy-->
   ```

   Dieser Befehl gibt die UUID der neu erstellten VM zurück.

   Beispiel:

   ```
   xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786
      ef4 \
       template="win7sp1" sr-name-label=Local\ storage  \
       new-name-label=newcentos
       7cd98710-bf56-2045-48b7-e4ae219799db
   <!--NeedCopy-->
   ```

2. Wenn die relevanten BIOS-Zeichenfolgen vom Host erfolgreich in die VM kopiert wurden, bestätigt der Befehl `vm-is-bios-customized` diesen Erfolg:

   ```
   xe vm-is-bios-customized uuid=VM uuid
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
       This VM is BIOS-customized.
   <!--NeedCopy-->
   ```


> **Hinweis:**
>
> Wenn Sie die VM starten, wird sie auf dem physischen Host gestartet, von dem Sie die BIOS-Strings kopiert haben.

> **Warnung:**
>
> Es liegt in Ihrer Verantwortung, die EULAs einzuhalten, die die Verwendung von BIOS-gesperrten Betriebssystemen regeln, die Sie installieren.

Benutzerdefinierte BIOS-Zeichenfolgen Der Benutzer hat die Möglichkeit, mithilfe von CLI/API benutzerdefinierte Werte in ausgewählten BIOS-Strings festzulegen. Gehen Sie wie folgt vor, um das Medium in einer VM mit benutzerdefiniertem BIOS zu installieren.

Verwenden der Befehlszeilenschnittstelle:

1. Führen Sie den Befehl `vm-install` aus (ohne `copy-bios-strings-from`):

```
xe vm-install template=template name sr-name-label=name of sr \
      new-name-label=name for new VM
<!--NeedCopy-->
```

   Dieser Befehl gibt die UUID der neu erstellten VM zurück.

   Beispiel:

```
xe vm-install template="win7sp1" sr-name-label=Local\ storage  \
      new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
<!--NeedCopy-->
```

2. Um benutzerdefinierte BIOS-Strings festzulegen, führen Sie den folgenden Befehl aus, bevor Sie die VM zum ersten Mal starten:

```
xe vm-param-set uuid=VM_UUID bios-strings:bios-vendor=VALUE \
    bios-strings:bios-version=VALUE bios-strings:system-
       manufacturer=VALUE \
    bios-strings:system-product-name=VALUE bios-strings:system-
       version=VALUE \
    bios-strings:system-serial-number=VALUE bios-strings:enclosure
       -asset-tag=VALUE
<!--NeedCopy-->
```

   Beispiel:

```
xe vm-param-set uuid=7cd98710-bf56-2045-48b7-e4ae219799db \
    bios-strings:bios-vendor="vendor name" \
    bios-strings:bios-version=2.4 \
    bios-strings:system-manufacturer="manufacturer name" \
```



```
    bios-strings:system-product-name=guest1 \
    bios-strings:system-version=1.0 \
    bios-strings:system-serial-number="serial number" \
    bios-strings:enclosure-asset-tag=abk58hr
<!--NeedCopy-->
```

Hinweise:

- Sobald die benutzerdefinierten BIOS-Strings in einem einzigen CLI/API-Aufruf festgelegt wurden, können sie nicht mehr geändert werden.
- Sie können entscheiden, wie viele Parameter Sie angeben möchten, um die benutzerdefinierten BIOS-Zeichenfolgen festzulegen.

Warnung:

Es liegt in Ihrer Verantwortung:

- Erfüllen Sie alle EULAs und Standards für die Werte, die im BIOS der VM festgelegt werden.
- Stellen Sie sicher, dass die Werte, die Sie für die Parameter angeben, Arbeitsparameter sind. Die Angabe falscher Parameter kann zum Fehler bei der Boot-/Medieninstallation führen.

Zuweisen einer GPU zu einer Windows-VM (zur Verwendung mit Citrix Virtual Desktops)

Mit XenServer können Sie einer Windows-VM, die auf demselben Host läuft, eine physische GPU im XenServer-Host zuweisen. Diese GPU-Pass-Through-Funktion kommt leistungsstarken Grafikbenutzern wie CAD-Designern zugute, die leistungsstarke Grafikfunktionen benötigen. Es wird nur für die Verwendung mit Citrix Virtual Desktops unterstützt.

XenServer unterstützt zwar nur eine GPU für jede VM, erkennt und gruppiert jedoch automatisch identische physische GPUs auf Hosts im selben Pool. Nach der Zuweisung zu einer Gruppe von GPUs kann eine VM auf jedem Host im Pool gestartet werden, der über eine verfügbare GPU in der Gruppe verfügt. Wenn eine VM an eine GPU angeschlossen ist, verfügt sie über bestimmte Funktionen, die nicht mehr verfügbar sind, darunter Livemigration, VM-Snapshots mit Speicher und Aussetzen/Fortsetzen.

Das Zuweisen einer GPU zu einer VM in einem Pool beeinträchtigt nicht den Betrieb anderer VMs im Pool. VMs mit angeschlossenen GPUs werden jedoch als nicht agil betrachtet. Wenn VMs mit angeschlossenen GPUs Mitglieder eines Pools mit aktivierter Hochverfügbarkeit sind, übersehen beide Funktionen diese VMs. Die virtuellen Maschinen können nicht automatisch migriert werden.

GPU-Passthrough kann mit XenCenter oder der xe-CLI aktiviert werden.

Anforderungen

GPU-Passthrough wird für bestimmte Maschinen und GPUs unterstützt. In allen Fällen muss die IOMMU-Chipsatzfunktion (bekannt als VT-d für Intel-Modelle) auf dem XenServer-Host verfügbar und aktiviert sein. Bevor Sie die GPU-Passthrough-Funktion aktivieren, besuchen Sie die Hardwarekompatibilitätsliste.

Vor dem Zuweisen einer GPU zu einer VM

Bevor Sie einer VM eine GPU zuweisen, platzieren Sie die entsprechenden physischen GPUs in Ihrem XenServer-Host und starten Sie den Computer neu. Beim Neustart erkennt XenServer automatisch alle physischen GPUs. Verwenden Sie den Befehl `xe pgpu-list`, um alle physischen GPUs auf allen Hosts im Pool anzuzeigen.

Stellen Sie sicher, dass die IOMMU-Chipsatzfunktion auf dem Host aktiviert ist. Geben Sie dazu Folgendes ein:

```
xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=
    iommu
<!--NeedCopy-->
```

Wenn der gedruckte Wert lautet **`false`**, ist IOMMU nicht aktiviert, und GPU-Passthrough ist mit dem angegebenen XenServer-Host nicht verfügbar.

So weisen Sie einer Windows-VM über XenCenter eine GPU zu:

1. Fahren Sie die VM herunter, der Sie eine GPU zuweisen möchten.
2. Öffnen Sie die VM-Eigenschaften: Rechtsklicken Sie auf die VM und wählen Sie **Eigenschaften**
3. Weisen Sie der VM eine GPU zu: Wählen Sie GPU aus der Liste der VM-Eigenschaften aus, und wählen Sie dann einen GPU-Typ aus. Klicken Sie auf **OK**.
4. Starten Sie die VM.

So weisen Sie einer Windows-VM über die xe-CLI eine GPU zu:

1. Fahren Sie die VM herunter, der Sie eine GPU-Gruppe zuweisen möchten, mit dem Befehl `xe vm-shutdown`.
2. Suchen Sie die UUID der GPU-Gruppe, indem Sie Folgendes eingeben:

   ```
   xe gpu-group-list
   <!--NeedCopy-->
   ```

   Dieser Befehl druckt alle GPU-Gruppen im Pool. Notieren Sie die UUID der entsprechenden GPU-Gruppe.

3. Hängen Sie die VM an eine GPU-Gruppe an, indem Sie Folgendes eingeben:

```
xe vpgu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
<!--NeedCopy-->
```

   Führen Sie den Befehl `xe vgpu-list` aus, um sicherzustellen, dass die GPU-Gruppe angehängt wurde.

4. Starten Sie die VM mit dem Befehl `xe vm-start`.

5. Installieren Sie nach dem Start der VM die Grafikkartentreiber auf der VM.

   Die Installation der Treiber ist unerlässlich, da die VM direkten Zugriff auf die Hardware auf dem Host hat. Die Treiber werden von Ihrem Hardwarehersteller bereitgestellt.

> **Hinweis:**
>
> Wenn Sie versuchen, eine VM mit GPU-Passthrough auf dem Host ohne verfügbare GPU in der entsprechenden GPU-Gruppe zu starten, gibt XenServer einen Fehler aus.

So trennen Sie eine Windows-VM über XenCenter von einer GPU:

1. Fahren Sie die VM herunter.
2. Öffnen Sie die VM-Eigenschaften: Rechtsklicken Sie auf die VM und wählen Sie **Eigenschaften**
3. Trennen Sie die GPU von der VM: Wählen Sie **GPU** aus der Liste der VM-Eigenschaften aus und wählen Sie dann **Keine** als GPU-Typ aus. Klicken Sie auf **OK**.
4. Starten Sie die VM.

So trennen Sie eine Windows-VM mit der xe-CLI von einer GPU:

1. Fahren Sie die VM mit dem Befehl `xe vm-shutdown` herunter.
2. Suchen Sie die UUID der an die VM angeschlossenen vGPU, indem Sie Folgendes eingeben:

```
xe vgpu-list vm-uuid=uuid_of_vm
<!--NeedCopy-->
```

3. Trennen Sie die GPU von der VM, indem Sie Folgendes eingeben:

```
xe vgpu-destroy uuid=uuid_of_vgpu
<!--NeedCopy-->
```

4. Starten Sie die VM mit dem Befehl `xe vm-start`.

Erstellen von ISO-Images

XenServer kann ISO-Images als Installationsmedien und Datenquellen für Windows- oder Linux-VMs verwenden. In diesem Abschnitt wird beschrieben, wie ISO-Images von CD/DVD-Medien erstellt wer-

den.

So erstellen Sie ein ISO-Image auf einem Linux-System:

1. Legen Sie den CD- oder DVD-ROM-Datenträger in das Laufwerk ein. Stellen Sie sicher, dass die Datenträger nicht gemountet ist. Um dies zu überprüfen, führen Sie den Befehl aus:

   ```
   mount
   <!--NeedCopy-->
   ```

   Wenn der Datenträger bereitgestellt ist, heben Sie die Bereitstellung des Datenträgers auf. Falls erforderlich, finden Sie in der Dokumentation Ihres Betriebssystems Unterstützung.

2. Führen Sie als root den Befehl aus

   ```
   dd if=/dev/cdrom of=/path/cdimg_filename.iso
   <!--NeedCopy-->
   ```

   Dieser Befehl benötigt einige Zeit. Wenn der Vorgang erfolgreich abgeschlossen wurde, sehen Sie Folgendes:

   ```
   1187972+0 records in
   1187972+0 records out
   <!--NeedCopy-->
   ```

   Ihre ISO-Datei ist fertig.

So erstellen Sie ein ISO-Image auf einem Windows-System:

Windows-Computer haben keinen entsprechenden Betriebssystembefehl zum Erstellen eines ISO-Werts. Die meisten CD-Brennwerkzeuge haben die Möglichkeit, eine CD als ISO-Datei zu speichern.

VNC für Linux-VMs aktivieren

February 24, 2024

Virtuelle Rechner sind möglicherweise nicht für die Unterstützung von Virtual Network Computing (VNC) eingerichtet, das XenServer zur Remotesteuerung von VMs verwendet. Bevor Sie eine Verbindung mit XenCenter herstellen können, stellen Sie sicher, dass der VNC-Server und ein X-Display-Manager auf der VM installiert und ordnungsgemäß konfiguriert sind. In diesem Abschnitt wird beschrieben, wie VNC auf jeder der unterstützten Linux-Betriebssystemverteilungen konfiguriert wird, um ordnungsgemäße Interaktionen mit XenCenter zu ermöglichen.

Verwenden Sie für CentOS-basierte VMs die nachstehenden Anweisungen für die Red Hat-basierten VMs, da sie denselben Basiscode verwenden, um grafischen VNC-Zugriff zu ermöglichen. CentOS *X* basiert auf Red Hat Enterprise Linux *X*.

Eine grafische Konsole auf Debian-VMs aktivieren

> **Hinweis:**
>
> Bevor Sie eine grafische Konsole auf Ihrer Debian-VM aktivieren, stellen Sie sicher, dass Sie die XenServer VM Tools für Linux installiert haben. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Die grafische Konsole für virtuelle Debian-Maschinen wird von einem VNC-Server bereitgestellt, der innerhalb der VM läuft. In der empfohlenen Konfiguration steuert ein Standard-Display-Manager die Konsole, sodass ein Anmeldedialogfeld bereitgestellt wird.

1. Installieren Sie Ihren Debian-Gast mit den Desktop-Systempaketen oder installieren Sie GDM (den Displaymanager) mit APT (gemäß den Standardverfahren).
2. Installieren Sie den Xvnc-Server mit `apt-get` (oder ähnlich):

   ```
   apt-get install vnc4server
   <!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Die grafische Debian-Desktop-Umgebung, die den Gnome Display Manager-Dämon der Version 3 verwendet, kann erhebliche CPU-Zeit in Anspruch nehmen. Deinstallieren Sie das Gnome Display Manager-Paket `gdm3` und installieren Sie das Paket `gdm` wie folgt:

   ```
   apt-get install gdm
   apt-get purge gdm3
   <!--NeedCopy-->
   ```

3. Richten Sie ein VNC-Kennwort ein (keines zu haben ist ein ernstes Sicherheitsrisiko), indem Sie den Befehl `vncpasswd` verwenden. Geben Sie einen Dateinamen ein, in den die Kennwortinformationen geschrieben werden sollen. Beispiel:

   ```
   vncpasswd /etc/vncpass
   <!--NeedCopy-->
   ```

4. Ändern Sie Ihre Datei `gdm.conf` (`/etc/gdm/gdm.conf`), um einen VNC-Server für die Verwaltung der Anzeige `0` zu konfigurieren, indem Sie die Abschnitte `[servers]` und `[daemon]` wie folgt erweitern:

   ```
   [servers]
   0=VNC
   [daemon]
   VTAllocation=false
   [server-VNC]
   name=VNC
   command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/
      vncpass BlacklistTimeout=0
   ```



```
    flexible=true
<!--NeedCopy-->
```

5. Starten Sie GDM neu und warten Sie dann, bis XenCenter die grafische Konsole erkennt:

```
/etc/init.d/gdm restart
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können überprüfen, ob der VNC-Server ausgeführt wird, indem Sie einen Befehl wie `ps ax | grep vnc` verwenden.

Aktivieren einer grafischen Konsole auf Red Hat-, CentOS- oder Oracle Linux-VMs

> **Hinweis:**
>
> Bevor Sie Ihre Red Hat VMs für VNC einrichten, stellen Sie sicher, dass Sie die XenServer VM Tools für Linux installiert haben. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux.

Um VNC auf Red Hat VMs zu konfigurieren, ändern Sie die GDM-Konfiguration. Die GDM-Konfiguration befindet sich in einer Datei, deren Speicherort je nach verwendeter Version von Red Hat Linux variiert. Bevor Sie es ändern, ermitteln Sie zunächst den Speicherort dieser Konfigurationsdatei. Diese Datei wird in mehreren nachfolgenden Verfahren in diesem Abschnitt geändert.

Bestimmen Sie den Speicherort Ihrer VNC-Konfigurationsdatei

Wenn Sie Red Hat Linux verwenden, ist die GDM-Konfigurationsdatei `/etc/gdm/custom.conf`. Diese Datei ist eine geteilte Konfigurationsdatei, die nur vom Benutzer angegebene Werte enthält, die die Standardkonfiguration überschreiben. Dieser Dateityp wird standardmäßig in neueren Versionen von GDM verwendet. Es ist in diesen Versionen von Red Hat Linux enthalten.

Konfigurieren Sie GDM für die Verwendung von VNC

1. Führen Sie als Stammverzeichnis auf der Text-CLI in der VM den Befehl `rpm -q vnc-server gdm` aus. Die Paketnamen `vnc-server` und `gdm` werden mit den angegebenen Versionsnummern angezeigt.

   Die angezeigten Paketnamen zeigen die Pakete an, die bereits installiert sind. Wenn Sie eine Meldung sehen, die besagt, dass ein Paket nicht installiert ist, haben Sie möglicherweise die Optionen für den grafischen Desktop während der Installation nicht ausgewählt. Installieren

Sie diese Pakete, bevor Sie fortfahren können. Einzelheiten zur Installation weiterer Software auf Ihrer VM finden Sie im entsprechenden Red Hat Linux x86-Installationshandbuch.

2. Öffnen Sie die GDM-Konfigurationsdatei mit Ihrem bevorzugten Texteditor und fügen Sie der Datei folgende Zeilen hinzu:

```
1     [server-VNC]
2     name=VNC Server
3     command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
          depth 16 \
4     -BlacklistTimeout 0
5     flexible=true
6  <!--NeedCopy-->
```

   Bei Konfigurationsdateien auf Red Hat Linux fügen Sie diese Zeilen in den leeren `[servers]`-Abschnitt ein.

3. Ändern Sie die Konfiguration so, dass der `Xvnc`-Server anstelle des Standard-X-Servers verwendet wird:

   - `0=Standard`

     Ändern Sie es zum Lesen:

     `0=VNC`

   - Wenn Sie Red Hat Linux verwenden, fügen Sie die obige Zeile direkt unter dem `[servers]`-Abschnitt und vor dem `[server-VNC]`-Abschnitt hinzu.

4. Speichern und schließen Sie die Datei.

Starten Sie GDM neu, damit Ihre Konfigurationsänderung wirksam wird, indem Sie den Befehl `/usr/sbin/gdm-restart` ausführen.

> **Hinweis:**
>
> Red Hat Linux verwendet Runlevel 5 für den grafischen Start. Wenn Ihre Installation in Runlevel 3 startet, ändern Sie diese Konfiguration, damit der Displaymanager gestartet wird, und erhalten Sie Zugriff auf eine grafische Konsole. Weitere Informationen finden Sie unter Ausführungsebenen überprüfen.

Firewalleinstellungen

Die Firewallkonfiguration erlaubt standardmäßig keinen VNC-Datenverkehr. Wenn Sie eine Firewall zwischen der VM und XenCenter haben, lassen Sie Datenverkehr über den Port zu, den die VNC-Verbindung verwendet. Standardmäßig wartet ein VNC-Server auf Verbindungen von einem VNC-Viewer am TCP-Port `5900 + n`, wobei `n` die Anzeigenummer (normalerweise Null) ist. Ein VNC-Server-Setup für Display-0 lauscht also auf dem TCP-Port `5900TCP-5901`, Display-1 ist und so

weiter. Konsultieren Sie Ihre Firewall-Dokumentation, um sicherzustellen, dass diese Ports geöffnet sind. Weitere Informationen finden Sie unter Von XenServer verwendete Kommunikationsports.

Wenn Sie die IP-Verbindungsverfolgung verwenden oder die Initiierung von Verbindungen auf nur von einer Seite beschränken möchten, konfigurieren Sie Ihre Firewall weiter.

So konfigurieren Sie die Red Hat-basierte VMS-Firewall zum Öffnen des VNC-Ports:

1. Verwenden Sie für RedHat Linux `system-config-securitylevel-tui`.
2. Wählen Sie **Anpassen** aus und fügen Sie `5900` zur Liste der anderen Ports hinzu.

Alternativ können Sie die Firewall bis zum nächsten Neustart deaktivieren, indem Sie den Befehl `service iptables stop` ausführen oder dauerhaft `chkconfig iptables off` ausführen. Diese Konfiguration kann zusätzliche Dienste für die Außenwelt verfügbar machen und die allgemeine Sicherheit Ihrer VM verringern.

VNC-Bildschirmauflösung

Nach dem Herstellen einer Verbindung zu einer VM über die grafische Konsole stimmt die Bildschirmauflösung manchmal nicht überein. Beispielsweise ist das VM-Display zu groß, um bequem in den Bereich der grafischen Konsole zu passen. Steuern Sie dieses Verhalten, indem Sie den VNC-Serverparameter `geometry` wie folgt festlegen:

1. Öffnen Sie die GDM-Konfigurationsdatei mit Ihrem bevorzugten Texteditor. Weitere Informationen finden Sie unter Bestimmen des Speicherorts Ihrer VNC-Konfigurationsdatei.
2. Suchen Sie den Abschnitt `[server-VNC]`, den Sie oben hinzugefügt haben.
3. Bearbeiten Sie die Befehlszeile zum Lesen, zum Beispiel:

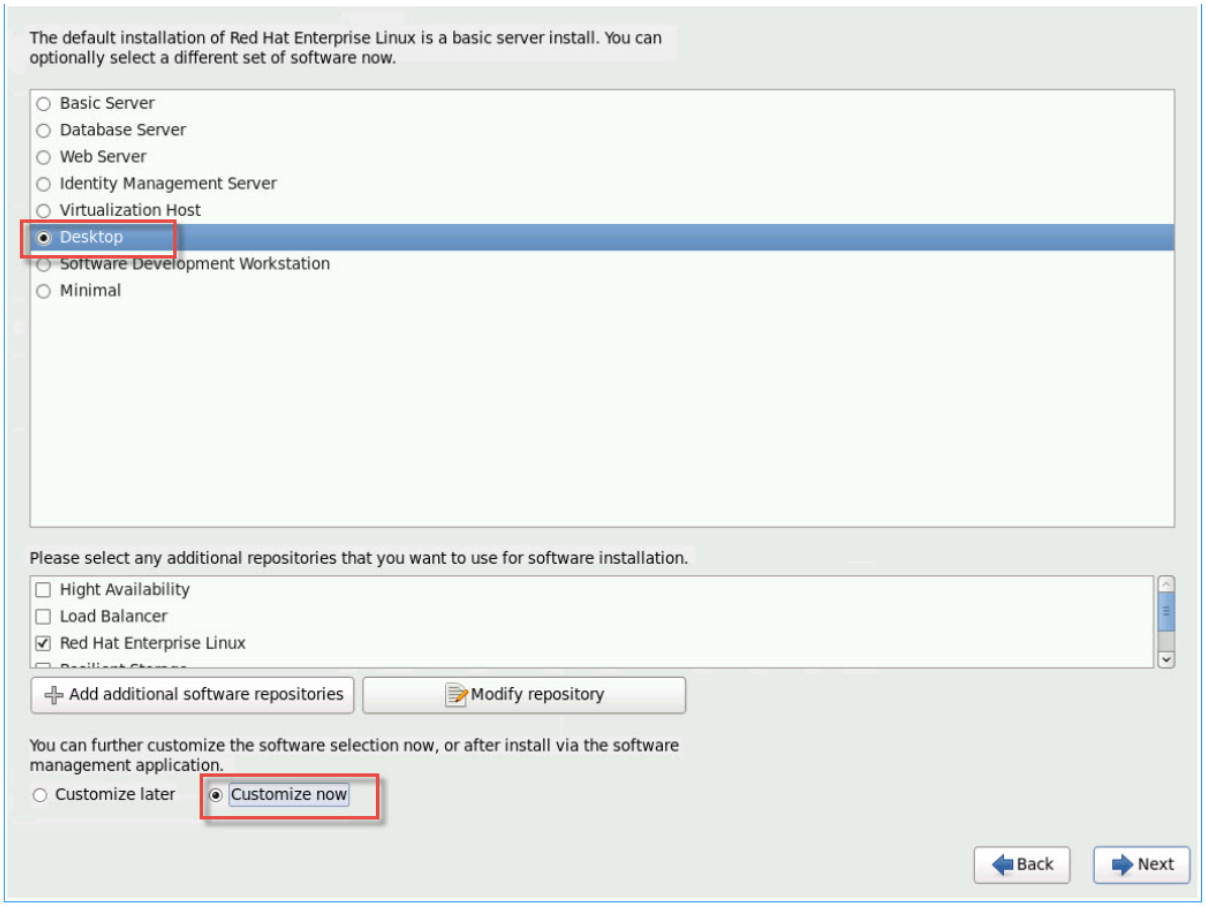
   ```
   command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
   <!--NeedCopy-->
   ```

   Der Wert des Parameters `geometry` kann eine beliebige gültige Bildschirmbreite und -höhe sein.
4. Speichern und schließen Sie die Datei.

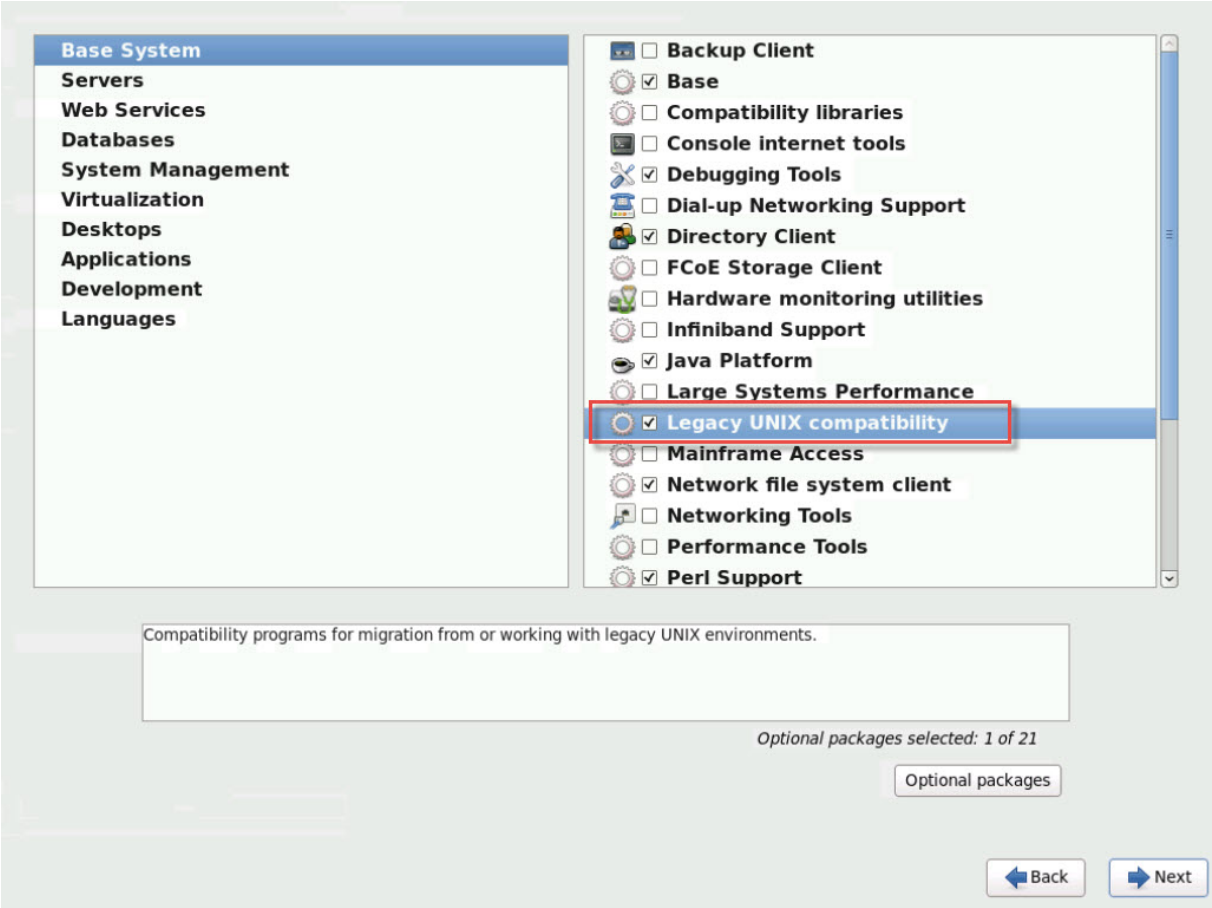
VNC für RHEL-, CentOS- oder OEL-VMs aktivieren

Wenn Sie Red Hat Linux verwenden, ist die GDM-Konfigurationsdatei `/etc/gdm/custom.conf`. Diese Datei ist eine geteilte Konfigurationsdatei, die nur vom Benutzer angegebene Werte enthält, die die Standardkonfiguration überschreiben. Standardmäßig wird dieser Dateityp in neueren Versionen von GDM verwendet und ist in diesen Versionen von Red Hat Linux enthalten.

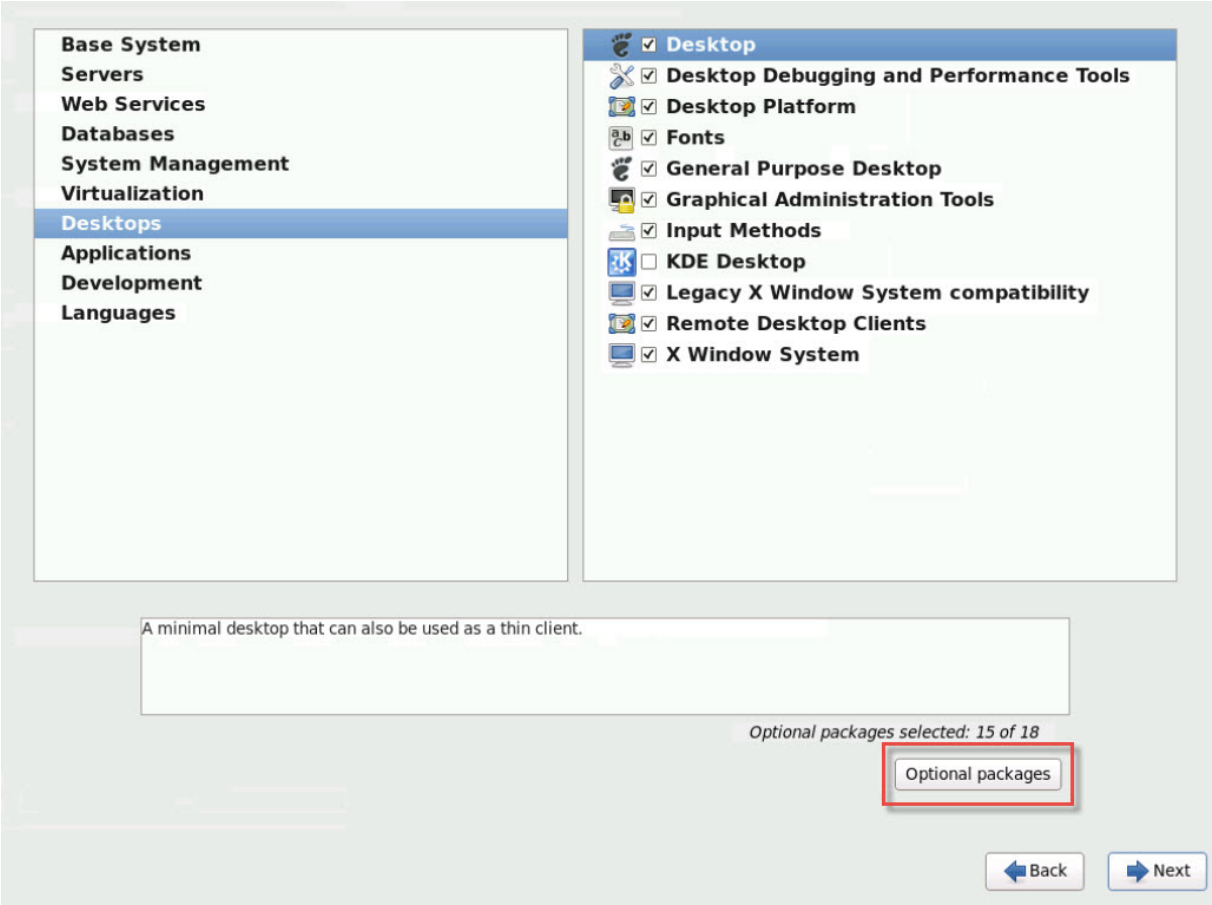
Wählen Sie während der Betriebssysteminstallation den **Desktop-Modus** aus. Wählen Sie auf dem RHEL-Installationsbildschirm **Desktop** > **Jetzt anpassen** aus und klicken Sie dann auf **Weiter**:



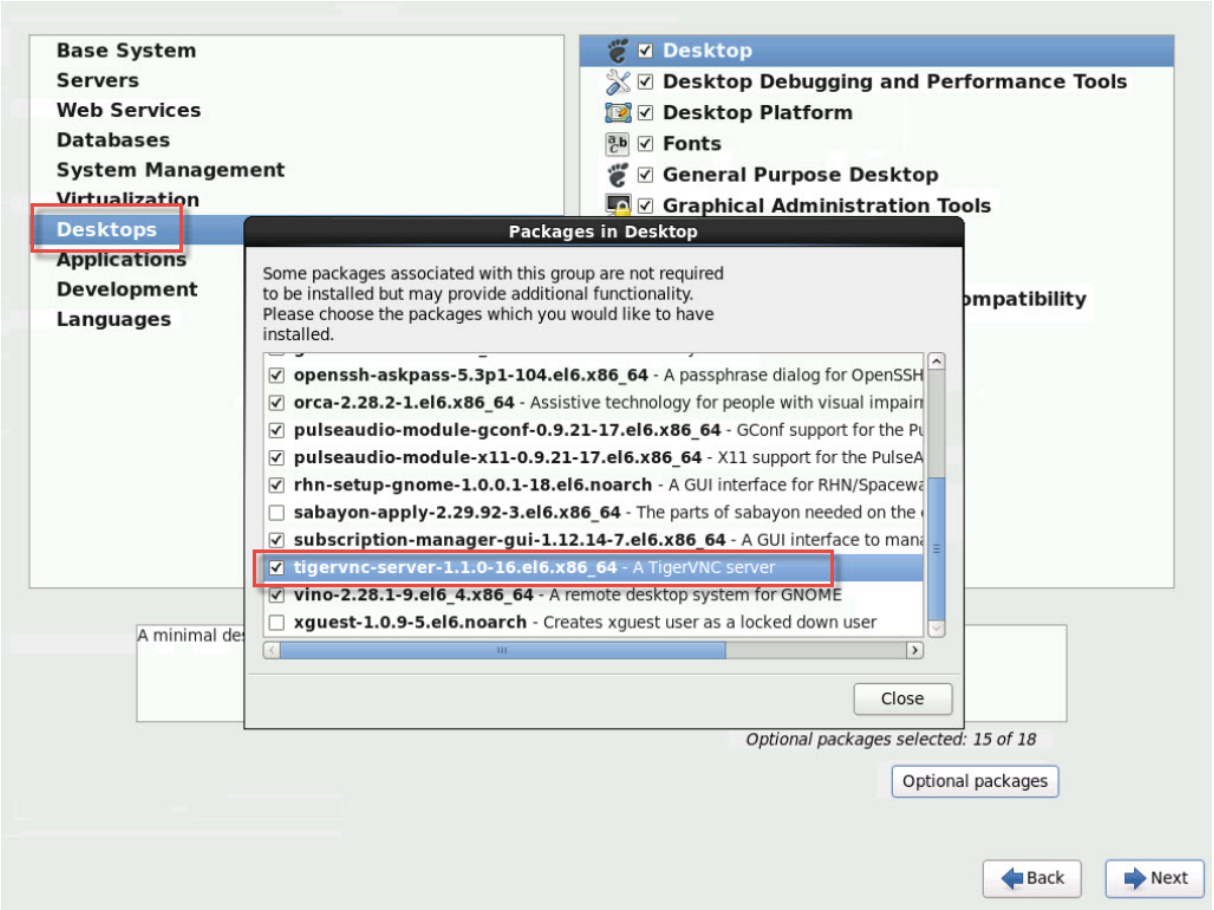
Diese Aktion zeigt den Bildschirm Basissystem an. Stellen Sie sicher, dass **Legacy-UNIX-Kompatibilität** ausgewählt ist:



Wählen Sie **Desktops** > **Optionale Pakete**aus und klicken Sie dann auf **Weiter**:



Diese Aktion zeigt das Fenster **Pakete in Desktop** an, wählen Sie **tigervnc-server-<version_number>** und klicken Sie dann auf **Weiter**:



Führen Sie die folgenden Schritte durch, um die Einrichtung Ihrer RHEL VMs fortzusetzen:

1. Öffnen Sie die GDM-Konfigurationsdatei mit Ihrem bevorzugten Texteditor und fügen Sie die folgenden Zeilen zu den entsprechenden Abschnitten hinzu:

```
    [security]
    DisallowTCP=false

    [xdmcp]
    Enable=true
<!--NeedCopy-->
```

2. Erstellen Sie die Datei `/etc/xinetd.d/vnc-server-stream`:

```
    service vnc-server
    {

                  id = vnc-server
            disable = no
               type = UNLISTED
               port = 5900
         socket_type = stream
               wait = no
               user = nobody
```



```
                group = tty
               server = /usr/bin/Xvnc
          server_args = -inetd -once -query localhost -
              SecurityTypes None \
          -geometry 800x600 -depth 16
      }

<!--NeedCopy-->
```

3. Geben Sie den folgenden Befehl ein, um den Dienst `xinetd` zu starten:

```
# service xinetd start
<!--NeedCopy-->
```

4. Öffne die Datei `/etc/sysconfig/iptables`. Füge die folgende Zeile über dem Zeilenwert hinzu `-A INPUT -j REJECT --reject-with icmp-host-prohibited`:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
<!--NeedCopy-->
```

5. Geben Sie den folgenden Befehl ein, um `iptables` neu zu starten:

```
# service iptables restart
<!--NeedCopy-->
```

6. Geben Sie den folgenden Befehl ein, um `gdm` neu zu starten:

```
    # telinit 3
    # telinit 5
<!--NeedCopy-->
```

> **Hinweis:**
>
> Red Hat Linux verwendet Runlevel 5 für den grafischen Start. Wenn Ihre Installation in Runlevel 3 startet, ändern Sie diese Konfiguration, damit der Displaymanager gestartet wird und um Zugriff auf eine grafische Konsole zu erhalten. Weitere Informationen finden Sie unter Ausführungsebenen überprüfen.

Einrichten von SLES-basierten VMs für VNC

> **Hinweis:**
>
> Bevor Sie Ihre SUSE Linux Enterprise Server-VMs für VNC einrichten, stellen Sie sicher, dass Sie die XenServer VM Tools für Linux installiert haben. Weitere Informationen finden Sie unter Installieren der XenServer VM Tools für Linux .

SLES bietet Unterstützung für die Aktivierung von "Remote Administration"als Konfigurationsoption in `YaST`. Sie können auswählen, dass die Remote-Verwaltung während der Installation aktiviert

werden soll. Diese Option ist im Bildschirm **Netzwerkdienste** des SLES-Installationsprogramms verfügbar. Mit dieser Funktion können Sie einen externen VNC-Viewer mit Ihrem Gast verbinden, damit Sie die grafische Konsole anzeigen können. Die Methode zur Verwendung der SLES-Remoteverwaltungsfunktion unterscheidet sich geringfügig von der von XenCenter bereitgestellten Methode. Es ist jedoch möglich, die Konfigurationsdateien in Ihrer SUSE Linux-VM so zu ändern, dass sie in die grafische Konsolenfunktion integriert sind.

Suchen Sie nach einem VNC-Server

Bevor Sie die Konfiguration ändern, stellen Sie sicher, dass Sie einen VNC-Server installiert haben. SUSE liefert standardmäßig mit `tightvnc`-Server. Dieser Server ist ein geeigneter VNC-Server, aber Sie können auch die RealVNC-Standardverteilung verwenden.

Sie können überprüfen, ob die `tightvnc`-Software installiert ist, indem Sie den folgenden Befehl ausführen:

```
rpm -q tightvnc
<!--NeedCopy-->
```

Remote-Verwaltung aktivieren

Wenn die Remoteverwaltung während der Installation der SLES-Software nicht aktiviert war, können Sie sie wie folgt aktivieren:

1. Öffnen Sie eine Textkonsole auf der VM und führen Sie das Dienstprogramm `YaST` aus:

   ```
   yast
   <!--NeedCopy-->
   ```

2. Wählen Sie mit den Pfeiltasten im linken Menü **Netzwerkdienste** aus. Gehen Sie mit der **Tabulatortaste** zum rechten Menü und wählen Sie mit den Pfeiltasten **Remoteverwaltung** aus. Drücken Sie die **Eingabetaste**.

3. Gehen Sie im Fenster **Remote-Verwaltung** mit der **Tabulatortaste** zum Abschnitt **Einstellungen der Remote-Verwaltung** . Wählen Sie mit den Pfeiltasten die Option **Remoteverwaltung zulassen** aus, und drücken **Sie die Eingabetaste**, um ein X in das Kontrollkästchen zu setzen.

4. Gehen**Sie mit der Tabulatortaste** zum Abschnitt **Firewall-Einstellungen** . Wählen Sie mit den Pfeiltasten **Port in Firewall öffnen** aus und drücken Sie die **Eingabetaste**, um ein X in das Kontrollkästchen zu setzen.

5. Drücken Sie die **Tabulatortaste**, um zur Schaltfläche **Fertig stellen** zu gelangen und drücken Sie die **Eingabetaste**.

6. Ein Meldungsfeld wird angezeigt, in dem Sie aufgefordert werden, den Displaymanager neu zu starten, damit Ihre Einstellungen wirksam werden. Drücken Sie die **Eingabetaste**, um die Meldung zu bestätigen.
7. Das ursprüngliche oberste Menü von YaST wird angezeigt. Wechseln Sie mit der **Tabulatortaste** zur **Quit**-Taste und drücken Sie die **Eingabetaste**.

Ändern der `xinetd`-Konfiguration

Ändern Sie nach der Aktivierung der Remoteverwaltung eine Konfigurationsdatei, wenn XenCenter eine Verbindung herstellen soll. Verwenden Sie alternativ einen VNC-Client eines Drittanbieters.

1. Öffnen Sie die Datei `/etc/xinetd.d/vnc` in Ihrem bevorzugten Texteditor.
2. Die Datei enthält Abschnitte wie die folgenden:

```
    service vnc1
    {

    socket_type = stream
    protocol    = tcp
    wait        = no
    user        = nobody
    server      = /usr/X11R6/bin/Xvnc
    server_args = :42 -inetd -once -query localhost -geometry 1024
       x768 -depth 16
    type        = UNLISTED
    port        = 5901
     }

<!--NeedCopy-->
```

3. Bearbeiten Sie die `port`-Zeile zu read

```
port = 5900
<!--NeedCopy-->
```

4. Speichern und schließen Sie die Datei.
5. Starten Sie den Display-Manager und den Dienst `xinetd` mit den folgenden Befehlen neu:

```
/etc/init.d/xinetd restart
rcxdm restart
<!--NeedCopy-->
```

SUSE Linux verwendet Runlevel 5 für den grafischen Start. Wenn Ihr Remotedesktop nicht angezeigt wird, überprüfen Sie, ob Ihre VM für den Start in Runlevel 5 konfiguriert ist. Weitere Informationen finden Sie unter Ausführungsebenen überprüfen.

Firewalleinstellungen

Standardmäßig lässt die Firewallkonfiguration keinen VNC-Datenverkehr zu. Wenn Sie eine Firewall zwischen der VM und XenCenter haben, lassen Sie Datenverkehr über den Port zu, den die VNC-Verbindung verwendet. Standardmäßig wartet ein VNC-Server auf Verbindungen von einem VNC-Viewer am TCP-Port `5900 + n`, wobei `n` die Anzeigenummer (normalerweise Null) ist. Ein VNC-Server-Setup für Display-0 lauscht also auf dem TCP-Port `5900TCP-5901`, Display-1 ist usw. Konsultieren Sie Ihre Firewall-Dokumentation, um sicherzustellen, dass diese Ports geöffnet sind. Weitere Informationen finden Sie unter Von XenServer verwendete Kommunikationsports.

Wenn Sie die IP-Verbindungsverfolgung verwenden oder die Initiierung von Verbindungen auf nur von einer Seite beschränken möchten, konfigurieren Sie Ihre Firewall weiter.

So öffnen Sie den VNC-Port auf der SLES 11.x-VMs-Firewall:

1. Öffnen Sie eine Textkonsole auf der VM und führen Sie das Dienstprogramm `YaST` aus:

   ```
   yast
   <!--NeedCopy-->
   ```

2. Wählen Sie mit den Pfeiltasten im linken Menü **Sicherheit und Benutzer** aus. Gehen**Sie mit der Tabulatortaste** zum rechten Menü und wählen Sie mit den Pfeiltasten **Firewall** Drücken Sie die **Eingabetaste**.
3. Wählen Sie im **Firewall-Bildschirm** mit den Pfeiltasten im linken Menü **Benutzerdefinierte Regeln** aus und drücken Sie dann die **Eingabetaste**.
4. Klicken Sie im Abschnitt **Benutzerdefinierte zulässige Regeln** mit der**Tabulatortaste** auf die Schaltfläche **Hinzufügen** und drücken Sie dann die **Eingabetaste**.
5. Geben Sie im Feld **Quellnetzwerk***0/0*ein. Gehen Sie mit der **Tabulatortaste** zum Feld **Zielport** und geben Sie *5900* ein.
6. **Klicken Sie mit der Tabulatortaste** auf die Schaltfläche **Hinzufügen** und drücken **Sie dann die Eingabetaste**.
7. **Wechseln Sie mit der Tabulatortaste** zur Schaltfläche **Weiter** und **drücken**
8. Gehen Sie im Bildschirm **Zusammenfassung** mit der **Tabulatortaste** zur Schaltfläche **Fertig stellen** und **drücken Sie**
9. Auf dem `YaST`-Bildschirm der obersten Ebene wechseln Sie mit der **Tabulatortaste** zur Schaltfläche **Beenden** und drücken Sie die **Eingabetaste**.
10. Starten Sie den Display-Manager und den Dienst `xinetd` mit den folgenden Befehlen neu:

    ```
    /etc/init.d/xinetd restart
    rcxdm restart
    <!--NeedCopy-->
    ```


Alternativ können Sie die Firewall bis zum nächsten Neustart deaktivieren, indem Sie den Befehl **rcSuSEfirewall2 stop** ausführen, oder dauerhaft mit YaST. Diese Konfiguration kann zusätzliche Dienste für die Außenwelt verfügbar machen und die allgemeine Sicherheit Ihrer VM verringern.

VNC-Bildschirmauflösung

Nach dem Herstellen einer Verbindung mit einer virtuellen Maschine über die grafische Konsole stimmt die Bildschirmauflösung manchmal nicht überein. Beispielsweise ist das VM-Display zu groß, um bequem in den Bereich der grafischen Konsole zu passen. Steuern Sie dieses Verhalten, indem Sie den VNC-Serverparameter `geometry` wie folgt festlegen:

1. Öffnen Sie die Datei `/etc/xinetd.d/vnc` mit Ihrem bevorzugten Texteditor und suchen Sie den Abschnitt `service_vnc1` (entspricht `displayID` 1).
2. Ändern Sie das Argument `geometry` in der Zeile `server-args` auf die gewünschte Bildschirmauflösung. Beispiel:

   ```
   server_args  = :42 -inetd -once -query localhost -geometry 800x600
       -depth 16
   <!--NeedCopy-->
   ```

   Der Wert des Parameters `geometry` kann eine beliebige gültige Bildschirmbreite und -höhe sein.
3. Speichern und schließen Sie die Datei.
4. Starten Sie den VNC-Server neu:

   ```
   /etc/init.d/xinetd restart
   rcxdm restart
   <!--NeedCopy-->
   ```

Prüfe die Laufstufen

Red Hat und SUSE Linux-VMs verwenden Runlevel 5 für den grafischen Start. In diesem Abschnitt wird beschrieben, wie Sie überprüfen können, ob Ihre VM in Runlevel 5 gestartet wird, und wie Sie diese Einstellung ändern können.

1. Prüfen Sie in `/etc/inittab` wie Standard-Runlevel eingestellt ist. Suchen Sie nach der Zeile mit der Aufschrift:

   ```
   id:n:initdefault:
   <!--NeedCopy-->
   ```

   Wenn *n* nicht 5 ist, bearbeiten Sie die Datei, damit dies der Fall ist.

2. Sie können den Befehl `telinit q ; telinit 5` nach dieser Änderung ausführen, um zu vermeiden, dass Sie neu starten müssen, um die Laufstufen zu wechseln.

Beheben von VM-Problemen

September 19, 2023

XenServer bietet zwei Formen der Unterstützung:

- Kostenloser Selbsthilfe-Support auf der XenServer-Website
- Kostenpflichtige Support-Services, die Sie auf der Support-Website erwerben können.

Mit dem technischen Support von XenServer können Sie online einen Supportfall eröffnen oder sich bei technischen Problemen telefonisch an das Support Center wenden.

Auf der XenServer-Supportwebsite finden Sie mehrere Ressourcen, die für Sie hilfreich sein können, wenn Sie auf ungewöhnliches Verhalten, Abstürze oder andere Probleme stoßen. Zu den Ressourcen gehören: Supportforen, Artikel der Knowledge Base und Produktdokumentation.

Wenn Sie ein ungewöhnliches VM-Verhalten feststellen, soll dieser Abschnitt Ihnen helfen, das Problem zu lösen. In diesem Abschnitt wird beschrieben, wo sich Anwendungsprotokolle befinden, und weitere Informationen, die Ihrem XenServer Solution Provider helfen können, das Problem zu verfolgen und zu lösen.

> **Wichtig:**
>
> Folgen Sie den Informationen zur Problembehandlung in diesem Abschnitt nur unter Anleitung Ihres XenServer Solution Providers oder des Support-Teams.
>
> Hersteller-Updates: Halten Sie Ihre VMs mit vom Hersteller des Betriebssystems bereitgestellten Updates auf dem neuesten Stand. Der Anbieter hat möglicherweise Korrekturen für abgestürzte VM und andere Fehler bereitgestellt.

VM stürzt ab

Wenn bei Ihnen VM-Abstürze auftreten, ist es möglich, dass ein Kernel-Absturz-Dump helfen kann, das Problem zu identifizieren. Reproduzieren Sie den Absturz, wenn möglich, und gehen Sie wie folgt vor. Wenden Sie sich an Ihren Anbieter des Gastbetriebssystems, um weitere Untersuchungen zu diesem Problem

Das Crashdump-Verhalten Ihrer VMs kann mit dem Parameter `actions-after-crash` gesteuert werden. Im Folgenden sind die möglichen Werte:

Wert	Beschreibung
`preserve`	Lassen Sie die VM in einem angehaltenen Zustand. (Zur Analyse)
`restart`	Kein Core-Dump, VM neu starten. (Dies ist die Standardeinstellung)
`destroy`	Kein Core-Dump, VM angehalten lassen.

Um das Speichern von VM-Crash-Dumps zu aktivieren:

1. Ermitteln Sie auf dem XenServer-Host die UUID der gewünschten VM, indem Sie den folgenden Befehl ausführen:

```
xe vm-list name-label=<name> params=uuid --minimal
<!--NeedCopy-->
```

2. Ändern Sie den Wert `actions-after-crash` indem Sie `xe vm-param-set` verwenden. Führen Sie z. B. den folgenden Befehl auf dom0 aus:

```
xe vm-param-set uuid=<vm_uuid> actions-after-crash=preserve
<!--NeedCopy-->
```

3. Absturz der VM.

   a) Ermitteln Sie die Domänen-ID der VM, indem Sie den folgenden Befehl auf dom0 ausführen:

```
xe vm-param-get uuid=<vm_uuid> param-name=dom-id
<!--NeedCopy-->
```

   b) Führen Sie den Befehl `xl trigger` in dom0 aus, um den Absturz auszulösen:

```
xl trigger <dom_id> nmi
<!--NeedCopy-->
```

Crashdump-Verhalten von Windows-VMs

Standardmäßig werden Windows-Absturzabbilder in `%SystemRoot%\Minidump` der Windows-VM eingefügt. Sie können die VM-Absturzabbildebene konfigurieren, indem Sie dem Menüpfad **Arbeitsplatz > Eigenschaften > Erweitert > Starten und Wiederherstellen** folgen.

UEFI- und Secure Boot-Probleme

Wie ändere ich die Bildschirmauflösung der XenCenter Konsole auf einer UEFI-fähigen VM?

So ändern Sie die Bildschirmauflösung der XenCenter Konsole auf einer UEFI-fähigen VM:

1. Öffnen Sie die **Windows-Einstellungen**
2. Klicken Sie auf **Update & Sicherheit**
3. Drücken Sie auf der Registerkarte "Wiederherstellung"die Schaltfläche **Jetzt neu starten**.
4. Navigieren Sie zu **Problembehandlung** > **Erweiterte Optionen** > **UEFI-Firmware-Einstellungen**.
5. Drücken Sie **Neustart**. Während des Neustarts wird das UEFI-Einstellungsmenü geladen.
6. Navigieren Sie zu **Geräte-Manager** > **OVMF-Plattformkonfiguration**. Dadurch wird die aktuelle Bildschirmauflösung angezeigt.
7. Drücken Sie die **Eingabetaste**, um die Optionen der Bildschirmauflösung anzuzeigen.
8. Wählen Sie mit den Pfeiltasten die gewünschte Bildschirmauflösung aus und drücken Sie die **Eingabetaste**.
9. Drücken Sie **F10**, um die Änderungen zu speichern und Ihre Auswahl zu bestätigen.
10. Starten Sie die VM neu, um die XenCenter Konsole in einer aktualisierten Bildschirmauflösung anzuzeigen.

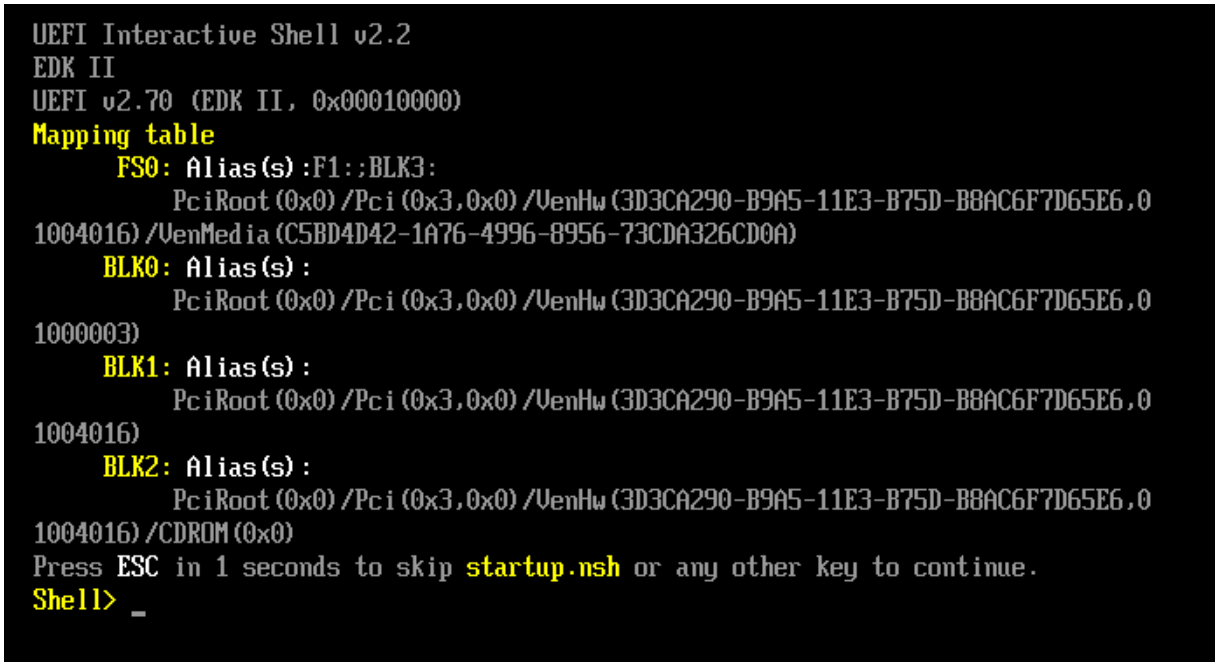
Warum kann ich keine UEFI Secure Boot VM erstellen?

Stellen Sie sicher, dass Ihr VM-Betriebssystem den sicheren UEFI-Startmodus unterstützt. Die folgenden Betriebssysteme unterstützen Secure Boot:

- Windows 10 (64-Bit)
- Windows 11 (64 Bit)
- Windows Server 2016 (64-Bit)
- Windows Server 2019 (64-Bit)
- Windows Server 2022 (64 Bit)

Warum startet meine UEFI Secure Boot VM nicht?

Wenn Sie die folgenden Meldungen auf der Konsole Ihrer UEFI Secure Boot VM und eine Warnung in XenCenter sehen, ist der Secure Bootvorgang fehlgeschlagen und Ihre VM wird nicht gestartet.



Dies wird normalerweise durch die Installation von nicht signierten Treibern in die VM verursacht. Untersuchen Sie, welche Treiber seit dem letzten erfolgreichen Secure Boot aktualisiert oder installiert wurden.

Sie können Secure Boot deaktivieren und die VM im Setup-Modus starten, um die nicht signierten Treiber zu entfernen.

> **Wichtig:**
>
> Bevor Sie dies tun, erstellen Sie ein Backup der VM, indem Sie einen Snapshot erstellen.

Um eine UEFI Secure Boot-VM in eine UEFI-Boot-VM zu ändern, führen Sie den folgenden Befehl auf dem XenServer-Host aus, der die VM hostet:

```
varstore-sb-state <VM_UUID> setup
```

Nachdem Sie Ihre VM repariert haben, führen Sie den folgenden Befehl aus, um Secure Boot wieder zu aktivieren:

```
varstore-sb-state <VM_UUID> user
```

Verursacht Secure Boot ein Problem auf meiner VM?

Um zu diagnostizieren, ob ein Problem auf Ihrer VM dadurch verursacht wird, dass Secure Boot für die VM aktiviert ist, deaktivieren Sie Secure Boot und versuchen Sie, das Problem zu reproduzieren.

Um Secure Boot zu deaktivieren, führen Sie den folgenden Befehl auf dem XenServer-Host aus, der die VM hostet:


```
varstore-sb-state <VM_UUID> setup
```

Nachdem Sie das Problem debuggt haben, können Sie den folgenden Befehl ausführen, um Secure Boot erneut zu aktivieren:

```
varstore-sb-state <VM_UUID> user
```

Wie führe ich Windows-Debug auf einer Secure Boot Windows-VM aus?

Sie können Windows Debug nicht auf einer Secure Boot Windows-VM ausführen. Um Windows Debug auf Ihrer VM auszuführen, können Sie eines der folgenden Dinge tun:

- Wechseln Sie Ihre VM in den UEFI-Startmodus, indem Sie den folgenden Befehl ausführen:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=false
  ```

  Starten Sie die VM neu.

  Nachdem Sie das Problem debuggt haben, können Sie den folgenden Befehl ausführen, um Secure Boot erneut zu aktivieren:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=auto
  ```

  Starten Sie die VM neu.

- Deaktivieren Sie Secure Boot, indem Sie den folgenden Befehl auf dem XenServer-Host ausführen, der die VM hostet:

  ```
  varstore-sb-state <VM_UUID> setup
  ```

  Nachdem Sie das Problem debuggt haben, können Sie den folgenden Befehl ausführen, um Secure Boot erneut zu aktivieren:

  ```
  varstore-sb-state <VM_UUID> user
  ```

Warum werden nur zwei NICs für meine UEFI-fähige Windows-VM angezeigt?

Selbst wenn Sie beim Erstellen Ihrer UEFI-fähigen VM mehr als zwei NICs einrichten, sehen Sie beim ersten Start der VM nur zwei Netzwerkkarten. Nachdem die XenServer VM Tools für Windows in der VM installiert wurden, werden diese Informationen korrekt angezeigt.

Warum werden meine emulierten Geräte auf einer UEFI-Windows-VM als andere Typen angezeigt als erwartet?

UEFI Secure Boot VMs verwenden NVME und E1000 für emulierte Geräte. Wenn die VM jedoch zum ersten Mal startet, werden die emulierten Geräte als unterschiedliche Typen angezeigt. Nachdem die XenServer VM Tools für Windows in der VM installiert wurden, werden diese Informationen korrekt angezeigt.

Warum kann ich meine Vorlagen nicht vom BIOS-Modus in den UEFI- oder UEFI-Secure-Boot-Modus konvertieren?

Sie können eine UEFI-fähige VM-Vorlage nur aus einer im Lieferumfang von XenServer enthaltenen Vorlage erstellen.

Verwenden Sie den Befehl `xe template-param-set` nicht für Vorlagen, auf denen etwas installiert ist, oder für Vorlagen, die Sie aus einem Snapshot erstellt haben. Der Startmodus dieser Snapshots kann nicht geändert werden, und wenn Sie versuchen, den Startmodus zu ändern, startet die VM nicht.

Wie überprüfe ich UEFI- und UEFI Secure Boot-Variablen?

Führen Sie auf dem XenServer-Host, auf dem die UEFI- oder UEFI Secure Boot-VM gehostet wird, die folgenden Befehle aus:

```
varstore-ls
```

Dieser Befehl listet die GUIDs und Namen der verfügbaren Variablen auf. Verwenden Sie die GUID und den Namen im folgenden Befehl:

```
varstore-get <VM\_ID> <GUID> <name> | hexdump -C
```

Warum kann ich keinen Testtreiber mit einer Secure Boot VM verwenden?

Wenn Sie auch mit einem Drittanbieter zusammenarbeiten, um Probleme in seiner UEFI Secure Boot VM zu debuggen und zu beheben, stellt der Drittanbieter möglicherweise unsignierte Treiber zu Test- oder Überprüfungszwecken zur Verfügung. Diese Treiber funktionieren nicht in einer UEFI Secure Boot VM.

Fordern Sie beim Drittanbieter einen signierten Fahrer an. Oder Sie können Ihre UEFI Secure Boot VM in den Setup-Modus versetzen, um sie mit dem unsignierten Treiber auszuführen.

Xentop-Hilfsprogramm

Das xentop-Hilfsprogramm zeigt Echtzeitinformationen über ein XenServer-System und laufende Domänen in einem halbgrafischen Format an. Mit diesem Tool können Sie den Status der Domäne untersuchen, die einer VM zugeordnet ist.

Um das Xentop-Hilfsprogramm auszuführen:

1. Stellen Sie über SSH eine Verbindung zum XenServer-Host her oder wechseln Sie in XenCenter zur Registerkarte **Konsole** des Hosts.
2. Führen Sie den folgenden Befehl aus: `xentop`

   Die Konsole zeigt Informationen über den Host in einer Tabelle an. Die Informationen werden regelmäßig aktualisiert.

Ausgabespalten

Das Hilfsprogramm xentop zeigt die folgenden Spalten in der Konsole an:

- **NAME** —Der Name der Domäne. „Domain-0"ist die XenServer-Steuerdomäne. Andere Domänen gehören zu den VMs.
- **STATE** —Der Status der Domäne. Der Status kann einen der folgenden Werte haben:
  - d - Die Domäne stirbt
  - s - Die Domäne wird heruntergefahren
  - b - Die Domäne ist gesperrt
  - c - Die Domäne ist abgestürzt
  - p - Die Domäne wurde angehalten
  - r - Die Domäne läuft aktiv auf einer der CPUs
- **CPU (sec)** —Die CPU-Auslastung der Domäne in Sekunden
- **CPU (%)** —Die CPU-Auslastung der Domäne als Prozentsatz
- **MEM (k)** - Der aktuelle Speicherverbrauch der Domäne in KiB
- **MEM (%)** —Die aktuelle Speichernutzung der Domäne als Prozentsatz
- **MAXMEM (k)** - Die maximale Speichernutzung der Domäne in KiB
- **MAXMEM (%)** —Die maximale Speichernutzung der Domäne als Prozentsatz
- **VCPUS** —Die Anzahl der virtuellen CPUs, die der Domäne zugewiesen sind
- **NETS** —Die Anzahl der von der Domäne verwendeten virtuellen Netzwerke
- **NETTX (k)** —Der Betrag der gesamten Netzwerk-TX in KiB

- **NETRX (k)** —Der Betrag der gesamten Netzwerk-RX in KiB
- **VBDS** - Die Anzahl der virtuellen Blockgeräte
- **VBD_OO** —Die Gesamtzahl der Fälle, in denen bei der VBD ein Fehler aufgetreten ist, der keine Anfragen mehr enthält. In diesem Fall werden I/O-Anfragen für die VBD verzögert.
- **VBD_RD** - Die Gesamtzahl der VBD-Leseanforderungen
- **VBD_WR** - Die Gesamtzahl der VBD-Schreibanforderungen
- **VBD_RSECT** - Die VBD-Lesesektoren
- **VBD_WSECT** - Die VBD-Schreibsektoren

Xentop-Parameter

Sie können die folgenden Parameter verwenden, um die Ausgabe für den Befehl xentop zu konfigurieren:

- **-h** —Gibt die Befehlshilfe für den Befehl xentop aus.
- **-V** —Gibt die Version des xentop-Befehls aus.
- **-d** oder –**delay=SECONDS** - Legt die Anzahl der Sekunden zwischen Aktualisierungen fest
- **-n** oder –**networks** - Gibt die Daten für jedes VIF-Netzwerk aus, das einer Domäne zugeordnet ist
- **-x** oder –**vbds** —Gibt die Daten für jedes VBD-Blockgerät aus, das einer Domäne zugeordnet ist
- **-r** oder **repeat-header** - Wiederholen Sie den Tabellenheader vor jeder Domäne
- **-v** oder –**vcpus** —Gibt die Daten für jede vCPU aus, die einer Domäne zugeordnet ist
- **-i** oder –**iterations** - Anzahl der Iterationen (Aktualisierungen), die angezeigt werden sollen, bevor Xentop beendet wird
- **-f** oder –**full-name** - Gibt den vollständigen Domainnamen anstelle eines verkürzten Namens aus

Sie können die meisten dieser Parameter auch im Xentop-Dienstprogramm konfigurieren.

---

layout: doc
description: Configure high availability in your XenServer pool to ensure that VMs continue to run in the case of disrupted networking or host hardware failures.—

Hohe Verfügbarkeit

Bei Hochverfügbarkeit handelt es sich um eine Reihe automatischer Funktionen, mit denen Probleme, die XenServer-Hosts ausfallen oder nicht erreichbar sind, geplant und sicher behoben werden können. Zum Beispiel bei physisch gestörten Netzwerk- oder Host-Hardwareausfällen.

Übersicht

Hohe Verfügbarkeit stellt sicher, dass, wenn ein Host unerreichbar oder instabil wird, die auf diesem Host laufenden VMs automatisch sicher auf einem anderen Host neu gestartet werden. Dadurch müssen die virtuellen Maschinen nicht mehr manuell neu gestartet werden, was zu minimalen Ausfallzeiten der virtuellen Maschinen führt.

Wenn der Poolkoordinator nicht mehr erreichbar oder instabil wird, kann Hochverfügbarkeit auch die administrative Kontrolle über einen Pool wiederherstellen. Hochverfügbarkeit stellt sicher, dass die administrative Kontrolle ohne manuellen Eingriff automatisch wiederhergestellt wird.

Optional kann Hochverfügbarkeit auch den Neustart von VMs auf Hosts automatisieren, die sich ohne manuellen Eingriff in einem guten Zustand befinden. Diese VMs können für den Neustart in Gruppen geplant werden, damit die Dienste gestartet werden können. Damit können Infrastruktur-VMs vor ihren abhängigen VMs gestartet werden (z. B. ein DHCP-Server vor seinem abhängigen SQL-Server).

> **Warnungen:**
>
> Verwenden Sie Hochverfügbarkeit zusammen mit Multipath-Speicher und gebundenem Netzwerk. Konfigurieren Sie Multipathed Storage und Bonded Networking, bevor Sie versuchen, Hochverfügbarkeit einzurichten. Kunden, die keinen Multipath-Speicher und kein Bonded Networking einrichten, können bei einer Instabilität der Infrastruktur ein unerwartetes Verhalten beim Neustart des Hosts (Self-Fencing) feststellen.
>
> Alle Grafiklösungen (NVIDIA vGPU, Intel GVT-D, Intel GVT-G und vGPU Passthrough) können in einer Umgebung mit hoher Verfügbarkeit verwendet werden. VMs, die diese Grafiklösungen verwenden, können jedoch nicht mit hoher Verfügbarkeit geschützt werden. Diese VMs können nach bestem Ermessen neu gestartet werden, während es Hosts mit den entsprechenden freien Ressourcen gibt.

Übermäßiges Engagement

Ein Pool ist überbelegt, wenn die derzeit laufenden VMs nach einer benutzerdefinierten Anzahl von Hostausfällen nicht an anderer Stelle neu gestartet werden können. Eine Überbelegung kann auftreten, wenn im Pool nicht genügend freier Speicher vorhanden ist, um diese VMs nach einem Ausfall auszuführen. Es gibt jedoch auch subtilere Änderungen, die eine hohe Verfügbarkeit unhaltbar

machen können: Änderungen an Virtual Block Devices (VBDs) und Netzwerken können sich darauf auswirken, welche VMs auf welchen Hosts neu gestartet werden können. XenServer kann nicht alle potenziellen Aktionen überprüfen und feststellen, ob sie zu einer Verletzung der Hochverfügbarkeitsanforderungen führen. Es wird jedoch eine asynchrone Benachrichtigung gesendet, wenn die Hochverfügbarkeit nicht mehr nachhaltig wird.

XenServer verwaltet dynamisch einen Failover-Plan, der detailliert beschreibt, was zu tun ist, wenn eine Gruppe von Hosts in einem Pool zu einem bestimmten Zeitpunkt ausfällt. Ein wichtiges Konzept, das es zu verstehen gilt, ist der Wert `host failures to tolerate`, der als Teil der Hochverfügbarkeitskonfiguration definiert wird. Der Wert von `host failures to tolerate` bestimmt die Anzahl der Hostausfälle, die zulässig sind, ohne dass alle geschützten virtuellen Maschinen neu gestartet werden können. Stellen Sie sich beispielsweise einen Ressourcenpool vor, der aus 64 Hosts `host failures to tolerate` besteht und auf 3 festgelegt ist. In diesem Fall berechnet der Pool einen Failoverplan, der den Ausfall von drei beliebigen Hosts ermöglicht, und startet dann die VMs auf anderen Hosts neu. Wenn kein Plan gefunden werden kann, gilt der Pool als überbeansprucht. Der Plan wird basierend auf VM-Lebenszyklusvorgängen und -verlagerung dynamisch neu berechnet. Wenn Änderungen (z. B. das Hinzufügen neuer VMs zum Pool) dazu führen, dass der Pool überlastet wird, werden Warnungen entweder über XenCenter oder per E-Mail gesendet.

Warnung vor Überbelegung

Wenn Versuche, eine VM zu starten oder fortzusetzen, dazu führen würden, dass der Pool überbeansprucht wird, wird in XenCenter eine Warnmeldung angezeigt. Sie können dann wählen, ob Sie den Vorgang abbrechen oder trotzdem fortfahren möchten. Wenn Sie fortfahren, wird der Pool überlastet und eine Nachricht wird an alle konfigurierten E-Mail-Adressen gesendet. Dies ist auch als Nachrichteninstanz über die Management-API verfügbar. Die Menge an Arbeitsspeicher, die von VMs mit unterschiedlichen Prioritäten belegt wird, wird auf Pool- und Host-Ebene angezeigt.

Host-Fencing

Manchmal kann ein Host aufgrund eines Verlusts der Netzwerkkonnektivität ausfallen oder wenn ein Problem mit dem Control Stack auftritt. In solchen Fällen grenzt sich der XenServer-Host selbst ab, um sicherzustellen, dass die VMs nicht auf zwei Hosts gleichzeitig ausgeführt werden. Wenn eine Fence-Aktion ausgeführt wird, wird der Host sofort und abrupt neu gestartet, wodurch alle darauf laufenden VMs gestoppt werden. Die anderen Hosts erkennen, dass die VMs nicht mehr laufen, und dann werden die VMs gemäß den ihnen zugewiesenen Neustartprioritäten neu gestartet. Der eingezäunte Host geht in eine Neustartsequenz über und versucht nach dem Neustart, wieder dem Ressourcenpool beizutreten.

> **Hinweis:**
>
> Hosts in Clusterpools können sich auch selbst absichern, wenn sie nicht mit mehr als der Hälfte der anderen Hosts im Ressourcenpool kommunizieren können. Weitere Informationen finden Sie unter Clustered-Pools.

Anforderungen an die Konfiguration

Um die Hochverfügbarkeitsfunktion nutzen zu können, benötigen Sie:

- XenServer-Pool (diese Funktion bietet Hochverfügbarkeit auf Hostebene innerhalb eines einzelnen Ressourcenpools).

  > **Hinweis:**
  >
  > Wir empfehlen, Hochverfügbarkeit nur in Pools zu aktivieren, die mindestens 3 XenServer-Hosts enthalten. Weitere Informationen finden Sie unter CTX129721 —Hochverfügbarkeitsverhalten, wenn der Heartbeat in einem Pool verloren geht.

- Gemeinsam genutzter Speicher, einschließlich mindestens einer iSCSI-, NFS- oder Fibre-Channel-LUN mit einer Größe von 356 MB oder mehr —das *Heartbeat-SR*. Der Hochverfügbarkeitsmechanismus erstellt zwei Volumes auf dem Heartbeat-SR:

  - 4 MB Heartbeat-Volume: Wird verwendet, um einen Heartbeat bereitzustellen.
  - 256-MB-Metadaten-Volume: Zum Speichern von Poolkoordinator-Metadaten, die bei einem Failover des Poolkoordinators verwendet werden sollen.

  > **Hinweis:**
  >
  > Bisher haben wir empfohlen, ein dediziertes NFS- oder iSCSI-Speicher-Repository als Heartbeat-Disk mit hoher Verfügbarkeit zu verwenden. Dies ist jedoch nur von Vorteil, wenn das Speicher-Repository keine Ressourcen auf der zugrunde liegenden Speicher-Appliance teilt, andernfalls erhöht es lediglich die Komplexität und den Ressourcenverbrauch in der Steuerdomäne (dom0) des Hosts.
  >
  > Wenn Ihr Pool ein Clusterpool ist, muss Ihr Heartbeat-SR ein GFS2-SR sein.
  >
  > Mit SMB oder iSCSI verbundener Speicher bei der Authentifizierung mit CHAP kann nicht als Heartbeat-SR verwendet werden.

- Statische IP-Adressen für alle Hosts.

  > **Warnung:**
  >
  > Wenn sich die IP-Adresse eines Hosts ändert, während Hochverfügbarkeit aktiviert ist, geht die Hochverfügbarkeit davon aus, dass das Netzwerk des Hosts ausgefallen ist. Die

> Änderung der IP-Adresse kann den Host umzäunen und ihn in einem nicht bootfähigen Zustand belassen. Um dieses Problem zu beheben, deaktivieren Sie die Hochverfügbarkeit mit dem Befehl `host-emergency-ha-disable`, setzen Sie den Poolkoordinator mit `pool-emergency-reset-master` zurück und aktivieren Sie dann wieder die Hochverfügbarkeit.

- Für maximale Zuverlässigkeit empfehlen wir die Verwendung einer dedizierten gebundenen Schnittstelle als Hochverfügbarkeitsverwaltungsnetzwerk.

Damit eine VM durch Hochverfügbarkeit geschützt werden kann, muss sie agil sein. Das bedeutet die VM:

- Muss seine virtuellen Datenträger auf freigegebenem Speicher haben. Sie können jede Art von gemeinsam genutztem Speicher verwenden. iSCSI-, NFS- oder Fibre-Channel-LUN ist nur für den Speicher-Heartbeat erforderlich und kann für virtuellen Datenträgerspeicher verwendet werden.
- Kann Live-Migration verwenden.
- Es ist keine Verbindung zu einem lokalen DVD-Laufwerk konfiguriert.
- Hat seine virtuellen Netzwerkschnittstellen in poolweiten Netzwerken.

Darüber hinaus können VMs mit angehängtem vTPM nicht durch Hochverfügbarkeit geschützt werden.

> **Hinweis:**
>
> Wenn Hochverfügbarkeit aktiviert ist, empfehlen wir dringend, eine gebündelte Verwaltungsschnittstelle auf den Hosts im Pool und Multipath-Speicher für den Heartbeat-SR zu verwenden.

Wenn Sie VLANs und gebundene Schnittstellen über die CLI erstellen, sind sie möglicherweise nicht angeschlossen und aktiv, obwohl sie erstellt wurden. In dieser Situation kann eine VM nicht agil erscheinen und ist nicht durch Hochverfügbarkeit geschützt. Sie können den CLI-Befehl `pif-plug` verwenden, um das VLAN aufzurufen und PIFs zu binden, damit die VM agil werden kann. Sie können auch genau bestimmen, warum eine VM nicht agil ist, indem Sie den CLI-Befehl `xe diagnostic-vm-status` verwenden. Dieser Befehl analysiert die Platzierungsbeschränkungen, und Sie können bei Bedarf Abhilfemaßnahmen ergreifen.

Konfigurationseinstellungen neu starten

Virtuelle Maschinen können als geschützt, nach bestem Ermessen oder durch Hochverfügbarkeit ungeschützt betrachtet werden. Der Wert von `ha-restart-priority` definiert, ob eine VM als geschützt, nach bestem Aufwand oder ungeschützt behandelt wird. Das Neustartverhalten von virtuellen Rechnern in jeder dieser Kategorien ist unterschiedlich.

Geschützt

Hochverfügbarkeit garantiert den Neustart einer geschützten VM, die offline geht oder deren Host offline geht, vorausgesetzt, der Pool ist nicht überlastet und die VM agil ist.

Wenn eine geschützte VM nicht neu gestartet werden kann, wenn ein Host ausfällt, versucht High Availability, die VM zu starten, wenn in einem Pool zusätzliche Kapazität vorhanden ist. Versuche, die VM zu starten, wenn zusätzliche Kapazität vorhanden ist, sind jetzt möglicherweise erfolgreich.

`ha-restart-priority` Wert: `restart`

Beste Bemühung

Wenn der Host einer VM mit bestem Aufwand offline geht, versucht Hochverfügbarkeit, die VM mit der besten Leistung auf einem anderen Host neu zu starten. Dieser Versuch wird erst unternommen, nachdem alle geschützten VMs erfolgreich neu gestartet wurden. Hochverfügbarkeit macht nur einen Versuch, eine VM mit bestem Aufwand neu zu starten. Schlägt dieser Versuch fehl, unternimmt Hochverfügbarkeit keine weiteren Versuche, die VM neu zu starten.

`ha-restart-priority` Wert: `best-effort`

Ungeschützt

Wenn eine ungeschützte VM oder der Host, auf dem sie ausgeführt wird, angehalten wird, versucht High Availability nicht, die VM neu zu starten.

`ha-restart-priority` Value: Der Wert ist eine leere Zeichenfolge

> **Hinweis:**
>
> Hochverfügbarkeit stoppt oder migriert niemals eine laufende VM, um Ressourcen für einen Neustart einer geschützten oder nach besten Kräften verfügbaren VM freizugeben.

Wenn im Pool Hostausfälle auftreten und die Anzahl der tolerierbaren Ausfälle auf Null sinkt, kann nicht garantiert werden, dass die geschützten VMs neu gestartet werden. In solchen Fällen wird eine Systemwarnung generiert. Tritt ein weiterer Fehler auf, verhalten sich alle VMs mit festgelegter Neustartpriorität entsprechend dem Bestleistungsverhalten.

Bestellung starten

Die Startreihenfolge ist die Reihenfolge, in der XenServer High Availability versucht, geschützte VMs neu zu starten, wenn ein Fehler auftritt. Die Werte der `order`-Eigenschaft für jede der geschützten VMs bestimmen die Startreihenfolge.

Die `order`-Eigenschaft einer VM wird von der Hochverfügbarkeit und auch von anderen Funktionen verwendet, die VMs starten und herunterfahren. Bei jeder VM kann die `order`-Eigenschaft festgelegt werden, nicht nur die VMs, die für Hochverfügbarkeit als geschützt gekennzeichnet sind. Bei hoher Verfügbarkeit wird die `order`-Eigenschaft jedoch nur für geschützte VMs verwendet.

Der Wert der `order`-Eigenschaft ist eine Ganzzahl. Der Standardwert ist 0, was die höchste Priorität ist. Geschützte virtuelle Maschinen mit einem `order`-Wert von 0 werden zuerst durch Hochverfügbarkeit neu gestartet. Je höher der Wert der `order`-Eigenschaft ist, desto später wird die VM in der Reihenfolge neu gestartet.

Sie können den Wert der Eigenschaft `order` einer VM über die Befehlszeilenschnittstelle festlegen:

```
xe vm-param-set uuid=VM_UUID order=int
<!--NeedCopy-->
```

Oder setzen Sie in XenCenter im Bereich **Startoptionen** für eine VM die **Startreihenfolge** auf den erforderlichen Wert.

Aktivieren Sie Hochverfügbarkeit in Ihrem XenServer-Pool

Sie können die Hochverfügbarkeit in einem Pool aktivieren, indem Sie entweder XenCenter oder die Befehlszeilenschnittstelle (CLI) verwenden. In beiden Fällen geben Sie eine Reihe von Prioritäten an, die festlegen, welche VMs die höchste Neustartpriorität erhalten, wenn ein Pool überlastet ist.

> **Warnungen:**
>
> - Wenn Sie Hochverfügbarkeit aktivieren, werden einige Vorgänge, die den Plan für den Neustart von VMs gefährden (z. B. das Entfernen eines Hosts aus einem Pool), möglicherweise deaktiviert. Sie können die Hochverfügbarkeit vorübergehend deaktivieren, um solche Vorgänge durchzuführen, oder alternativ, VMs, die durch Hochverfügbarkeit geschützt sind, ungeschützt machen.
> - Wenn Hochverfügbarkeit aktiviert ist, können Sie kein Clustering in Ihrem Pool aktivieren. Deaktivieren Sie vorübergehend Hochverfügbarkeit, um Clustering zu ermöglichen. Anschließend können Sie die Hochverfügbarkeit in Ihrem Clusterpool aktivieren. Ein gewisses Hochverfügbarkeitsverhalten, wie z. B. Self-Fencing, unterscheidet sich bei Clusterpools. Weitere Informationen finden Sie unter Clustered-Pools.

Ermöglichen Sie Hochverfügbarkeit über die CLI

1. Stellen Sie sicher, dass ein kompatibles Storage Repository (SR) an Ihren Pool angeschlossen ist. iSCSI-, NFS- oder Fibre-Channel-SRs sind kompatibel. Informationen zum Konfigurieren eines solchen Speicherrepositorys über die CLI finden Sie unter Verwalten von Speicherrepositories.

2. Legen Sie für jede VM, die Sie schützen möchten, eine Neustartpriorität und Startreihenfolge fest. Sie können die Neustartpriorität wie folgt festlegen:

```
xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
<!--NeedCopy-->
```

3. Aktivieren Sie Hochverfügbarkeit im Pool und geben Sie optional einen Timeout an:

```
xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
   timeout in seconds
<!--NeedCopy-->
```

   Das Timeout ist der Zeitraum, in dem das Netzwerk oder der Speicher für die Hosts in Ihrem Pool nicht zugänglich ist. Wenn Sie bei der Aktivierung der Hochverfügbarkeit kein Timeout angeben, verwendet XenServer das Standardtimeout von 60 Sekunden. Wenn ein XenServer-Host innerhalb des Timeout-Zeitraums nicht auf Netzwerk oder Speicher zugreifen kann, kann er sich selbst abgrenzen und neu starten.

4. Führen Sie den Befehl `pool-ha-compute-max-host-failures-to-tolerate` aus. Dieser Befehl gibt die maximale Anzahl von Hosts zurück, die ausfallen können, bevor nicht genügend Ressourcen zur Ausführung aller geschützten VMs im Pool vorhanden sind.

```
xe pool-ha-compute-max-host-failures-to-tolerate
<!--NeedCopy-->
```

   Die Anzahl der tolerierten Fehler bestimmt, wann eine Warnung gesendet wird. Das System berechnet einen Failoverplan neu, wenn sich der Status des Pools ändert. Mit dieser Berechnung wird die Poolkapazität ermittelt und wie viele weitere Ausfälle möglich sind, ohne dass die Nutzungsgarantie für geschützte VMs verloren geht. Eine Systemwarnung wird generiert, wenn dieser berechnete Wert unter den angegebenen Wert für fällt `ha-host-failures-to-tolerate`.

5. Geben Sie den Parameter `ha-host-failures-to-tolerate` an. Der Wert muss kleiner oder gleich dem berechneten Wert sein:

```
xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
<!--NeedCopy-->
```

Entfernen des Hochverfügbarkeitsschutzes von einer VM über die CLI

Um Hochverfügbarkeitsfunktionen für eine VM zu deaktivieren, verwenden Sie den Befehl `xe vm-param-set`, um den Parameter `ha-restart-priority` auf eine leere Zeichenfolge festzulegen. Durch Festlegen des Parameters `ha-restart-priority` werden die Einstellungen für die Startreihenfolge nicht gelöscht. Sie können die Hochverfügbarkeit für eine VM wieder aktivieren, indem Sie den Parameter `ha-restart-priority` nach Bedarf auf `restart` oder `best-effort`

festlegen.

Stellen Sie einen nicht erreichbaren Host wieder her

Wenn ein Host aus irgendeinem Grund nicht auf die Hochverfügbarkeitsstatusdatei zugreifen kann, ist es möglich, dass ein Host nicht mehr erreichbar ist. Um Ihre XenServer-Installation wiederherzustellen, müssen Sie möglicherweise die Hochverfügbarkeit mit dem `host-emergency-ha-disable` folgenden Befehl deaktivieren:

```
xe host-emergency-ha-disable --force
<!--NeedCopy-->
```

Wenn der Host der Poolkoordinator war, wird er wie gewohnt mit deaktivierter Hochverfügbarkeit gestartet. Poolmitglieder verbinden sich erneut und deaktivieren automatisch die Hochverfügbarkeit. Wenn der Host ein Poolmitglied war und den Poolkoordinator nicht kontaktieren kann, müssen Sie möglicherweise eine der folgenden Aktionen ausführen:

- Erzwingen des Hostneustarts als Poolkoordinator (`xe pool-emergency-transition-to-master`)

  ```
  xe pool-emergency-transition-to-master uuid=host_uuid
  <!--NeedCopy-->
  ```

- Teilen Sie dem Host mit, wo sich der neue Poolkoordinator befindet (`xe pool-emergency-reset-master`):

  ```
  xe pool-emergency-reset-master master-address=
     new_pool_coordinator_hostname
  <!--NeedCopy-->
  ```

Wenn alle Hosts erfolgreich neu gestartet wurden, aktivieren Sie die Hochverfügbarkeit erneut:

```
xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
<!--NeedCopy-->
```

Herunterfahren eines Hosts bei aktivierter Hochverfügbarkeit

Achten Sie beim Herunterfahren oder Neustarten eines Hosts besonders darauf, dass der Hochverfügbarkeitsmechanismus davon ausgeht, dass der Host ausgefallen ist. Um einen Host sauber herunterzufahren, wenn Hochverfügbarkeit aktiviert ist, deaktivieren Sie den Host, evakuieren Sie den Host und fahren Sie den Host schließlich mit XenCenter oder der CLI herunter. Führen Sie die folgenden Befehle aus, um einen Host in einer Umgebung herunterzufahren, in der Hochverfügbarkeit aktiviert ist:


```
xe host-disable host=host_name
xe host-evacuate uuid=host_uuid
xe host-shutdown host=host_name
<!--NeedCopy-->
```

Fahren Sie eine VM herunter, die durch hohe Verfügbarkeit geschützt ist

Wenn eine VM durch einen Hochverfügbarkeitsplan geschützt und für einen automatischen Neustart eingerichtet ist, kann sie nicht heruntergefahren werden, solange dieser Schutz aktiv ist. Um eine VM herunterzufahren, deaktivieren Sie zuerst ihren Hochverfügbarkeitsschutz und führen Sie dann den CLI-Befehl aus. XenCenter bietet Ihnen ein Dialogfeld zum automatischen Deaktivieren des Schutzes, wenn Sie die Schaltfläche **Herunterfahren** einer geschützten VM auswählen.

> **Hinweis:**
>
> Wenn Sie eine VM innerhalb des Gastes herunterfahren und die VM geschützt ist, wird sie unter den Bedingungen des Hochverfügbarkeitsausfalls automatisch neu gestartet. Durch den automatischen Neustart wird sichergestellt, dass ein Bedienerfehler nicht dazu führt, dass eine geschützte VM versehentlich heruntergefahren wird. Wenn Sie diese VM herunterfahren möchten, deaktivieren Sie zuerst ihren Hochverfügbarkeitsschutz.

Notfallwiederherstellung und Backup

December 6, 2023

Mit der XenServer Disaster Recovery (DR) -Funktion können Sie virtuelle Maschinen (VMs) und vApps nach einem Hardwarefehler wiederherstellen, der einen ganzen Pool oder eine ganze Site zerstört. Informationen zum Schutz vor Ausfällen einzelner Hosts finden Sie unter Hochverfügbarkeit.

> **Hinweis:**
>
> Sie müssen mit Ihrem *Root-Konto* angemeldet sein oder die Rolle des *Pool-Betreibers* oder höher haben, um die DR-Funktion nutzen zu können.

Grundlegendes zu XenServer DR

XenServer DR speichert alle Informationen, die für die Wiederherstellung Ihrer geschäftskritischen VMs und vApps erforderlich sind, in Speicherrepositorien (SRs). Die SRs werden dann von Ihrer primären (Produktions-) Umgebung in eine Backup-Umgebung repliziert. Wenn ein geschützter

Pool an Ihrem primären Standort ausfällt, können Sie die VMs und vApps in diesem Pool aus dem replizierten Speicher wiederherstellen, der an einem sekundären (DR) -Site mit minimalen Anwendungs- oder Benutzerausfallzeiten neu erstellt wurde.

Die **Disaster Recovery-Einstellungen** in XenCenter können verwendet werden, um den Speicher abzufragen und ausgewählte VMs und vApps während einer Katastrophe in einen Wiederherstellungspool zu importieren. Wenn die VMs im Wiederherstellungspool ausgeführt werden, werden auch die Metadaten des Wiederherstellungspool repliziert. Durch die Replikation der Poolmetadaten können Änderungen an den VM-Einstellungen wieder in den primären Pool übernommen werden, wenn der primäre Pool wiederhergestellt wird. Manchmal können sich Informationen für dieselbe VM an mehreren Stellen befinden. Zum Beispiel Speicher vom primären Standort, Speicher vom Disaster Recovery-Standort und auch im Pool, in den die Daten importiert werden sollen. Wenn XenCenter feststellt, dass die VM-Informationen an zwei oder mehr Stellen vorhanden sind, wird sichergestellt, dass nur die neuesten Informationen verwendet werden.

Die Disaster Recovery-Funktion kann mit XenCenter und der xe CLI verwendet werden. CLI-Befehle finden Sie unter Disaster Recovery-Befehle.

> **Tipp:**
>
> Sie können die Disaster Recovery-Einstellungen auch verwenden, um Testfailover für unterbrechungsfreie Tests Ihres Disaster Recovery-Systems durchzuführen. Bei einem Test-Failover sind alle Schritte identisch mit einem Failover. Die VMs und vApps werden jedoch nicht gestartet, nachdem sie auf der Disaster Recovery-Site wiederhergestellt wurden. Wenn der Test abgeschlossen ist, wird eine Bereinigung durchgeführt, um alle virtuellen Maschinen, vApps und Speicher zu löschen, die auf der DR-Site neu erstellt wurden.

XenServer-VMs bestehen aus zwei Komponenten:

- Virtuelle Laufwerke, die von der VM verwendet werden, die in konfigurierten Speicherrepositories (SRs) im Pool gespeichert sind, in dem sich die VMs befinden.
- Metadaten, die die VM-Umgebung beschreiben. Diese Informationen sind erforderlich, um die VM neu zu erstellen, wenn die ursprüngliche VM nicht verfügbar oder beschädigt ist. Die meisten Metadatenkonfigurationsdaten werden beim Erstellen der VM geschrieben und nur aktualisiert, wenn Sie die VM-Konfiguration ändern. Für VMs in einem Pool wird eine Kopie dieser Metadaten auf jedem Host im Pool gespeichert.

In einer DR-Umgebung werden VMs auf einem sekundären Standort mithilfe der Poolmetadaten und Konfigurationsinformationen zu allen VMs und vApps im Pool neu erstellt. Die Metadaten für jede VM enthalten ihren Namen, ihre Beschreibung und den Universal Unique Identifier (UUID) sowie ihren Speicher, ihre virtuelle CPU sowie die Netzwerk- und Speicherkonfiguration. Es umfasst auch VM-Startoptionen —Startreihenfolge, Verzögerungsintervall, Hochverfügbarkeit und Neustartpriorität. Die VM-Startoptionen werden verwendet, wenn die VM in einer Hochverfügbarkeits- oder

DR-Umgebung neu gestartet wird. Wenn beispielsweise VMs während der Notfallwiederherstellung wiederhergestellt werden, werden VMs innerhalb einer vApp in der in den VM-Metadaten angegebenen Reihenfolge und unter Verwendung der angegebenen Verzögerungsintervalle im DR-Pool neu gestartet.

Anforderungen an die DR-Infrastruktur

Richten Sie die entsprechende DR-Infrastruktur sowohl am primären als auch am sekundären Standort ein, um XenServer DR zu verwenden.

- Der für Poolmetadaten verwendete Speicher *und* die von den VMs verwendeten virtuellen Laufwerke müssen von der primären (Produktions-) Umgebung in eine Backupumgebung repliziert werden. Die Speicherreplikation wie die Verwendung der Spiegelung variiert je nach Gerät. Wenden Sie sich daher an Ihren Anbieter von Speicherlösungen, um die Speicherreplikation zu
- Nachdem die VMs und vApps, die Sie in einem Pool auf Ihrer DR-Site wiederhergestellt haben, betriebsbereit sind, müssen die SRs, die die DR-Poolmetadaten und virtuellen Datenträger enthalten, repliziert werden. Durch die Replikation können die wiederhergestellten VMs und vApps wieder am primären Standort wiederhergestellt werden *(fehlgeschlagen)*, wenn der primäre Standort wieder online ist.
- Die Hardware-Infrastruktur an Ihrem DR-Standort muss nicht mit dem primären Standort übereinstimmen. Die XenServer-Umgebung muss sich jedoch auf derselben Version- und Patch-Ebene befinden.
- Die Hosts und Pools am sekundären Standort müssen dieselbe Lizenzedition wie die am primären Standort haben. Diese XenServer-Lizenzen gelten zusätzlich zu denen, die Hosts am primären Standort zugewiesen wurden.
- Im Zielpool müssen ausreichende Ressourcen konfiguriert werden, damit alle Failover-VMs neu erstellt und gestartet werden können.

> **Warnung:**
>
> Die Disaster Recovery-Einstellungen steuern keine Storage-Array-Funktionen.
>
> Benutzer der Disaster Recovery-Funktion müssen sicherstellen, dass der Metadatenspeicher auf irgendeine Weise zwischen den beiden Standorten repliziert wird. Einige Speicher-Arrays enthalten "Mirroring"-Funktionen, um die Replikation automatisch zu erreichen. Wenn Sie diese Funktionen verwenden, müssen Sie die Spiegelfunktion deaktivieren ("Spiegelung ist defekt"), bevor Sie VMs auf der Wiederherstellungs-Site neu starten.

Überlegungen zur Bereitstellung

Lesen Sie die folgenden Schritte, bevor Sie Disaster Recovery aktivieren.

Schritte vor einer Katastrophe

Im folgenden Abschnitt werden die Schritte beschrieben, die vor einer Katastrophe zu ergreifen sind.

- Konfigurieren Sie Ihre virtuellen Maschinen und vApps.
- Beachten Sie, wie Ihre VMs und vApps SRs und SRs LUNs zugeordnet werden. Achten Sie besonders auf die Benennung der Parameter `name_label` und `name_description`. Das Wiederherstellen von VMs und vApps aus repliziertem Speicher ist einfacher, wenn die Namen der SRs erfassen, wie VMs und vApps SRs und SRs LUNs zugeordnet werden.
- Vereinbaren Sie die Replikation der LUNs.
- Aktivieren Sie die Replikation der Poolmetadaten auf eine oder mehrere SRs auf diesen LUNs.
- Stellen Sie sicher, dass die SRs, für die Sie die primären Poolmetadaten replizieren, nur an einen Pool angehängt sind.

Schritte, die nach einer Katastrophe zu unternehmen sind

Im folgenden Abschnitt werden die Schritte beschrieben, die nach einer Katastrophe zu ergreifen sind.

- Brechen Sie alle vorhandenen Speicherspiegel auf, sodass die Wiederherstellungs-Site Lese-/Schreibzugriff auf den freigegebenen Speicher hat.
- Stellen Sie sicher, dass die LUNs, aus denen Sie VM-Daten wiederherstellen möchten, nicht an einen anderen Pool angehängt sind, da sonst eine Beschädigung auftreten kann.
- Wenn Sie die *Wiederherstellungs-Site* vor einem Notfall schützen möchten, müssen Sie die Poolmetadatenreplikation auf eine oder mehrere SRs auf der Wiederherstellungs-Site aktivieren.

Schritte nach einer Erholung

Im folgenden Abschnitt werden die Schritte beschrieben, die nach einer erfolgreichen Datenwiederherstellung ausgeführt werden müssen.

- Synchronisieren Sie alle Speicherspiegel neu.

- Fahren Sie auf der Wiederherstellungs-Site die VMs oder vApps, die Sie zurück zur primären Site verschieben möchten, sauber herunter.
- Gehen Sie auf dem primären Standort genauso vor wie beim Failover im vorherigen Abschnitt, um ausgewählte VMs oder vApps auf den primären Standort zurückzusenden
- Um den primären Standort vor zukünftigen Katastrophen zu schützen, müssen Sie die Replikation der Poolmetadaten auf eine oder mehrere SRs auf den replizierten LUNs erneut aktivieren.

Disaster Recovery aktivieren

September 19, 2023

In diesem Abschnitt wird beschrieben, wie Disaster Recovery in XenCenter aktiviert wird. Verwenden **Sie die Option DR konfigurieren**, um Speicherrepositories zu identifizieren, in denen die Poolmetadaten, Konfigurationsinformationen zu allen VMs und vApps im Pool gespeichert sind. Die Metadaten werden jedes Mal aktualisiert, wenn Sie die VM- oder vApp-Konfiguration innerhalb des Pools ändern.

> **Hinweis:**
>
> Sie können Disaster Recovery nur aktivieren, wenn Sie LVM über HBA oder LVM über iSCSI verwenden. Auf diesem Speicher wird eine kleine Menge Speicherplatz für eine neue LUN benötigt, die die Informationen zur Poolwiederherstellung enthält.

Bevor Sie beginnen, stellen Sie sicher, dass die für die Notfallwiederherstellung verwendeten SRs nur an den Pool am primären Standort angeschlossen sind. SRs, die für DR verwendet werden, dürfen nicht an den Pool am sekundären Standort angeschlossen werden.

Führen Sie die folgenden Schritte aus, um Disaster Recovery zu konfigurieren:

1. Wählen Sie auf dem primären Standort den Pool aus, den Sie schützen möchten. Zeigen Sie im Menü **Pool** auf **Disaster Recovery**, und wählen Sie dann **Konfigurieren**aus.
2. Wählen Sie bis zu 8 SRs aus, in denen die Poolmetadaten gespeichert werden können. Auf diesem Speicher wird eine kleine Menge Speicherplatz für eine neue LUN benötigt, die die Informationen zur Poolwiederherstellung enthält.

   > **Hinweis:**
   >
   > Informationen für alle virtuellen Maschinen im Pool werden gespeichert, VMs müssen zum Schutz nicht unabhängig ausgewählt werden.

3. Wählen Sie **OK**. Ihr Pool ist jetzt geschützt.

Wiederherstellen von VMs und vApps während einer Katastrophe (Failover)

In diesem Abschnitt wird erläutert, wie Sie Ihre VMs und vApps auf der sekundären (Wiederherstellungs-) Site wiederherstellen.

1. Wählen Sie in XenCenter den sekundären Pool aus, und wählen Sie im Menü **Pool** die Option **Disaster Recovery** und dann **Disaster Recovery-Assistent**aus.

   Der Assistent zur Notfallwiederherstellung zeigt drei Wiederherstellungsoptionen an: **Failover**, **Failback** und **Test Failover**. Um die Wiederherstellung an Ihrem sekundären Standort durchzuführen, wählen Sie **Failover** und dann **Weiter**aus.

   > **Warnung:**
   >
   > Wenn Sie gemeinsam genutzten Fibre-Channel-Speicher mit LUN-Spiegelung verwenden, um Daten an den sekundären Standort zu replizieren, brechen Sie die Spiegelung auf, bevor Sie versuchen, VMs wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der sekundäre Standort Lese-/Schreibzugriff hat.

2. Wählen Sie die Speicherrepositories (SRs) aus, die die Poolmetadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

   Standardmäßig zeigt die Liste auf dieser Assistentenseite alle SRs an, die derzeit im Pool angehängt sind. Um nach weiteren SRs zu suchen, wählen Sie **Speicherrepositories suchen** und dann den Speichertyp aus, nach dem gesucht werden soll:

   - Um nach allen verfügbaren Hardware-HBA-SRs zu **suchen, wählen Sie Hardware-HBA-SRs**suchen.
   - Um nach Software-iSCSI-SRs zu suchen, wählen Sie **Software-iSCSI-SRs suchen aus und geben Sie** dann die Zielhost-, IQN- und LUN-Details ein.

   Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

3. Wählen Sie die VMs und vApps aus, die Sie wiederherstellen möchten. Wählen Sie die entsprechende Option **Energiezustand nach Wiederherstellung** aus, um anzugeben, ob der Assistent sie nach der Wiederherstellung automatisch starten soll. Alternativ können Sie sie auch manuell starten, nachdem das Failover abgeschlossen ist.

   Wählen Sie **Weiter**, um zur nächsten Seite des Assistenten zu gelangen und Failover-Vorprüfungen zu starten.

4. Der Assistent führt mehrere Vorprüfungen durch, bevor der Failover gestartet wird Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist. Falls zu diesem Zeitpunkt noch Speicherplatz fehlt, können Sie auf dieser

Seite die Option **SR anhängen** auswählen, um die entsprechende SR zu finden und anzuhängen.

Beheben Sie alle Probleme auf der Seite Vorabprüfungen, und wählen Sie dann **Failover** aus, um den Wiederherstellungsvorgang zu starten.

5. Auf einer Fortschrittsseite wird das Ergebnis des Wiederherstellungsprozesses für jede VM und vApp angezeigt. Der Failover-Prozess exportiert die Metadaten für VMs und vApps aus dem replizierten Speicher. Daher hängt die für den Failover benötigte Zeit von den VMs und vApps ab, die Sie wiederherstellen. Die VMs und vApps werden im primären Pool neu erstellt, und die SRs, die die virtuellen Laufwerke enthalten, werden den neu erstellten VMs zugeordnet. Falls angegeben, werden die virtuellen Maschinen gestartet.
6. Wenn das Failover abgeschlossen ist, wählen Sie **Weiter** aus, um den zusammenfassenden Bericht anzuzeigen. Wählen Sie auf der Seite mit der Zusammenfassung des Berichts die Option **Fertig stellen** aus, um den Assistenten zu schließen.

Wenn der primäre Standort verfügbar ist, arbeiten Sie den Disaster Recovery-Assistenten durch und wählen Sie **Failback** aus, um Ihre VMs wieder auf dieser Site auszuführen.

Wiederherstellen von VMs und vApps am primären Standort nach einem Notfall (Failback)

In diesem Abschnitt wird erläutert, wie VMs und vApps aus repliziertem Speicher wiederhergestellt werden. Sie können VMs und vApps wieder in einem Pool an Ihrem primären (Produktions-) Standort wiederherstellen, wenn der primäre Standort nach einer Katastrophe wieder verfügbar ist. Verwenden Sie zum Failback von VMs und vApps an Ihren primären Standort den Disaster Recovery-Assistenten.

1. Wählen Sie in XenCenter den primären Pool aus, und wählen Sie im Menü Pool die Option **Disaster Recovery** und dann **Disaster Recovery-Assistent**aus.

   Der Assistent zur Notfallwiederherstellung zeigt drei Wiederherstellungsoptionen an: **Failover**, **Failback** und **Test Failover**. Um VMs und vApps auf Ihrer primären Site wiederherzustellen, wählen Sie **Failback** und dann **Weiter**aus.

   > **Warnung:**
   >
   > Wenn Sie gemeinsam genutzten Fibre-Channel-Speicher mit LUN-Spiegelung verwenden, um Daten an den primären Standort zu replizieren, brechen Sie die Spiegelung auf, bevor Sie versuchen, VMs wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der primäre Standort Lese-/Schreibzugriff hat.

2. Wählen Sie die Speicherrepositories (SRs) aus, die die Poolmetadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

Standardmäßig zeigt die Liste auf dieser Assistentenseite alle SRs an, die derzeit im Pool angehängt sind. Um nach weiteren SRs zu suchen, wählen Sie **Speicherrepositories suchen**, und wählen Sie dann den Speichertyp aus, nach dem gesucht werden soll:

- Um nach allen verfügbaren Hardware-HBA-SRs zu **suchen, wählen Sie Hardware-HBA-SRs**suchen.
- Um nach Software-iSCSI-SRs zu suchen, wählen Sie **Software-iSCSI-SRs suchen aus und geben Sie** dann die Zielhost-, IQN- und LUN-Details ein.

Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

3. Wählen Sie die VMs und vApps aus, die Sie wiederherstellen möchten. Wählen Sie die entsprechende Option **Energiezustand nach Wiederherstellung** aus, um anzugeben, ob der Assistent sie nach der Wiederherstellung automatisch starten soll. Alternativ können Sie sie auch manuell starten, nachdem das Failback abgeschlossen ist.

   Wählen Sie **Weiter**, um zur nächsten Seite des Assistenten zu gelangen und Failback-Vorprüfungen zu starten.

4. Der Assistent führt vor dem Failback mehrere Vorabprüfungen durch. Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist. Falls zu diesem Zeitpunkt noch Speicherplatz fehlt, können Sie **auf dieser Seite die Option SR anhängen** auswählen, um die entsprechende SR zu finden und anzuhängen.

   Beheben Sie alle Probleme auf der Seite Vorabprüfungen, und wählen Sie dann **Failback** aus, um den Wiederherstellungsvorgang zu starten.

5. Auf einer Fortschrittsseite wird das Ergebnis des Wiederherstellungsprozesses für jede VM und vApp angezeigt. Der Failback-Prozess exportiert die Metadaten für VMs und vApps aus dem replizierten Speicher. Daher kann das Failback je nach Anzahl der wiederherzustellenden VMs und vApps einige Zeit dauern. Die VMs und vApps werden im primären Pool neu erstellt, und die SRs, die die virtuellen Laufwerke enthalten, werden den neu erstellten VMs zugeordnet. Falls angegeben, werden die virtuellen Maschinen gestartet.

6. Wenn das Failback abgeschlossen ist, wählen Sie **Weiter** aus, um den zusammenfassenden Bericht anzuzeigen. Wählen Sie auf der Seite mit der Zusammenfassung des Berichts die Option **Fertig stellen** aus, um den Assistenten zu schließen.

Testen des Failovers

Failover-Tests sind ein wesentlicher Bestandteil der Disaster Recovery-Planung. Sie können den Disaster Recovery-Assistenten verwenden, um unterbrechungsfreie Tests Ihres Disaster Recovery-Systems durchzuführen. Während eines Test-Failover-Vorgangs sind die Schritte dieselben wie beim Failover.

Anstatt jedoch gestartet zu werden, nachdem sie auf dem DR-Standort wiederhergestellt wurden, werden die VMs und vApps in einen angehaltenen Zustand versetzt. Am Ende eines Test-Failover-Vorgangs werden alle virtuellen Maschinen, vApps und Speicher, die auf der DR-Site neu erstellt wurden, automatisch gelöscht. Stellen Sie nach der ersten DR-Konfiguration und nachdem Sie wesentliche Konfigurationsänderungen in einem DR-fähigen Pool vorgenommen haben, sicher, dass das Failover ordnungsgemäß funktioniert, indem Sie ein Test-Failover durchführen.

1. Wählen Sie in XenCenter den sekundären Pool aus, und wählen Sie im Menü **Pool** die Option **Disaster Recovery** aus, um den **Disaster Recovery-Assistenten zu öffnen.**

   Der Assistent zur Notfallwiederherstellung zeigt drei Wiederherstellungsoptionen an: **Failover**, **Failback** und **Test Failover**. Um Ihr Disaster-Recovery-System zu testen, wählen Sie **Test Failover** und dann **Weiter**aus.

   > **Hinweis:**
   >
   > Wenn Sie gemeinsam genutzten Fibre-Channel-Speicher mit LUN-Spiegelung verwenden, um Daten an den sekundären Standort zu replizieren, brechen Sie die Spiegelung auf, bevor Sie versuchen, Daten wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der sekundäre Standort Lese-/Schreibzugriff hat.

2. Wählen Sie die Speicherrepositories (SRs) aus, die die Poolmetadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

   Standardmäßig zeigt die Liste auf dieser Assistentenseite alle SRs an, die derzeit im Pool angehängt sind. Um nach weiteren SRs zu suchen, wählen Sie "**Speicherrepositories suchen** "und anschließend den Speichertyp, nach dem gesucht werden soll:

   - Um nach allen verfügbaren Hardware-HBA-SRs zu **suchen, wählen Sie Hardware-HBA-SRs**suchen.
   - Um nach Software-iSCSI-SRs zu **suchen, wählen Sie Software-iSCSI SRs** suchen aus, und geben Sie dann den Zielhost, den IQN und die LUN-Details in das Feld ein.

   Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

3. Wählen Sie die VMs und vApps aus, die Sie wiederherstellen möchten, und wählen Sie dann **Weiter** aus, um zur nächsten Seite zu gelangen und Failover-Vorprüfungen zu starten.

4. Vor Beginn des Testfailovers führt der Assistent mehrere Vorabprüfungen durch. Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist.

   - **Prüfen Sie, ob Speicher verfügbar ist**. Wenn ein Speicher fehlt, können Sie auf dieser Seite "SR anhängen"auswählen, um das entsprechende SR zu suchen und anzuhängen.

- **Stellen Sie sicher, dass die Hochverfügbarkeit im Ziel-DR-Pool nicht aktiviert ist**. Die Hochverfügbarkeit muss im sekundären Pool deaktiviert werden, um zu verhindern, dass dieselben VMs sowohl im primären als auch im DR-Pool ausgeführt werden. Die Hochverfügbarkeit muss deaktiviert werden, um sicherzustellen, dass die wiederhergestellten VMs und vApps nach der Wiederherstellung nicht automatisch gestartet werden. Um die Hochverfügbarkeit im sekundären Pool zu deaktivieren, können Sie einfach **HA deaktivieren** auf der Seite auswählen. Wenn die Hochverfügbarkeit zu diesem Zeitpunkt deaktiviert ist, wird sie am Ende des Test-Failover-Prozesses automatisch wieder aktiviert.

Beheben Sie alle Probleme auf der Seite Vorabprüfungen, und wählen Sie dann **Failover** aus, um das Testfailover zu starten.

5. Auf einer Fortschrittsseite wird das Ergebnis des Wiederherstellungsprozesses für jede VM und vApp angezeigt. Beim Failover-Prozess werden Metadaten für die VMs und vApps aus dem replizierten Speicher wiederhergestellt. Daher kann ein Failover je nach Anzahl der wiederherzustellenden VMs und vApps einige Zeit dauern. Die VMs und vApps werden im DR-Pool neu erstellt, die SRs, die die virtuellen Datenträger enthalten, werden an die neu erstellten VMs angeschlossen.

   Die wiederhergestellten VMs werden in einen angehaltenen Zustand versetzt: Sie werden während eines Test-Failovers nicht am sekundären Standort gestartet.

6. Wenn Sie sich sicher sind, dass das Test-Failover erfolgreich durchgeführt wurde, wählen Sie im Assistenten Weiter aus, damit der Assistent auf der DR-Site bereinigt:

   - VMs und vApps, die während des Test-Failovers wiederhergestellt wurden, werden gelöscht.
   - Speicher, der während des Test-Failovers wiederhergestellt wurde, wird getrennt.
   - Wenn die Hochverfügbarkeit im DR-Pool in der Vorabprüfungsphase deaktiviert wurde, damit das Test-Failover stattfinden kann, wird sie automatisch wieder aktiviert.

   Der Fortschritt des Bereinigungsvorgangs wird im Assistenten angezeigt.

7. Wählen Sie **Fertig stellen**, um den Assistenten zu schließen.

vApps

September 19, 2023

Eine vApp ist eine logische Gruppe aus einer oder mehreren verwandten virtuellen Maschinen (VMs). vApps können im Katastrophenfall als eine Einheit gestartet werden. Wenn eine vApp gestartet wird,

werden die in der vApp enthaltenen VMs in einer vom Benutzer vordefinierten Reihenfolge gestartet. Durch die Startreihenfolge können voneinander abhängige VMs automatisch sequenziert werden. Ein Administrator muss den Start abhängiger VMs nicht mehr manuell sequenzieren, wenn ein ganzer Dienst einen Neustart erfordert. Zum Beispiel während eines Softwareupdates. Die VMs innerhalb der vApp müssen sich nicht auf einem Host befinden und werden nach den normalen Regeln innerhalb eines Pools verteilt. Die vApp-Funktion ist in der Disaster Recovery (DR) -Situation nützlich. In einem DR-Szenario kann ein Administrator alle VMs im selben Speicherrepository gruppieren oder die sich auf dasselbe Service Level Agreement (SLA) beziehen.

Gehen Sie folgendermaßen vor, um VMs in einer vApp zu gruppieren:

1. Wählen Sie den Pool aus und klicken Sie im Menü **Pool** auf **vApps verwalten**.
2. Geben Sie einen Namen für die vApp und optional eine Beschreibung ein, und klicken Sie dann auf **Weiter**.

   Sie können einen beliebigen Namen wählen, aber ein informativer Name ist am besten. Wir empfehlen Ihnen zwar zu vermeiden, dass mehrere vApps denselben Namen verwenden, dies ist jedoch nicht erforderlich. XenCenter erzwingt keine Einschränkungen in Bezug auf eindeutige vApp-Namen. Es ist nicht notwendig, Anführungszeichen für Namen zu verwenden, die Leerzeichen enthalten.
3. Wählen Sie aus, welche VMs in die neue vApp aufgenommen werden sollen, und klicken Sie dann auf **Weiter**.

   Sie können die Suchoption verwenden, um nur VMs mit Namen aufzulisten, die die angegebene Textzeichenfolge enthalten.
4. Geben Sie die Startsequenz für die VMs in der vApp an und klicken Sie dann auf **Weiter**.

   Startreihenfolge: Gibt die Reihenfolge an, in der einzelne VMs innerhalb der vApp gestartet werden, sodass bestimmte VMs vor anderen neu gestartet werden können. VMs mit einem Startreihenfolgenwert von 0 (Null) werden zuerst gestartet. Als Nächstes werden VMs mit einem Startreihenfolgenwert von 1 gestartet, und dann die VMs mit dem Wert 2 usw.

   Versuch, die nächste VM danach zu starten: Ein Verzögerungsintervall, das angibt, wie lange nach dem Start der VM gewartet werden soll, bevor versucht wird, die nächste Gruppe von VMs in der Startsequenz zu starten.
5. Sie können die vApp-Konfiguration auf der letzten Seite überprüfen. Klicken Sie auf **Zurück**, um zurückzugehen und Einstellungen zu ändern, oder auf **Fertig stellen**, um die vApp zu erstellen.

> **Hinweis:**
>
> Eine vApp kann sich über mehrere Hosts in einem einzigen Pool erstrecken, kann sich jedoch nicht über mehrere Pools erstrecken.

Verwalten von vApps in XenCenter

Mit der Einstellung **vApps verwalten** in XenCenter können Sie vApps erstellen, löschen und ändern. Sie können damit auch vApps starten und herunterfahren sowie vApps innerhalb des ausgewählten Pools importieren und exportieren. Wenn Sie eine vApp in der Liste auswählen, werden die darin enthaltenen VMs im Detailbereich aufgeführt. Weitere Informationen finden Sie unter vApps in der XenCenter-Dokumentation.

Backup und Wiederherstellen von Hosts und VMs

September 19, 2023

Lassen Sie den Installationsstatus der XenServer-Hosts nach Möglichkeit unverändert. Das heißt, installieren Sie keine zusätzlichen Pakete und starten Sie keine zusätzlichen Dienste auf XenServer-Hosts und behandeln Sie sie als Appliances. Die beste Methode zur Wiederherstellung besteht dann darin, die XenServer-Hostsoftware vom Installationsmedium neu zu installieren. Wenn Sie mehrere XenServer-Hosts haben, ist es am besten, einen TFTP-Server und entsprechende Antwortdateien für diesen Zweck zu konfigurieren. Weitere Informationen finden Sie unter Netzwerkstartinstallationen.

Wir empfehlen Ihnen, eine Backuplösung zu verwenden, die von einem unserer zertifizierten Partner angeboten wird. Weitere Informationen finden Sie unter Citrix Ready Marketplace.

Kunden der XenServer Premium Edition können die Vorteile des schnelleren Changed-Only-Backups nutzen. Weitere Informationen finden Sie in der geänderten Dokumentation zur Blockverfolgung.

Es wird empfohlen, dass Sie häufig so viele der folgenden Backupverfahren wie möglich durchführen, um nach einem möglichen Server- und Softwarefehler wiederherzustellen.

Backup von Poolmetadaten:

1. Führen Sie den Befehl aus:

   ```
   xe pool-dump-database file-name=backup
   <!--NeedCopy-->
   ```

2. Um die Datenbank wiederherzustellen, führen Sie den Befehl aus:

   ```
   xe pool-restore-database file-name=backup dry-run=true
   <!--NeedCopy-->
   ```

   Mit diesem Befehl wird überprüft, ob der Zielcomputer über eine angemessene Anzahl von entsprechend benannten Netzwerkkarten verfügt, die für den Erfolg der Backup erforderlich sind.

Backup der Hostkonfiguration und -software:

1. Führen Sie den Befehl aus:

```
xe host-backup host=host file-name=hostbackup
<!--NeedCopy-->
```

> **Hinweise:**
>
> - Erstellen Sie das Backup nicht in der Kontrolldomäne.
> - Das Backupverfahren kann eine große Backupdatei erstellen.
> - Um eine Wiederherstellung abzuschließen, müssen Sie die ursprüngliche Installations-CD neu starten.
> - Diese Daten können nur auf dem Originalgerät wiederhergestellt werden.

Backup einer VM:

1. Stellen Sie sicher, dass die zu sichernde VM offline ist.
2. Führen Sie den Befehl aus:

```
xe vm-export vm=vm_uuid filename=backup
<!--NeedCopy-->
```

> **Hinweis:**
>
> Diese Backup sichert auch alle VM-Daten. Beim Importieren einer VM können Sie den Speichermechanismus angeben, der für die gesicherten Daten verwendet werden soll.
>
> **Warnung:**
>
> Der Backupvorgang kann länger dauern, da alle VM-Daten gespeichert werden.

Nur Backup der VM-Metadaten erstellen:

Führen Sie den Befehl aus:

```
xe vm-export vm=vm_uuid filename=backup metadata=true
<!--NeedCopy-->
```

Backup der VM-Metadaten

XenServer-Hosts verwenden auf jedem Host eine Datenbank, um Metadaten über VMs und zugehörige Ressourcen wie Speicher und Netzwerke zu speichern. In Kombination mit SRs bildet diese Datenbank die vollständige Ansicht aller im Pool verfügbaren VMs. Daher ist es wichtig zu wissen, wie ein

Backup dieser Datenbank erstellt wird, um sie nach einem physischen Hardwareausfall und anderen Katastrophenszenarien wiederherzustellen.

In diesem Abschnitt wird zunächst beschrieben, wie Sie ein Backup der Metadaten für Single-Host-Installationen und dann für komplexere Poolsetups erstellen.

Backups von Einzelhost-Installationen

Verwenden Sie die CLI, um ein Backup der Pooldatenbank anzulegen. Um eine konsistente Pool-Metadaten-Backup-Datei zu erhalten, führen Sie sie `pool-dump-database` auf dem XenServer-Host aus und archivieren Sie die resultierende Datei. Die Backupdatei enthält vertrauliche Authentifizierungsinformationen über den Pool. Stellen Sie daher sicher, dass sie sicher gespeichert sind.

Um die Pool-Datenbank wiederherzustellen, verwenden Sie den Befehl `xe pool-restore-database` aus einer früheren Dumpdatei. Wenn Ihr XenServer-Host vollständig ausgefallen ist, müssen Sie zuerst eine Neuinstallation durchführen und dann den `pool-restore-database` Befehl für den neu installierten XenServer-Host ausführen.

Nachdem Sie die Pooldatenbank wiederhergestellt haben, sind einige VMs möglicherweise noch als solche registriert `Suspended`. Wenn das Speicherrepository mit dem im Feld `suspend-VDI-uuid` definierten Status des angehaltenen Speichers jedoch ein lokales SR ist, ist das SR möglicherweise nicht verfügbar, da der Host neu installiert wurde. Um diese VMs wieder auf den Status `Halted` zurückzusetzen, damit sie neu gestartet werden können, verwenden Sie den Befehl `xe vm-shutdown vm=vm_name -force` oder verwenden Sie den Befehl `xe vm-reset-powerstate vm=vm_name -force`.

> **Warnung:**
>
> XenServer behält die UUIDs der mit dieser Methode wiederhergestellten Hosts bei. Wenn Sie auf einer anderen physischen Maschine wiederherstellen, während der ursprüngliche XenServer-Host noch läuft, sind möglicherweise doppelte UUIDs vorhanden. Infolgedessen weigert sich XenCenter, eine Verbindung zum zweiten XenServer-Host herzustellen. Das Pooldatenbankbackup ist nicht der empfohlene Mechanismus zum Klonen physischer Hosts. Verwenden Sie stattdessen die automatische Installationsunterstützung. Weitere Informationen finden Sie unter Installation.

Backup gepoolter Installationen

In einem Poolszenario stellt der Poolkoordinator eine autoritative Datenbank bereit, die synchron auf alle Hosts der Poolmitglieder gespiegelt wird. Dieser Prozess bietet eine integrierte Redundanz für einen Pool. Jedes Poolmitglied kann den Poolkoordinator ersetzen, da jedes Poolmitglied über eine

korrekte Version der Pooldatenbank verfügt. Weitere Informationen zum Übergang eines Mitglieds in einen Poolkoordinator finden Sie unter Hosts und Ressourcenpools.

Dieses Schutzniveau ist möglicherweise nicht ausreichend. Wenn beispielsweise für freigegebenen Speicher, der die VM-Daten enthält, an mehreren Orten ein Backup angelegt wird, für den lokalen Serverspeicher (der die Poolmetadaten enthält) jedoch nicht. Um einen Pool mit einem Satz von gemeinsam genutztem Speicher neu zu erstellen, müssen Sie zuerst ein Backup der Datei `pool-dump-database` auf dem Poolkoordinatorhost anlegen und diese Datei archivieren. So stellen Sie dieses Backup später auf einer brandneuen Gruppe von Hosts wieder her:

1. Installieren Sie einen neuen Satz von XenServer-Hosts vom Installationsmedium oder starten Sie gegebenenfalls das Netzwerk von Ihrem TFTP-Server aus.
2. Verwenden Sie den `xe pool-restore-database` auf dem Host, der als neuer Poolkoordinator bezeichnet wurde.
3. Führen Sie den Befehl `xe host-forget` auf dem neuen Poolkoordinator aus, um die alten Mitgliedsmaschinen zu entfernen.
4. Verwenden Sie den Befehl `xe pool-join` auf den Mitgliedshosts, um sie mit dem neuen Pool zu verbinden.

XenServer-Hosts sichern

In diesem Abschnitt werden die Verfahren zum Sichern und Wiederherstellen der XenServer-Hoststeuerungsdomäne beschrieben. Bei diesen Verfahren werden *nicht* die Speicher-Repositorys gesichert, in denen sich die VMs befinden, sondern nur die privilegierte Kontrolldomäne, auf der Xen und der XenServer-Agent ausgeführt werden.

> **Hinweis:**
>
> Die privilegierte Steuerdomäne wird am besten wie installiert belassen, ohne sie mit anderen Paketen anzupassen. Als Wiederherstellungsstrategie empfehlen wir, dass Sie eine Netzwerk-Boot-Umgebung einrichten, um XenServer sauber von den XenServer-Medien zu installieren. In der Regel müssen Sie kein Backup der Steuerdomäne anlegen, aber wir empfehlen, die Poolmetadaten zu speichern (siehe Backup der Metadaten virtueller Maschinen). Betrachten Sie diese Backupmethode als Ergänzung zum Backup der Poolmetadaten.

Die xe-Befehle `host-backup` und `host-restore` ist ein weiterer Ansatz, den Sie wählen können. Der xe-Befehl `host-backup` archiviert die aktive Partition in einer von Ihnen angegebenen Datei. Der xe-Befehl `host-restore` extrahiert ein Archiv, das von xe `host-backup` über die aktuell inaktive Datenträgerpartition des Hosts erstellt wurde. Diese Partition kann dann aktiviert werden, indem Sie von der Installations-CD booten und auswählen, dass die entsprechende Backup wiederhergestellt werden soll.

Nachdem Sie die Schritte im vorherigen Abschnitt ausgeführt und den Host neu gestartet haben, stellen Sie sicher, dass die VM-Metadaten in einem konsistenten Zustand wiederhergestellt werden. Führen Sie `xe pool-restore-database` auf `/var/backup/pool-database-${ DATE }` aus, um die VM-Metadaten wiederherzustellen. Diese Datei wird mit `xe host-backup` und dem Befehl `xe pool-dump-database` vor dem Archivieren des laufenden Dateisystems erstellt, um einen konsistenten Status der VM-Metadaten zu erstellen.

So sichern Sie Ihren XenServer-Host:

Führen Sie auf einem Remotehost mit ausreichend Speicherplatz den folgenden Befehl aus

```
xe host-backup file-name=filename -h hostname -u root -pw password
<!--NeedCopy-->
```

Mit diesem Befehl wird ein komprimiertes Image des Dateisystems der Steuerdomäne erstellt. Das Image wird an dem durch das Argument `file-name` angegebenen Ort gespeichert.

So stellen Sie einen laufenden XenServer-Host wieder her:

1. Wenn Sie Ihren XenServer-Host aus einem bestimmten Backup wiederherstellen möchten, führen Sie den folgenden Befehl aus, während der XenServer-Host aktiv und erreichbar ist:

   ```
   xe host-restore file-name=filename -h hostname -u root -pw
      password
   <!--NeedCopy-->
   ```

   Mit diesem Befehl wird das komprimierte Image wieder auf der Festplatte des XenServer-Hosts wiederhergestellt, auf dem dieser Befehl ausgeführt wird (nicht auf dem Host, auf dem sich der Befehl `filename` befindet). In diesem Zusammenhang kann "Wiederherstellen"eine Fehlbezeichnung sein, da das Wort normalerweise darauf hindeutet, dass der gesicherte Zustand vollständig eingerichtet wurde. Der Befehl restore entpackt nur die komprimierte Backupdatei und stellt sie in ihrer normalen Form wieder her. Es wird jedoch auf eine andere Partition (`/dev/sda2`) geschrieben und überschreibt *nicht* die aktuelle Version des Dateisystems.

2. Um die wiederhergestellte Version des Root-Dateisystems zu verwenden, starten Sie den XenServer-Host mit der XenServer-Installations-CD neu und wählen Sie die Option **Aus Backup wiederherstellen** .

   Nachdem die Wiederherstellung aus dem Backup abgeschlossen ist, starten Sie den XenServer-Host neu und er wird vom wiederhergestellten Image aus gestartet.

3. Stellen Sie abschließend die VM-Metadaten mit dem folgenden Befehl wieder her:

   ```
   xe pool-restore-database file-name=/var/backup/pool-database-* -h
      hostname -u root -pw password
   <!--NeedCopy-->
   ```


> **Hinweis:**
>
> Durch das Wiederherstellen aus einem Backup wie in diesem Abschnitt beschrieben wird die Backuppartition nicht zerstört.

Um einen abgestürzten XenServer-Host neu zu starten:

Wenn Ihr XenServer-Host abgestürzt ist und nicht erreichbar ist, verwenden Sie die XenServer-Installations-CD, um eine Upgrade-Installation durchzuführen. Wenn die Upgrade-Installation abgeschlossen ist, starten Sie den Computer neu und stellen Sie sicher, dass Ihr Host mit XenCenter oder Remote CLI erreichbar ist.

Fahren Sie dann mit dem Sichern der XenServer-Hosts fort, wie in diesem Abschnitt beschrieben.

VM-Backups

Wir empfehlen Ihnen, eine Backuplösung zu verwenden, die von einem unserer zertifizierten Partner angeboten wird. Weitere Informationen finden Sie unter Citrix Ready Marketplace.

Kunden der XenServer Premium Edition können die Vorteile des schnelleren Changed-Only-Backups nutzen. Weitere Informationen finden Sie im Citrix Blog über Backup-APIs mit geänderter Blockverfolgung.

---

layout: doc
description: Understand how to take a snapshot of your VM storage and metadata in order to restore your VM to a previous state. Use the Scheduled Snapshots feature to back up and restore your critical service VMs.—

VM-Snapshots

XenServer bietet einen praktischen Mechanismus, mit dem zu einem bestimmten Zeitpunkt ein Snapshot eines VM-Speichers und der Metadaten erstellt werden kann. Falls erforderlich, werden I/O während der Snapshot-Erstellung vorübergehend angehalten, um sicherzustellen, dass ein selbstkonsistentes Disk-Image erfasst werden kann.

Snapshot-Vorgänge führen zu einer Snapshot-VM, die einer Vorlage ähnelt. Der VM-Snapshot enthält alle Speicherinformationen und die VM-Konfiguration, einschließlich angehängter VIFs, sodass sie für Backupzwecke exportiert und wiederhergestellt werden können. Snapshots werden auf allen Speichertypen unterstützt. Für die LVM-basierten Speichertypen müssen jedoch die folgenden Anforderungen erfüllt sein:

- Wenn das Speicher-Repository auf einer früheren Version von XenServer erstellt wurde, muss es aktualisiert worden sein
- Das Volume muss das Standardformat haben (Sie können keinen Snapshot von `type=raw`-Volumes erstellen)

Der Snapshot-Vorgang ist ein zweistufiger Prozess:

- Metadaten als Vorlage erfassen.
- Erstellen eines VDI-Snapshots der Datenträger.

Die folgenden Typen von VM-Snapshots werden unterstützt: regulär und Snapshot mit Speicher.

Regelmäßige Schnappschüsse

Regelmäßige Snapshots sind absturzkonsistent und können auf allen VM-Typen, einschließlich Linux-VMs, durchgeführt werden.

Schnappschüsse mit Speicher

Snapshots mit Speicher speichern nicht nur den Arbeitsspeicher (Speicher) und die Metadaten der virtuellen Maschinen, sondern speichern auch den Status (RAM) der virtuellen Maschinen. Diese Funktion kann nützlich sein, wenn Sie Software aktualisieren oder patchen, aber Sie möchten auch die Option haben, zum VM-Status (RAM) vor der Änderung zurückzukehren. Das Zurücksetzen auf einen Snapshot mit Arbeitsspeicher erfordert keinen Neustart der VM.

Sie können einen Snapshot mit dem Speicher einer laufenden oder angehaltenen VM erstellen, indem Sie die Verwaltungs-API, die XE-CLI oder XenCenter verwenden.

Erstellen eines VM-Snapshots

Bevor Sie einen Snapshot erstellen, lesen Sie die folgenden Informationen zu speziellen betriebssystemspezifischen Konfigurationen und Überlegungen:

- Vorbereiten des Klonens einer Windows-VM mithilfe von Sysprep
- Vorbereitung zum Klonen einer Linux-VM

Stellen Sie zunächst sicher, dass die VM läuft oder angehalten wird, damit der Speicherstatus erfasst werden kann. Der einfachste Weg, die VM auszuwählen, auf der der Vorgang ausgeführt werden soll, ist die Angabe des Arguments `vm=name` oder `vm=vm uuid`.

Führen Sie den `vm-snapshot`Befehl aus, um einen Snapshot einer VM zu erstellen.


```
xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
<!--NeedCopy-->
```

Erstellen Sie einen Snapshot mit Speicher

Führen Sie den Befehl `vm-checkpoint` aus und geben Sie einen beschreibenden Namen für den Snapshot mit Speicher, damit Sie ihn später identifizieren können:

```
xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
<!--NeedCopy-->
```

Wenn XenServer die Erstellung des Snapshots mit Speicher abgeschlossen hat, wird seine UUID angezeigt.

Beispiel:

```
xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \
new-name-label=example_checkpoint_1
b3c0f369-59a1-dd16-ecd4-a1211df29886
<!--NeedCopy-->
```

Ein Snapshot mit Arbeitsspeicher benötigt mindestens 4 MB Speicherplatz pro Datenträger plus die Größe des Arbeitsspeichers plus etwa 20% Overhead. Ein Checkpoint mit 256 MB RAM würde also etwa 300 MB Speicher benötigen.

> **Hinweis:**
>
> Während des Checkpoint-Erstellungsprozesses wird die VM für einen kurzen Zeitraum angehalten und kann in diesem Zeitraum nicht verwendet werden.

Um alle Snapshots in Ihrem XenServer-Pool aufzulisten

Führen Sie den Befehl `snapshot-list` aus:

```
xe snapshot-list
<!--NeedCopy-->
```

Dieser Befehl listet alle Snapshots im XenServer-Pool auf.

So listen Sie die Snapshots auf einer bestimmten VM auf

Rufen Sie die UUID der bestimmten VM ab, indem Sie den Befehl `vm-list` ausführen.

```
xe vm-list
<!--NeedCopy-->
```


Dieser Befehl zeigt eine Liste aller VMs und ihrer UUIDs an. Beispiel:

```
xe vm-list
uuid ( RO): 116dd310-a0ef-a830-37c8-df41521ff72d
name-label ( RW): Windows Server 2016 (1)
power-state ( RO): halted

uuid ( RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
name-label ( RW): Control domain on host
power-state ( RO): running
<!--NeedCopy-->
```

VMs können auch angegeben werden, indem die vollständige Liste der VMs nach den Werten von Feldern gefiltert wird.

Wenn Sie beispielsweise `power-state=halted` angeben, werden alle VMs ausgewählt, deren Energiestatusfeld “angehalten”entspricht. Wenn mehrere VMs übereinstimmen, muss die Option `--multiple` angegeben werden, um den Vorgang durchzuführen. Rufen Sie die vollständige Liste der Felder ab, die mit dem Befehl abgeglichen werden können `xe vm-list params=all`.

Suchen Sie die erforderliche VM und geben Sie dann Folgendes ein:

```
xe snapshot-list snapshot-of=vm uuid
<!--NeedCopy-->
```

Beispiel:

```
xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
<!--NeedCopy-->
```

Dieser Befehl listet die Momentaufnahmen auf dieser VM auf:

```
    uuid ( RO): d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
    name-label ( RW): Regular
    name-description ( RW):
    snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
    snapshot_time ( RO): 20090914T15:37:00Z

    uuid ( RO): 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef
    name-label ( RW): Snapshot with memory
    name-description ( RW):
    snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
    snapshot_time ( RO): 20090914T15:39:45Z
<!--NeedCopy-->
```

Wiederherstellen einer VM in ihren vorherigen Zustand

Stellen Sie sicher, dass Sie über die UUID des Snapshots verfügen, zu dem Sie zurückkehren möchten, und führen Sie dann den Befehl `snapshot-revert` aus:

1. Führen Sie den Befehl `snapshot-list` aus, um die UUID des Snapshots oder Checkpoints zu finden, zu dem Sie zurückkehren möchten:

```
xe snapshot-list
<!--NeedCopy-->
```

2. Notieren Sie sich die UUID des Snapshots und führen Sie dann zum Zurücksetzen den folgenden Befehl aus:

```
xe snapshot-revert snapshot-uuid=snapshot uuid
<!--NeedCopy-->
```

   Beispiel:

```
xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
   a1211df29886
<!--NeedCopy-->
```

   Nach dem Zurücksetzen einer VM zu einem Checkpoint wird die VM angehalten.

> **Hinweise:**
>
> - Wenn nicht genügend Speicherplatz zur Verfügung steht, um den Snapshot dick bereitzustellen, können Sie den Snapshot erst wiederherstellen, wenn der Status des aktuellen Datenträgers freigegeben wurde. Wenn dieses Problem auftritt, wiederholen Sie den Vorgang.
> - Es ist möglich, zu jedem Snapshot zurückzukehren. Vorhandene Snapshots und Checkpoints werden während des Wiederherstellungsvorgangs nicht gelöscht.

Löschen eines Schnappschusses

Stellen Sie sicher, dass Sie über die UUID des Checkpoints oder Snapshots verfügen, den Sie entfernen möchten, und führen Sie dann den folgenden Befehl aus:

1. Führen Sie den Befehl `snapshot-list` aus, um die UUID des Snapshots oder Checkpoints zu finden, zu dem Sie zurückkehren möchten:

```
xe snapshot-list
<!--NeedCopy-->
```

2. Notieren Sie sich die UUID des Snapshots und führen Sie dann den Befehl `snapshot-uninstall` aus, um ihn zu entfernen:

```
xe snapshot-uninstall snapshot-uuid=snapshot-uuid
<!--NeedCopy-->
```


3. Dieser Befehl weist Sie auf die VM und die VDIs hin, die gelöscht wurden. Geben Sie zur Bestätigung `yes` ein.

Beispiel:

```
    xe snapshot-uninstall snapshot-uuid=1760561d-a5d1-5d5e-2be5-
       d0dd99a3b1ef
    The following items are about to be destroyed
    VM : 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef (Snapshot with memory)
    VDI: 11a4aa81-3c6b-4f7d-805a-b6ea02947582 (0)
    VDI: 43c33fe7-a768-4612-bf8c-c385e2c657ed (1)
    VDI: 4c33c84a-a874-42db-85b5-5e29174fa9b2 (Suspend image)
    Type 'yes' to continue
    yes
    All objects destroyed
<!--NeedCopy-->
```

Wenn Sie nur die Metadaten eines Checkpoints oder Snapshots entfernen möchten, führen Sie den folgenden Befehl aus:

```
xe snapshot-destroy snapshot-uuid=snapshot-uuid
<!--NeedCopy-->
```

Beispiel:

```
xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
<!--NeedCopy-->
```

Snapshot-Vorlagen

Erstellen einer Vorlage aus einem Snapshot

Sie können eine VM-Vorlage aus einem Snapshot erstellen. Sein Speicherzustand wird jedoch entfernt.

1. Verwenden Sie den Befehl `snapshot-copy` und geben Sie **`new`**`-name-`**`label`** für die Vorlage an:

   ```
   xe snapshot-copy new-name-label=vm-template-name \
         snapshot-uuid=uuid of the snapshot
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   xe snapshot-copy new-name-label=example_template_1
         snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
   <!--NeedCopy-->
   ```


> **Hinweis:**
>
> Dieser Befehl erstellt ein Vorlagenobjekt im SAME-Pool. Diese Vorlage ist in der XenServer-Datenbank nur für den aktuellen Pool vorhanden.

2. Um zu überprüfen, ob die Vorlage erstellt wurde, führen Sie den folgenden Befehl aus `template-list`:

```
xe template-list
<!--NeedCopy-->
```

Dieser Befehl listet alle Vorlagen auf dem XenServer-Host auf.

Exportieren eines Schnappschusses in eine Vorlage

Wenn Sie einen VM-Snapshot exportieren, wird eine vollständige Kopie der VM (einschließlich Disk-Images) als einzelne Datei auf Ihrem lokalen Computer gespeichert. Diese Datei hat eine `.xva`-Dateinamenerweiterung.

1. Verwenden Sie den Befehl `snapshot-export-to-template`, um eine Vorlagendatei zu erstellen:

```
xe snapshot-export-to template snapshot-uuid=snapshot-uuid \
       filename=template-  filename
<!--NeedCopy-->
```

Beispiel:

```
xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16-
   ecd4-a1211df29886 \
      filename=example_template_export
<!--NeedCopy-->
```

Die VM-Export-/Importfunktion kann auf verschiedene Arten verwendet werden:

- Als praktische Backup-Funktion für Ihre VMs. Eine exportierte VM-Datei kann verwendet werden, um eine gesamte VM in einem Katastrophenszenario wiederherzustellen.
- Um eine VM schnell zu kopieren, z. B. eine spezielle Serverkonfiguration, die Sie häufig verwenden. Sie konfigurieren die VM einfach so, wie Sie es möchten, exportieren sie und importieren sie dann, um Kopien Ihrer ursprünglichen VM zu erstellen.
- Als einfache Methode zum Verschieben einer VM auf einen anderen Host.

Weitere Informationen zur Verwendung von Vorlagen finden Sie unter Erstellen von VMs und im Artikel Verwalten von VMs in der XenCenter-Dokumentation.

Geplante Snapshots

Die Funktion Geplante Snapshots bietet ein einfaches Backup- und Wiederherstellungsdienstprogramm für Ihre kritischen Service-VMs. Regelmäßig geplante Snapshots werden automatisch erstellt und können zur Wiederherstellung einzelner VMs verwendet werden. Geplante Snapshots verfügen über poolweite Snapshot-Zeitpläne für ausgewählte VMs im Pool. Wenn ein Snapshot-Zeitplan aktiviert ist, werden Snapshots der angegebenen VM jede Stunde, Tag oder Woche zur geplanten Zeit erstellt. In einem Pool können mehrere geplante Snapshots aktiviert werden, die verschiedene VMs und unterschiedliche Zeitpläne abdecken. Eine VM kann jeweils nur einem Snapshot-Zeitplan zugewiesen werden.

XenCenter bietet eine Reihe von Tools, die Sie bei der Verwendung dieser Funktion unterstützen:

- Verwenden Sie den Assistenten zum Erstellen eines neuen **Snapshot-Zeitplans**, um einen geplanten Snapshot zu definieren.
- Um geplante Snapshots für einen Pool zu aktivieren, zu deaktivieren, zu bearbeiten und zu löschen, verwenden Sie das Dialogfeld **VM-Snapshot-Zeitpläne** .
- Um einen Snapshot-Zeitplan zu bearbeiten, öffnen Sie das zugehörige **Eigenschaften-Dialogfeld** im Dialogfeld **VM-Snapshot-Zeitpläne** .
- Um eine VM auf einen geplanten Snapshot zurückzusetzen, wählen Sie den Snapshot auf der Registerkarte **Snapshots** aus, und stellen Sie die VM wieder her.

Weitere Informationen finden Sie unter Geplante Snapshots in der XenCenter-Dokumentation.

Umgang mit Maschinenausfällen

September 19, 2023

Dieser Abschnitt enthält Einzelheiten zur Wiederherstellung nach verschiedenen Ausfallszenarien. Alle Szenarien zur Wiederherstellung nach einem Ausfall erfordern die Verwendung eines oder mehrerer der unter Backup aufgeführten Backuptypen.

Ausfälle von Mitgliedern

Wenn keine HA vorhanden ist, erkennen Poolkoordinatorknoten die Ausfälle von Mitgliedern, indem sie regelmäßige Heartbeat-Meldungen empfangen. Wenn 600 Sekunden lang kein Heartbeat empfangen wurde, geht der Poolkoordinator davon aus, dass das Mitglied tot ist. Es gibt zwei Möglichkeiten, dieses Problem zu beheben:

- Reparieren Sie den toten Host (z. B. indem Sie ihn physisch neu starten). Wenn die Verbindung zu dem Mitglied wiederhergestellt ist, markiert der Poolkoordinator das Mitglied wieder als aktiv.
- Fahren Sie den Host herunter und weisen Sie den Poolkoordinator mit dem CLI-Befehl `xe host-forget` an, den Mitgliedsknoten zu vergessen. Sobald das Mitglied vergessen wurde, werden alle VMs, die dort ausgeführt wurden, als offline markiert und können auf anderen XenServer-Hosts neu gestartet werden.

  Es ist wichtig sicherzustellen, dass der XenServer-Host tatsächlich offline ist, da es sonst zu einer Beschädigung der VM-Daten kommen kann.

  Teilen Sie Ihren Pool nicht mithilfe von in mehrere Pools eines einzelnen Hosts auf `xe host-forget`. Diese Aktion kann dazu führen, dass alle denselben gemeinsam genutzten Speicher zuordnen und VM-Daten beschädigen.

> **Warnung:**
>
> - Wenn Sie den vergessenen Host wieder als aktiven Host verwenden möchten, führen Sie eine Neuinstallation der XenServer-Software durch.
> - Verwenden Sie nicht den Befehl `xe host-forget`, wenn HA im Pool aktiviert ist. Deaktivieren Sie zuerst HA, vergessen Sie dann den Host und aktivieren Sie dann HA erneut.

Wenn ein XenServer-Mitgliedshost ausfällt, sind möglicherweise noch VMs im *laufenden* Zustand registriert. Wenn Sie sicher sind, dass der XenServer-Mitgliedshost definitiv ausgefallen ist, verwenden Sie den `xe vm-reset-powerstate` CLI-Befehl, um den Betriebsstatus der VMs auf einzustellen. `halted` Weitere Informationen finden Sie unter vm-reset-powerstate .

> **Warnung:**
>
> Eine falsche Verwendung dieses Befehls kann zu einer Beschädigung der Daten führen. Verwenden Sie diesen Befehl nur bei Bedarf.

Bevor Sie VMs auf einem anderen XenServer-Host starten können, müssen Sie auch die Sperren für den VM-Speicher aufheben. Nur ein Host gleichzeitig kann jeden Datenträger in einem SR verwenden. Es ist wichtig, die Festplatte für andere XenServer-Hosts zugänglich zu machen, sobald ein Host ausgefallen ist. Führen Sie dazu das folgende Skript auf dem Pool-Koordinator für jede SR aus, die Festplatten aller betroffenen VMs enthält: `/opt/xensource/sm/resetvdis.py host_UUID SR_UUID master`

Sie müssen nur die dritte Zeichenfolge („Master“) angeben, wenn der ausgefallene Host zum Zeitpunkt des Absturzes der SR-Pool-Koordinator war. (Der SR-Poolkoordinator ist der Poolkoordinator oder ein XenServer-Host, der lokalen Speicher verwendet.)

> **Warnung:**
>
> Stellen Sie sicher, dass der Host ausgefallen ist, bevor Sie diesen Befehl ausführen. Eine falsche Verwendung dieses Befehls kann zu einer Beschädigung der Daten führen.

Wenn Sie versuchen, eine VM auf einem anderen XenServer-Host zu starten, bevor Sie das `resetvdis.py` Skript ausführen, erhalten Sie die folgende Fehlermeldung: `VDI <UUID> already attached RW`.

Ausfälle des Poolkoordinators

Jedes Mitglied eines Ressourcenpools enthält alle Informationen, die erforderlich sind, um bei Bedarf die Rolle des Poolkoordinators zu übernehmen. Wenn ein Poolkoordinatorknoten ausfällt, tritt die folgende Abfolge von Ereignissen auf:

1. Wenn HA aktiviert ist, wird automatisch ein anderer Poolkoordinator gewählt.
2. Wenn HA nicht aktiviert ist, wartet jedes Mitglied auf die Rückkehr des Poolkoordinators.

Wenn der Poolkoordinator zu diesem Zeitpunkt wieder auftaucht, stellt er die Kommunikation mit seinen Mitgliedern wieder her, und der Betrieb wird wieder normal.

Wenn der Poolkoordinator tot ist, wählen Sie eines der Mitglieder aus und führen Sie den Befehl `xe pool-emergency-transition-to-master` darauf aus. Sobald er der Pool-Koordinator geworden ist, führen Sie den Befehl aus `xe pool-recover-slaves` und die Mitglieder zeigen nun auf den neuen Pool-Koordinator.

Wenn Sie den Host, der der ursprüngliche Poolkoordinator war, reparieren oder ersetzen, können Sie ihn einfach aufrufen, die XenServer-Software installieren und ihn dem Pool hinzufügen. Da die XenServer-Hosts im Pool homogen sein müssen, besteht keine wirkliche Notwendigkeit, den ersetzten Host zum Poolkoordinator zu machen.

Wenn ein XenServer-Mitgliedshost in einen Poolkoordinator umgewandelt wird, überprüfen Sie, ob das Standard-Pool-Speicher-Repository auf einen geeigneten Wert gesetzt ist. Diese Prüfung kann mit dem Befehl `xe pool-param-list` durchgeführt werden. Überprüfen Sie, ob der Parameter **`default`**`-SR` auf ein gültiges Speicherrepository verweist.

Pool-Ausfälle

In dem unglücklichen Fall, dass Ihr gesamter Ressourcenpool ausfällt, müssen Sie die Pooldatenbank von Grund auf neu erstellen. Stellen Sie sicher, dass Sie mit dem CLI-Befehl `xe pool-dump-database` regelmäßig Backups Ihrer Pool-Metadaten erstellen (siehe `pool-dump-database`).

So stellen Sie einen vollständig ausgefallenen Pool wieder her:

1. Installieren Sie einen neuen Satz von Hosts. Bündeln Sie sie zu diesem Zeitpunkt nicht.
2. Stellen Sie für den als Poolkoordinator nominierten Host die Pooldatenbank aus Ihrem Backup mit dem Befehl `xe pool-restore-database` wieder her (siehe pool-restore-database).
3. Stellen Sie mithilfe von XenCenter eine Verbindung zum Poolkoordinator her und stellen Sie sicher, dass Ihr gesamter gemeinsam genutzter Speicher und Ihre VMs wieder verfügbar sind.
4. Führen Sie einen Pool-Join-Vorgang auf den verbleibenden frisch installierten Mitgliedshosts durch und starten Sie Ihre VMs auf den entsprechenden Hosts.

Bewältigen Sie Fehler aufgrund von Konfigurationsfehlern

Wenn der physische Host-Computer betriebsbereit ist, aber die Software- oder Host-Konfiguration beschädigt ist:

1. Führen Sie den folgenden Befehl aus, um die Hostsoftware und -konfiguration wiederherzustellen:

```
xe host-restore host=host file-name=hostbackup
<!--NeedCopy-->
```

2. Starten Sie auf der Host-Installations-CD neu und wählen Sie **Aus Backup wiederherstellen**.

Physischer Maschinenausfall

Wenn der physische Host-Computer ausgefallen ist, verwenden Sie zur Wiederherstellung das entsprechende Verfahren aus der folgenden Liste.

> **Warnung:**
>
> Alle virtuellen Maschinen, die auf einem früheren Mitglied (oder dem vorherigen Host) ausgeführt wurden und ausgefallen sind, werden weiterhin als `Running` in der Datenbank gekennzeichnet. Dieses Verhalten dient der Sicherheit. Das gleichzeitige Starten einer VM auf zwei verschiedenen Hosts würde zu einer schweren Datenträgerbeschädigung führen. Wenn Sie sicher sind, dass die Maschinen (und VMs) offline sind, können Sie den Betriebszustand der VM auf `Halted`Folgendes zurücksetzen:
>
> `xe vm-reset-powerstate vm=vm_uuid --force`
>
> VMs können dann mit XenCenter oder der CLI neu gestartet werden.

So ersetzen Sie einen ausgefallenen Poolkoordinator durch ein noch laufendes Mitglied:

1. Führen Sie die folgenden Befehle aus:


```
xe pool-emergency-transition-to-master
xe pool-recover-slaves
<!--NeedCopy-->
```

2. Wenn die Befehle erfolgreich sind, starten Sie die virtuellen Maschinen neu.

Das Wiederherstellen eines Pools mit allen Hosts ist fehlgeschlagen:

1. Führen Sie den Befehl aus:

```
xe pool-restore-database file-name=backup
<!--NeedCopy-->
```

> **Warnung:**
>
> Dieser Befehl ist nur erfolgreich, wenn der Zielcomputer über eine entsprechende Anzahl von entsprechend benannten NICs verfügt.

2. Wenn der Zielcomputer eine andere Ansicht des Speichers hat als die ursprüngliche Maschine, ändern Sie die Speicherkonfiguration mit dem Befehl `pbd-destroy`. Verwenden Sie als Nächstes den Befehl `pbd-create`, um Speicherkonfigurationen neu zu erstellen. Eine Dokumentation dieser Befehle finden Sie unter pbd-Befehle .
3. Wenn Sie eine Speicherkonfiguration erstellt haben, verwenden Sie `pbd-plug` oder das Menüelement **Speicher > Speicherrepository reparieren** in XenCenter, um die neue Konfiguration zu verwenden.
4. Starten Sie alle virtuellen Maschinen neu.

So stellen Sie eine VM wieder her, wenn VM-Speicher nicht verfügbar ist:

1. Führen Sie den folgenden Befehl aus:

```
xe vm-import filename=backup metadata=true
<!--NeedCopy-->
```

2. Wenn der Metadatenimport fehlschlägt, führen Sie den Befehl aus:

```
xe vm-import filename=backup metadata=true --force
<!--NeedCopy-->
```

   Mit diesem Befehl wird versucht, die VM-Metadaten nach bestem Aufwand wiederherzustellen.

3. Starten Sie alle virtuellen Maschinen neu.

---

layout: doc
description: Use Workload Balancing to create reports and recommendations about the placement of VMs in your XenServer pool.—

Workload Balancing

> **Hinweise:**
>
> - Workload Balancing ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.
> - Workload Balancing 8.3.0 und höher sind mit XenServer 8 kompatibel. Wenn Sie ein Rolling-Pool-Upgrade von Citrix Hypervisor 8.2 CU1 auf XenServer 8 durchführen, können Sie Workload Balancing 8.2.2 nicht mit Ihren XenServer 8-Pools verwenden. Aktualisieren Sie die virtuelle Workload Balancing-Appliance auf 8.3.0, bevor Sie das Rolling Pool-Upgrade durchführen. Sie können die neueste Version der virtuellen Workload Balancing-Appliance von der XenServer-Downloadseite herunterladen.

Workload Balancing ist eine XenServer Premium Edition-Komponente, die als virtuelle Appliance verpackt ist und die folgenden Funktionen bietet:

- Erstellen Sie Berichte über die Leistung virtueller Maschinen (VM) in Ihrer XenServer-Umgebung
- Evaluiert die Ressourcenauslastung und lokalisiert virtuelle Maschinen auf den bestmöglichen Hosts im Pool für die Anforderungen ihrer Workload
- VM-Workloads auf mehrere Hosts in einem XenServer-Ressourcenpool verteilen
- Den besten Host ermitteln, auf dem eine VM gestartet werden soll
- Den besten Host ermitteln, auf dem eine ausgeschaltete VM wieder aufgenommen werden kann
- Den besten Host ermitteln, auf den eine VM verschoben werden kann, wenn ein Host ausfällt
- Den optimalen Server für jede virtuelle Maschine des Hosts ermitteln, wenn Sie einen Host in den Wartungsmodus versetzen oder aus dem Wartungsmodus nehmen

Je nach Ihren Vorlieben kann der Workload Balancing diese Aufgaben automatisch ausführen oder Sie auffordern, die Empfehlungen zur Neuverteilung und Platzierung zu akzeptieren. Sie können den Workload Balancing auch so konfigurieren, dass Hosts zu bestimmten Tageszeiten automatisch ausgeschaltet werden. Konfigurieren Sie Ihre Hosts beispielsweise so, dass sie nachts ausgeschaltet werden, um Strom zu sparen.

Workload Balancing kann in XenCenter Benachrichtigungen über die ergriffenen Maßnahmen senden. Weitere Informationen zum Konfigurieren der Warnstufe für Workload Balancing-Warnungen mithilfe der xe-CLI finden Sie unter Festlegen der Warnstufe für Workload Balancing-Warnungen in XenCenter.

Workload Balancing funktioniert, indem die Verwendung von VMs in einem Pool ausgewertet wird. Wenn ein Host einen Leistungsschwellenwert überschreitet, verlagert der Workload Balancing die VM

auf einen weniger besteuerten Host im Pool. Um die Workloaden wieder auszugleichen, verschiebt der Workload Balancing VMs, um die Ressourcennutzung auf Hosts auszugleichen.

Um sicherzustellen, dass die Empfehlungen zur Neuverteilung und Platzierung den Anforderungen Ihrer Umgebung entsprechen, können Sie den Workload Balancing auf eine der folgenden Arten konfigurieren, um die Workloaden zu optimieren:

- Um die Ressourcenleistung zu maximieren
- Um die Anzahl der virtuellen Maschinen zu maximieren, die auf Hosts passen

Diese Optimierungsmodi können so konfiguriert werden, dass sie sich automatisch zu vordefinierten Zeiten ändern oder immer gleich bleiben. Optimieren Sie für zusätzliche Granularität die Gewichtung einzelner Ressourcenmetriken: CPU, Netzwerk, Datenträger und Speicher.

Um Ihnen bei der Kapazitätsplanung zu helfen, bietet der Workload Balancing historische Berichte über den Status von Host und Pool, die Optimierung und die VM-Leistung und den VM-Bewegungsverlauf.

Da Workload Balancing Leistungsdaten erfasst, können Sie diese Komponente auch verwenden, um Berichte, sogenannte Workload-Berichte, über Ihre virtualisierte Umgebung zu erstellen. Weitere Informationen finden Sie unter Erstellen von Workloadberichten.

Grundlegende Konzepte für Workload Balancing

Wenn virtuelle Maschinen ausgeführt werden, verbrauchen sie Rechenressourcen auf dem physischen Host. Zu diesen Ressourcen gehören CPU, Arbeitsspeicher, Netzwerklesevorgänge, Netzwerkschreibvorgänge, Datenträgerlesevorgänge und Datenträgerschreibvorgänge. Einige VMs verbrauchen je nach Workload möglicherweise mehr CPU-Ressourcen als andere VMs auf demselben Host. Die Workload wird durch die auf einer VM ausgeführten Anwendungen und deren Benutzertransaktionen definiert. Der kombinierte Ressourcenverbrauch aller VMs auf einem Host reduziert die verfügbaren Ressourcen auf dem Host.

Workload Balancing erfasst Daten für die Ressourcenleistung auf VMs und physischen Hosts und speichert sie in einer Datenbank. Der Workload Balancing verwendet diese Daten in Kombination mit den von Ihnen festgelegten Einstellungen, um Optimierungs- und Platzierungsempfehlungen bereitzustellen.

Optimierungen sind eine Methode, mit der Hosts “verbessert”werden, um sie an Ihren Zielen auszurichten: Workload Balancing gibt Empfehlungen zur Neuverteilung der VMs auf die Hosts im Pool, um entweder die Leistung oder die Dichte zu erhöhen. Wenn Workload Balancing Empfehlungen ausspricht, werden diese vor dem Hintergrund seines Ziels gestellt: Balance oder Harmonie zwischen den Hosts im Pool zu schaffen. Wenn der Workload Balancing auf diese Empfehlungen reagiert, wird die Aktion als Optimierung bezeichnet.

Wenn der Workload Balancing aktiviert ist, bietet XenCenter Sternbewertungen, um die optimalen Hosts für den Start einer VM anzuzeigen. Diese Bewertungen werden auch bereitgestellt:

- Wenn Sie die VM starten möchten, wenn sie ausgeschaltet ist
- Wenn Sie die VM starten möchten, wenn sie angehalten ist
- Wenn Sie die VM auf einen anderen Host migrieren möchten (Migrate- und Wartungsmodus)

In einem Workload-Balancing-Kontext:

- **Leistung** ist die Nutzung physischer Ressourcen auf einem Host (z. B. CPU-, Speicher-, Netzwerk- und Datenträgerauslastung auf einem Host). Wenn Sie Workload Balancing so einrichten, dass die Leistung maximiert wird, sollten VMs platziert werden, um sicherzustellen, dass für jede VM die maximale Menge an Ressourcen verfügbar ist.
- **Dichte** ist die Anzahl der virtuellen Maschinen auf einem Host. Wenn Sie den Workload Balancing zur Maximierung der Dichte festlegen, wird empfohlen, VMs zu platzieren, damit Sie die Anzahl der in einem Pool eingeschalteten Hosts reduzieren können. Es stellt sicher, dass die VMs über ausreichende Rechenleistung verfügen.

Der Workload Balancing steht nicht in Konflikt mit den Einstellungen, die Sie bereits für Hochverfügbarkeit angegeben haben: Diese Funktionen sind kompatibel.

---

layout: doc
description: Discover the features added in the latest Workload Balancing virtual appliance.—

Was ist neu in Workload Balancing

Die neueste Version der virtuellen Workload Balancing-Appliance ist Version 8.3.0. Sie können diese Version der virtuellen Workload Balancing-Appliance von der XenServer-Downloadseite herunterladen.

Was ist neu in 8.3.0

Veröffentlicht am 23. Februar 2023

Dieses Update beinhaltet die folgenden Verbesserungen:

- Sie können jetzt die Warnstufe für Workload Balancing-Warnungen in XenCenter mithilfe der Management-API festlegen.

Dieses Update beinhaltet Änderungen an der WLB-Datenbank. Stellen Sie sicher, dass Sie das bereitgestellte Migrationsskript verwenden, wenn Sie Ihren WLB auf diese Version aktualisieren. Weitere Informationen zur Verwendung des Migrationsskripts finden Sie unter Migrieren von Daten von einer vorhandenen virtuellen Appliance.

Behobene Probleme in 8.3.0

Dieses Update behebt die folgenden Probleme:

- Während des Wartungsfensters für den Workload Balancing kann der Workload Balancing keine Platzierungsempfehlungen geben. Wenn diese Situation eintritt, wird der Fehler angezeigt: "Die 4010-Pool-Erkennung wurde nicht abgeschlossen. Verwenden des ursprünglichen Algorithmus. "Das Wartungsfenster für den Workload Balancing ist weniger als 20 Minuten lang und standardmäßig um Mitternacht geplant.
- Für eine virtuelle Workload Balancing-Appliance Version 8.2.2 und höher, die kein LVM verwendet, können Sie den verfügbaren Speicherplatz nicht erweitern.
- Aufgrund eines nicht reagierenden API-Aufrufs wird der Workload Balancing manchmal während der Poolerkennung blockiert.
- In XenCenter sind der Datumsbereich und einige Zeitstempel, die im Workload Balancing Pool Auditbericht angezeigt werden, falsch.
- In XenCenter werden einige Zeichenfolgen für Workload-Berichte nicht korrekt angezeigt.
- Wenn die virtuelle Workload Balancing-Appliance längere Zeit läuft, wird sie vom Betriebssystem heruntergefahren, weil sie viel Arbeitsspeicher beansprucht.
- Die Datenbank kann nicht automatisch neu gestartet werden, nachdem die virtuelle Workload Balancing-Appliance abnormal heruntergefahren wurde.

Frühere Releases

In diesem Abschnitt werden Funktionen früherer Versionen zusammen mit ihren behobenen Problemen aufgeführt. Diese früheren Versionen werden durch die neueste Version der virtuellen Workload Balancing-Appliance ersetzt. Aktualisieren Sie auf die neueste Version der virtuellen Workload Balancing-Appliance, sobald diese verfügbar ist.

XenCenter 8.2.2

Veröffentlicht am 30. September 2021

Dieses Update beinhaltet Änderungen an der WLB-Datenbank. Stellen Sie sicher, dass Sie das bereitgestellte Migrationsskript verwenden, wenn Sie Ihren WLB auf diese Version aktualisieren. Weitere

Informationen zur Verwendung des Migrationsskripts finden Sie unter Migrieren von Daten von einer vorhandenen virtuellen Appliance.

Behobene Probleme Dieses Update enthält Korrekturen für die folgenden Probleme:

- Die Workload Balancing-Datenbank kann sehr schnell wachsen und den Datenträger füllen.
- Eine Racebedingung kann manchmal dazu führen, dass Datensätze in der WLB-Datenbank dupliziert werden. In diesem Fall wird dem Benutzer möglicherweise die folgende Fehlermeldung angezeigt: “WLB hat eine unbekannte Ausnahme erhalten”.

XenCenter 8.2.1

Veröffentlicht am 15. September 2020

Dieses Update beinhaltet die folgenden Verbesserungen:

- Mit dem Migrationsskript können Sie jetzt Ihre Workload Balancing-Datenbank von der virtuellen Workload Balancing-Appliance 8.0.0 (die mit Citrix Hypervisor 8.0 und 8.1 bereitgestellt wurde) zur virtuellen Workload Balancing-Appliance 8.2.1 migrieren, die mit Citrix Hypervisor 8.2 bereitgestellt wird.

  Weitere Informationen zur Verwendung des Migrationsskripts finden Sie unter Migrieren von Daten von einer vorhandenen virtuellen Appliance.

Behobene Probleme Dieses Update enthält Korrekturen für die folgenden Probleme:

- Wenn mehrere VMs gleichzeitig gestartet werden, empfiehlt Workload Balancing, die Platzierung der VMs auf allen Hosts im Pool gleichmäßig auszugleichen. Manchmal empfiehlt Workload Balancing jedoch, viele VMs auf demselben XenServer-Host zu platzieren. Dieses Problem tritt auf, wenn der Workload Balancing verspätetes Feedback von XAPI zur VM-Platzierung erhält

---

layout: doc
description: Install and set up the Workload Balancing virtual appliance to benefit from the Workload Balancing feature in your XenServer pools.—

Erste Schritte mit dem Workload Balancing

Sie können die virtuelle Workload Balancing-Appliance in nur wenigen Schritten konfigurieren:

1. Prüfen Sie die erforderlichen Informationen und planen Sie die Verwendung des Workload Balancings.
2. Laden Sie das virtuelle Workload Balancing Appliance herunter.
3. Importieren Sie das virtuelle Workload Balancing-Appliance in XenCenter.
4. Konfigurieren Sie die virtuelle Workload Balancing-Appliance über die Konsole der virtuellen Anwendung.
5. (Optional) Wenn Sie bereits eine frühere Version von Workload Balancing installiert haben, können Sie Daten von einer vorhandenen virtuellen Appliance migrieren.

   > **Hinweis:**
   >
   > Wenn Sie ein Rolling-Pool-Upgrade von Citrix Hypervisor 8.2 CU1 auf XenServer 8 durchführen, können Sie Workload Balancing 8.2.2 und früher nicht mit Ihren XenServer 8-Pools verwenden. Aktualisieren Sie Ihre virtuelle Workload Balancing-Appliance auf Version 8.3.0, bevor Sie das Rolling Pool-Upgrade durchführen. Sie können die neueste Version der virtuellen Workload Balancing-Appliance von der XenServer-Downloadseite herunterladen.

6. Verbinden Sie Ihren Pool über XenCenter mit der virtuellen Workload Balancing-Appliance.

   Die Registerkarte Workload Balancing wird in XenCenter nur angezeigt, wenn Ihr Pool über die erforderliche Lizenz zur Verwendung des Workload Balancing verfügt.

Vorbereitung

Die virtuelle Workload Balancing-Appliance ist eine einzelne vorinstallierte VM, die für die Ausführung auf einem XenServer-Host konzipiert ist. Lesen Sie vor dem Importieren die erforderlichen Informationen und Überlegungen.

Voraussetzungen

- Workload Balancing 8.3.0 und höher sind mit XenServer 8 kompatibel. Wir empfehlen, die XenCenter Management Console zum Importieren der virtuellen Appliance zu verwenden.
- Wenn Sie ein Rolling-Pool-Upgrade von Citrix Hypervisor 8.2 CU1 auf XenServer 8 durchführen, können Sie Workload Balancing 8.2.2 und früher nicht mit Ihren XenServer 8-Pools verwenden. Aktualisieren Sie Ihre virtuelle Workload Balancing-Appliance auf Version 8.3.0, bevor Sie das

Rolling Pool-Upgrade durchführen. Sie können die neueste Version der virtuellen Workload Balancing-Appliance von der XenServer-Downloadseite herunterladen.

- Wenn Sie derzeit eine frühere Version der virtuellen Workload Balancing-Appliance verwenden, können Sie das Migrationsskript verwenden, um Ihre vorhandenen Daten zu migrieren, wenn Sie auf die neueste Version aktualisieren. Weitere Informationen finden Sie unter Migrieren von einer vorhandenen virtuellen Appliance.
- Die virtuelle Workload Balancing-Appliance benötigt mindestens 2 GB RAM und 30 GB Speicherplatz zur Ausführung. Standardmäßig werden der virtuellen Workload Balancing-Appliance 2 vCPUs zugewiesen. Dieser Wert ist ausreichend für Pools, die 1000 virtuelle Maschinen hosten. Sie müssen es normalerweise nicht erhöhen. Reduzieren Sie nur die Anzahl der vCPUs, die der virtuellen Appliance zugewiesen sind, wenn Sie über eine kleine Umgebung verfügen. Weitere Informationen finden Sie unter Ändern der Konfiguration der virtuellen Appliance für den Workload Balancing.

Anforderungen an den Pool

Um einen Pool mit Workload Balancing auszugleichen, muss der Pool die folgenden Anforderungen erfüllen:

- Alle Hosts sind mit einer Premium Edition-Lizenz lizenziert
- Alle Hosts erfüllen die Anforderungen für die Live-Migration:
  - Gemeinsam genutzter Remote-Speicher
  - Ähnliche Prozessorkonfigurationen
  - Gigabit-Ethernet
- Der Pool enthält keine vGPU-fähigen virtuellen Maschinen. Der Workload Balancing kann keinen Kapazitätsplan für VMs erstellen, an die vGPUs angeschlossen sind.

Eine einzelne virtuelle Workload Balancing-Appliance kann mehrere Pools bis zu maximal 100 Pools verwalten, abhängig von den Ressourcen der virtuellen Appliance (vCPU, Arbeitsspeicher, Datenträgergröße). In diesen Pools kann die virtuelle Appliance bis zu 1000 VMs verwalten. Wenn ein Pool jedoch eine große Anzahl von VMs hat (z. B. mehr als 400 VMs), empfehlen wir, eine virtuelle Workload Balancing-Appliance nur für diesen Pool zu verwenden.

Überlegungen

Bevor Sie die virtuelle Appliance importieren, notieren Sie sich die folgenden Informationen und nehmen Sie gegebenenfalls die entsprechenden Änderungen an Ihrer Umgebung vor.

- **Kommunikations-Anschluss**. Bevor Sie den Assistenten für die Konfiguration des Workloadausgleichs starten, legen Sie den Port fest, über den die virtuelle Workload Balancing-Appliance kommunizieren soll. Sie werden während der Konfiguration des Workloadausgleichs zur Eingabe dieses Port aufgefordert. Standardmäßig verwendet der Workload Balancing-Server 8012.

  > **Hinweis:**
  >
  > Stellen Sie den Workload Balancing-Port nicht auf Port 443 ein. Die virtuelle Workload Balancing-Appliance kann keine Verbindungen über Port 443 (den Standard-TLS/HTTPS-Port) akzeptieren.

- **Konten für den Workload Balancing**. Es gibt drei verschiedene Konten, die verwendet werden, wenn Sie Ihre virtuelle Workload Balancing-Appliance konfigurieren und mit XenServer verbinden.

  Der Konfigurations-Assistent für den Workload Balancing erstellt die folgenden Konten mit einem Benutzernamen und einem Kennwort, die Sie angeben:

  - *Konto für den Workloadausgleich*

    Dieses Konto wird vom XenServer-Host verwendet, um eine Verbindung zum Workload Balancing-Server herzustellen. Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`. Dieser Benutzer wird während der Konfiguration des Workloadausgleichs auf der virtuellen Appliance Workload Balancing erstellt.

  - *Datenbank-Konto*

    Dieses Konto wird für den Zugriff auf die PostgreSQL-Datenbank auf der virtuellen Workload Balancing-Appliance verwendet. In der Standardeinstellung lautet der Benutzername `postgres`. Sie legen das Kennwort für dieses Konto während der Konfiguration des Workload Balancing fest.

  Wenn Sie die virtuelle Workload Balancing-Appliance mit einem XenServer-Pool verbinden, müssen Sie ein vorhandenes Konto angeben:

  - *XenServer-Konto*

    Dieses Konto wird von der virtuellen Workload Balancing-Appliance verwendet, um eine Verbindung zum XenServer-Pool herzustellen und die RRDs zu lesen. Stellen Sie sicher, dass dieses Benutzerkonto über die Berechtigungen zum Lesen der XenServer-Pool-, Host- und VM-RRDs verfügt. Geben Sie beispielsweise die Anmeldeinformationen für einen Benutzer mit der Rolle `pool-admin` oder `pool-operator` an.

- **Überwachung über Pools hinweg**. Sie können die virtuelle Workload Balancing-Appliance in einem Pool ablegen und damit einen anderen Pool überwachen. (Die virtuelle Workload

Balancing-Appliance befindet sich beispielsweise in Pool A, aber Sie verwenden sie zur Überwachung von Pool B.)

- **Zeitsynchronisierung** Für die virtuelle Workload Balancing-Appliance muss die Zeit auf dem physischen Computer, auf dem die virtuelle Appliance gehostet wird, mit der vom überwachten Pool verwendeten Zeit übereinstimmt. Es gibt keine Möglichkeit, die Uhrzeit auf der virtuellen Workload Balancing-Appliance zu ändern. Wir empfehlen, sowohl den physischen Computer, der den Workload Balancing hostet, als auch die Hosts in dem Pool, den er überwacht, auf denselben NTP-Server (Network Time) zu verweisen.
- **XenServer und Workload Balancing kommunizieren über HTTPS**. Daher erstellt Workload Balancing während der Konfiguration des Workload Balancing automatisch ein selbstsigniertes Zertifikat in Ihrem Namen. Sie können dieses Zertifikat in eines von einer Zertifizierungsstelle ändern oder XenServer so konfigurieren, dass das Zertifikat oder beide überprüft werden. Weitere Informationen finden Sie in den Zertifikaten.
- **Speicherung historischer Daten und Speicherplatzgröße**. Die Menge der historischen Daten, die Sie speichern können, basiert auf folgenden Daten:
  - Die Größe des virtuellen Laufwerks, das dem Workload Balancing zugewiesen ist (standardmäßig 30 GB)
  - Der minimale Datenträgerspeicher, der standardmäßig 2.048 MB beträgt und durch den Parameter `GroomingRequiredMinimumDiskSizeInMB` in der Datei `wlb.conf` gesteuert wird.

  Je mehr historische Daten Workload Balancing sammelt, desto genauer und ausgewogener sind die Empfehlungen. Wenn Sie viele historische Daten speichern möchten, können Sie einen der folgenden Schritte ausführen:

  - Archivieren Sie die Daten wie in Datenbankdaten archivierenbeschrieben
  - Erhöhen Sie die Größe des virtuellen Datenträgers, die der virtuellen Workload Balancing-Appliance zugewiesen ist, wie unter Datenträger der virtuellen Appliance erweitern beschrieben.

  Wenn Sie beispielsweise die Workload Balancing-Pool-Audit-Protokollfunktion verwenden und die Berichtsgranularität auf mittel oder höher konfigurieren möchten.
- **Lastenausgleich Workloadausgleich**. Wenn Sie Ihre virtuelle Workload Balancing-Appliance zur Selbstverwaltung verwenden möchten, geben Sie beim Importieren der virtuellen Appliance gemeinsam genutzten Remote-Speicher an.

  > **Hinweis:**
  >
  > Der Workloadausgleich kann die Empfehlung zum Starten bei der Platzierung für die virtuelle Workload Balancing-Appliance nicht ausführen, wenn Sie den Workload

> Balancing zur Verwaltung verwenden. Der Grund, warum Workload Balancing keine Platzierungsempfehlungen aussprechen kann, wenn es sich selbst verwaltet, liegt darin, dass die virtuelle Appliance ausgeführt werden muss, um diese Funktion auszuführen. Es kann jedoch die virtuelle Workload Balancing-Appliance so ausgleichen, wie es jede andere VM, die es verwaltet, ausgleichen würde.

- **Planen Sie die Dimensionierung des Ressourcenpools**. Der Workload Balancing erfordert bestimmte Konfigurationen, um in großen Pools erfolgreich ausgeführt zu werden. Weitere Informationen finden Sie unter Ändern der Konfiguration der virtuellen Appliance für den Workload Balancing.

Laden Sie das virtuelle Gerät herunter

Die virtuelle Workload Balancing-Appliance ist in einem `.xva`-Format verpackt. Sie können das virtuelle Gerät von der XenServer-Downloadseite herunterladen. Speichern Sie die Datei beim Herunterladen in einem Ordner auf Ihrer lokalen Datenträger (normalerweise auf dem Computer, auf dem XenCenter installiert ist).

Wenn der `.xva`-Download abgeschlossen ist, können Sie ihn in XenCenter importieren, wie unter Importieren des virtuellen Workload Balancing-Appliance beschrieben.

Importieren der virtuellen Workload Balancing-Appliance

Verwenden Sie XenCenter, um das virtuelle Workload Balancing-Appliance in einen Pool zu importieren.

Um das virtuelle Gerät in XenServer zu importieren:

1. Öffnen Sie XenCenter.
2. Klicken Sie mit der rechten Maustaste auf den Pool (oder Host), in den Sie das Paket der virtuellen Appliance importieren möchten, und wählen Sie **Importieren**.
3. Navigieren Sie zum Paket `vpx-wlb.xva`.
4. Wählen Sie den Pool oder Homeserver aus, auf dem Sie die virtuelle Workload Balancing-Appliance ausführen möchten.

   Wenn Sie den Pool auswählen, wird die VM automatisch auf dem am besten geeigneten Host in diesem Pool gestartet.

   Wenn Sie die virtuelle Workload Balancing-Appliance nicht mithilfe des Workload Balancing verwalten, können Sie alternativ einen Homeserver für die virtuelle Workload Balancing-Appliance einrichten. Diese Einstellung stellt sicher, dass die virtuelle Appliance immer auf demselben Host gestartet wird.

5. Wählen Sie ein Speicherrepository aus, auf dem das virtuelle Laufwerk für die virtuelle Workload Balancing-Appliance gespeichert werden soll. Dieses Repository muss mindestens 30 GB freien Speicherplatz haben.

   Sie können entweder lokalen oder Remote-Speicher wählen. Wenn Sie jedoch lokalen Speicher wählen, können Sie die virtuelle Appliance nicht mit dem Workload Balancing verwalten.

6. Definieren Sie die virtuellen Schnittstellen für die virtuelle Workload Balancing-Appliance. In dieser Version wurde der Workload Balancing für die Kommunikation auf einer einzigen virtuellen Schnittstelle entwickelt.

7. Wählen Sie ein Netzwerk aus, das auf den Pool zugreifen kann, den Workload Balancing verwalten soll.

8. Lassen **Sie das Kontrollkästchen VMs nach dem Import starten** aktiviert und klicken Sie auf **Fertigstellen**, um die virtuelle Appliance zu importieren.

9. Nachdem Sie den Import der Workload Balancing-Datei (`.xva`) abgeschlossen haben, wird die Workload Balancing-VM im **Ressourcenbereich** in XenCenter angezeigt.

Konfigurieren Sie nach dem Importieren der virtuellen Workload Balancing-Appliance die virtuelle Appliance wie unter Konfigurieren der virtuellen Workload Balancing-Appliancebeschrieben.

Konfigurieren der virtuellen Workload Balancing-Appliance

Nachdem Sie den Import der virtuellen Workload Balancing-Appliance abgeschlossen haben, müssen Sie sie konfigurieren, bevor Sie sie zur Verwaltung Ihres Pools verwenden können. Um Sie durch die Konfiguration zu führen, bietet Ihnen die virtuelle Workload Balancing-Appliance einen Konfigurationsassistenten in XenCenter. Um sie anzuzeigen, wählen Sie die virtuelle Appliance im Bereich **Ressource** aus und klicken Sie auf die Registerkarte **Konsole** . Drücken Sie für alle Optionen die **EINGABETASTE**, um die Standardauswahl zu übernehmen.

1. Klicken Sie nach dem Importieren der virtuellen Workload Balancing-Appliance auf die Registerkarte **Konsole** .

2. Geben Sie ein `yes`, um die Bedingungen der Lizenzvereinbarung zu akzeptieren. Um die EULA abzulehnen, geben Sie ein `no`.

   > **Hinweis:**
   >
   > Die virtuelle Workload Balancing-Appliance unterliegt auch den Lizenzen, die im Verzeichnis `/opt/vpx/wlb` der virtuellen Workload Balancing-Appliance enthalten sind.

3. Geben Sie ein neues Root-Kennwort für die Workload Balancing-VM ein und bestätigen Sie es. Wir empfehlen, ein sicheres Kennwort zu wählen.

> **Hinweis:**
>
> Wenn Sie das Kennwort eingeben, zeigt die Konsole keine Platzhalter wie Sternchen für die Zeichen an.

4. Geben Sie den Computernamen ein, den Sie der virtuellen Workload Balancing-Appliance zuweisen möchten.
5. Geben Sie das Domänensuffix für die virtuelle Appliance ein.

   Wenn beispielsweise der vollqualifizierte Domänenname (FQDN) für die virtuelle Appliance `wlb-vpx-pos-pool.domain4.bedford4.ctx` ist, geben Sie `domain4.bedford4.ctx` ein.

   > **Hinweis:**
   >
   > Die virtuelle Workload Balancing-Appliance fügt ihren FQDN nicht automatisch zu Ihrem DNS-Server (Domain Name System) hinzu. Wenn Sie möchten, dass der Pool einen FQDN verwendet, um eine Verbindung zum Workload Balancing herzustellen, müssen Sie den FQDN zu Ihrem DNS-Server hinzufügen.

6. Geben Sie ein `y` ein, um DHCP zu verwenden und die IP-Adresse für die Workload Balancing-VM automatisch abzurufen. Andernfalls geben Sie `n` und dann eine statische IP-Adresse, eine Subnetzmaske und ein Gateway für die VM ein.

   > **Hinweis:**
   >
   > Die Verwendung von DHCP ist zulässig, sofern die Lease der IP-Adresse nicht abläuft. Es ist wichtig, dass sich die IP-Adresse nicht ändert: Wenn sie sich ändert, wird die Verbindung zwischen XenServer und Workload Balancing unterbrochen.

7. Geben Sie einen Benutzernamen für die Workload Balancing-Datenbank ein, oder drücken **Sie die Eingabetaste**, um den Standardbenutzernamen (Postgres) des Datenbankkontos zu verwenden.

   Sie erstellen ein Konto für die Workload Balancing-Datenbank. Die Workload Balancing-Dienste verwenden dieses Konto zum Lesen/Schreiben in die Workload Balancing-Datenbank. Notieren Sie den Benutzernamen und das Kennwort. Sie benötigen sie möglicherweise, wenn Sie jemals direkt die PostgreSQL-Datenbank des Workload Balancing verwalten möchten (z. B. wenn Sie Daten exportieren möchten).

8. Geben Sie ein Kennwort für die Workload Balancing-Datenbank ein. Nachdem Sie die **Eingabetaste**gedrückt haben, werden Meldungen angezeigt, dass der Konfigurationsassistent Datenbankobjekte lädt.
9. Geben Sie einen Benutzernamen und ein Kennwort für den Workload Balancing Server ein.

Diese Aktion erstellt das Konto, mit dem XenServer eine Verbindung zum Workload Balancing herstellt. Der Standardbenutzername ist **wlbuser**.

10. Geben Sie den Port für den Workload Balancing-Server ein. Der Workload Balancing-Server kommuniziert mithilfe dieses Port.

    Standardmäßig verwendet der Workload Balancing-Server 8012. Die Portnummer kann nicht auf 443 festgelegt werden, was die standardmäßige TLS-Portnummer ist.

    > **Hinweis:**
    >
    > Wenn Sie den Port hier ändern, geben Sie diese neue Portnummer an, wenn Sie den Pool mit dem Workload Balancing verbinden. Zum Beispiel, indem Sie den Port im Dialog Mit **WLB Server verbinden** angeben.

    Stellen Sie sicher, dass der Port, den Sie für den Workloadausgleich angeben, in allen Firewalls geöffnet ist.

    Nachdem Sie die **Eingabetaste**gedrückt haben, setzt der Workload Balancing die Konfiguration der virtuellen Appliance fort, einschließlich der Erstellung selbstsignierter

11. Jetzt können Sie sich auch bei der virtuellen Appliance anmelden, indem Sie den VM-Benutzernamen (normalerweise `root`) und das zuvor erstellte Root-Kennwort eingeben. Die Anmeldung ist jedoch nur erforderlich, wenn Sie Workload Balancing-Befehle ausführen oder die Workload Balancing-Konfigurationsdatei bearbeiten möchten.

Verbinden Sie nach dem Konfigurieren des Workload Balancing Ihren Pool mit der virtuellen Workload Balancing-Appliance, wie unter Verbinden mit der virtuellen Workload Balancing-Appliancebeschrieben

Falls erforderlich, finden Sie die Workload Balancing-Konfigurationsdatei an folgendem Speicherort: `/opt/vpx/wlb/wlb.conf`. Weitere Informationen finden Sie unter Bearbeiten der Workload Balancing-Konfigurationsdatei.

Die Workload Balancing-Protokolldatei befindet sich an diesem Speicherort: `/var/log/wlb/LogFile.log`. Weitere Informationen finden Sie unter Erhöhen der Details im Workload Balancing-Protokoll.

Verbinden mit der virtuellen Workload Balancing-Appliance

Verbinden Sie nach der Konfiguration des Workload Balancing die Pools, die Sie verwalten möchten, über die CLI oder XenCenter mit der virtuellen Workload Balancing-Appliance.

> **Hinweis:**
>
> Eine einzelne virtuelle Workload Balancing-Appliance kann mehrere Pools bis zu maximal 100 Pools verwalten, abhängig von den Ressourcen der virtuellen Appliance (vCPU, Arbeitsspeicher, Datenträgergröße). In diesen Pools kann die virtuelle Appliance bis zu 1000 VMs verwalten. Wenn ein Pool jedoch eine große Anzahl von VMs hat (z. B. mehr als 400 VMs), empfehlen wir, eine virtuelle Workload Balancing-Appliance nur für diesen Pool zu verwenden.

Um einen Pool mit Ihrer virtuellen Workload Balancing-Appliance zu verbinden, benötigen Sie die folgenden Informationen:

- IP-Adresse oder FQDN der virtuellen Workload Balancing-Appliance
  - So rufen Sie die IP-Adresse für die virtuelle Workload Balancing-Appliance ab:
    1. Wechseln Sie in XenCenter zur Registerkarte Workload Balancing Virtual Appliance **Console** .
    2. Melden Sie sich als `root` mit dem root-Kennwort an, das Sie beim Importieren der Appliance erstellt haben.
    3. Führen Sie den folgenden Befehl aus: `ifconfig`.
  - Um den FQDN für den Workload Balancing anzugeben, wenn Sie eine Verbindung zum Workload Balancing-Server herstellen, fügen Sie zuerst den Hostnamen und die IP-Adresse Ihrem DNS-Server hinzu.
- Die Portnummer der virtuellen Workload Balancing-Appliance. Standardmäßig stellt XenServer eine Verbindung zu Workload Balancing auf Port 8012 her.

  Bearbeiten Sie die Portnummer nur, wenn Sie sie während der Konfiguration des Workloadausgleichs geändert haben. Die Portnummer, die während der Konfiguration des Workloadausgleichs, in allen Firewallregeln und im Dialogfeld Mit **WLB Server verbinden** angegeben wurde, muss übereinstimmen.
- Anmeldeinformationen für das Workload Balancing-Konto, das Sie während der Workload Balancing-Konfiguration erstellt haben

  Dieses Konto wird oft als Workloadausgleich-Benutzerkonto bezeichnet. XenServer verwendet dieses Konto für die Kommunikation mit Workload Balancing. Sie haben dieses Konto während der Konfiguration des Workloadausgleichs auf der virtuellen Appliance für den Workloadausgleich erstellt
- Anmeldeinformationen für den Ressourcenpool (d. h. den Poolkoordinator), den der Workload Balancing überwachen soll.

  Dieses Konto wird von der virtuellen Workload Balancing-Appliance verwendet, um eine Verbindung zum XenServer-Pool herzustellen. Dieses Konto wird auf dem XenServer-Poolkoordinator erstellt und hat die Rolle `pool-admin` oder `pool-operator`.

Wenn Sie zum ersten Mal eine Verbindung mit dem Workload Balancing herstellen, werden die Standardschwellenwerte und -einstellungen für den Ausgleich von Workloaden verwendet. Automatische Funktionen wie automatisierter Optimierungsmodus, Energieverwaltung und Automatisierung sind standardmäßig deaktiviert.

Mit Zertifikaten arbeiten

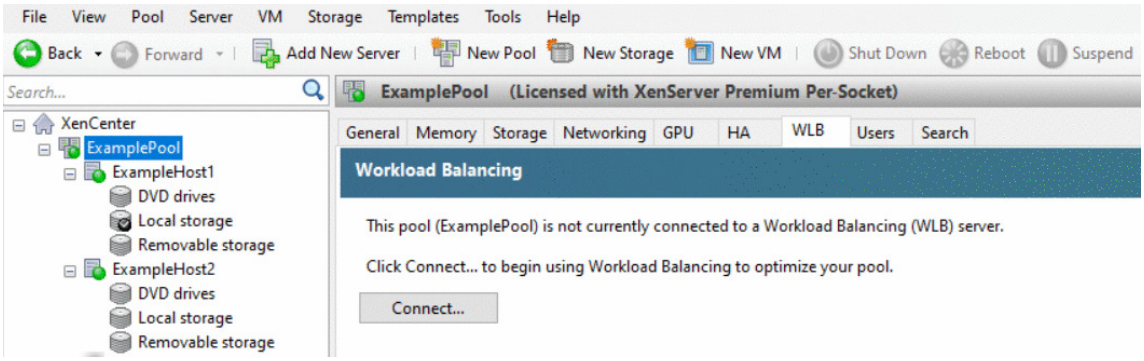
Wenn Sie ein anderes (vertrauenswürdiges) Zertifikat hochladen oder die Zertifikatsüberprüfung konfigurieren möchten, beachten Sie Folgendes, bevor Sie Ihren Pool mit dem Workload Balancing verbinden:

- Wenn Sie möchten, dass XenServer das selbstsignierte Workload Balancing-Zertifikat überprüft, müssen Sie die Workload Balancing-IP-Adresse verwenden, um eine Verbindung zum Workload Balancing herzustellen. Das selbstsignierte Zertifikat wird basierend auf seiner IP-Adresse für den Workload Balancing ausgestellt.
- Wenn Sie ein Zertifikat einer Zertifizierungsstelle verwenden möchten, ist es einfacher, den FQDN anzugeben, wenn Sie eine Verbindung zum Workload Balancing herstellen. Sie können jedoch im Dialog Mit **WLB Server verbinden** eine statische IP-Adresse angeben. Verwenden Sie diese IP-Adresse als alternativen Subject Name (SAN) im Zertifikat.

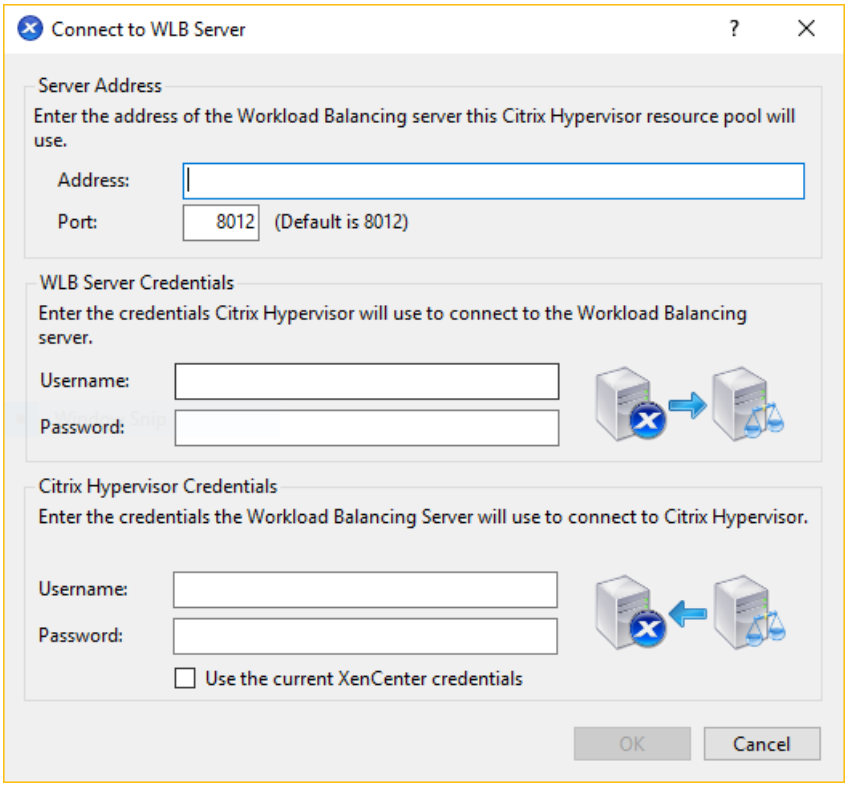
Weitere Informationen finden Sie unter Zertifikate.

So verbinden Sie Ihren Pool mit der virtuellen Workload Balancing-Appliance

1. Wählen Sie in XenCenter Ihren Ressourcenpool aus und klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **WLB** . Auf der Registerkarte **WLB** wird die Schaltfläche **Verbinden** angezeigt.



2. Klicken Sie auf der Registerkarte **WLB** auf **Verbinden**. Das Dialogfeld Mit **WLB Server verbinden** wird angezeigt.



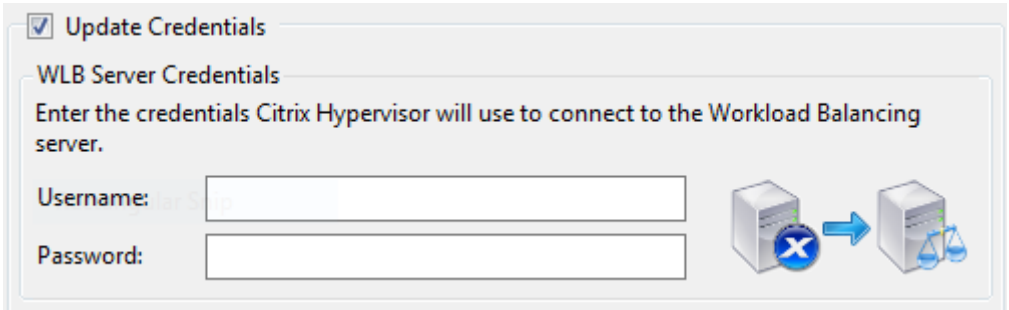
3. Geben Sie im Abschnitt **Serveradresse** Folgendes ein:

   a) Geben Sie in das Feld **Adresse** die IP-Adresse oder den FQDN der virtuellen Workload Balancing-Appliance ein. Beispiel: `WLB-appliance-computername.yourdomain.net`.

   b) (Optional) Wenn Sie den Workload Balancing-Port während der Konfiguration des Workload Balancings geändert haben, geben Sie die Portnummer in das Feld **Port** ein. XenServer verwendet diesen Port für die Kommunikation mit Workload Balancing.

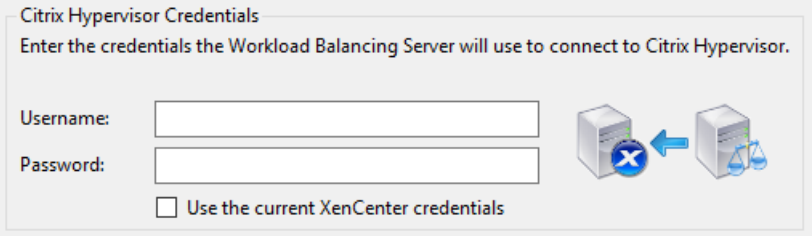
   Standardmäßig stellt XenServer eine Verbindung zu Workload Balancing auf Port 8012 her.

4. Geben Sie im Abschnitt **WLB Server-Anmeldeinformationen** den Benutzernamen und das Kennwort ein, die der Pool für die Verbindung mit der virtuellen Workload Balancing-Appliance verwendet.



Diese Anmeldeinformationen müssen das Konto sein, das Sie während der Konfiguration des Workload Balancings erstellt haben Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`.

5. Geben Sie im Abschnitt **Citrix Hypervisor Credentials** den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren. Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung zu den Hosts im Pool herzustellen.



Um die Anmeldeinformationen zu verwenden, mit denen Sie derzeit bei XenServer angemeldet sind, wählen Sie **Aktuelle XenCenter-Anmeldeinformationen verwenden**aus. Wenn Sie diesem Konto mithilfe der Zugriffssteuerungsfunktion (RBAC) eine Rolle zugewiesen haben, stellen Sie sicher, dass die Rolle über ausreichende Berechtigungen zum Konfigurieren des Workloadausgleichs verfügt. Weitere Informationen finden Sie unter Zugriffssteuerungsberechtigungen für den Workloadausgleich.

Nachdem Sie den Pool mit der virtuellen Appliance Workload Balancing verbunden haben, beginnt der Workload Balancing automatisch mit der Überwachung des Pools mit den Standardoptimierungseinstellungen. Um diese Einstellungen zu ändern oder die Priorität bestimmter Ressourcen zu ändern, warten Sie mindestens 60 Sekunden, bevor Sie fortfahren. Oder warten Sie, bis das XenCenter Log anzeigt, dass die Discovery abgeschlossen ist.

> **Wichtig:**
>
> Wenn der Workload Balancing eine Zeit lang ausgeführt wurde und Sie keine Empfehlungen für die optimale Platzierung erhalten, bewerten Sie Ihre Leistungsschwellenwerte. Diese Auswertung wird unter Verstehen beschrieben, wann der Workload Balancing Empfehlungen ausspricht. Es ist wichtig, den Workload-Balancing auf die richtigen Schwellenwerte für Ihre Umgebung festzulegen, da die Empfehlungen möglicherweise nicht angemessen sind.

Migrieren von Daten aus einer vorhandenen virtuellen Appliance

Wenn Sie das mit XenServer bereitgestellte virtuelle Workload Balancing-Appliance verwenden, können Sie das Migrationsskript verwenden, um Ihre vorhandenen Daten zu migrieren, wenn Sie auf die neueste Version aktualisieren (Workload Balancing 8.2.1 oder höher).

Die derzeit mit XenServer bereitgestellte Version von Workload Balancing ist 8.3.0. Workload Balancing 8.2.0, 8.2.1 und 8.2.2 waren jedoch zuvor mit früheren Versionen von Citrix Hypervisor verfügbar.

Sie können dieses Migrationsskript auch verwenden, um von Workload Balancing 8.2.1 oder 8.2.2 zu Workload Balancing 8.3.0 zu migrieren.

Um das Migrate-Skript verwenden zu können, benötigen Sie die folgenden Informationen:

- Das Root-Kennwort der vorhandenen virtuellen Workload Balancing-Appliance für den Remote-SSH-Zugriff
- Das Kennwort des Datenbankbenutzers `postgres` auf der vorhandenen virtuellen Workload Balancing-Appliance
- Das Kennwort des Datenbankbenutzers `postgres` auf der neuen virtuellen Workload Balancing-Appliance

Lassen Sie die vorhandene virtuelle Workload Balancing-Appliance in Ihrem Pool ausgeführt, während Sie die Migrationsschritte abschließen.

1. Befolgen Sie die Schritte im vorherigen Abschnitt, um die neue virtuelle Workload Balancing-Appliance zu importieren.
2. Führen Sie in der SSH-Konsole der neuen virtuellen Workload Balancing-Appliance einen der folgenden Befehle aus.

   - Führen Sie für die virtuelle Appliance Workload Balancing 8.2.1 Folgendes aus:

     ```
     1  /opt/vpx/wlb/migrate_db.sh 8.2.1 <IP of existing Workload
        Balancing appliance>
     ```

   - Führen Sie für die virtuelle Appliance Workload Balancing 8.2.2 Folgendes aus:

     ```
     1  /opt/vpx/wlb/migrate_db.sh 8.2.2 <IP of existing Workload
        Balancing appliance>
     ```

   Der Befehl fordert Sie bei Bedarf zur Eingabe von Kennwortinformationen auf.
3. Verbinden Sie den XenServer-Pool mit der neuen virtuellen Workload Balancing-Appliance.
4. Nachdem Sie mit dem Verhalten dieser Version der virtuellen Workload Balancing-Appliance zufrieden sind, können Sie die alte Version der virtuellen Appliance archivieren.

> **Hinweise:**
>
> - Importieren Sie im Falle eines nicht wiederherstellbaren Fehlers die neueste Version der virtuellen Workload Balancing-Appliance erneut.
> - Trennen Sie die vorhandene virtuelle Workload Balancing-Appliance nicht. Andernfalls werden die Daten auf der vorhandenen virtuellen Appliance entfernt.
> - Bewahren Sie die vorhandene virtuelle Workload Balancing-Appliance auf, bis Sie sichergestellt haben, dass die neue virtuelle Workload Balancing-Appliance wie erforderlich

> - Bei Bedarf können Sie diese Migration rückgängig machen, indem Sie die alte Version der virtuellen Workload Balancing-Appliance erneut mit dem XenServer-Pool verbinden.

---

layout: doc
description: Use Workload Balancing to regularly perform these basic tasks that help you optimize your XenServer environment.—

Grundlegende Aufgaben für den Workloadausgleich

Wenn Sie den Workload Balancing zum ersten Mal verwenden, gibt es einige grundlegende Aufgaben, für die Sie den Workload Balancing regelmäßig verwenden:

- Ermitteln des besten Hosts, auf dem eine VM ausgeführt werden soll
- Empfehlungen zur Optimierung des Workloadausgleichs akzeptieren
- Ausführen von Berichten über die Workloaden in Ihrer Umgebung

Workload Balancing ermöglicht Ihnen nicht nur die Ausführung dieser grundlegenden Aufgaben, sondern ist auch eine leistungsstarke XenServer-Komponente, die die Workloads in Ihrer Umgebung optimiert. Zu den Funktionen, mit denen Sie Ihre Workloads optimieren können, gehören:

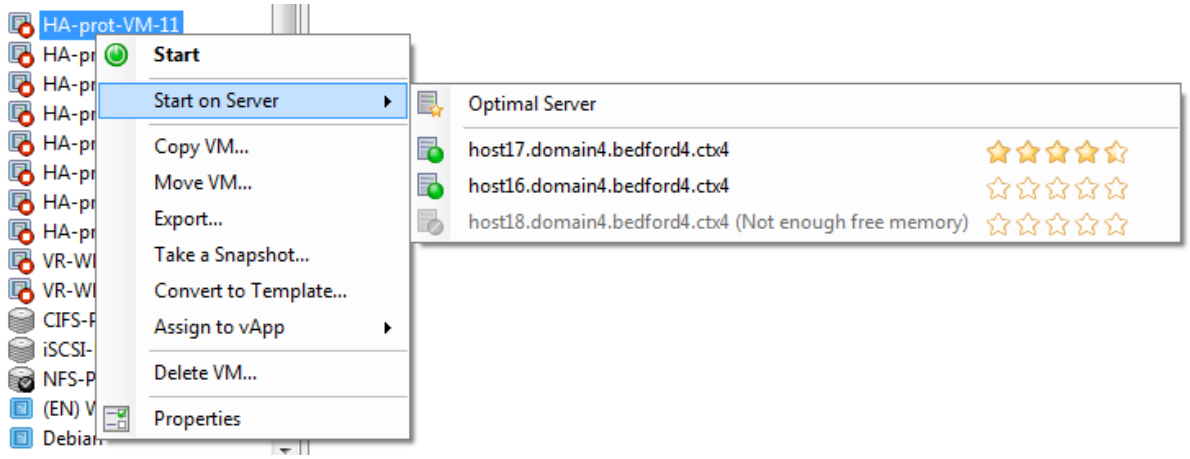
- Host-Energieverwaltung
- Änderungen im Optimierungsmodus planen
- Auswertungen ausführen
- Feinabstimmung der Kriterien, anhand derer Workload Balancing Optimierungsempfehlungen ausspricht.

Weitere Informationen zu diesen komplexeren Funktionen finden Sie unter Verwalten des Workloadausgleichs.

> **Hinweise:**
>
> - Workload Balancing ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.
> - Workload Balancing 8.3.0 ist mit XenServer 8 und Citrix Hypervisor 8.2 CU1 kompatibel.

Ermitteln Sie den besten Host, auf dem eine VM ausgeführt werden soll

Wenn Sie den Workload Balancing aktiviert haben und eine Offline-VM neu starten, empfiehlt XenCenter die optimalen Poolmitglieder zum Starten der VM. Die Empfehlungen werden auch als Sternebewertungen bezeichnet, da Sterne verwendet werden, um den besten Host anzuzeigen.



Wenn der Workload Balancing aktiviert ist, bietet XenCenter Sternbewertungen, um die optimalen Hosts für den Start einer VM anzuzeigen. Diese Bewertungen werden auch bereitgestellt:

- Wenn Sie die VM starten möchten, wenn sie ausgeschaltet ist
- Wenn Sie die VM starten möchten, wenn sie angehalten ist
- Wenn Sie die VM auf einen anderen Host migrieren möchten (Migrate- und Wartungsmodus)

Wenn Sie diese Funktionen mit aktiviertem Workload-Balancing verwenden, werden Hostempfehlungen neben dem Namen des physischen Hosts als Sternbewertungen angezeigt. Fünf leere Sterne stehen für die niedrigste Bewertung und somit für den am wenigsten optimalen Host. Wenn Sie eine VM nicht starten oder auf einen Host migrieren können, ist der Hostname im Menübefehl für eine Platzierungsfunktion abgeblendet. Der Grund, warum die VM nicht akzeptiert werden kann, wird daneben angezeigt.

Der Begriff *optimal* bezeichnet den physischen Host, der sich am besten für das Hosten Ihres Workloads eignet. Es gibt mehrere Faktoren, die der Workload Balancing verwendet, um zu bestimmen, welcher Host für einen Workload optimal ist:

- **Die Menge an Ressourcen, die auf jedem Host im Pool verfügbar**sind. Wenn ein Pool im Modus “Maximale Leistung”ausgeführt wird, versucht der Workload Balancing, die VMs über die Hosts hinweg auszugleichen, sodass alle VMs eine gute Leistung aufweisen. Wenn ein Pool im Modus “Maximale Dichte”ausgeführt wird, platziert der Workload Balancing VMs so dicht wie möglich auf Hosts und stellt gleichzeitig sicher, dass die VMs über ausreichende Ressourcen verfügen.
- **Der Optimierungsmodus, in dem der Pool ausgeführt wird (Maximale Leistung oder maximale Dichte)**. Wenn ein Pool im Modus “Maximale Leistung”ausgeführt wird, platziert der Workload Balancing VMs auf Hosts mit den meisten verfügbaren Ressourcen des Typs, den die VM benötigt. Wenn ein Pool im Modus “Maximale Dichte”ausgeführt wird, platziert der Workload Balancing VMs auf Hosts, auf denen bereits VMs ausgeführt werden. Dieser Ansatz stellt sicher, dass virtuelle Maschinen auf so wenigen Hosts wie möglich ausgeführt werden.

- **Die Menge und Art der Ressourcen, die die VM benötigt**. Nachdem der Workload Balancing eine VM für eine Weile überwacht hat, verwendet er die VM-Metriken, um Platzierungsempfehlungen entsprechend der Art der Ressourcen abzugeben, die die VM benötigt. Zum Beispiel könnte Workload Balancing einen Host mit weniger verfügbarer CPU, aber mehr verfügbarem Speicher auswählen, wenn die VM dies benötigt.

Im Allgemeinen funktioniert der Workload Balancing effektiver und bietet bessere, weniger häufige Optimierungsempfehlungen, wenn Sie VMs auf den empfohlenen Hosts starten. Um den Hostempfehlungen zu folgen, verwenden Sie eines der Platzierungs-Features, um den Host mit den meisten Sternen auszuwählen. Platzierungsempfehlungen können auch in Citrix Virtual Desktops-Umgebungen nützlich sein.

So starten Sie eine VM auf dem optimalen Host

1. Wählen Sie im Bereich Ressourcen von XenCenter die VM aus, die Sie starten möchten.
2. Wählen Sie im VM-MenüStart on Server und dann eine der folgenden Optionen aus:
    - **Optimaler Server**. Der optimale Server ist der physische Host, der sich am besten für die Ressourcenanforderungen der VM eignet, die Sie starten. Der Workload Balancing bestimmt den optimalen Server auf der Grundlage seiner historischen Aufzeichnungen von Leistungsmetriken und Ihrer Platzierungsstrategie. Der optimale Server ist der Host mit den meisten Sternen.
    - **Einer der Server mit Sternebewertungen**, die unter dem Befehl Optimaler Server aufgeführt sind. Fünf Sterne stehen für den am meisten empfohlenen (optimalen) Host und fünf leere Sterne stehen für den am wenigsten empfohlenen Host.

> **Tipp:**
>
> Sie können auch Auf Server starten auswählen, indem Sie im Bereich Ressourcen mit der rechten Maustaste auf die VM klicken, die Sie starten möchten.

So nehmen Sie eine VM auf dem optimalen Host wieder auf

1. Wählen Sie im Bereich Ressourcen von XenCenter die angehaltene VM aus, die Sie fortsetzen möchten.
2. Wählen Sie im VM-MenüResume on Server und dann eine der folgenden Optionen aus:
    - **Optimaler Server**. Der optimale Server ist der physische Host, der sich am besten für die Ressourcenanforderungen der VM eignet, die Sie starten. Der Workload Balancing bestimmt den optimalen Server auf der Grundlage seiner historischen Aufzeichnungen von

Leistungsmetriken und Ihrer Platzierungsstrategie. Der optimale Server ist der Host mit den meisten Sternen.

- **Einer der Server mit Sternebewertungen**, die unter dem Befehl Optimaler Server aufgeführt sind. Fünf Sterne stehen für den am meisten empfohlenen (optimalen) Host und fünf leere Sterne stehen für den am wenigsten empfohlenen Host.

> **Tipp:**
>
> Sie können auch Auf Server fortsetzen auswählen, indem Sie im Bereich Ressourcen mit der rechten Maustaste auf die angehaltene VM klicken.

Akzeptieren Sie Empfehlungen zur Optimierung des Workload

Nachdem der Workload Balancing für eine Weile ausgeführt wird, werden Empfehlungen zu Möglichkeiten zur Verbesserung der Umgebung abgegeben. Wenn Ihr Ziel beispielsweise darin besteht, die VM-Dichte auf Hosts zu verbessern, empfiehlt der Workload Balancing möglicherweise, dass Sie VMs auf einem Host konsolidieren. Wenn Sie nicht im automatisierten Modus arbeiten, können Sie diese Empfehlung entweder annehmen und anwenden oder ignorieren.

> **Wichtig:**
>
> Wenn der Workload Balancing eine Zeit lang ausgeführt wurde und Sie keine Empfehlungen für die optimale Platzierung erhalten, bewerten Sie Ihre Leistungsschwellenwerte. Diese Auswertung wird unter Verstehen beschrieben, wann der Workload Balancing Empfehlungen ausspricht. Es ist wichtig, den Workload-Balancing auf die richtigen Schwellenwerte für Ihre Umgebung festzulegen, da die Empfehlungen möglicherweise nicht angemessen sind.

Optimierungsempfehlungen basieren auf folgenden Kriterien:

- Die von Ihnen gewählte Platzierungsstrategie (d. h. den Optimierungsmodus).

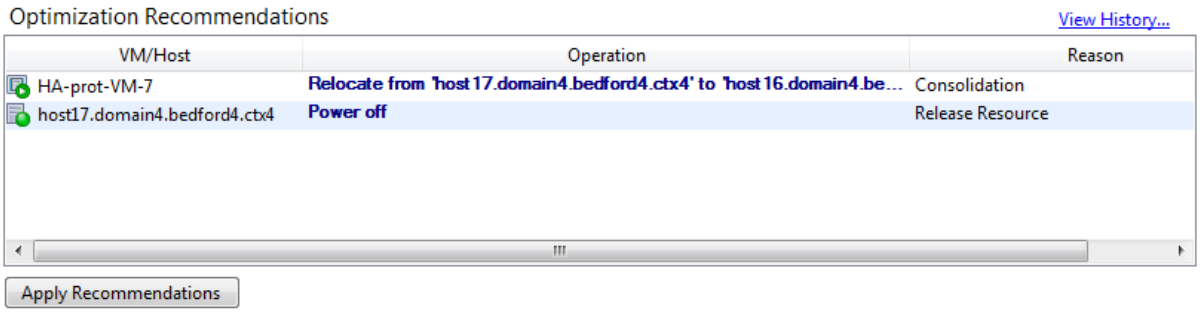
  Ermitteln Sie den Optimierungsmodus für einen Pool, indem Sie XenCenter verwenden, um den Pool auszuwählen. Suchen Sie im Abschnitt “Konfiguration”der Registerkarte “WLB”nach den Informationen.

- Leistungsmetriken für Ressourcen wie CPU-, Arbeitsspeicher-, Netzwerk- und Datenträgerauslastung eines physischen Hosts.

- Die Rolle des Hosts im Ressourcenpool.

  Bei der Festlegung von Platzierungsempfehlungen berücksichtigt Workload Balancing den Poolkoordinator für die Platzierung der virtuellen Maschinen nur, wenn kein anderer Host den Workload annehmen kann. Wenn ein Pool im Modus “Maximale Dichte”ausgeführt wird, berücksichtigt der Workload Balancing bei der Festlegung der Reihenfolge, in der Hosts mit VMs gefüllt werden sollen, als letzter den Poolkoordinator.

Optimierungsempfehlungen werden auf der Registerkarte **WLB-Optimierung** in XenCenter angezeigt.



Optimierungsempfehlungen enthalten die folgenden Informationen:

- Der Name der VM, die Workload Balancing empfiehlt, zu verlagern
- Der Host, auf dem sich die VM derzeit befindet
- Der Host Workload Balancing empfiehlt als neuer Standort.

Die Optimierungsempfehlungen zeigen auch den Grund an, warum Workload Balancing das Verschieben der VM empfiehlt. In der Empfehlung wird beispielsweise "CPU"angezeigt, um die CPU-Auslastung zu verbessern. Wenn die Energieverwaltung für den Workload Balancing aktiviert ist, zeigt der Workload Balancing auch Optimierungsempfehlungen für Hosts an, die ein- oder ausgeschaltet werden sollten. Diese Empfehlungen beziehen sich insbesondere auf Konsolidierungen.

Sie können auf **Empfehlungen anwenden**klicken, um alle in der Liste Optimierungsempfehlungen aufgeführten Vorgänge auszuführen.

So akzeptieren Sie eine Optimierungsempfehlung

1. Wählen Sie im Bereich Ressourcen von XenCenter den Ressourcenpool aus, für den Sie Empfehlungen anzeigen möchten.
2. Klicken Sie auf die Registerkarte WLB. Wenn es empfohlene Optimierungen für VMs im ausgewählten Ressourcenpool gibt, werden diese auf der Registerkarte WLB im Abschnitt Optimierungsempfehlungen angezeigt.
3. Um die Empfehlungen anzunehmen, klicken Sie auf Empfehlungen anwenden. XenServer beginnt mit der Ausführung aller Vorgänge, die in der Spalte Operationen des Abschnitts Optimierungsempfehlungen aufgeführt sind.

   Nachdem Sie auf Empfehlungen anwenden geklickt haben, zeigt XenCenter automatisch die Registerkarte Protokolle an, damit Sie den Fortschritt der VM-Migration verfolgen können.

Verstehen Sie die Empfehlungen für den Workload Balancing

Wenn Sie Workload Balancing und XenServer High Availability im selben Pool aktiviert haben, ist es hilfreich zu verstehen, wie die beiden Funktionen interagieren. Der Workload-Balancing ist so konzipiert, dass die hohe Verfügbarkeit nicht beeinträchtigt wird. Wenn ein Konflikt zwischen einer Workload Balancing-Empfehlung und einer Einstellung für Hochverfügbarkeit besteht, hat die Einstellung **Hochverfügbarkeit** immer Vorrang. In der Praxis bedeutet dieser Vorrang:

- Wenn der Versuch, eine VM auf einem Host zu starten, gegen den Hochverfügbarkeitsplan verstößt, erhalten Sie beim Workload Balancing keine Sternebewertungen.
- Der Workload Balancing schaltet nicht automatisch Hosts aus, die über die im Feld Zulässige Fehler im Dialogfeld **HA konfigurieren** angegebene Anzahl hinausgehen.
  - Der Workload Balancing gibt jedoch möglicherweise immer noch Empfehlungen zum Ausschalten von mehr Hosts ab, als die Anzahl der Hostausfälle toleriert werden muss. (Workload Balancing empfiehlt beispielsweise weiterhin, zwei Hosts auszuschalten, wenn Hochverfügbarkeit nur so konfiguriert ist, dass ein Hostausfall toleriert wird.) Wenn Sie jedoch versuchen, die Empfehlung anzuwenden, zeigt XenCenter möglicherweise eine Fehlermeldung an, dass Hochverfügbarkeit nicht mehr garantiert ist.
  - Wenn der Workload Balancing im automatisierten Modus ausgeführt wird und die Energieverwaltung aktiviert ist, werden Empfehlungen ignoriert, die die Anzahl der tolerierten Hostausfälle überschreiten. In dieser Situation zeigt das Workload Balancing-Protokoll eine Meldung an, dass die Energieverwaltungsempfehlung nicht angewendet wurde, da Hochverfügbarkeit aktiviert ist.

Generieren von Workloadberichten

Der Workload Balancing erfasst Leistungsdaten und kann diese Daten verwenden, um Berichte, sogenannte Workload-Berichte, über Ihre virtualisierte Umgebung zu erstellen, einschließlich Berichten über Hosts und VMs. Die Workload Balancing-Berichte können Ihnen helfen, die Kapazitätsplanung durchzuführen, den Status des virtuellen Servers zu bestimmen und zu bewerten, wie effektiv Ihre konfigurierten Schwellenwerte sind.

Sie können den Poolintegritätsbericht verwenden, um zu bewerten, wie effektiv Ihre Optimierungsschwellenwerte sind. Während der Workload Balancing Standardschwelleneinstellungen bereitstellt, müssen Sie diese Standardeinstellungen möglicherweise anpassen, damit sie einen Mehrwert in Ihrer Umgebung bieten. Wenn Sie die Optimierungsschwellenwerte nicht auf die richtige Ebene für Ihre Umgebung angepasst haben, sind die Empfehlungen für den Workload Balancing möglicherweise nicht für Ihre Umgebung geeignet.

Um Berichte auszuführen, müssen Sie Workload Balancing nicht konfigurieren, um Platzierungsempfehlungen abzugeben oder VMs zu verschieben. Sie müssen jedoch die Komponente Workload Balancing konfigurieren. Im Idealfall müssen Sie kritische Schwellenwerte auf Werte festlegen, die den Punkt widerspiegeln, an dem sich die Leistung der Hosts in Ihrem Pool verschlechtert. Im Idealfall führt der Pool Workload Balancing für einige Stunden oder lange genug aus, um die in den Berichten anzuzeigenden Daten zu generieren.

Mit dem Workload Balancing können Sie Berichte zu drei Objekttypen erstellen: physische Hosts, Ressourcenpools und VMs. Auf hoher Ebene bietet Workload Balancing zwei Arten von Berichten:

- Historische Berichte, die Informationen nach Datum anzeigen
- "Roll Up"-Berichte, die einen zusammenfassenden Überblick über einen Bereich bieten
- Berichte zu Überwachungszwecken, sodass Sie beispielsweise ermitteln können, wie oft eine VM verschoben wurde
- Chargeback-Bericht, der die VM-Nutzung aufzeigt und Ihnen dabei helfen kann, Kosten zu messen und zuzuweisen

Generieren eines Workload Balancing-Berichts

1. Wählen Sie in XenCenter im Menü **Pool** die Option **Workload-Berichte anzeigen**aus.

   Sie können den Bildschirm **Workload Reports** auch von der Registerkarte **WLB** aus aufrufen, indem Sie auf die Schaltfläche **Berichte** klicken.

2. Wählen Sie im Bildschirm **Workload-Berichte** im Bereich **Berichte** einen Bericht aus.
3. Wählen Sie das **Startdatum** und das **Enddatum** für den Berichtszeitraum. Je nachdem, welchen Bericht Sie auswählen, müssen Sie möglicherweise einen Host in der **Hostliste** angeben.
4. Klicken Sie auf **Bericht ausführen**. Der Bericht wird im Berichtsfenster angezeigt. Informationen zur Bedeutung der Berichte finden Sie im Workload Balancing-Berichts-Glossar.

Navigieren in einem Workload Balancing-Bericht

Nachdem Sie einen Bericht generiert haben, können Sie die Symbolleistenschaltflächen im Bericht verwenden, um zu navigieren und bestimmte Aufgaben auszuführen. Um den Namen einer Werkzeugleisten-Schaltfläche anzuzeigen, halten Sie die Maus über das Symbol der Werkzeugleiste.

Werkzeugleisten-	Beschreibung
	Mit**Document Map** können Sie eine Dokumentzuordnung anzeigen, mit der Sie durch lange Berichte navigieren können.
	Mit**Seite vorwärts/rückwärts** können Sie im Bericht eine Seite vor oder zurück bewegen.
	**Zurück zum übergeordneten Bericht** ermöglicht es Ihnen, zum übergeordneten Bericht zurückzukehren, wenn Sie mit Drill-Through-Berichten arbeiten. **Hinweis:** Diese Schaltfläche ist nur in Drill-Through-Berichten verfügbar, z. B. im Poolintegritätsbericht.
	**Rendering beenden** bricht die Berichtsgenerierung ab.
	Mit**Drucken** können Sie einen Bericht drucken und allgemeine Druckoptionen festlegen. Zu diesen Optionen gehören: der Drucker, die Anzahl der Seiten und die Anzahl der Kopien.
	Mit**Layout drucken** können Sie eine Vorschau des Berichts anzeigen, bevor Sie ihn drucken. Um das Drucklayout zu beenden, klicken Sie erneut auf die Schaltfläche **Drucklayout** .
	Mit**Seiteneinrichtung** können Sie Druckoptionen wie Papierformat, Seitenausrichtung und Ränder festlegen.
	**Exportieren** ermöglicht es Ihnen, den Bericht als Acrobat-Datei (.PDF) oder als Excel-Datei mit der.XLS-Erweiterung zu exportieren.
	Mit**Suchen** können Sie in einem Bericht nach einem Wort suchen, z. B. nach dem Namen einer VM.

Exportieren eines Workload Balancing-Berichts

Sie können einen Bericht entweder in den Formaten Microsoft Excel oder Adobe Acrobat (PDF) exportieren.

1. Nachdem Sie den Bericht erstellt haben, klicken Sie auf die folgende Schaltfläche Exportieren:
2. Wählen Sie im Schaltflächenmenü "Exportieren"eines der folgenden Elemente aus:
    - [Excel]
    - Acrobat (PDF) -Datei

> **Hinweis:**
>
> Je nachdem, welches Exportformat Sie auswählen, enthält der Bericht unterschiedliche Datenmengen. In Excel exportierte Berichte enthalten alle Daten, die für Berichte verfügbar sind, einschließlich "Drilldown"-Daten. In PDF exportierte und in XenCenter angezeigte Berichte enthalten nur die Daten, die Sie beim Erstellen des Berichts ausgewählt haben.

Glossar zum Workload Balancing-Bericht

Dieser Abschnitt enthält Informationen zu den folgenden Workload Balancing-Berichten:

- Analyse der Chargeback-Auslastung
- Hostintegritätsverlauf
- Leistungsverlauf der Pooloptimierung
- Poolauditliste
- Poolintegrität
- Poolintegritätsverlauf
- Pooloptimierungsverlauf
- VM-Bewegungsverlauf
- VM-Leistungsverlauf

Analyse der Chargeback-Auslastung

Sie können den Bericht zur Analyse der Chargeback-Auslastung ("Chargeback-Bericht") verwenden, um zu ermitteln, wie viel einer Ressource eine bestimmte Abteilung in Ihrer Organisation verwendet hat. Insbesondere enthält der Bericht Informationen zu allen VMs in Ihrem Pool, einschließlich ihrer Verfügbarkeit und Ressourcennutzung. Da dieser Bericht die VM-Betriebszeit anzeigt, kann er Ihnen helfen, die Einhaltung und Verfügbarkeit von Service Level Agreements nachzuweisen.

Der Chargeback-Bericht kann Ihnen helfen, eine einfache Rückbuchungslösung zu implementieren und die Abrechnung zu vereinfachen. Um Kunden eine bestimmte Ressource in Rechnung zu stellen,

erstellen Sie den Bericht, speichern Sie ihn als Excel und bearbeiten Sie die Tabelle so, dass sie Ihren Preis pro Einheit enthält. Alternativ können Sie die Excel-Daten in Ihr Abrechnungssystem importieren.

Wenn Sie internen oder externen Kunden die VM-Nutzung in Rechnung stellen möchten, sollten Sie erwägen, Abteilungs- oder Kundennamen in Ihre VM-Namenskonventionen aufzunehmen. Diese Vorgehensweise erleichtert das Lesen von Rückbuchungsberichten.

Die Ressourcenberichterstattung im Chargeback-Bericht basiert manchmal auf der Zuweisung physischer Ressourcen zu einzelnen VMs.

Die durchschnittlichen Speicherdaten in diesem Bericht basieren auf der Menge an Arbeitsspeicher, die derzeit der VM zugewiesen ist. XenServer ermöglicht Ihnen eine feste Speicherzuweisung oder eine sich automatisch anpassende Speicherzuweisung (Dynamic Memory Control).

Der Chargeback-Bericht enthält die folgenden Datenspalten:

- **VM-Name**. Der Name der VM, für die die Daten in den Spalten in dieser Zeile gelten.
- **VM-Betriebszeit**. Die Anzahl der Minuten, in denen die VM eingeschaltet wurde (oder insbesondere in XenCenter mit einem grünen Symbol daneben angezeigt wird).
- **vCPU-Zuweisung**. Die Anzahl der auf der VM konfigurierten virtuellen CPUs. Jede virtuelle CPU erhält den gleichen Anteil der physischen CPUs auf dem Host. Stellen Sie sich beispielsweise den Fall vor, dass Sie acht virtuelle CPUs auf einem Host konfiguriert haben, der zwei physische CPUs enthält. Wenn die Spalte **vCPU-Zuweisung** "1"enthält, entspricht dieser Wert 2/16 der gesamten Verarbeitungsleistung auf dem Host.
- **Minimale CPU-Auslastung (%)**. Der niedrigste aufgezeichnete Wert für die virtuelle CPU-Auslastung im Berichtszeitraum. Dieser Wert wird als Prozentsatz der vCPU-Kapazität der VM ausgedrückt. Die Kapazität basiert auf der Anzahl der vCPUs, die der VM zugewiesen sind. Wenn Sie beispielsweise einer VM eine vCPU zugewiesen haben, stellt die **minimale CPU-Auslastung** den niedrigsten Prozentsatz der aufgezeichneten vCPU-Auslastung dar. Wenn Sie der VM zwei vCPUs zugewiesen haben, ist der Wert die niedrigste Auslastung der kombinierten Kapazität beider vCPUs in Prozent.

  Letztlich stellt der Prozentsatz der CPU-Auslastung die niedrigste aufgezeichnete Workload dar, die die virtuelle CPU verarbeitet hat. Wenn Sie beispielsweise einer VM eine vCPU zuweisen und die pCPU auf dem Host 2,4 GHz beträgt, werden 0,3 GHz der VM zugewiesen. Wenn die **minimale CPU-Auslastung** für die VM 20% betrug, betrug die niedrigste Auslastung der CPU des physischen Hosts im Berichtszeitraum durch die VM 60 MHz.
- **Maximale CPU-Auslastung (%)**. Der höchste Prozentsatz der virtuellen CPU-Kapazität der VM, den die VM im Berichtszeitraum verbraucht hat. Die verbrauchte CPU-Kapazität ist ein Prozentsatz der virtuellen CPU-Kapazität, die Sie der VM zugewiesen haben. Wenn Sie der VM beispielsweise eine vCPU zugewiesen haben, stellt die Maximale CPU-Auslastung den höchsten

aufgezeichneten Prozentsatz der vCPU-Auslastung während des Berichtszeitraums dar. Wenn Sie der VM zwei virtuelle CPUs zugewiesen haben, stellt der Wert in dieser Spalte die höchste Auslastung aus der kombinierten Kapazität beider virtueller CPUs dar.

- **Durchschnittliche CPU-Auslastung (%)**. Die durchschnittliche Menge, ausgedrückt als Prozentsatz, der virtuellen CPU-Kapazität der VM, die im Berichtszeitraum verwendet wurde. Die CPU-Kapazität ist die virtuelle CPU-Kapazität, die Sie der VM zugewiesen haben. Wenn Sie der VM zwei virtuelle CPUs zugewiesen haben, stellt der Wert in dieser Spalte die durchschnittliche Auslastung aus der kombinierten Kapazität beider virtueller CPUs dar.
- **Gesamte Speicherzuweisung (GB)**. Der Speicherplatz, der derzeit der VM zum Zeitpunkt der Ausführung des Berichts zugewiesen ist. Dieser Speicherplatz ist häufig, sofern Sie ihn nicht geändert haben, der Speicherplatz, den Sie der VM bei der Erstellung zugewiesen haben.
- **Virtuelle NIC-Zuordnung**. Die Anzahl der virtuellen Schnittstellen (VIFs), die der VM zugewiesen sind.
- **Aktueller minimaler dynamischer Speicher (MB)**.
  - **Feste Speicherzuweisung**. Wenn Sie einer VM eine feste Menge an Arbeitsspeicher zugewiesen haben (z. B. 1.024 MB), wird dieselbe Speichermenge in den folgenden Spalten angezeigt: Aktueller minimaler dynamischer Speicher (MB), Aktueller maximaler dynamischer Speicher (MB), Aktuell zugewiesener Speicher (MB) und Durchschnittlich zugewiesener Speicher (MB).
  - **Dynamische Speicherzuweisung**. Wenn Sie XenServer für die Verwendung von Dynamic Memory Control konfiguriert haben, wird die im Bereich angegebene Mindestspeichermenge in dieser Spalte angezeigt. Wenn der Bereich 1.024 MB als Mindestspeicher und 2.048 MB als maximalen Speicher umfasst, werden in der Spalte "**Aktueller minimaler dynamischer Speicher (MB)** "1.024 MB angezeigt.
- **Aktueller maximaler dynamischer Speicher (MB)**.
  - **Dynamische Speicherzuweisung**. Wenn XenServer den Arbeitsspeicher einer VM automatisch anhand eines Bereichs anpasst, wird die in dem Bereich angegebene maximale Speichermenge in dieser Spalte angezeigt. Wenn die Speicherbereichswerte beispielsweise mindestens 1.024 MB und maximal 2.048 MB betragen, werden 2.048 MB in der Spalte **Current Maximum Dynamic Memory (MB)** angezeigt.
  - **Feste Speicherzuweisung**. Wenn Sie einer VM eine feste Menge an Arbeitsspeicher zuweisen (z. B. 1,024 MB), wird dieselbe Menge an Arbeitsspeicher in den folgenden Spalten angezeigt: Aktueller minimaler dynamischer Speicher (MB), Aktueller maximaler dynamischer Speicher (MB), Aktueller zugewiesener Speicher (MB) und Durchschnittlicher zugewiesener Speicher (MB).
- **Aktuell zugewiesener Speicher (MB)**.

  - **Dynamische Speicherzuweisung**. Wenn Dynamic Memory Control konfiguriert ist, gibt dieser Wert die Speichermenge an, die XenServer der VM zuweist, wenn der Bericht ausgeführt wird.
  - **Feste Speicherzuweisung**. Wenn Sie einer VM eine feste Menge an Arbeitsspeicher zuweisen (z. B. 1,024 MB), wird dieselbe Menge an Arbeitsspeicher in den folgenden Spalten angezeigt: Aktueller minimaler dynamischer Speicher (MB), Aktueller maximaler dynamischer Speicher (MB), Aktueller zugewiesener Speicher (MB) und Durchschnittlicher zugewiesener Speicher (MB).

> **Hinweis:**
>
> Wenn Sie die Speicherzuweisung der VM unmittelbar vor dem Ausführen dieses Berichts ändern, spiegelt der in dieser Spalte angegebene Wert die neue Speicherzuweisung wider, die Sie konfiguriert haben.

- **Durchschnittlicher zugewiesener Speicher (MB)**.
  - **Dynamische Speicherzuweisung**. Wenn Dynamic Memory Control konfiguriert ist, gibt dieser Wert die durchschnittliche Speichermenge an, die XenServer der VM im Berichtszeitraum zugewiesen hat.
  - **Feste Speicherzuweisung**. Wenn Sie einer VM eine feste Menge an Arbeitsspeicher zuweisen (z. B. 1,024 MB), wird dieselbe Menge an Arbeitsspeicher in den folgenden Spalten angezeigt: Aktueller minimaler dynamischer Speicher (MB), Aktueller maximaler dynamischer Speicher (MB), Aktueller zugewiesener Speicher (MB) und Durchschnittlicher zugewiesener Speicher (MB).

> **Hinweis:**
>
> Wenn Sie die Speicherzuweisung der VM unmittelbar vor dem Ausführen dieses Berichts ändern, ändert sich der Wert in dieser Spalte möglicherweise nicht von dem, was zuvor angezeigt wurde. Der Wert in dieser Spalte spiegelt den Durchschnitt über den Zeitraum wider.

- **Durchschnittliche Netzwerk-Lesevorgänge (BPS)**. Die durchschnittliche Datenmenge (in Bit pro Sekunde), die die VM im Berichtszeitraum empfangen hat.
- **Durchschnittliche Netzwerk-Schreibvorgänge (BPS)**. Die durchschnittliche Datenmenge (in Bit pro Sekunde), die die VM im Berichtszeitraum gesendet hat.
- **Durchschnittliche Netzwerkauslastung (BPS)**. Die kombinierte Summe (in Bit pro Sekunde) der durchschnittlichen Netzwerk-Lesevorgänge und der durchschnittlichen Netzwerk-Schreibvorgänge. Wenn eine VM im Berichtszeitraum durchschnittlich 1.027 Bit/s sendet und im Berichtszeitraum durchschnittlich 23.831 Bps empfängt, ist die durchschnittliche Netzwerknutzung die kombinierte Summe dieser Werte: 24.858 bps.

- **Gesamtnetzwerknutzung (BPS)**. Die Summe aller Lese- und Schreibtransaktionen im Netzwerk in Bit pro Sekunde im Berichtszeitraum.

Hostintegritätsverlauf

In diesem Bericht wird die Leistung von Ressourcen (CPU, Arbeitsspeicher, Netzwerk-Lesezugriffe und Netzwerkschreibvorgänge) auf einem bestimmten Host in Bezug auf Schwellenwerte angezeigt.

Die farbigen Linien (rot, grün, gelb) stellen Ihre Schwellenwerte dar. Sie können diesen Bericht zusammen mit dem Bericht "Poolintegrität"für einen Host verwenden, um zu ermitteln, wie sich die Leistung des Hosts auf die allgemeine Poolintegrität auswirken kann. Wenn Sie die Leistungsschwellenwerte bearbeiten, können Sie diesen Bericht verwenden, um einen Einblick in die Host-Leistung zu erhalten.

Sie können die Ressourcenauslastung als Tages- oder Stundendurchschnitt anzeigen. Mit dem Stundendurchschnitt können Sie die durchschnittlich verkehrsreichsten Stunden des Tages für den Zeitraum anzeigen.

Um Berichtsdaten anzuzeigen, die nach Stunde gruppiert sind, erweitern Sie unter **Host-Integritätsverlauf** die Option **Klicken, um Berichtsdaten für den Zeitraum nach Haus gruppiert anzuzeigen**.

Der Workload Balancing zeigt den Durchschnitt für jede Stunde für den von Ihnen festgelegten Zeitraum an. Der Datenpunkt basiert auf einem Nutzungsdurchschnitt für diese Stunde für alle Tage im Zeitraum. Beispiel: In einem Bericht vom 1. Mai 2009 bis 15. Mai 2009 stellt der Datenpunkt "Durchschnittliche CPU-Auslastung"die Ressourcenauslastung aller 15 Tage um 12:00 Uhr dar. Diese Informationen werden als Durchschnitt kombiniert. Wenn die CPU-Auslastung am 1. Mai um 12 Uhr 82%, am 2. Mai um 12 Uhr 88% und an allen anderen Tagen 75% betrug, beträgt der angezeigte Durchschnitt für 12 Uhr 76,3%.

> **Hinweis:**
>
> Der Workload Balancing glättet Spitzen und Spitzen, sodass die Daten nicht künstlich hoch erscheinen.

Leistungsverlauf der Pooloptimierung

Der Bericht zur Optimierungsleistung zeigt Optimierungsereignisse anhand der durchschnittlichen Ressourcenauslastung dieses Pools an. Bei diesen Ereignissen haben Sie einen Ressourcenpool optimiert. Insbesondere zeigt es die Ressourcennutzung für CPU, Speicher, Netzwerk-Lesevorgänge und Netzwerk-Schreibvorgänge an.

Die gepunktete Linie stellt die durchschnittliche Nutzung des Pools über den von Ihnen ausgewählten Zeitraum dar. Ein blauer Balken zeigt den Tag an, an dem Sie den Pool optimiert haben.

Mithilfe dieses Berichts können Sie feststellen, ob der Workload Balancing in Ihrer Umgebung erfolgreich funktioniert. Sie können diesen Bericht verwenden, um zu sehen, was zu Optimierungsereignissen geführt hat (d. h. die Ressourcennutzung vor der vom Workload Balancing empfohlenen Optimierung).

Dieser Bericht zeigt die durchschnittliche Ressourcennutzung für den Tag an. Es zeigt nicht die Spitzenauslastung an, z. B. wenn das System belastet ist. Sie können diesen Bericht auch verwenden, um zu sehen, wie sich ein Ressourcenpool entwickelt, wenn der Workload Balancing keine Optimierungsempfehlungen ausspricht.

Im Allgemeinen nimmt der Ressourcenverbrauch nach einem Optimierungsereignis ab oder bleibt konstant. Wenn nach der Optimierung keine verbesserte Ressourcennutzung angezeigt wird, sollten Sie Schwellenwerte neu justieren. Überlegen Sie außerdem, ob der Ressourcenpool zu viele VMs enthält und ob Sie in dem von Ihnen angegebenen Zeitraum neue VMs hinzugefügt oder entfernt haben.

Poolauditliste

In diesem Bericht wird der Inhalt des XenServer-Auditprotokolls angezeigt. Das Auditprotokoll ist eine XenServer-Funktion, mit der Versuche protokolliert werden, nicht autorisierte Aktionen auszuführen und autorisierte Aktionen auszuwählen. Zu diesen Aktionen gehören:

- Importieren und exportieren
- Host- und Poolbackups
- Zugriff auf Gäste- und Host-Konsole.

Der Bericht enthält aussagekräftigere Informationen, wenn Sie XenServer-Administratoren mithilfe der RBAC-Funktion eigene Benutzerkonten mit unterschiedlichen Rollen zuweisen.

> **Wichtig:**
>
> Um den Überwachungsprotokollbericht ausführen zu können, müssen Sie die Funktion Überwachungsprotokollierung aktivieren. Standardmäßig ist das Überwachungsprotokoll in der virtuellen Appliance “Workload Balancing”immer aktiviert.

Mit der erweiterten Poolauditlistenfunktion können Sie die Granularität des Auditprotokollberichts angeben. Sie können die Auditlistenprotokolle auch nach bestimmten Benutzern, Objekten und nach Zeit durchsuchen und filtern. Die Pool-Audit-Trail-Granularität ist standardmäßig auf Minimum gesetzt. Diese Option erfasst eine begrenzte Datenmenge für bestimmte Benutzer und Objekttypen. Sie können die Einstellung jederzeit basierend auf der Detailebene ändern, die Sie in Ihrem Bericht benötigen. Legen Sie beispielsweise die Granularität auf Mittel fest, um einen benutzerfreundlichen Bericht über das Überwachungsprotokoll zu erhalten. Wenn Sie einen detaillierten Bericht benötigen, setzen Sie die Option auf Maximum.

Der Poolauditlistenbericht enthält die folgenden Informationen:

- Zeit. Der Zeitpunkt, zu dem XenServer die Aktion des Benutzers aufgezeichnet hat.
- Nutzername. Der Name der Person, die die Sitzung erstellt hat, in der die Aktion ausgeführt wurde. Manchmal kann dieser Wert die Benutzer-ID sein
- Event-Objekt. Das Objekt, das Gegenstand der Aktion war (z. B. eine VM).
- Event-Aktion. Die Aktion, die aufgetreten ist. Definitionen dieser Aktionen finden Sie unter Namen von Überwachungsprotokollereignissen.
- Zugriff. Ob der Benutzer die Berechtigung hatte, die Aktion auszuführen.
- Objektname. Der Name des Objekts (z. B. der Name der VM).
- Objekt UUID. Die UUID des Objekts (z. B. die UUID der VM).
- Erfolgreich. Diese Informationen geben den Status der Aktion an (d. h. ob sie erfolgreich war).

Ereignisnamen des Prüfprotokolls Der Auditprotokollbericht protokolliert XenServer-Ereignisse, Ereignisobjekte und Aktionen, einschließlich Import/Export, Host- und Pool-Backups sowie Zugriff auf Gast- und Hostkonsolen. In der folgenden Tabelle werden einige der typischen Ereignisse definiert, die häufig im XenServer Audit Log and Pool Audit Trail-Bericht auftreten. Die Tabelle gibt auch die Granularität dieser Ereignisse an.

Im Poolauditlistenbericht gelten die in der Spalte `Event Action` aufgeführten Ereignisse für einen Pool, eine VM oder einen Host. Um zu bestimmen, wofür die Ereignisse gelten, lesen Sie die Spalten `Event Object` und `Object Name` im Bericht. Weitere Ereignisdefinitionen finden Sie im Abschnitt Ereignisse der XenServer Management API.

Poolauditliste - Granularität	Event-Aktion	Benutzer-Aktion
Minimum	`pool.join`	Der Host wurde angewiesen, einem neuen Pool beizutreten
Minimum	`pool.join_force`	Der Host wurde angewiesen (gezwungen), einem Pool beizutreten
Medium	`SR.destroy`	Das Speicherrepository zerstört
Medium	`SR.create`	Erstellt ein Speicherrepository
Medium	`VDI.snapshot`	Nahm einen schreibgeschützten Snapshot des VDI und gab einen Verweis auf den Snapshot zurück

Poolauditliste - Granularität	Event-Aktion	Benutzer-Aktion
Medium	VDI.clone	Exakte Kopie des VDI erstellt und einen Verweis auf den neuen Datenträger zurückgegeben
Medium	VIF.plug	Die angegebene VIF wurde im laufenden Betrieb angeschlossen und dynamisch an die laufende VM angehängt
Medium	VIF.unplug	Die angegebene VIF wurde im laufenden Betrieb getrennt und dynamisch von der laufenden VM getrennt
Maximum	auth.get_subject_identifier	Der externe Verzeichnisdienst wurde abgefragt, um die Betreff-ID als Zeichenfolge aus dem für Menschen lesbaren Antragstellernamen abzurufen
Maximum	task.cancel	Angefordert, dass eine Aufgabe abgebrochen wird
Maximum	VBD.insert	Neue Medien in das Gerät eingefügt
Maximum	VIF.get_by_uuid	Erhielt einen Verweis auf die VIF-Instanz mit der angegebenen UUID
Maximum	VDI.get_sharable	Das gemeinsam nutzbare Feld des angegebenen VDI erhalten
Maximum	SR.get_all	Gibt eine Liste aller SRs zurück, die dem System bekannt sind
Maximum	pool.create_new_blob	Erstellt einen Platzhalter für ein benanntes binäres Datenelement, das mit diesem Pool verknüpft ist
Maximum	host.send_debug_keys	Die angegebene Zeichenfolge als Debugging-Schlüssel in Xen injiziert

Poolauditliste - Granularität	Event-Aktion	Benutzer-Aktion
Maximum	`VM.get_boot_record`	Es wurde ein Datensatz zurückgegeben, der den dynamischen Status der virtuellen Maschine beschreibt, beim Booten der VM initialisiert und aktualisiert, um Änderungen der Laufzeitkonfiguration widerzuspiegeln, z. B.

Poolintegrität

Der Bericht "Poolintegrität"zeigt den Prozentsatz der Zeit an, die ein Ressourcenpool und seine Hosts in vier verschiedenen Schwellenwertbereichen verbracht haben: Kritisch, Hoch, Mittel und Niedrig. Sie können den Poolintegritätsbericht verwenden, um die Wirksamkeit Ihrer Leistungsschwellenwerte zu bewerten.

Einige Punkte zur Interpretation dieses Berichts:

- Die Ressourcenauslastung im mittleren Schwellenwert (blau) ist unabhängig von der gewählten Platzierungsstrategie die optimale Ressourcenauslastung. Ebenso zeigt der blaue Abschnitt im Tortendiagramm an, wie lange der Host Ressourcen optimal genutzt hat.
- Die Ressourcenauslastung im Durchschnitt niedrigen Schwellenwert Prozent (grün) ist nicht unbedingt positiv. Ob eine geringe Ressourcenauslastung positiv ist, hängt von Ihrer Platzierungsstrategie ab. Wenn Ihre Platzierungsstrategie "Maximale Dichte"lautet und die Ressourcennutzung grün ist, entspricht der Workload Balancing möglicherweise nicht der maximalen Anzahl von VMs auf diesem Host oder Pool. Wenn dies der Fall ist, passen Sie die Performance-Schwellenwerte an, bis der größte Teil der Ressourcenauslastung in den Schwellenwert "Mittelwert"(blau) fällt.
- Die Ressourcenauslastung in Prozent des durchschnittlichen kritischen Schwellenwerts (rot) gibt an, wie lange die durchschnittliche Ressourcenauslastung den kritischen Schwellenwert erreicht oder überschritten hat.

Wenn Sie auf ein Kreisdiagramm für die Ressourcennutzung eines Hosts doppelklicken, zeigt XenCenter den Bericht "Hostintegritätsverlauf"für diese Ressource auf diesem Host an. Wenn Sie in der Symbolleiste auf **Zurück zum übergeordneten Bericht** klicken, gelangen Sie zum Bericht über den Verlauf des Po

Wenn Sie feststellen, dass die meisten Berichtsergebnisse nicht im Bereich Durchschnittlicher mittlerer Schwellenwert liegen, passen Sie den kritischen Schwellenwert für diesen Pool an. Während der Workload Balancing Standardschwellenwerte bereitstellt, sind diese Standardeinstellungen nicht in allen Umgebungen wirksam. Wenn Sie die Schwellenwerte nicht auf die richtige Ebene für Ihre Umgebung angepasst haben, sind die Empfehlungen zur Optimierung und Platzierung des Workloadausgleichs möglicherweise nicht geeignet. Weitere Informationen finden Sie unter Ändern der kritischen Schwellenwerte.

Poolintegritätsverlauf

Dieser Bericht enthält ein Liniendiagramm der Ressourcenauslastung auf allen physischen Hosts in einem Pool im Zeitverlauf. Sie können den Trend der Ressourcennutzung erkennen - wenn sie im Verhältnis zu Ihren Schwellenwerten (Kritisch, Hoch, Mittel und Niedrig) tendenziell zunimmt. Sie können die Effektivität Ihrer Leistungsschwellen bewerten, indem Sie Trends der Datenpunkte in diesem Bericht überwachen.

Der Workload Balancing extrapoliert die Schwellenwertbereiche von den Werten, die Sie für die kritischen Schwellenwerte festgelegt haben, als Sie den Pool mit dem Workload Balancing verbunden haben. Obwohl er dem Bericht "Poolintegrität"ähnelt, zeigt der Bericht "Poolintegritätsverlauf" die durchschnittliche Auslastung einer Ressource an einem bestimmten Datum an. Anstelle der Gesamtzeit, die die Ressource in einem Schwellenwert verbracht hat.

Mit Ausnahme des Diagramms "Durchschnittlich freier Speicher"liegen die Datenpunkte nie über der kritischen Schwellenwertlinie (rot). Für das Diagramm "Durchschnittlich freier Speicher"liegen die Datenpunkte nie im Durchschnitt *unterhalb* der kritischen Schwellenwertlinie (die sich am unteren Rand des Diagramms befindet). Da dieses Diagramm *freien* Speicher anzeigt, ist der kritische Schwellenwert im Gegensatz zu den anderen Ressourcen ein niedriger Wert.

Einige Punkte zur Interpretation dieses Berichts:

- Wenn sich die Linie für die durchschnittliche Nutzung im Diagramm dem durchschnittlichen mittleren Schwellenwert (blau) nähert, zeigt dies an, dass die Ressourcenauslastung des Pools optimal ist. Diese Angabe ist unabhängig von der konfigurierten Platzierungsstrategie.
- Die Ressourcenauslastung, die sich dem durchschnittlichen niedrigen Schwellenwert (grün) nähert, ist nicht unbedingt positiv Ob eine geringe Ressourcenauslastung positiv ist, hängt von Ihrer Platzierungsstrategie ab. In dem Fall wo:
  - Ihre Platzierungsstrategie ist Maximale Dichte
  - An den meisten Tagen befindet sich die Zeile für die durchschnittliche Nutzung an oder unter der grünen Linie. Durch den
    Workload Balancing werden VMs möglicherweise nicht so dicht wie möglich in diesem Pool platziert. Wenn dies der Fall ist, passen Sie die kritischen Schwellenwerte des Pools

an, bis der größte Teil der Ressourcenauslastung in den Schwellenbereich Durchschnittlich (blau) fällt.

- Wenn sich die Zeile für durchschnittliche Nutzung mit dem durchschnittlichen kritischen Schwellenwert (rot) schneidet, zeigt dies an, wenn die durchschnittliche Ressourcenauslastung den kritischen Schwellenwert für diese Ressource erreicht oder überschritten hat.

Wenn die Datenpunkte in den Diagrammen nicht im Bereich "Durchschnittlicher mittlerer Schwellenwert"liegen, die Leistung jedoch zufriedenstellend ist, können Sie den kritischen Schwellenwert für diesen Pool anpassen. Weitere Informationen finden Sie unter Ändern der kritischen Schwellenwerte.

Pooloptimierungsverlauf

Der Bericht zum Pool-Optimierungsverlauf bietet chronologischen Einblick in die Optimierungsaktivitäten des Workload Balancing

Die Optimierungsaktivität wird grafisch und in einer Tabelle zusammengefasst. Bei Drillings in ein Datumsfeld innerhalb der Tabelle werden detaillierte Informationen zu jeder für diesen Tag durchgeführten Pool-Optimierung angezeigt.

In diesem Bericht werden die folgenden Informationen angezeigt:

- VM-Name: Der Name der VM, die Workload Balancing optimiert hat.
- Grund: Der Grund für die Optimierung.
- Methode: Ob die Optimierung erfolgreich war.
- Vom Host: Der physische Host, auf dem die VM ursprünglich gehostet wurde.
- Zum Host: Der physische Host, auf den die VM migriert wurde.
- Zeit: Der Zeitpunkt, zu dem die Optimierung stattgefunden hat.

> **Tipp:**
>
> Sie können auch einen Pool-Optimierungsverlaufsbericht auf der Registerkarte WLB generieren, indem Sie auf den Link Verlauf anzeigen klicken.

VM-Bewegungsverlauf

Dieses Liniendiagramm zeigt an, wie oft VMs in einem Ressourcenpool über einen Zeitraum migriert wurden. Es zeigt an, ob eine Migration aus einer Optimierungsempfehlung resultiert und auf welchen Host die VM verschoben wurde. Dieser Bericht gibt auch den Grund für die Optimierung an. Mit diesem Bericht können Sie die Anzahl der Migrationen in einem Pool überwachen.

Einige Punkte zur Interpretation dieses Berichts:

- Die Zahlen auf der linken Seite des Diagramms entsprechen der Anzahl der möglichen Migrationen. Dieser Wert basiert darauf, wie viele virtuelle Rechner sich in einem Ressourcenpool befinden.
- Sie können sich Details der Migrationen an einem bestimmten Datum ansehen, indem Sie das +-Zeichen im Abschnitt Datum des Berichts erweitern.

VM-Leistungsverlauf

In diesem Bericht werden Leistungsdaten für jede VM auf einem bestimmten Host für einen von Ihnen angegebenen Zeitraum angezeigt. Der Workload Balancing basiert die Leistungsdaten auf der Menge der virtuellen Ressourcen, die für die VM zugewiesen sind. Wenn die durchschnittliche CPU-Auslastung für Ihre VM beispielsweise 67% beträgt, nutzt Ihre VM für den angegebenen Zeitraum durchschnittlich 67% ihrer vCPU.

In der ersten Ansicht des Berichts wird ein Durchschnittswert für die Ressourcenauslastung über den von Ihnen angegebenen Zeitraum angezeigt.

Durch Erweitern des +-Zeichens werden Liniendiagramme für einzelne Ressourcen angezeigt Mithilfe dieser Diagramme können Sie Trends bei der Ressourcennutzung im Laufe der Zeit erkennen.

In diesem Bericht werden Daten zur CPU-Auslastung, zum freien Speicher, zum Lesen/Schreiben im Netzwerk und zum Datenträger-Lesen/Schreiben angezeigt.

Konfigurieren des Workload Balancing-Verhaltens

April 13, 2024

Nachdem Sie eine Verbindung mit der virtuellen Workload Balancing-Appliance hergestellt haben, können Sie die Einstellungen bearbeiten, die Workload Balancing zur Berechnung der Platzierung und Die Workload Balancing-Einstellungen gelten gemeinsam für alle VMs und Hosts im Pool.

Zu den Platzierungs- und Optimierungseinstellungen, die Sie ändern können, gehören:

- Änderung der Platzierungsstrategie
- Konfigurieren automatischer Optimierungen und Energieverwaltung
- Bearbeiten von Leistungsschwellenwerten und metrischen Gewichtungen
- Ohne Hosts.

Vorausgesetzt, die Netzwerk- und Datenträgerschwellenwerte stimmen mit der Hardware in Ihrer Umgebung überein, sollten Sie zunächst die meisten Standardwerte im Workload-Balancing verwenden. Nachdem der Workload Balancing für eine Weile aktiviert wurde, empfehlen wir, Ihre Leistungsschwellenwerte zu bewerten und zu entscheiden, ob Sie sie bearbeiten möchten. Stellen Sie sich zum Beispiel die folgenden Fälle vor:

- Empfehlungen einholen, wenn sie noch nicht benötigt werden. Wenn ja, versuchen Sie, die Schwellenwerte anzupassen, bis der Workload Balancing geeignete Empfehlungen liefert.
- Sie erhalten keine Empfehlungen, wenn Sie sie erwarten. Wenn Ihr Netzwerk beispielsweise über unzureichende Bandbreite verfügt und Sie keine Empfehlungen erhalten, müssen Sie möglicherweise Ihre Einstellungen anpassen. Wenn ja, versuchen Sie, die kritischen Netzwerkschwellenwerte zu senken, bis der Workload Balancing Empfehlungen bereitstellt.

Bevor Sie Ihre Schwellenwerte bearbeiten, können Sie für jeden physischen Host im Pool einen Poolintegritätsbericht und den Poolintegritätsverlauf erstellen. Weitere Informationen finden Sie unter Erstellen von Workloadberichten.

> **Hinweise:**
>
> - Workload Balancing ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.
> - Workload Balancing 8.3.0 ist mit XenServer 8 und Citrix Hypervisor 8.2 CU1 kompatibel.

In diesem Artikel wird davon ausgegangen, dass Sie Ihren Pool bereits mit einer virtuellen Workload Balancing-Appliance verbunden Informationen zum Herunterladen, Importieren, Konfigurieren und Herstellen einer Verbindung zu einer virtuellen Workload Balancing-Appliance finden Sie unter Erste Schritte.

Passen Sie den Optimierungsmodus

Der Workload Balancing gibt Empfehlungen zur Neuverteilung oder Optimierung der VM-Workload in Ihrer Umgebung auf der Grundlage einer von Ihnen ausgewählten Platzierungsstrategie. Die Platzierungsstrategie wird als Optimierungsmodus bezeichnet.

Sie können aus den folgenden Optimierungsmodi wählen:

- **Leistung maximieren** (Standard)

  Der Workload Balancing versucht, die Workload gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, den CPU-, Arbeitsspeicher- und Netzwerkdruck für alle Hosts zu minimieren. Wenn “Leistung maximieren”Ihre Platzierungsstrategie ist, empfiehlt Workload Balancing eine Optimierung, wenn ein Host den Schwellenwert “Hoch”erreicht.

- **Maximieren der Dichte**

  Workload Balancing versucht, die Anzahl der physischen Hosts, die online sein müssen, zu minimieren, indem die aktiven VMs konsolidiert werden.

  Wenn Sie "Dichte maximieren"als Platzierungsstrategie auswählen, können Sie ähnliche Parameter wie unter "Leistung maximieren"angeben. Workload Balancing verwendet diese Parameter jedoch, um zu bestimmen, wie VMs auf einen Host gepackt werden können. Wenn "Maximize Density"Ihre Platzierungsstrategie ist, empfiehlt Workload Balancing Konsolidierungsoptimierungen, wenn eine VM den Schwellenwert "Niedrig"erreicht.

Mit dem Workload Balancing können Sie diese Optimierungsmodi auch immer anwenden, *fest* oder für bestimmte Zeiträume zwischen den Modi wechseln, *geplant*:

Optimierungsmodi korrigiert

Feste Optimierungsmodi setzen Workload Balancing so, dass er immer ein bestimmtes Optimierungsverhalten hat. Dieses Verhalten kann entweder darin bestehen, die beste Leistung zu erzielen, oder um die höchste Dichte zu erzielen.

Führen Sie die folgenden Schritte aus, um einen festen Optimierungsmodus festzulegen:

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Optimierungsmodus**.
5. Wählen Sie im Bereich **Fixed** der Seite **Optimierungsmodus** einen der folgenden Optimierungsmodi aus:

   - Leistung maximieren (Standard). Versucht, die Workload gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, den CPU-, Arbeitsspeicher- und Netzwerkdruck für alle Hosts zu minimieren.
   - Dichte maximieren. Versucht, so viele VMs wie möglich auf einen physischen Host zu passen. Ziel ist es, die Anzahl der physischen Hosts zu minimieren, die online sein müssen.

Geplante Optimierungsmodi

Mit den Geplanten Optimierungsmodi können Sie festlegen, dass der Workload Balancing je nach Tageszeit unterschiedliche Optimierungsmodi anwenden kann. Beispielsweise möchten Sie den Workload Balancing möglicherweise so konfigurieren, dass die Leistung während des Tages, an dem

Benutzer verbunden sind, optimiert wird. Um Energie zu sparen, können Sie dann festlegen, dass der Workload Balancing für die maximale Dichte bei Nacht optimiert wird.

Wenn Sie geplante Optimierungsmodi konfigurieren, wechselt der Workload Balancing zu Beginn des von Ihnen angegebenen Zeitraums automatisch in den Optimierungsmodus. Sie können jeden Tag, Wochentage, Wochenende oder einzelne Tage konfigurieren. Für die Stunde wählen Sie eine Tageszeit aus.

Führen Sie die folgenden Schritte aus, um einen Zeitplan für Ihre Optimierungsmodi festzulegen:

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Optimierungsmodus**.
5. Wählen Sie im Bereich **Optimierungsmodus** die Option **Geplant**aus. Der Abschnitt "**Geplant** "wird verfügbar.
6. Klicken Sie auf **Neu hinzufügen**.
7. Wählen Sie im Feld **Ändern** in einen der folgenden Modi aus:
   - Maximieren Sie die Leistung. Versucht, die Workload gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, den CPU-, Arbeitsspeicher- und Netzwerkdruck für alle Hosts zu minimieren.
   - Dichte maximieren. Versucht, so viele VMs wie möglich auf einen physischen Host zu passen. Ziel ist es, die Anzahl der physischen Hosts zu minimieren, die online sein müssen.
8. Wählen Sie den Wochentag und die Uhrzeit aus, zu der der Workloadausgleich in diesem Modus gestartet werden soll.
9. Wiederholen Sie die vorherigen Schritte, um weitere Aufgaben im geplanten Modus zu erstellen, bis Sie die benötigte Anzahl haben. Wenn Sie nur eine Aufgabe planen, wechselt der Workload Balancing wie geplant in diesen Modus, wechselt dann aber nie zurück.
10. Klicken Sie auf **OK**.

Führen Sie die folgenden Schritte aus, um Ihre Zeitplaneinstellungen zu ändern.

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Optimierungsmodus**.

5. Wählen Sie in der Liste **Änderungen im geplanten Modus** die Aufgabe aus, die Sie löschen oder deaktivieren möchten.
6. Führen Sie einen der folgenden Schritte aus:

   - **Löschen Sie die Aufgabe dauerhaft**: Klicken Sie auf die Schaltfläche **Löschen**.
   - **Beenden Sie die Ausführung der Aufgabe vorübergehend**: Klicken Sie mit der rechten Maustaste auf die Aufgabe und klicken Sie auf **Deaktivieren**.

     Tipps:

     ```
     - Sie können Tasks auch deaktivieren oder aktivieren, indem Sie die Task auswählen, auf **Bearbeiten** klicken und im Dialogfeld **Optimierungsmodus-Planer** das Kontrollkästchen **Task aktivieren** aktivieren.
     ```

     - Um eine Aufgabe neu zu aktivieren, klicken Sie in der Liste **Änderungen im geplanten Modus** mit der rechten Maustaste auf die Aufgabe und klicken Sie auf **Aktivieren**.

   - **Bearbeiten Sie die Aufgabe**: Doppelklicken Sie auf die Aufgabe, die Sie bearbeiten möchten. Wählen Sie im Feld **Ändern** in einen anderen Modus aus, oder nehmen Sie nach Bedarf andere Änderungen vor.

> **Hinweis:**
>
> Wenn Sie auf Abbrechen klicken, bevor Sie auf OK klicken, werden alle auf der Registerkarte Optimierung vorgenommenen Änderungen rückgängig gemacht, einschließlich des Löschens einer Aufgabe.

Optimieren und verwalten Sie die Stromversorgung automatisch

Sie können Workload Balancing so konfigurieren, dass Empfehlungen automatisch angewendet und Hosts automatisch ein- oder ausgeschaltet werden. Um Hosts automatisch herunterzufahren (z. B. in Zeiten geringer Auslastung), müssen Sie den Workload Balancing so konfigurieren, dass Empfehlungen automatisch angewendet und die Energieverwaltung aktiviert wird. Sowohl die Energieverwaltung als auch die Automatisierung werden in den folgenden Abschnitten beschrieben.

Empfehlungen automatisch anwenden

Mit dem Workload Balancing können Sie so konfigurieren, dass Empfehlungen in Ihrem Namen angewendet werden und die empfohlenen Optimierungsaktionen automatisch ausgeführt werden. Sie können diese Funktion, die als automatische Optimierungsakzeptanz bezeichnet wird,

verwenden, um alle Empfehlungen automatisch anzuwenden, einschließlich Empfehlungen zur Leistungsverbesserung oder zum Herunterfahren von Hosts. Um Hosts bei sinkender Nutzung von VMs herunterzufahren, müssen Sie jedoch Automatisierung, Energieverwaltung und den Modus "Maximale Dichte"konfigurieren.

Standardmäßig wendet der Workload Balancing Empfehlungen nicht automatisch an. Wenn Sie möchten, dass Workload Balancing Empfehlungen automatisch anwendet, aktivieren Sie die Automatisierung. Wenn Sie dies nicht tun, müssen Sie Empfehlungen manuell anwenden, indem Sie auf **Empfehlungen anwenden**klicken.

Workload Balancing wendet Empfehlungen nicht automatisch auf Hosts oder VMs an, wenn die Empfehlungen mit den HA-Einstellungen in Konflikt stehen. Wenn ein Pool durch Anwenden der Optimierungsempfehlungen für den Workload Balancing überschrieben wird, werden Sie von XenCenter aufgefordert, ob Sie die Empfehlung weiterhin anwenden möchten. Wenn die Automatisierung aktiviert ist, wendet Workload Balancing keine Empfehlungen zur Energieverwaltung an, die die Anzahl der im HA-Plan zu tolerierenden Hostausfälle überschreiten.

Wenn der Workload Balancing mit aktivierter Automatisierungsfunktion ausgeführt wird, wird dieses Verhalten manchmal als Ausführung im automatisierten Modus bezeichnet.

Es ist möglich zu optimieren, wie der Workload Balancing Empfehlungen im automatisierten Modus anwendet. Weitere Informationen finden Sie unter Festlegen konservativer oder aggressiver automatisierter Empfehlungen.

So wenden Sie Optimierungsempfehlungen automatisch an

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Automatisierung**.
5. Wählen Sie eines oder mehrere der folgenden Kontrollkästchen aus:

    - **Wenden Sie Optimierungsempfehlungen automatisch an**. Wenn Sie diese Option auswählen, müssen Sie Optimierungsempfehlungen nicht manuell akzeptieren. Workload Balancing akzeptiert automatisch die von ihm abgegebenen Optimierungs- und Platzierungsempfehlungen.
    - **Wenden Sie die Empfehlungen zur Energieverwaltung automatisch an**. Das Verhalten dieser Option hängt vom Optimierungsmodus des Pools ab:
        - Maximaler Leistungsmodus: Wenn die Option **Energieverwaltungsempfehlungen automatisch anwenden** aktiviert ist, schaltet Workload Balancing Hosts automatisch ein, wenn dadurch die Hostleistung verbessert wird.

- Modus für maximale Dichte: Wenn die Option **Energieverwaltungsempfehlungen automatisch anwenden** aktiviert ist, schaltet Workload Balancing Hosts automatisch aus, wenn die Ressourcenauslastung unter den niedrigen Schwellenwert fällt. Das heißt, der Workload Balancing schaltet Hosts bei geringer Auslastung automatisch aus.

6. (Fakultativ.) Optimieren Sie die Optimierungsempfehlungen, indem Sie im linken Bereich des **Einstellungsdialogs** auf **Erweitert** klicken und eine oder mehrere der folgenden Aktionen ausführen:

   - Geben Sie an, wie oft der Workload Balancing eine Optimierungsempfehlung abgeben muss, bevor die Empfehlung automatisch angewendet wird. Die Standardeinstellung ist dreimal, was bedeutet, dass die Empfehlung beim dritten Mal angewendet wird.
   - Wählen Sie die niedrigste Optimierungsstufe aus, die der Workload Balancing automatisch anwenden soll. Der Standardwert ist "Hoch".
   - Änderung der Aggressivität, mit der Workload Balancing seine Optimierungsempfehlungen anwendet.

     Möglicherweise möchten Sie auch angeben, wie viele Minuten der Workload Balancing warten muss, bevor Sie eine Optimierungsempfehlung auf eine kürzlich verschobene VM anwenden.

     All diese Einstellungen werden unter Konservative oder aggressive automatisierte Empfehlungen festlegenausführlicher erläutert.

7. (optional) Wenn Sie die Energieverwaltung konfigurieren möchten, klicken Sie auf **Automatisierung/Energieverwaltung**

   a) Wählen Sie im Abschnitt **Energieverwaltung** die Hosts aus, deren Ein- und Ausschalten vom Workload Balancing empfohlen werden soll.

   > **Hinweis:**
   >
   > Wenn Sie Hosts für Energieverwaltungsempfehlungen auswählen, ohne **Energieverwaltungsempfehlungen automatisch anwenden** auszuwählen, schlägt Workload Balancing Empfehlungen zur Energieverwaltung vor, wendet sie jedoch nicht automatisch für Sie an.

   Wenn keiner der Hosts im Ressourcenpool die Remote-Energieverwaltung unterstützt, zeigt Workload Balancing die Meldung an: "Keine Hosts unterstützen Power Management."

   b) Klicken Sie auf **OK**.

8. Um die Konfiguration der Automatisierung abzuschließen, klicken Sie auf **OK**.

Energieverwaltung für Workload Balancing aktivieren

Der Begriff Energiemanagement bezeichnet die Fähigkeit, die Stromversorgung für physische Hosts ein- oder auszuschalten. Im Kontext des Workload Balancing bedeutet dieser Begriff, dass Hosts in einem Pool basierend auf der Gesamtauslastung des Pools ein- oder ausgeschaltet werden.

Die Konfiguration der Energieverwaltung für den Workload Balancing auf einem Host erfordert Folgendes:

- Die Hardware für den Host verfügt über Funktionen zum Ein- und Ausschalten per Fernzugriff.
- Die Host-Power-On-Funktion ist für den Host konfiguriert. Informationen zum Konfigurieren der Host-Power-On-Funktion für den Host finden Sie unter Host-Einschaltfunktion konfigurieren.
- Der Host wurde ausdrücklich als Host für die Teilnahme an der Energieverwaltung des Workload Balancing ausgewählt.

Wenn Sie möchten, dass Workload Balancing Hosts automatisch ausschaltet, konfigurieren Sie Workload Balancing außerdem so, dass er die folgenden Aktionen ausführt:

- Empfehlungen automatisch anwenden
- Energieverwaltungsempfehlungen automatisch anwenden

Wenn ein Host so eingestellt ist, dass er an der Energieverwaltung teilnimmt, gibt Workload Balancing nach Bedarf Empfehlungen zum Ein- und Ausschalten.

Wenn Sie im Modus “Maximale Dichte”laufen:

- Wenn Workload Balancing ungenutzte Ressourcen in einem Pool erkennt, empfiehlt es sich, Hosts auszuschalten, bis alle überschüssigen Kapazitäten entfernt sind.
- Wenn im Pool nicht genügend Hostkapazität vorhanden ist, um Hosts herunterzufahren, empfiehlt Workload Balancing, die Hosts eingeschaltet zu lassen, bis die Pool-Workload ausreichend gesunken ist.
- Wenn Sie Workload Balancing so konfigurieren, dass zusätzliche Hosts automatisch ausgeschaltet werden, wendet es diese Empfehlungen automatisch an und verhält sich daher genauso.

Wenn Sie im Modus “Maximale Leistung”ausgeführt werden:

- Wenn Sie Workload Balancing so konfigurieren, dass Hosts automatisch eingeschaltet werden, schaltet Workload Balancing Hosts ein, wenn die Ressourcenauslastung auf einem Host den Schwellenwert Hoch überschreitet.
- Workload Balancing schaltet Hosts niemals aus, nachdem sie eingeschaltet wurden.

Wenn Sie die Option zum automatischen Anwenden von Energieverwaltungsempfehlungen aktivieren, tun Sie dies auf Poolebene. Sie können jedoch angeben, welche Hosts aus dem Pool Sie an der Energieverwaltung teilnehmen möchten.

Konfiguration der Host-Power-On-Funktion Gehen Sie wie folgt vor, um die Host-Power-On-Funktion für Ihren Host zu konfigurieren:

1. Wählen Sie in XenCenter Ihren Host aus und klicken Sie auf **Eigenschaften**.
2. Klicken Sie im linken Bereich **auf Power On**.
3. Wählen Sie für **den Power-On-ModusDell Remote Access Controller (DRAC)**.
4. Geben Sie für die **Konfigurationsoptionen**die DRAC-IP-Adresse Ihres Servers ein. Dies ist die IP-Adresse des BMC-Management-Ports. Weitere Informationen finden Sie in der DRAC-Karten-Anleitung
   [PDF].
5. Nachdem der Dell Remote Access Controller (DRAC) konfiguriert wurde, wählen Sie Ihren Pool aus.
6. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
7. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
8. Klicken Sie im linken Bereich auf **Automatisierung**.
9. Wählen Sie für **Automatisierung**die folgenden Kontrollkästchen aus:

   - **Wenden Sie Optimierungsempfehlungen automatisch an**. Wenn Sie diese Option auswählen, müssen Sie Optimierungsempfehlungen nicht manuell akzeptieren. Workload Balancing akzeptiert automatisch die von ihm abgegebenen Optimierungs- und Platzierungsempfehlungen.
   - **Wenden Sie die Empfehlungen zur Energieverwaltung automatisch an**. Das Verhalten dieser Option hängt vom Optimierungsmodus des Pools ab:

     – Maximaler Leistungsmodus: Wenn die Option **Energieverwaltungsempfehlungen automatisch anwenden** aktiviert ist, schaltet Workload Balancing Hosts automatisch ein, wenn dadurch die Hostleistung verbessert wird.

     – Modus für maximale Dichte: Wenn die Option **Energieverwaltungsempfehlungen automatisch anwenden** aktiviert ist, schaltet Workload Balancing Hosts automatisch aus, wenn die Ressourcenauslastung unter den niedrigen Schwellenwert fällt. Das heißt, der Workload Balancing schaltet Hosts bei geringer Auslastung automatisch aus.

10. Wählen Sie für **Power Management**den Namen des **Hostservers** aus, den Sie gerade konfigurieren.

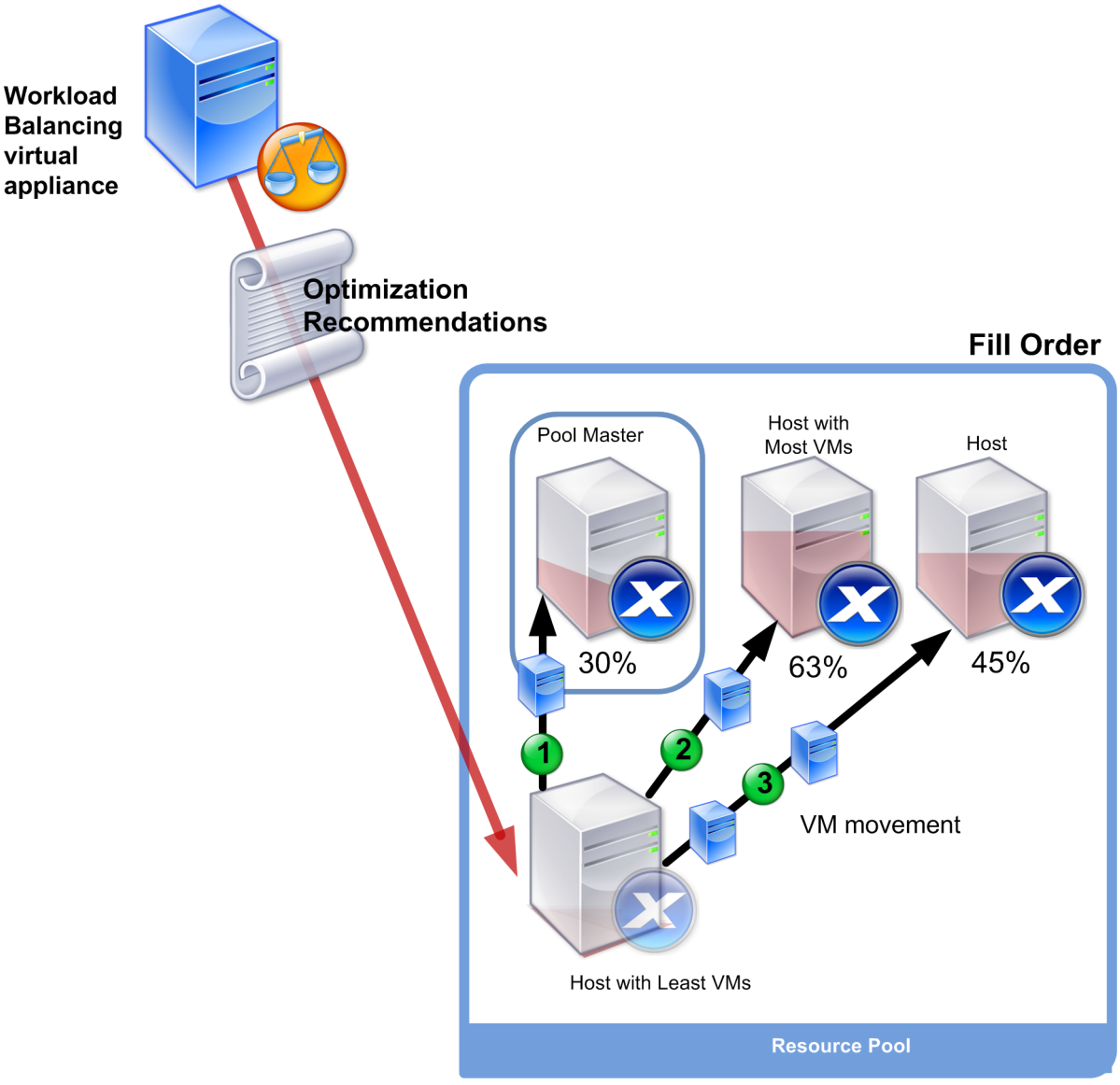
Verstehen des Energieverwaltungsverhalten

Bevor Workload Balancing empfiehlt, Hosts ein- oder auszuschalten, wählt es die Hosts aus, auf die VMs übertragen werden sollen. Es tut dies in der folgenden Reihenfolge:

1. Füllen des Poolkoordinators, da dieser Host nicht ausgeschaltet werden kann.
2. Den Host mit den meisten VMs füllen.
3. Füllen nachfolgender Hosts entsprechend den Hosts, auf denen die meisten VMs laufen.

Wenn Workload Balancing den Poolkoordinator füllt, geht es von künstlich niedrigen Schwellenwerten für den Koordinator aus. Der Workload Balancing verwendet diese niedrigen Schwellenwerte als Puffer, um zu verhindern, dass der Poolkoordinator überlastet wird.

Der Workload Balancing füllt Hosts in dieser Reihenfolge, um die Dichte zu fördern.



Wenn Workload Balancing ein Leistungsproblem feststellt, während sich der Pool im Modus Maximale Dichte befindet, empfiehlt es sich, Workloads zwischen den eingeschalteten Hosts zu migrieren. Wenn der Workload Balancing das Problem mit dieser Methode nicht lösen kann, wird versucht, einen Host einzuschalten. Der Workload Balancing bestimmt, welche Hosts eingeschaltet werden sollen, indem dieselben Kriterien angewendet werden, die auch gelten, wenn der Optimierungsmodus auf Maximale Leistung eingestellt wäre.

Wenn Workload Balancing im Modus “Maximale Leistung”ausgeführt wird, empfiehlt Workload Balancing, Hosts einzuschalten, bis die Ressourcenauslastung aller Poolmitglieder unter den Schwellenwert “Hoch”fällt.

Wenn der Workload Balancing bei der Migration von VMs feststellt, dass eine Erhöhung der Kapazität der Gesamtleistung des Pools zugute kommt, werden die Hosts automatisch eingeschaltet oder es wird empfohlen, dies zu tun.

> **Wichtig:**
>
> Der Workload Balancing empfiehlt nur, einen Host einzuschalten, auf dem der Workload Balancing ausgeschaltet ist.

Designumgebungen für Energieverwaltung und VM-Konsolidierung

Wenn Sie eine XenServer-Implementierung planen und die automatische VM-Konsolidierung und Energieverwaltung konfigurieren möchten, sollten Sie Ihr Workload-Design berücksichtigen. Sie können beispielsweise Folgendes tun:

- Platzieren Sie verschiedene Arten von Workloaden in getrennten Pools.

  Wenn Sie über eine Umgebung mit unterschiedlichen Arten von Workloaden verfügen, sollten Sie überlegen, ob Sie die VMs, die diese Workloaden hosten, in verschiedenen Pools suchen sollten. Erwägen Sie auch, VMs, die Anwendungstypen hosten, die mit bestimmten Hardwaretypen bessere Leistungen erbringen, in verschiedene Pools aufzuteilen.

  Da Energieverwaltung und VM-Konsolidierung auf Poolebene verwaltet werden, entwerfen Sie Pools so, dass sie Workloaden enthalten, die konsolidiert werden sollen. Stellen Sie sicher, dass Sie Überlegungen berücksichtigen, wie sie unter Konfigurieren erweiterter Einstellungenbeschrieben wurden.

- Schließen Sie Hosts vom Workload Balancing aus.

  Einige Hosts müssen möglicherweise immer aktiviert sein. Weitere Informationen findest du unter Hosts von Empfehlungen ausschließen.

Verstehen, wann Workload Balancing Empfehlungen gibt

Workload Balancing bewertet kontinuierlich die Ressourcenmetriken von physischen Hosts und VMs in den Pools, die es verwaltet, anhand von Schwellenwerten. Schwellenwerte sind voreingestellte Werte, die wie Grenzen funktionieren, die ein Host überschreiten muss, bevor Workload Balancing eine Optimierungsempfehlung aussprechen kann. Der Workload Balancing-Prozess ist wie folgt:

1. Der Workload Balancing erkennt, dass der Schwellenwert für eine Ressource verletzt wurde.
2. Der Workload Balancing bewertet, ob er eine Optimierungsempfehlung ausspricht.
3. Der Workload Balancing bestimmt, welche Hosts als Zielhosts empfohlen werden und in welcher Reihenfolge Optimierungen vorgenommen werden sollen. Ein Zielhost ist der Host, auf dem Workload Balancing empfiehlt, eine oder mehrere VMs zu verlagern.
4. Workload Balancing gibt eine Optimierungsempfehlung ab.

Bei der Bewertung von Hosts im Pool, um eine Optimierungsempfehlung abzugeben, verwendet Workload Balancing Schwellenwerte und Gewichtungen wie folgt:

- **Schwellenwerte** sind die Grenzwerte, mit denen Workload Balancing die Ressourcenmetriken Ihres Pools vergleicht. Anhand der Schwellenwerte wird bestimmt, ob eine Empfehlung ausgesprochen werden soll und welche Hosts sich für das Hosten von umgesiedelten VMs eignen.
- **Gewichtungen** sind eine Möglichkeit, Ressourcen danach zu ordnen, wie viel sie berücksichtigt werden sollen. Sie werden verwendet, um die Verarbeitungsreihenfolge zu bestimmen. Nachdem der Workload Balancing beschlossen hat, eine Empfehlung abzugeben, werden Ihre Spezifikationen verwendet, welche Ressourcen wichtig sind, um Folgendes zu bestimmen:
  - Die Leistung welcher Hosts muss zuerst angesprochen werden
  - Welche VMs sollten zuerst migriert werden

Für jede Ressource, die der Workload Balancing überwacht, gibt es vier Schwellenwertstufen: Kritisch, Hoch, Mittel und Niedrig. Workload Balancing bewertet, ob eine Empfehlung ausgesprochen werden soll, wenn eine Ressourcenmetrik auf einem Host:

- Überschreitet den Schwellenwert “Hoch”, wenn der Pool im Modus “Maximale Leistung”ausgeführt wird (Verbesserung der Leistung)
- Sinkt unter den niedrigen Schwellenwert, wenn der Pool im Modus “Maximale Dichte”ausgeführt wird (VMs auf Hosts konsolidieren)
- Überschreitet den kritischen Schwellenwert, wenn der Pool im Modus “Maximale Dichte”ausgeführt wird (Leistung verbessern)

Wenn der Schwellenwert “Hoch”für einen Pool, der im Modus “Maximale Leistung”ausgeführt wird, 80% beträgt und die CPU-Auslastung auf einem Host 80,1% erreicht, bewertet Workload Balancing, ob eine Empfehlung ausgegeben werden soll.

Wenn eine Ressource ihren Schwellenwert verletzt, wertet der Workload Balancing die Ressourcenmetrik anhand der historischen Leistung aus, um zu verhindern, dass eine Optimierungsempfehlung basierend auf einer vorübergehenden Spitze abgegeben wird. Zu diesem Zweck erstellt der Workload Balancing eine historisch gemittelte Nutzungsmetrik, indem die Daten für die Ressourcenauslastung ausgewertet werden, die zu den folgenden Zeiten erfasst wurden:

Erfasste Daten	Gewicht
Sofort, zum Zeitpunkt wurde der Schwellenwert überschritten. Das heißt, Echtzeitdaten.	70%
30 Minuten bevor der Schwellenwert überschritten wurde	25%
24 Stunden bevor der Schwellenwert überschritten wurde	5%

Wenn die CPU-Auslastung auf dem Host den Schwellenwert um 12:02 Uhr überschreitet, überprüft Workload Balancing die Auslastung an diesem Tag um 11:32 Uhr und am Vortag um 12:02 Uhr. Wenn die CPU-Auslastung beispielsweise die folgenden Werte aufweist, gibt der Workload Balancing keine Empfehlung ab:

- 80,1% um 12:02 Uhr an diesem Tag
- 50% um 11:32 Uhr an diesem Tag
- 78% um 12:32 Uhr am Vortag

Dieses Verhalten ist darauf zurückzuführen, dass die historisch gemittelte Auslastung 72,5% beträgt, sodass der Workload Balancing davon ausgeht, dass die Auslastung ein vorübergehender Anstieg ist. Wenn die CPU-Auslastung jedoch um 11:32 Uhr 83% betrug, gibt der Workload Balancing eine Empfehlung ab, da die historisch gemittelte Auslastung 80,1% beträgt.

Optimierung und Konsolidierung

Der Workload Balancing-Prozess zur Bestimmung potenzieller Optimierungen variiert je nach Optimierungsmodus - Maximale Leistung oder Maximale Dichte. Unabhängig vom Optimierungsmodus werden die Optimierungs- und Platzierungsempfehlungen jedoch in einem zweistufigen Verfahren abgegeben:

1. Ermitteln Sie mögliche Optimierungen: welche VMs von Hosts migriert werden sollen.
2. Bestimmen Sie Platzierungsempfehlungen: Welche Hosts wären geeignete Kandidaten für neue VMs.

> **Hinweis:**
>
> Workload Balancing empfiehlt nur die Migration von VMs, die die XenServer-Kriterien für die Livemigration erfüllen. Eines dieser Kriterien ist, dass der Zielhost über den Speicher verfügen muss, den die VM benötigt. Der Zielhost muss außerdem über ausreichende Ressourcen verfügen, um das Hinzufügen der VM zu ermöglichen, ohne die Schwellenwerte des im Pool konfigurierten Optimierungsmodus zu überschreiten. Beispielsweise der Schwellenwert "Hoch"im Modus "Maximale Leistung"und der Schwellenwert "Kritisch"für den Modus "Maximale Dichte".

Wenn der Workload Balancing im automatisierten Modus ausgeführt wird, können Sie die Art und Weise anpassen, in der Empfehlungen angewendet werden. Weitere Informationen finden Sie unter Festlegen konservativer oder aggressiver automatisierter Empfehlungen.

Optimierungs-Empfehlungsprozess im Modus "Maximale Leistung" Beim Ausführen im Modus "Maximale Leistung"verwendet der Workload Balancing den folgenden Prozess, um potenzielle Optimierungen zu ermitteln:

1. Alle zwei Minuten bewertet Workload Balancing die Ressourcenauslastung für jeden Host im Pool. Dazu wird auf jedem Host überwacht und festgestellt, ob die Auslastung der einzelnen Ressourcen den Schwellenwert "Hoch"überschreitet. Weitere Informationen finden Sie unter Ändern des kritischen Schwellenwerts.

   Wenn im Modus "Maximale Leistung"die Auslastung einer Ressource den Schwellenwert "Hoch" überschreitet, startet der Workload Balancing den Prozess, um zu bestimmen, ob eine Optimierungsempfehlung abgegeben werden soll. Der Workload Balancing legt fest, ob eine Optimierungsempfehlung abgegeben wird, basierend darauf, ob dies Leistungseinschränkungen, z. B. durch den Schwellenwert "Hoch", vereinfachen kann.

   Stellen Sie sich beispielsweise den Fall vor, in dem Workload Balancing feststellt, dass unzureichende CPU-Ressourcen die Leistung der VMs auf einem Host negativ beeinflussen. Wenn Workload Balancing einen anderen Host mit geringerer CPU-Auslastung finden kann, empfiehlt es sich, eine oder mehrere VMs auf einen anderen Host zu verschieben.

2. Wenn die Auslastung einer Ressource auf einem Host den entsprechenden Schwellenwert überschreitet, kombiniert Workload Balancing die folgenden Daten, um die historisch gemittelte Auslastung zu bilden:

   - Die aktuelle Auslastung der Ressource
   - Historische Daten von vor 30 Minuten
   - Verlaufsdaten von vor 24 Stunden
     Wenn die historisch gemittelte Auslastung den Schwellenwert einer Ressource überschreitet, bestimmt der Workload Balancing, dass eine Optimierungsempfehlung abgegeben wird.

3. Workload Balancing verwendet metrische Gewichtungen, um zu bestimmen, welche Hosts zuerst optimiert werden sollen. Die Ressource, der Sie das meiste Gewicht zugewiesen haben, versucht der Workload Balancing zuerst zu adressieren. Weitere Informationen finden Sie unter Einstellen der metrischen Gewichtung.

4. Der Workload Balancing bestimmt, welche Hosts die VMs unterstützen können, die von Hosts migriert werden sollen.

   Workload Balancing trifft diese Entscheidung, indem es die prognostizierten Auswirkungen der Platzierung verschiedener Kombinationen von VMs auf Hosts auf die Ressourcennutzung berechnet. Der Workload Balancing verwendet eine Methode zur Durchführung dieser Berechnungen, die in der Mathematik als Permutation bezeichnet wird.

   Zu diesem Zweck erstellt Workload Balancing eine einzelne Metrik oder Bewertung, um die Auswirkungen der Migration einer VM auf den Host vorherzusagen. Die Punktzahl gibt an, ob ein Host als Heim für mehr VMs geeignet ist.

   Um die Hostleistung zu bewerten, kombiniert Workload Balancing die folgenden Metriken:

   - Die aktuellen Metriken des Hosts
   - Die Metriken des Hosts der letzten 30 Minuten
   - Die Metriken des Hosts von vor 24 Stunden
   - Die Metriken der VM.

5. Nach der Bewertung von Hosts und VMs versucht Workload Balancing, virtuelle Modelle zu erstellen, wie die Hosts mit verschiedenen Kombinationen von VMs aussehen. Workload Balancing verwendet diese Modelle, um den besten Host für die Platzierung der VM zu ermitteln.

   Im Modus Maximale Leistung verwendet Workload Balancing metrische Gewichtungen, um zu bestimmen, welche Hosts zuerst optimiert werden müssen und welche VMs auf diesen Hosts zuerst migriert werden sollen. Der Workload Balancing basiert bei seinen Modellen auf den metrischen Gewichtungen. Wenn der CPU-Auslastung beispielsweise die höchste Bedeutung zugewiesen wird, sortiert Workload Balancing Hosts und VMs, um sie nach den folgenden Kriterien zu optimieren:

   a) Welche Hosts laufen, die dem Schwellenwert “Hoch”für die CPU-Auslastung am nächsten kommen.
   b) Welche VMs haben die höchste CPU-Auslastung oder werden am nächsten an ihrem hohen Schwellenwert ausgeführt.

6. Der Workload Balancing berechnet weiterhin Optimierungen. Es betrachtet Hosts als Kandidaten für die Optimierung und VMs als Kandidaten für die Migration, bis die prognostizierte Ressourcenauslastung auf dem Host, der die VM hostet, unter den Schwellenwert “Hoch”fällt. Die prognostizierte Ressourcenauslastung ist die Ressourcenauslastung, die Workload Balanc-

ing für einen Host prognostiziert, nachdem Workload Balancing dem Host eine VM hinzugefügt oder von diesem entfernt hat.

Konsolidierungsprozess im Modus "Maximale Dichte" Der Workload Balancing bestimmt, ob eine Empfehlung abgegeben werden soll, basierend darauf, ob eine VM auf einen Host migriert und dieser Host dennoch unter dem kritischen Schwellenwert ausgeführt werden kann.

1. Wenn die Auslastung einer Ressource unter den Schwellenwert "Niedrig"fällt, beginnt der Workload Balancing mit der Berechnung potenzieller Konsolidierungsszenarien.
2. Wenn Workload Balancing eine Möglichkeit entdeckt, VMs auf einem Host zu konsolidieren, bewertet es, ob der Zielhost ein geeignetes Zuhause für die VM ist.
3. Wie im Modus Maximale Leistung bewertet Workload Balancing den Host, um festzustellen, ob ein Host als Home für neue VMs geeignet ist.

   Bevor Workload Balancing empfiehlt, VMs auf weniger Hosts zu konsolidieren, wird überprüft, ob die Ressourcenauslastung auf diesen Hosts nach der Verlagerung der VMs auf sie unter den kritischen Schwellenwerten liegt.

   > **Hinweis:**
   >
   > Der Workload Balancing berücksichtigt keine metrischen Gewichtungen, wenn er eine Konsolidierungsempfehlung ausspricht. Es berücksichtigt nur metrische Gewichtungen, um die Leistung auf Hosts sicherzustellen.

4. Nach der Bewertung von Hosts und VMs versucht Workload Balancing, virtuelle Modelle zu erstellen, wie die Hosts mit verschiedenen Kombinationen von VMs aussehen. Es verwendet diese Modelle, um den besten Host für die Platzierung der VM zu ermitteln.
5. Der Workload Balancing berechnet die Auswirkung des Hinzufügens von VMs zu einem Host, bis prognostiziert wird, dass das Hinzufügen einer weiteren VM dazu führt, dass eine Hostressource den kritischen Schwellenwert überschreitet.
6. In den Empfehlungen zum Workload Balancing wird immer empfohlen, zuerst den Poolkoordinator zu füllen, da der Host nicht ausgeschaltet werden kann. Der Workload Balancing wendet jedoch einen Puffer auf den Poolkoordinator an, sodass dieser nicht überlastet werden kann.
7. Workload Balancing empfiehlt weiterhin, VMs auf Hosts zu migrieren, bis alle verbleibenden Hosts einen kritischen Schwellenwert überschreiten, wenn eine VM auf sie migriert wird.

Ändern Sie die kritischen Schwellenwerte

Möglicherweise möchten Sie kritische Schwellenwerte ändern, um zu steuern, wann Optimierungsempfehlungen ausgelöst werden. In diesem Abschnitt finden Sie Anleitungen zu:

- So ändern Sie die standardmäßigen kritischen Schwellenwerte für Hosts im Pool
- Wie die für den kritischen Schwellenwert festgelegten Werte die Schwellenwerte Hoch, Mittel und Niedrig ändern.

Der Workload Balancing bestimmt, ob Empfehlungen basierend darauf erstellt werden sollen, ob die durchschnittliche historische Auslastung einer Ressource auf einem Host ihren Schwellenwert überschreitet. Empfehlungen für denWorkload Balancing werden ausgelöst, wenn der Schwellenwert "Hoch "im Modus "Maximale Leistung "oder der Schwellenwert "Niedrig"und "Kritisch"für den Modus "Maximale Dichte"verletzt werden. Weitere Informationen finden Sie unter Optimierungs- und Konsolidierungsprozess.

Nachdem Sie einen neuen kritischen Schwellenwert für eine Ressource angegeben haben, setzt der Workload Balancing die anderen Schwellenwerte der Ressource relativ zum neuen kritischen Schwellenwert zurück. Um die Benutzeroberfläche zu vereinfachen, ist der kritische Schwellenwert der einzige Schwellenwert, den Sie über XenCenter ändern können.

Die folgende Tabelle zeigt die Standardwerte für die Schwellenwerte für den Workloadausgleich:

Metrik	Kritisch	Hoch	Medium	Niedrig
CPU-Auslastung	90%	76.5%	45%	22.5%
Freier Speicher	51 MB	63,75 MB	510 MB	1020 MB
Netzwerk liest	25 MB/Sek	21,25 MB/Sek	12,5 MB/Sek	6,25 MB/Sek
Netzwerk schreibt	25 MB/Sek	21,25 MB/Sek	12,5 MB/Sek	6,25 MB/Sek
Disk liest	25 MB/Sek	21,25 MB/Sek	12,5 MB/Sek	6,25 MB/Sek
Disk schreibt	25 MB/Sek	21,25 MB/Sek	12,5 MB/Sek	6,25 MB/Sek

Um die Schwellenwerte für alle Metriken außer Speicher zu berechnen, multipliziert der Workload Balancing den neuen Wert für den kritischen Schwellenwert mit den folgenden Faktoren:

- **Hoher Schwellenwert-Faktor**: 0,85
- **Mittlerer Schwellenwert-Faktor**: 0,50
- **Niedriger Schwellenwert**: 0,25

Wenn Sie beispielsweise den kritischen Schwellenwert für die CPU-Auslastung auf 95% erhöhen, setzt der Workload Balancing die anderen Schwellenwerte wie folgt zurück:

- Hoch: 80,75%
- Mittel: 47,5%
- Niedrig: 23,75%

Um die Schwellenwerte für freien Speicher zu berechnen, multipliziert Workload Balancing den neuen Wert für den kritischen Schwellenwert mit den folgenden Faktoren:

- **Hoher Schwellenwert-Faktor**: 1,25
- **Mittlerer Schwellenwert-Faktor**: 10,0
- **Niedriger Schwellenwert-Faktor**: 20,0

Wenn Sie beispielsweise den kritischen Schwellenwert für freien Speicher auf 45 MB erhöhen, setzt der Workload Balancing die anderen Schwellenwerte wie folgt zurück:

- Hoch: 56,25 MB
- Mittel: 450 MB
- Niedrig: 900 MB

Um diese Berechnung für einen bestimmten Schwellenwert durchzuführen, multiplizieren Sie den Faktor für den Schwellenwert mit dem Wert, den Sie für den kritischen Schwellenwert für diese Ressource eingegeben haben:

```
1 High, Medium, or Low Threshold = Critical Threshold * High, Medium, or
      Low Threshold Factor
```

Während der kritische Schwellenwert viele Optimierungsempfehlungen auslöst, können auch andere Schwellenwerte Optimierungsempfehlungen auslösen, wie folgt:

- **Hoher Schwellenwert**.
  - **Maximale Leistung**. Das Überschreiten des Schwellenwerts "Hoch"löst Optimierungsempfehlungen aus, um eine VM auf einen Host mit geringerer Ressourcenauslastung zu verlagern.
  - **Maximale Dichte**. Workload Balancing empfiehlt nicht, eine VM auf dem Host zu platzieren, wenn das Verschieben dieser VM auf den Host dazu führt, dass die Hostressourcenauslastung einen hohen Schwellenwert überschreitet.
- **Niedriger Schwellenwert**.
  - **Maximale Leistung**. Der Workload Balancing löst keine Empfehlungen vom niedrigen Schwellenwert aus.
  - **Maximale Dichte**. Wenn ein Metrikwert unter den niedrigen Schwellenwert fällt, stellt Workload Balancing fest, dass die Hosts nicht ausgelastet sind, und gibt eine Optimierungsempfehlung ab, um VMs auf weniger Hosts zu konsolidieren. Workload Balancing empfiehlt weiterhin, VMs auf einen Host zu verschieben, bis die Metrikwerte für eine der Ressourcen des Hosts ihren Schwellenwert "Hoch"erreichen.

    Nach dem Umzug einer VM kann die Auslastung einer Ressource auf dem neuen Host der VM jedoch einen kritischen Schwellenwert überschreiten. In diesem Fall verwendet Workload Balancing vorübergehend einen Algorithmus, der dem Lastenausgleichsalgorhyth-

mus für maximale Leistung ähnelt, um einen neuen Host für die VMs zu finden. Workload Balancing verwendet diesen Algorithmus weiterhin, um das Verschieben von VMs zu empfehlen, bis die Ressourcenauslastung auf Hosts im Pool unter den Schwellenwert "Hoch"fällt.

So ändern Sie die kritischen Schwellenwerte:

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Wählen Sie im linken Bereich **Kritische Schwellenwerte**aus. Diese kritischen Schwellenwerte werden verwendet, um die Auslastung der Hostressourcen zu bewerten.
5. Geben Sie auf der Seite **Kritische Schwellenwerte** einen oder mehrere neue Werte in die Felder **Kritische Schwellenwerte** ein. Die Werte stellen die Ressourcenauslastung auf dem Host dar.

   Der Workload Balancing verwendet diese Schwellenwerte, wenn Empfehlungen zur VM-Platzierung und Pool-Optimierung abgegeben Workload Balancing zielt darauf ab, die Ressourcenauslastung auf einem Host unter den festgelegten kritischen Werten zu halten.

Metrische Gewichtungen einstellen

Wie Workload Balancing metrische Gewichtungen verwendet, um zu bestimmen, welche Hosts und VMs zuerst verarbeitet werden sollen, hängt vom Optimierungsmodus ab: Maximale Dichte oder Maximale Leistung. Im Allgemeinen werden Metrikgewichtungen verwendet, wenn sich ein Pool im Modus "Maximale Leistung"befindet. Wenn sich der Workloadausgleich jedoch im Modus "Maximale Dichte"befindet, werden metrische Gewichtungen verwendet, wenn eine Ressource den kritischen Schwellenwert überschreitet.

Wenn Workload Balancing Optimierungsempfehlungen verarbeitet, erstellt es einen Optimierungsauftrag. Der Workload Balancing bestimmt die Reihenfolge, indem die Hosts danach geordnet werden, welche Hosts die höchsten Metrikwerte für jede Ressource haben, die auf der Seite mit den Metrikgewichtungen als die wichtigste eingestuft wird.

Modus "Maximale Leistung"

Im Modus Maximale Leistung verwendet Workload Balancing metrische Gewichtungen, um Folgendes zu bestimmen:

- Auf welchen Hosts soll die Leistung zuerst adressiert werden
- Welche VMs sollten zuerst migriert werden

Wenn beispielsweise Network Writes die wichtigste Ressource ist, gibt Workload Balancing zunächst Optimierungsempfehlungen für den Host mit der höchsten Anzahl von Netzwerk-Schreibvorgängen pro Sekunde. Um Network Writes zur wichtigsten Ressource zu machen, bewegen Sie den Schieberegler **Metrische Gewichtung** nach rechts und alle anderen Schieberegler in die Mitte.

Wenn Sie alle Ressourcen so konfigurieren, dass sie gleich wichtig sind, adressiert der Workload Balancing zuerst die CPU-Auslastung und dann den Arbeitsspeicher, da diese Ressourcen normalerweise am stärksten eingeschränkt sind. Um alle Ressourcen gleich wichtig zu machen, legen Sie fest, dass der Schieberegler **Metrische Gewichtung** für alle Ressourcen an derselben Stelle ist.

Modus “Maximale Dichte”

Im Modus “Maximale Dichte”verwendet der Workload Balancing Metrik-Gewichtungen nur, wenn ein Host den kritischen Schwellenwert erreicht. Zu diesem Zeitpunkt wendet Workload Balancing einen Algorithmus an, der dem Algorithmus für maximale Leistung ähnelt, bis kein Host die kritischen Schwellenwerte überschreitet. Bei Verwendung dieses Algorithmus verwendet der Workload Balancing metrische Gewichtungen, um die Optimierungsreihenfolge auf die gleiche Weise zu bestimmen wie im Modus “Maximale Leistung”.

Wenn Ressourcen bei zwei oder mehr Hosts ihre kritischen Schwellenwerte überschreiten, überprüft Workload Balancing die Wichtigkeit, die Sie für jede Ressource festlegen. Es nutzt diese Wichtigkeit, um zu bestimmen, welcher Host zuerst optimiert werden soll und welche VMs auf diesem Host zuerst verlagert werden sollen.

Ihr Pool enthält beispielsweise Host A und Host B, die sich im folgenden Zustand befinden:

- Die CPU-Auslastung auf Host A überschreitet ihren kritischen Schwellenwert, und die metrische Gewichtung für die CPU-Auslastung ist auf **Wichtiger**gesetzt.
- Die Speicherauslastung auf Host B überschreitet ihren kritischen Schwellenwert, und die metrische Gewichtung für die Speichernutzung ist auf **Weniger wichtig**gesetzt.

Workload Balancing empfiehlt, zuerst Host A zu optimieren, da die Ressource, die den kritischen Schwellenwert erreicht hat, die Ressource ist, der das höchste Gewicht zugewiesen wurde. Nachdem Workload Balancing festgestellt hat, dass es die Leistung auf Host A berücksichtigen muss, empfiehlt Workload Balancing dann Platzierungen für VMs auf diesem Host. Es beginnt mit der VM mit der höchsten CPU-Auslastung, da diese CPU-Auslastung die Ressource mit dem höchsten Gewicht ist.

Nachdem Workload Balancing die Optimierung von Host A empfohlen hat, gibt es Optimierungsempfehlungen für Host B. Wenn es Platzierungen für die VMs auf Host B empfiehlt, geht es zuerst auf die CPU-Auslastung ein, da der CPU-Auslastung das höchste Gewicht zugewiesen wurde. Wenn mehr Hosts optimiert werden müssen, berücksichtigt der Workload Balancing die Leistung auf diesen Hosts entsprechend dem Host mit der dritthöchsten CPU-Auslastung.

Standardmäßig sind alle metrischen Gewichtungen auf den entferntesten Punkt des Schiebereglers eingestellt: Wichtiger.

> **Hinweis:**
>
> Die Gewichtung von Metriken ist relativ. Wenn alle Metriken auf dieselbe Ebene festgelegt sind, werden sie alle gleich gewichtet, auch wenn diese Ebene weniger wichtig ist. Die Beziehung der Metriken zueinander ist wichtiger als das tatsächliche Gewicht, mit dem Sie jede Metrik festlegen.

So bearbeiten Sie Metrikgewichtungsfaktoren

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Wählen Sie im linken Bereich **Metrische Gewichtung**aus.
5. Passen Sie auf der Seite **Metrische Gewichtung** die Schieberegler neben den einzelnen Ressourcen wie gewünscht an.

   Bewegen Sie den Schieberegler in Richtung **Weniger wichtig**, um anzuzeigen, dass es für diesen Pool nicht so wichtig ist, sicherzustellen, dass VMs immer über die höchste verfügbare Menge dieser Ressource verfügen.

Hosts von Empfehlungen ausschließen

Bei der Konfiguration von Workload Balancing können Sie angeben, dass bestimmte physische Hosts von den Optimierungs- und Platzierungsempfehlungen für den Workload Balancing ausgeschlossen werden, einschließlich Empfehlungen für die Platzierung am

Zu den Situationen, in denen Sie Hosts von Empfehlungen ausschließen möchten, gehören:

- Sie möchten den Pool im Modus “Maximale Dichte”ausführen und Hosts konsolidieren und herunterfahren, aber Sie möchten bestimmte Hosts von diesem Verhalten ausschließen.
- Sie haben zwei VM-Workloads, die immer auf demselben Host ausgeführt werden müssen. Zum Beispiel, wenn die VMs ergänzende Anwendungen oder Workloaden haben.
- Sie haben Workloaden, die Sie nicht verschieben möchten, z. B. einen Domänencontroller oder Datenbankserver.
- Sie möchten Wartungsarbeiten auf einem Host durchführen und möchten nicht, dass virtuelle Maschinen auf dem Host platziert werden.
- Die Leistung der Workload ist so kritisch, dass die Kosten für dedizierte Hardware irrelevant sind.

- Bestimmte Hosts führen Workloads mit hoher Priorität aus, und Sie möchten die HA-Funktion nicht verwenden, um diese VMs zu priorisieren.
- Die Hardware im Host ist nicht optimal für die anderen Workloads im Pool.

Unabhängig davon, ob Sie einen festen oder einen geplanten Optimierungsmodus angeben, bleiben ausgeschlossene Hosts ausgeschlossen, selbst wenn sich der Optimierungsmodus ändert. Wenn Sie also nur verhindern möchten, dass der Workload Balancing einen Host automatisch ausschaltet, sollten Sie stattdessen die Energieverwaltung für diesen Host deaktivieren. Weitere Informationen finden Sie unter Automatisches Optimieren und Verwalten der Energie.

Wenn Sie einen Host von den Empfehlungen ausschließen, geben Sie an, dass Workload Balancing diesen Host überhaupt nicht verwaltet. Diese Konfiguration bedeutet, dass Workload Balancing keine Optimierungsempfehlungen für einen ausgeschlossenen Host gibt. Wenn Sie dagegen keinen Host für die Teilnahme an der Energieverwaltung auswählen, verwaltet Workload Balancing den Host, gibt jedoch keine Energieverwaltungsempfehlungen für ihn ab.

Um Hosts vom Workload Balancing auszuschließen

Verwenden Sie dieses Verfahren, um einen Host in einem Pool, den Workload Balancing verwaltet, von Empfehlungen zur Energieverwaltung, Host-Evakuierung, Platzierung und Optimierung auszuschließen.

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Wählen Sie im linken Bereich **Ausgeschlossene Hosts**aus.
5. Wählen Sie auf der Seite **Ausgeschlossene Hosts** die Hosts aus, für die Workload Balancing keine alternativen Platzierungen und Optimierungen empfehlen soll.

Konfigurieren erweiterter Einstellungen

Workload Balancing bietet einige erweiterte Einstellungen, mit denen Sie steuern können, wie Workload Balancing automatisierte Empfehlungen anwendet. Diese Einstellungen werden auf der Seite **Erweitert** in der Konfiguration des Workload Balancing angezeigt. Führen Sie die folgenden Schritte aus, um zur Seite **Erweitert** zu gelangen:

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.

4. Wählen Sie im linken Bereich **Erweitert**aus.

In den folgenden Abschnitten werden die Verhaltensweisen beschrieben, die in den **erweiterten** Einstellungen konfiguriert werden können.

Festlegen konservativer oder aggressiver automatisierter Empfehlungen

Im automatisierten Modus ist die Häufigkeit der Optimierungs- und Konsolidierungsempfehlungen und wie schnell sie automatisch angewendet werden, auf mehrere Faktoren zurückzuführen, darunter:

- Wie lange Sie angeben, wartet der Workload Balancing nach dem Verschieben einer VM, bevor Sie eine weitere Empfehlung abgeben
- Die Anzahl der Empfehlungen, die Workload Balancing geben muss, bevor eine Empfehlung automatisch angewendet wird
- Der Schweregrad, den eine Empfehlung erreichen muss, bevor die Optimierung automatisch angewendet wird
- Das Maß an Konsistenz der Empfehlungen (empfohlene zu verschiebende VMs, Zielhosts), erfordert Workload Balancing, bevor Empfehlungen automatisch angewendet werden

Passen Sie die Einstellungen für diese Faktoren im Allgemeinen nur in den folgenden Fällen an:

- Sie erhalten Unterstützung vom technischen Support von XenServer
- Sie haben das Verhalten Ihres Pools mit aktiviertem Workload Balancing umfassend beobachtet und getestet.

Eine falsche Konfiguration dieser Einstellungen kann dazu führen, dass der Workload Balancing keine Empfehlungen abgibt.

VM-Migrationsintervall

Sie können angeben, wie viele Minuten der Workload Balancing nach dem letzten Verschieben einer VM wartet, bevor der Workload Balancing eine weitere Empfehlung für diese VM aussprechen kann. Das Empfehlungsintervall soll verhindern, dass Workload Balancing Empfehlungen aus künstlichen Gründen generiert, z. B. wenn es zu einer vorübergehenden Nutzungsspitze kam.

Wenn die Automatisierung konfiguriert ist, ist es besonders wichtig, beim Ändern des Empfehlungsintervalls vorsichtig zu sein. Wenn ein Problem auftritt, das zu kontinuierlichen, wiederkehrenden Spitzen führt, kann eine Verkürzung des Intervalls zu vielen Empfehlungen und damit zu Verlagerungen führen.

> **Hinweis:**
>
> Das Festlegen eines Empfehlungsintervalls hat keinen Einfluss darauf, wie lange Workload Balancing darauf wartet, kürzlich neu ausbalancierte Hosts in den Empfehlungen für Start-On-Platzierung, Wiederaufnahme und Wartungsmodus zu berücksichtigen.

Empfehlungsanzahl (Recommendation Count)

Alle zwei Minuten überprüft der Workload Balancing, ob er Empfehlungen für den überwachten Pool generieren kann. Wenn Sie die Automatisierung aktivieren, können Sie angeben, wie oft eine konsistente Empfehlung ausgesprochen werden muss, bevor der Workload Balancing die Empfehlung automatisch anwendet. Dazu konfigurieren Sie eine Einstellung, die als **Empfehlungsanzahl** bekannt ist, wie im Feld **Empfehlungen** angegeben. Mit der Einstellung **Empfehlungsanzahl** und der Einstellung **Optimierungsaggressivität** können Sie die automatisierte Anwendung von Empfehlungen in Ihrer Umgebung optimieren.

Der Workload Balancing verwendet die Ähnlichkeit der Empfehlungen, um die folgenden Überprüfungen durchzuführen:

1. Ob die Empfehlung wirklich benötigt wird
2. Ob der Zielhost über einen längeren Zeitraum stabil genug Leistung hat, um eine verlagerte VM zu akzeptieren, ohne sie in Kürze erneut vom Host entfernen zu müssen

Der Workload Balancing verwendet die Empfehlungsanzahl, um zu bestimmen, ob eine Empfehlung wiederholt werden muss, bevor der Workload Balancing die Empfehlung automatisch anwendet. Der Workload Balancing verwendet diese Einstellung wie folgt:

1. Jedes Mal, wenn der Workload Balancing eine Empfehlung generiert, die den Konsistenzanforderungen entspricht, wie in der Einstellung Optimierungsaggressivität angegeben, erhöht der Workload Balancing die Empfehlungsanzahl. Wenn die Empfehlung die Konsistenzanforderungen nicht erfüllt, setzt der Workload Balancing die Empfehlungsanzahl möglicherweise auf Null zurück. Dieses Verhalten hängt von den unter Optimierungsaggressivität beschriebenen Faktoren ab.
2. Wenn der Workload Balancing genügend konsistente Empfehlungen generiert, um den Wert für die Empfehlungsanzahl zu erfüllen, wie im Feld **Empfehlungen** angegeben, wird die Empfehlung automatisch angewendet.

Wenn Sie diese Einstellung ändern, variiert der festzulegenden Wert je nach Umgebung. Betrachten Sie diese Szenarien:

- Wenn die Hostlast und die Aktivität in Ihrer Umgebung schnell zunehmen, sollten Sie den Wert für die Anzahl der Empfehlungen erhöhen. Workload Balancing generiert alle zwei Minuten

Empfehlungen. Wenn Sie dieses Intervall beispielsweise auf **3**festlegen, wendet Workload Balancing sechs Minuten später die Empfehlung automatisch an.
- Wenn die Hostlast und die Aktivität in Ihrer Umgebung allmählich zunehmen, sollten Sie den Wert für die Anzahl der Empfehlungen verringern.

Das Akzeptieren von Empfehlungen verwendet Systemressourcen und beeinträchtigt die Leistung, wenn der Workload Balancing die VMs verlagert. Durch Erhöhen der Empfehlungsanzahl wird die Anzahl der übereinstimmenden Empfehlungen erhöht, die auftreten müssen, bevor der Workload Balancing die Empfehlung anwendet. Diese Einstellung regt den Workload Balancing an, konservativere, stabilere Empfehlungen anzuwenden, und kann das Potenzial für falsche VM-Verschiebungen verringern. Die Empfehlungsanzahl ist standardmäßig auf einen konservativen Wert festgelegt.

Aufgrund der möglichen Auswirkungen, die eine Anpassung dieser Einstellung auf Ihre Umgebung haben kann, sollten Sie sie nur mit äußerster Vorsicht ändern. Nehmen Sie diese Anpassungen vorzugsweise vor, indem Sie den Wert testen und iterativ ändern oder unter Anleitung des technischen Supports von XenServer.

Empfehlungsgewichtung

Alle Optimierungsempfehlungen enthalten eine Gewichtung (Kritisch, Hoch, Mittel, Niedrig), der die Bedeutung der Empfehlung angibt. Der Workload Balancing basiert bei dieser Bewertung auf einer Kombination von Faktoren, darunter die folgenden:

- Von Ihnen festgelegte Konfigurationsoptionen wie Schwellenwerte und metrische Tunings
- Für den Workload verfügbare Ressourcen
- Verlauf der Ressourcennutzung.

Die Gewichtung einer Empfehlung wird im Bereich **Optimierungsempfehlungen** auf der Registerkarte **WLB** angezeigt.

Wenn Sie den Workload Balancing so konfigurieren, dass Empfehlungen automatisch angewendet werden, können Sie die Mindestgewichtung festlegen, der einer Empfehlung zugeordnet werden soll, bevor der Workload Balancing ihn automatisch anwendet.

Optimierungsaggressivität

Um zusätzliche Sicherheit bei der Ausführung im automatisierten Modus zu bieten, verfügt der Workload Balancing über Konsistenzkriterien für die automatische Annahme von Optimierungen. Diese Kriterien können dazu beitragen, das Verschieben von VMs aufgrund von Spitzen und Anomalien zu verhindern. Im automatisierten Modus akzeptiert der Workload Balancing nicht die erste Empfehlung, die er erstellt. Stattdessen wartet Workload Balancing darauf, eine Empfehlung automatisch anzuwenden, bis ein Host oder eine VM im Laufe der Zeit ein konsistentes Verhalten

zeigt. Konsistentes Verhalten im Laufe der Zeit umfasst Faktoren wie die Frage, ob ein Host weiterhin Empfehlungen auslöst und ob dieselben VMs auf diesem Host weiterhin Empfehlungen auslösen.

Der Workload Balancing bestimmt, ob das Verhalten konsistent ist, indem Kriterien für die Konsistenz verwendet werden und Kriterien für die Anzahl, wie oft dieselbe Empfehlung ausgesprochen wird, verwendet werden. Mit der Einstellung **Optimierungsaggressivität** können Sie konfigurieren, wie genau der Workload Balancing die Konsistenzkriterien anwenden soll. Mit dieser Einstellung können Sie die gewünschte Stabilität in Ihrer Umgebung steuern, bevor der Workload Balancing eine Optimierungsempfehlung anwendet. Die stabilste Einstellung, Niedrige Aggressivität, ist standardmäßig konfiguriert. In diesem Zusammenhang bedeutet der Begriff stabil die Ähnlichkeit der empfohlenen Änderungen im Laufe der Zeit, wie in diesem Abschnitt erläutert. Aggressivität ist in den meisten Umgebungen nicht erwünscht. Daher ist Niedrig die Standardeinstellung.

Der Workload Balancing verwendet bis zu vier Kriterien, um die Konsistenz zu ermitteln. Die Anzahl der Kriterien, die erfüllt werden müssen, hängt von der Ebene ab, die Sie in der Einstellung **Optimierungsaggressivität** festgelegt haben. Je niedriger die Stufe (z. B. Niedrig oder Mittel), desto weniger aggressiv ist der Workload Balancing, wenn es darum geht, eine Empfehlung zu akzeptieren. Mit anderen Worten: Beim Workload Balancing müssen die Kriterien strenger erfüllt werden, wenn die Aggressivität auf Niedrig festgelegt ist.

Wenn die Aggressivitätsstufe beispielsweise auf Niedrig festgelegt ist, muss jedes Kriterium für Niedrig so oft erfüllt sein, wie im Wert von Recommendation Count angegeben wird, bevor die Empfehlung automatisch angewendet wird.

Wenn Sie die Empfehlungsanzahl auf **3**festlegen, wartet der Workload Balancing, bis alle für Niedrig aufgeführten Kriterien erfüllt sind, und wird in drei aufeinanderfolgenden Empfehlungen wiederholt. Mit dieser Einstellung wird sichergestellt, dass die VM tatsächlich verschoben werden muss und dass der empfohlene Zielhost über einen längeren Zeitraum eine stabile Ressourcennutzung aufweist. Dadurch wird die Wahrscheinlichkeit verringert, dass eine kürzlich verschobene VM aufgrund von Änderungen der Host-Leistung nach dem Umzug von einem Host verschoben wird. Standardmäßig ist diese Einstellung auf Niedrig eingestellt, um die Stabilität zu fördern.

Es wird nicht empfohlen, die Einstellung **Optimierungsaggressivität** zu erhöhen, um die Häufigkeit zu erhöhen, mit der Ihre Hosts optimiert werden. Wenn Sie der Meinung sind, dass Ihre Hosts nicht schnell oder häufig genug optimiert werden, versuchen Sie, die kritischen Schwellenwerte anzupassen. Vergleichen Sie die Schwellenwerte mit dem Bericht “Poolintegrität”.

Die mit den verschiedenen Aggressivitätsstufen verbundenen Konsistenzkriterien sind folgende:

Niedrig:

- Alle VMs in nachfolgenden Empfehlungen müssen identisch sein (wie durch übereinstimmende UUIDs in jeder Empfehlung gezeigt wird).
- In nachfolgenden Empfehlungen müssen alle Zielhosts identisch sein

- Die Empfehlung, die unmittelbar auf die ursprüngliche Empfehlung folgt, muss übereinstimmen, andernfalls wird die Anzahl der Empfehlungen auf 1 zurückgesetzt.

Mittel:

- Alle VMs in nachfolgenden Empfehlungen müssen von demselben Host stammen. Sie können sich jedoch von den VMs in der ersten Empfehlung unterscheiden.
- In nachfolgenden Empfehlungen müssen alle Zielhosts identisch sein
- Eine der nächsten beiden Empfehlungen, die unmittelbar auf die erste Empfehlung folgt, muss übereinstimmen, andernfalls wird die Anzahl der Empfehlungen auf 1 zurückgesetzt.

Hoch:

- Alle VMs in den Empfehlungen müssen von demselben Host stammen. Die Empfehlungen müssen jedoch nicht sofort aufeinander folgen.
- Der Host, von dem Workload Balancing die Verschiebung der VM empfohlen hat, muss in jeder Empfehlung derselbe sein
- Die Anzahl der Empfehlungen bleibt auf demselben Wert, auch wenn die beiden Empfehlungen, die der ersten Empfehlung folgen, nicht übereinstimmen.

Beispiel für Optimierungsaggressivität Das folgende Beispiel veranschaulicht, wie der Workload Balancing die Einstellung **Optimierungsaggressivität** und die Anzahl der Empfehlungen verwendet, um zu bestimmen, ob eine Empfehlung automatisch akzeptiert werden soll.

Jede vom Workload Balancing ausgegebene Optimierungsempfehlung schlägt drei VM-Platzierungen vor. Nach diesen vorgeschlagenen Positionierungen entspricht die Anzahl der Empfehlungen, die mit jeder Aggressivitätsstufe verknüpft sind, wie oft es aufeinanderfolgende Empfehlungen für diese Einstellung der Optimierungsaggressivität gegeben hat.

Wenn in den folgenden Beispielen die Einstellung **Optimierungsaggressivität** auf Hoch festgelegt ist, steigt die Anzahl der Empfehlungen nach Empfehlung 1, 2 und 3 weiter an. Diese Erhöhung tritt auf, obwohl dieselben VMs nicht in jeder Empfehlung für neue Platzierungen empfohlen werden. Workload Balancing wendet die Platzierungsempfehlung mit Empfehlung 3 an, da bei drei aufeinanderfolgenden Empfehlungen dasselbe Verhalten von diesem Host festgestellt wurde.

Im Gegensatz dazu erhöht sich die Anzahl der aufeinanderfolgenden Empfehlungen bei Einstellung auf Niedrige Aggressivität nicht für die ersten vier Empfehlungen. Die Empfehlungsanzahl wird bei jeder Empfehlung auf 1 zurückgesetzt, da dieselben VMs nicht für Platzierungen empfohlen wurden. Die Empfehlungsanzahl beginnt nicht zu steigen, bis dieselbe Empfehlung in Empfehlung #5 ausgesprochen wurde. Schließlich wendet der Workload Balancing automatisch die Empfehlung in Empfehlung #6 an, nachdem es zum dritten Mal dieselben Platzierungsempfehlungen ausgibt.

Empfehlung 1:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host B verschieben
- VM5 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl hohe Aggressivität: 1
- Empfehlungsanzahl mittlere Aggressivität: 1
- Empfehlungsanzahl niedrige Aggressivität: 1

Empfehlung 2:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host C verschieben
- VM7 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl hohe Aggressivität: 2
- Empfehlungsanzahl mittlere Aggressivität: 1
- Empfehlungsanzahl niedrige Aggressivität: 1

Empfehlung 3:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host C verschieben
- VM5 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl hohe Aggressivität: 3 (anwenden)
- Empfehlungsanzahl mittlere Aggressivität: 1
- Empfehlungsanzahl niedrige Aggressivität: 1

Empfehlung 4:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host B verschieben
- VM5 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl mittlere Aggressivität: 2
- Empfehlungsanzahl niedrige Aggressivität: 1

Empfehlung 5:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host B verschieben
- VM5 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl mittlere Aggressivität: 3 (Anwenden)
- Empfehlungsanzahl niedrige Aggressivität: 2

Empfehlung 6:

Vorgeschlagene Platzierungen:

- VM1 von Host A auf Host B verschieben
- VM3 von Host A auf Host B verschieben
- VM5 von Host A auf Host C verschieben

Empfehlungsanzahl:

- Empfehlungsanzahl niedrige Aggressivität: 3 (Anwenden)

Konfigurieren von VM-Empfehlungsintervallen

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Erweitert**.
5. Führen Sie im Abschnitt **VM-Empfehlungsintervall** eine oder mehrere der folgenden Aktionen aus:

    - Geben Sie im Feld **Minuten** einen Wert für die Anzahl der Minuten ein, die Workload Balancing wartet, bevor er eine weitere Optimierungsempfehlung für einen neu ausbalancierten Host ausgibt.
    - Geben Sie im Feld **Empfehlungen** einen Wert für die Anzahl der Empfehlungen ein, die der Workload Balancing aussprechen soll, bevor eine Empfehlung automatisch angewendet wird.

- Wählen Sie einen Mindestschweregrad aus, bevor Optimierungen automatisch angewendet werden.
- Ändern Sie, wie aggressiv Workload Balancing Optimierungsempfehlungen anwendet, wenn es im automatisierten Modus ausgeführt wird. Durch die Erhöhung der Aggressivität werden Einschränkungen hinsichtlich der Konsistenz der Empfehlungen reduziert, bevor sie automatisch angewendet werden. Die Einstellung **Optimierungsaggressivität** ergänzt direkt die Einstellung **Empfehlungen**, d. h. die Empfehlungsanzahl.

  > **Hinweis:**
  >
  > Wenn Sie in der Einstellung **Empfehlungen** den Wert "1"eingeben, ist die Einstellung **Optimierungsaggressivität** nicht relevant.

Anpassen der Granularitätseinstellungen der Poolauditliste

Gehen Sie wie folgt vor, um die Granularitätseinstellungen zu ändern:

1. Wählen Sie in XenCenter Ihren Pool aus.
2. Klicken Sie im Bereich **Eigenschaften** des Pools auf die Registerkarte **WLB**.
3. Klicken Sie auf der Registerkarte **WLB** auf **Einstellungen**.
4. Klicken Sie im linken Bereich auf **Erweitert**.
5. Klicken Sie auf der Seite **Erweitert** auf die Liste **Granularität des Poolauditlistenberichts**, und wählen Sie eine Option aus der Liste aus.

   > **Wichtig:**
   >
   > Wählen Sie die Granularität basierend auf den Anforderungen Ihres Auditprotokolls aus. Wenn Sie beispielsweise die Granularität Ihres Überwachungsprotokollberichts auf Minimum festlegen, erfasst der Bericht nur eine begrenzte Datenmenge für bestimmte Benutzer und Objekttypen. Wenn Sie die Granularität auf Mittelfestlegen, bietet der Bericht einen benutzerfreundlichen Bericht des Überwachungsprotokolls. Wenn Sie die Granularität auf Maximum festlegen, enthält der Bericht detaillierte Informationen zum Auditprotokollbericht. Das Festlegen des Überwachungsprotokollberichts auf Maximum kann dazu führen, dass der Workload Balancing-Server mehr Speicherplatz und Arbeitsspeicher beansprucht.

6. Um Ihre Änderungen zu bestätigen, klicken Sie auf **OK**.

Pool Audit Trail-Berichte anzeigen, die auf Objekten in XenCenter basieren

Gehen Sie wie folgt vor, um Berichte über den Poolauditliste basierend auf dem ausgewählten Objekt auszuführen und anzuzeigen:

1. Nachdem Sie die Granularitätseinstellung Pool Audit Trail festgelegt haben, klicken Sie auf **Berichte.** Die Seite Workload-Berichte wird angezeigt.
2. Wählen Sie im linken Bereich **Pool Audit Trail** aus.
3. Sie können die Berichte basierend auf einem bestimmten Objekt ausführen und anzeigen, indem Sie es aus der **Objektliste** auswählen. Wählen Sie beispielsweise **Host** aus der Liste aus, um die Berichte nur auf der Grundlage des Hosts zu erhalten.

Passen Sie die vom Pool Audit Trail erfassten Ereignisse, Objekte und Aktionen an

Um die vom Pool Audit Trail erfassten Ereignisobjekte und Aktionen anzupassen, müssen Sie sich bei der PostgreSQL-Datenbank auf der virtuellen Workload Balancing-Appliance anmelden, die entsprechenden Änderungen an der Liste der Ereignisobjekte oder Aktionen vornehmen und dann die virtuelle Workload Balancing-Appliance neu starten.

Melden Sie sich bei der PostgreSQL-Datenbank an

1. Melden Sie sich an der Konsole der virtuellen Workload Balancing-Appliance an.
2. Führen Sie den folgenden Befehl aus:

```
psql -Upostgres -dWorkloadBalancing
<!--NeedCopy-->
```

3. Geben Sie das Datenbankkennwort ein. Sie haben das Datenbankkennwort festgelegt, als Sie den Workload Balancing-Konfigurationsassistenten ausgeführt haben, nachdem Sie die virtuelle Appliance importiert haben.

Eventobjekte anpassen

> **Hinweis:**
>
> Stellt in der folgenden Befehlssyntax den Namen des Ereignisobjekts `event_object` dar, das Sie hinzufügen, aktualisieren oder deaktivieren möchten.

Aktivieren Sie ein Event-Objekt:

```
select * from update_audit_log_objects('event_object', true);
<!--NeedCopy-->
```


Deaktivieren Sie ein Event-Objekt:

```
select * from update_audit_log_objects('event_object', false);
<!--NeedCopy-->
```

Ruft eine Liste der Event-Objekte ab, die derzeit deaktiviert sind:

```
select * from hv_audit_log_get_event_objects(false);
<!--NeedCopy-->
```

Ruft eine Liste der Event-Objekte ab, die derzeit aktiviert sind:

```
select * from hv_audit_log_get_event_objects(true);
<!--NeedCopy-->
```

Event-Aktionen anpassen

> **Hinweis:**
>
> Stellt in der folgenden Befehlssyntax den Namen der Ereignisaktion `event_action` dar, die Sie hinzufügen, aktualisieren oder deaktivieren möchten.

Aktiviere eine Event-Aktion:

```
select * from update_audit_log_actions('event_action', true);
<!--NeedCopy-->
```

Deaktivieren Sie eine Event-Aktion:

```
select * from update_audit_log_actions('event_action', false);
<!--NeedCopy-->
```

Ruft eine Liste der Event-Aktionen ab, die derzeit deaktiviert sind:

```
select * from hv_audit_log_get_event_actions(false);
<!--NeedCopy-->
```

Ruft eine Liste der Event-Aktionen ab, die derzeit aktiviert sind:

```
select * from hv_audit_log_get_event_actions(true);
<!--NeedCopy-->
```

Starten Sie die virtuelle Workload Balancing-Appliance neu Führen Sie die folgenden Befehle aus, um PostgreSQL zu beenden und die virtuelle Workload Balancing-Appliance neu zu starten.

```
\q
<!--NeedCopy-->
```

```
systemctl restart workloadbalancing
<!--NeedCopy-->
```


Warnstufe für Workload Balancing-Warnungen in XenCenter festlegen

Sie können die Warnstufe für Workload Balancing-Warnungen in XenCenter mithilfe der Management-API festlegen.

Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl auf dem Poolkoordinator aus, um die Warnstufe für jeden Warncode festzulegen:

   ```
   xe pool-send-wlb-configuration config:<wlb-alert-code>=<alert-
      level>
   <!--NeedCopy-->
   ```

   Die 4 `wlb-alert-code`-Typen sind:

   - MESSAGE_PRIORITY_WLB_OPTIMIZATION_ALERT —Wenn Workload Balancing eine Optimierungsempfehlung gibt, wird diese Warnung ausgelöst.
   - MESSAGE_PRIORITY_WLB_VM_RELOCATION —Wenn Workload Balancing eine VM auf einen anderen Host verlagert, wird diese Warnung ausgelöst.
   - MESSAGE_PRIORITY_WLB_HOST_POWER_OFF —Wenn der Optimierungsmodus für den Workload Balancing auf `Maximize Density` festgelegt wurde und ein Host ausgeschaltet ist, weil auf dem Host keine VMs ausgeführt werden, wird diese Warnung ausgelöst.
   - MESSAGE_PRIORITY_WLB_HOST_POWER_ON —Wenn der Optimierungsmodus für den Workload Balancing auf `Maximize Performance` festgelegt wurde und ein Host eingeschaltet ist, weil dadurch die Hostleistung verbessert wird, wird diese Warnung ausgelöst.

   Die 6 `alert-level`-Typen sind:

   - 0 - Mute the alert
   - 1 - Critical
   - 2 - Major
   - 3 - Warnung
   - 4 - Minor
   - 5 - Informativ

2. Führen Sie den folgenden Befehl auf dem Poolkoordinator aus, um die für die Warncodes festgelegten Warnstufen anzuzeigen:

   ```
   xe pool-retrieve-wlb-configuration
   <!--NeedCopy-->
   ```

3. Um die Warnungen zu testen, lösen Sie eine Workload Balancing-Warnung aus und klicken Sie dann auf das `Notifications`-Panel, um die Warnung anzuzeigen.

Verwalten des Arbeitslastausgleichs

November 9, 2023

Nachdem der Workload Balancing eine Weile ausgeführt wurde, müssen Sie möglicherweise Routineaufgaben ausführen, damit der Workload Balancing optimal ausgeführt wird. Möglicherweise müssen Sie diese Aufgaben aufgrund von Änderungen an Ihrer Umgebung (z. B. unterschiedliche IP-Adressen oder Anmeldeinformationen), Hardwareaktualisierungen oder routinemäßiger Wartung ausführen.

Verbinden mit der virtuellen Workload Balancing-Appliance

Verbinden Sie nach der Konfiguration des Workload Balancings den Pool, den Sie verwalten möchten, über die CLI oder XenCenter mit der virtuellen Workload Balancing-Appliance. Ebenso müssen Sie möglicherweise irgendwann erneut eine Verbindung zu derselben virtuellen Appliance herstellen.

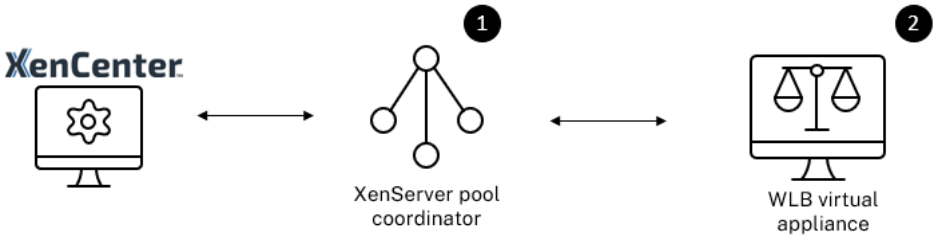
Um einen Pool mit Ihrer virtuellen Workload Balancing-Appliance zu verbinden, benötigen Sie die folgenden Informationen:

- IP-Adresse oder FQDN der virtuellen Workload Balancing-Appliance
  - So rufen Sie die IP-Adresse für die virtuelle Workload Balancing-Appliance ab:
    1. Wechseln Sie in XenCenter zur Registerkarte Workload Balancing Virtual Appliance **Console** .
    2. Melden Sie sich als `root` mit dem root-Kennwort an, das Sie beim Importieren der Appliance erstellt haben.
    3. Führen Sie den folgenden Befehl aus: `ifconfig`.
  - Um den FQDN für den Workload Balancing anzugeben, wenn Sie eine Verbindung zum Workload Balancing-Server herstellen, fügen Sie zuerst den Hostnamen und die IP-Adresse Ihrem DNS-Server hinzu.
- Die Portnummer der virtuellen Workload Balancing-Appliance. Standardmäßig stellt XenServer eine Verbindung zu Workload Balancing auf Port 8012 her.

  Bearbeiten Sie die Portnummer nur, wenn Sie sie während der Konfiguration des Arbeitslastausgleichs geändert haben. Die Portnummer, die während der Konfiguration des Arbeitslastausgleichs, in allen Firewallregeln und im Dialogfeld Mit WLB Server verbinden angegeben wurde, muss übereinstimmen.
- Anmeldeinformationen für den Ressourcenpool, den der Workload Balancing überwachen soll.

- Anmeldeinformationen für das Workload Balancing-Konto, das Sie während der Workload Balancing-Konfiguration erstellt haben

  Dieses Konto wird oft als Arbeitslastausgleich-Benutzerkonto bezeichnet. XenServer verwendet dieses Konto für die Kommunikation mit Workload Balancing. Sie haben dieses Konto während der Konfiguration des Arbeitslastausgleichs auf der virtuellen Appliance für den Arbeitslastausgleich erstellt



Wenn Sie zum ersten Mal eine Verbindung mit dem Workload Balancing herstellen, werden die Standardschwellenwerte und -einstellungen für den Ausgleich von Arbeitslasten verwendet. Automatische Funktionen wie automatisierter Optimierungsmodus, Energieverwaltung und Automatisierung sind standardmäßig deaktiviert.

Mit Zertifikaten arbeiten

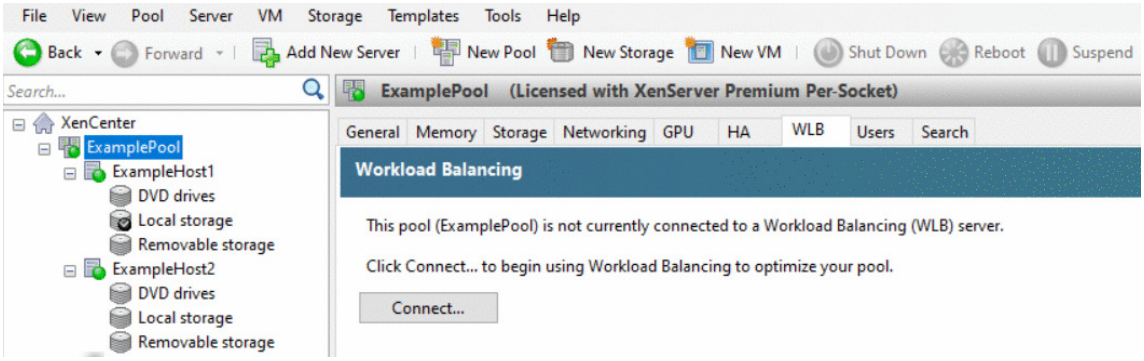
Wenn Sie ein anderes (vertrauenswürdiges) Zertifikat hochladen oder die Zertifikatsüberprüfung konfigurieren möchten, beachten Sie Folgendes, bevor Sie Ihren Pool mit dem Workload Balancing verbinden:

- Wenn Sie möchten, dass XenServer das selbstsignierte Workload Balancing-Zertifikat überprüft, müssen Sie die Workload Balancing-IP-Adresse verwenden, um eine Verbindung zum Workload Balancing herzustellen. Das selbstsignierte Zertifikat wird basierend auf seiner IP-Adresse für den Workload Balancing ausgestellt.
- Wenn Sie ein Zertifikat einer Zertifizierungsstelle verwenden möchten, ist es einfacher, den FQDN anzugeben, wenn Sie eine Verbindung zum Workload Balancing herstellen. Sie können jedoch im Dialog Mit **WLB Server verbinden** eine statische IP-Adresse angeben. Verwenden Sie diese IP-Adresse als alternativen Subject Name (SAN) im Zertifikat.

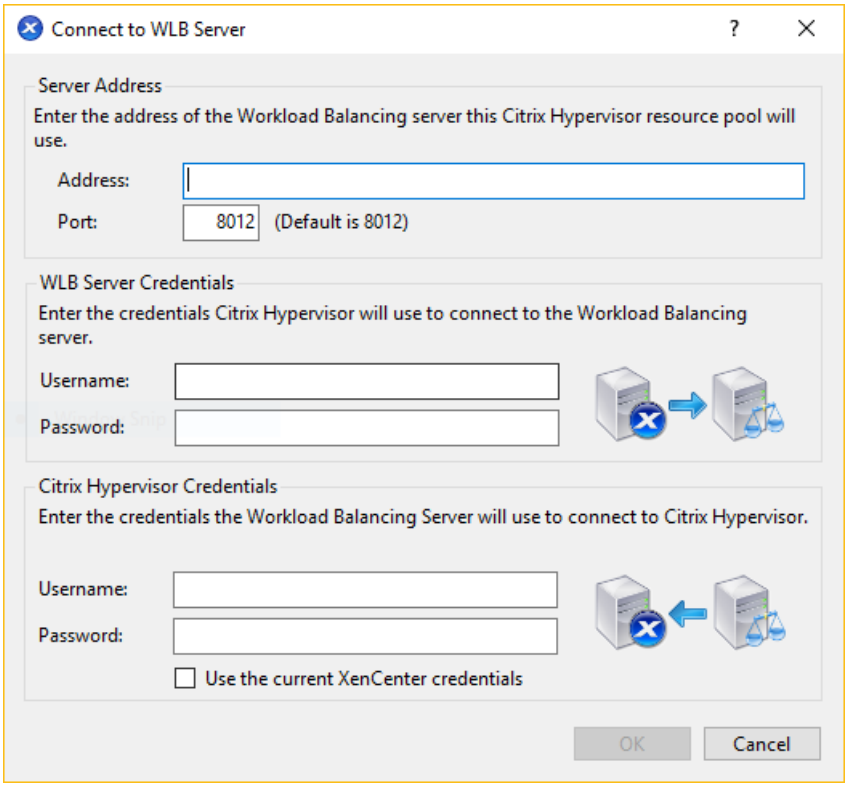
Weitere Informationen finden Sie unter Zertifikate.

So verbinden Sie Ihren Pool mit der virtuellen Workload Balancing-Appliance

1. Wählen Sie in XenCenter Ihren Ressourcenpool aus und klicken Sie im Bereich **Eigenschaften** auf die Registerkarte **WLB** . Auf der Registerkarte **WLB** wird die Schaltfläche **Verbinden** angezeigt.



2. Klicken Sie auf der Registerkarte **WLB** auf **Verbinden**. Das Dialogfeld Mit **WLB Server verbinden** wird angezeigt.



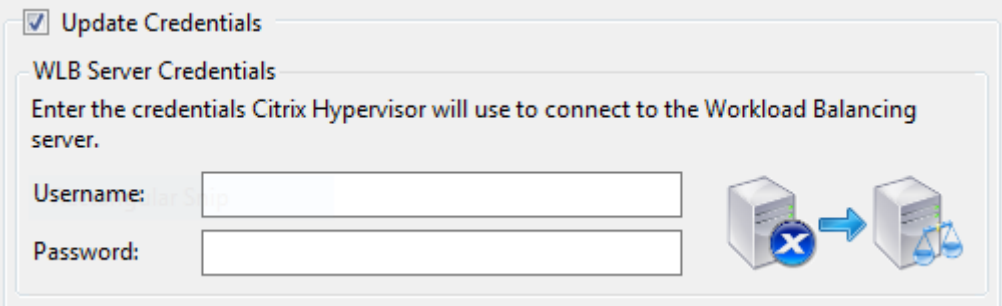
3. Geben Sie im Abschnitt **Serveradresse** Folgendes ein:

   a) Geben Sie in das Feld **Adresse** die IP-Adresse oder den FQDN der virtuellen Workload Balancing-Appliance ein. Beispiel: `WLB-appliance-computername.yourdomain.net`.

   b) (Optional) Wenn Sie den Workload Balancing-Port während der Konfiguration des Workload Balancings geändert haben, geben Sie die Portnummer in das Feld **Port** ein. XenServer verwendet diesen Port für die Kommunikation mit Workload Balancing.

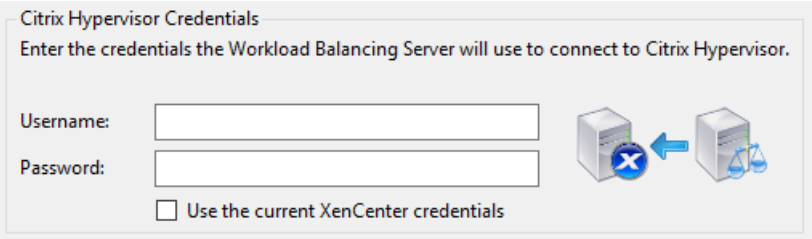
      Standardmäßig stellt XenServer eine Verbindung zu Workload Balancing auf Port 8012 her.

4. Geben Sie im Abschnitt **WLB Server-Anmeldeinformationen** den Benutzernamen und das Kennwort ein, die der Pool für die Verbindung mit der virtuellen Workload Balancing-Appliance verwendet.



   Diese Anmeldeinformationen müssen für das Konto gelten, das Sie während der Konfiguration des Workload Balancings erstellt haben. Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`.

5. Geben Sie im Abschnitt **Citrix Hypervisor Credentials** den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren. Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung zu den Hosts in diesem Pool herzustellen.



   Um die Anmeldeinformationen zu verwenden, mit denen Sie derzeit bei XenServer angemeldet sind, wählen Sie **Aktuelle XenCenter-Anmeldeinformationen verwenden**aus. Wenn Sie diesem Konto mithilfe der Funktion der rollenbasierten Zugriffssteuerung (RBAC) eine Rolle zugewiesen haben, stellen Sie sicher, dass die Rolle über ausreichende Berechtigungen zum Konfigurieren des Arbeitslastausgleichs verfügt. Weitere Informationen finden Sie unter Zugriffssteuerungsberechtigungen für den Arbeitslastausgleich.

Nachdem Sie den Pool mit der virtuellen Appliance Workload Balancing verbunden haben, beginnt der Workload Balancing automatisch mit der Überwachung des Pools mit den Standardoptimierungseinstellungen. Wenn Sie diese Einstellungen ändern oder die Priorität für Ressourcen ändern möchten, warten Sie, bis das XenCenter Log anzeigt, dass die Discovery abgeschlossen ist, bevor Sie fortfahren.

> **Wichtig:**
>
> Wenn der Workload Balancing eine Zeit lang ausgeführt wurde und Sie keine optimalen Empfehlungen erhalten, bewerten Sie Ihre Leistungsschwellenwerte wie unter Konfigurieren

> des Verhaltens des Arbeitslastausgleichsbeschrieben. Es ist wichtig, den Workload-Balancing auf die richtigen Schwellenwerte für Ihre Umgebung festzulegen, da die Empfehlungen möglicherweise nicht angemessen sind.

Zugriffsberechtigungen für den Arbeitslastausgleich

Wenn die rollenbasierte Zugriffssteuerung (RBAC) in Ihrer Umgebung implementiert ist, können alle Benutzerrollen die Registerkarte **WLB** anzeigen. Nicht alle Rollen können jedoch alle Vorgänge ausführen. In der folgenden Tabelle sind die Rollen aufgeführt, die Administratoren mindestens benötigen, um Workload Balancing-Funktionen zu verwenden

Berechtigung	Mindestens erforderliche Rolle
Konfigurieren, Initialisieren, Aktivieren, Deaktivieren von WLB	Poolbetreiber
WLB-Optimierungsempfehlungen auf der Registerkarte WLB anwenden	Poolbetreiber
Ändern von WLB-Berichtsabonnements	Poolbetreiber
Akzeptieren Sie die WLB-Plat	VM Power Admin
Generieren von WLB-Berichten einschließlich des Poolauditlistenberichts	Lesezugriff
WLB-Konfiguration anzeigen	Lesezugriff

In der folgenden Tabelle finden Sie weitere Informationen zu Berechtigungen.

Berechtigung	Erlaubt dem Empfänger zu
Konfigurieren, Initialisieren, Aktivieren, Deaktivieren von WLB	Konfiguration WLB
	WLB initialisieren und WLB-Server ändern
	WLB aktivieren
	WLB deaktivieren
WLB-Optimierungsempfehlungen auf der Registerkarte WLB anwenden	Wenden Sie alle Optimierungsempfehlungen an, die auf der Registerkarte **WLB** erscheinen
Ändern von WLB-Berichtsabonnements	Ändern des erzeugten WLB-Berichts oder seines Empfängers
Akzeptieren Sie die WLB-Plat	Wählen Sie einen der Hosts aus, die Workload Balancing für die Platzierung empfiehlt

Berechtigung	Erlaubt dem Empfänger zu
Generieren von WLB-Berichten einschließlich des Poolauditlistenberichts	Anzeigen und Ausführen von WLB-Berichten, einschließlich des Poolauditlistenberichts
WLB-Konfiguration anzeigen	Zeigen Sie die WLB-Einstellungen für einen Pool an, wie auf der Registerkarte WLB angezeigt

Wenn ein Benutzer versucht, den Workload Balancing zu verwenden, und dieser Benutzer nicht über ausreichende Berechtigungen verfügt, wird ein Dialogfeld mit Rollenerhöhung angezeigt. Weitere Informationen zu RBAC finden Sie unter Rollenbasierte Zugriffssteuerung.

Konfigurieren Sie einen Pool neu, um eine andere virtuelle Workload Balancing-Appliance

Sie können einen Ressourcenpool neu konfigurieren, um eine andere virtuelle Workload Balancing-Appliance zu verwenden.

Wenn Sie von einer älteren Version der virtuellen Workload Balancing-Appliance auf die neueste Version umsteigen, können Sie vor dem Trennen der alten virtuellen Appliance deren Daten auf die neue Version der virtuellen Appliance migrieren. Weitere Informationen finden Sie unter Migrieren von Daten von einer vorhandenen virtuellen Appliance.

Nachdem Sie einen Pool von der alten virtuellen Workload Balancing-Appliance getrennt haben, können Sie den Pool verbinden, indem Sie den Namen der neuen virtuellen Workload Balancing-Appliance angeben.

So verwenden Sie eine andere virtuelle Workload Balancing-Appliance:

1. (Optional) Migrieren Sie Daten von einer älteren Version der virtuellen Appliance. Weitere Informationen finden Sie unter Migrieren von Daten von einer vorhandenen virtuellen Appliance.
2. Wählen Sie in XenCenter im Menü **Pool** die Option **Workload Balancing Server trennen** und klicken Sie auf **Trennen, wenn Sie** dazu aufgefordert werden.
3. Klicken Sie auf der Registerkarte **WLB** auf **Verbinden**. Das Dialogfeld Mit **WLB Server verbinden** wird angezeigt.
4. Stellen Sie eine Verbindung zur neuen virtuellen Appliance her. Weitere Informationen finden Sie unter Verbinden mit der virtuellen Workload Balancing-Appliance

Ändern der Workload Balancing-Anmeldeinformationen

Wenn Sie nach der Erstkonfiguration die Anmeldeinformationen aktualisieren möchten, die XenServer und die Workload Balancing-Appliance für die Kommunikation verwenden, gehen Sie wie

folgt vor:

1. Um den Workload Balancing anzuhalten, wechseln Sie zur Registerkarte **WLB** und klicken Sie auf **Pause**.
2. Ändern Sie die Workload Balancing-Anmeldeinformationen, indem Sie den Befehl `wlbconfig` ausführen. Weitere Informationen finden Sie unter Befehle für den Arbeitslastausgleich.
3. Aktivieren Sie Workload Balancing erneut und geben Sie die neuen Anmeldeinformationen an
4. Nachdem der Fortschrittsbalken abgeschlossen ist, klicken Sie auf **Verbinden**.

   Das Dialogfeld Mit **WLB Server verbinden** wird angezeigt.
5. Klicken Sie auf **Anmeldeinformationen aktualisieren**.
6. Ändern Sie im Abschnitt **Serveradresse** die folgenden Einstellungen nach Bedarf:

   - Geben Sie in das Feld **Adresse** die IP-Adresse oder den FQDN der Workload Balancing-Appliance ein.
   - (Fakultativ.) Wenn Sie die Portnummer während der Konfiguration des Arbeitslastausgleichs geändert haben, geben Sie diese Portnummer ein. Die Portnummer, die Sie in diesem Feld und während der Workload Balancing-Konfiguration angeben, ist die Portnummer, die XenServer verwendet, um eine Verbindung zum Workload Balancing herzustellen.

     Standardmäßig stellt XenServer eine Verbindung zu Workload Balancing auf Port 8012 her.

     > **Hinweis:**
     >
     > Bearbeiten Sie diese Portnummer nur, wenn Sie sie bei der Ausführung des Konfigurations-Assistenten für den Workload Balancing geändert haben. Der Portnummernwert, der beim Ausführen des Workload Balancing-Konfigurationsassistenten und des Dialogfelds Mit WLB Server verbinden angegeben wurde, muss übereinstimmen.
7. Geben Sie im Abschnitt **WLB-Serveranmeldedaten** den Benutzernamen (z. B. `wlbuser`) und das Kennwort ein, mit dem XenServer eine Verbindung zum Workload Balancing-Server herstellt.
8. Geben Sie im Abschnitt **Citrix Hypervisor Credentials** den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren (normalerweise das Kennwort für den Poolkoordinator). Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung zu den Computern herzustellen, auf denen XenServer in diesem Pool ausgeführt wird.
9. Geben Sie im Abschnitt **Citrix Hypervisor Credentials** den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren. Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung zu den Computern herzustellen, auf denen XenServer in diesem Pool ausgeführt wird.

Um die Anmeldeinformationen zu verwenden, mit denen Sie derzeit bei XenServer angemeldet sind, wählen Sie **Aktuelle XenCenter-Anmeldeinformationen verwenden**aus.

Ändern der Workload Balancing IP-Adresse

Gehen Sie wie folgt vor, um die Workload Balancing-IP-Adresse zu ändern:

1. Um die aktuelle Workload Balancing-IP-Adresse anzuzeigen, führen Sie den Befehl `ifconfig` auf der virtuellen Appliance aus.
2. Öffnen Sie die Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` mit einem Bearbeitungstool wie vi.
3. Um das Protokoll von dhcp in static zu ändern, ändern Sie `BOOTPROTO=dhcp` in `BOOTPROTO=static`.
4. Geben Sie am Ende der Datei die IP-Adresse, die Netzmaske, das Gateway und die DNS-Adressen ein. Beispiel:

```
IPADDR=192.168.1.100
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=1.1.1.1
DNS2=8.8.8.8
<!--NeedCopy-->
```

> **Hinweis:**
>
> Fügen Sie so viele DNS-Einträge hinzu, wie Sie benötigen.

5. Speichern und schließen Sie die Datei.
6. Damit die Änderungen wirksam werden, müssen Sie das Netzwerksystem neu starten, indem Sie `systemctl restart network` ausführen.
7. Führen Sie nach dem Neustart des Netzwerksystems den Befehl `ifconfig` erneut aus, um die neue Workload Balancing-IP-Adresse anzuzeigen.
8. Führen Sie den Befehl `systemctl status workloadbalancing` aus, um zu überprüfen, ob der Workload Balancing-Dienst normal läuft.

   Wenn das zurückgegebene Ergebnis `Active: active (running)` enthält, läuft der Workload Balancing-Dienst normal. Wenn das Ergebnis `Active: inactive (dead)` oder einen anderen Status enthält, wird der Workload Balancing möglicherweise abnormal beendet.

Ändern der Konfiguration der virtuellen Workload Balancing-Appliance

Wenn Sie die virtuelle Workload Balancing-Appliance zum ersten Mal installieren, hat sie die folgende Standardkonfiguration:

Konfiguration	Value
Anzahl der vCPUs	2
Speicher (RAM)	2 GB
Speicherplatz	30 GB

Diese Werte sind für die meisten Umgebungen geeignet. Wenn Sie sehr große Pools überwachen, sollten Sie erwägen, diese Werte zu erhöhen.

Ändern der Anzahl der vCPUs, die der virtuellen Appliance zugewiesen sind

Standardmäßig werden der virtuellen Workload Balancing-Appliance 2 vCPUs zugewiesen. Dieser Wert ist ausreichend für Pools, die 1000 virtuelle Maschinen hosten. Sie müssen es normalerweise nicht erhöhen. Reduzieren Sie nur die Anzahl der vCPUs, die der virtuellen Appliance zugewiesen sind, wenn Sie über eine kleine Umgebung verfügen.

In diesem Verfahren wird erläutert, wie Sie die Anzahl der vCPUs ändern, die der virtuellen Workload Balancing-Appliance zugewiesen sind Fahren Sie die virtuelle Appliance herunter, bevor Sie diese Schritte ausführen. Der Workload Balancing ist etwa fünf Minuten lang nicht verfügbar.

1. Fahren Sie die virtuelle Workload Balancing-Appliance herunter.
2. Wählen Sie im XenCenter Ressourcenbereich die virtuelle Workload Balancing-Appliance aus.
3. Klicken Sie auf der Registerkarte **Allgemein** der virtuellen Appliance auf **Eigenschaften**. Das **Eigenschaften-Dialogfeld** wird geöffnet.
4. Bearbeiten Sie auf der Registerkarte “**CPU** “des **Eigenschaften-Dialogs** die CPU-Einstellungen auf die erforderlichen Werte.
5. Klicken Sie auf **OK**.
6. Starten Sie die virtuelle Workload Balancing-Appliance.

Die neuen vCPU-Einstellungen werden wirksam, wenn die virtuelle Appliance gestartet wird.

Ändern des Speichers der virtuellen Appliance

Standardmäßig werden der virtuellen Workload Balancing-Appliance 2 GB Arbeitsspeicher zugewiesen.

Stellen Sie für große Pools die virtuelle Workload Balancing-Appliance so ein, dass sie den maximalen Arbeitsspeicher belegt, den Sie ihr zur Verfügung stellen können (sogar bis zu 16 GB). Machen Sie sich keine Sorgen über eine hohe Speicherauslastung. Eine hohe Speicherauslastung ist für die virtuelle Appliance normal, da die Datenbank immer so viel Speicher verbraucht, wie sie erhalten kann.

> **Hinweis:**
>
> Dynamic Memory Control wird mit der virtuellen Workload Balancing-Appliance nicht unterstützt. Legen Sie einen festen Wert für den maximalen Arbeitsspeicher fest, der der virtuellen Appliance zugewiesen werden soll.

In diesem Verfahren wird erläutert, wie Sie die Speichergröße der virtuellen Workload Balancing-Appliance ändern. Fahren Sie die virtuelle Appliance herunter, bevor Sie diese Schritte ausführen. Der Workload Balancing ist etwa fünf Minuten lang nicht verfügbar.

1. Fahren Sie die virtuelle Workload Balancing-Appliance herunter.
2. Wählen Sie im XenCenter Ressourcenbereich die virtuelle Workload Balancing-Appliance aus.
3. Klicken Sie auf der Registerkarte **Speicher** der virtuellen Appliance auf **Bearbeiten**. Der Dialog **Speichereinstellungen** wird geöffnet.
4. Bearbeiten Sie die Speichereinstellungen auf die erforderlichen Werte.
5. Klicken Sie auf **OK**.
6. Starten Sie die virtuelle Workload Balancing-Appliance.

Die neuen Speichereinstellungen werden wirksam, wenn die virtuelle Appliance gestartet wird.

Datenträger der virtuellen Appliance erweitern

> **Warnung:**
>
> Sie können den verfügbaren Speicherplatz nur in den Versionen 8.3.0 und höher erweitern, da LVM vor 8.3.0 nicht unterstützt wurde.
>
> Workload Balancing unterstützt das Verringern des verfügbaren Speicherplatzes nicht.

Standardmäßig werden der virtuellen Workload Balancing-Appliance 30 GB Speicherplatz zugewiesen.

Je mehr VMs die virtuelle Workload Balancing-Appliance überwacht, desto mehr Speicherplatz verbraucht sie pro Tag.

Sie können die Datenträgergröße schätzen, die die virtuelle Appliance benötigt, indem Sie die folgende Formel verwenden:

```
Total estimated disk size = ( ( number of days * average disk usage ) +
    base disk usage ) * grooming multiplier
```

- *Anzahl der Tage* ist die Anzahl der Tage, an denen Daten aufbewahrt werden müssen
- *Die durchschnittliche Datenträgerauslastung* hängt von der Anzahl der überwachten VMs ab. Die folgenden Werte geben eine Annäherung für eine bestimmte Anzahl von virtuellen Rechnern:
  - Für 200 virtuelle Maschinen —0,246 GB/Tag
  - Für 400 virtuelle Maschinen —0,505 GB/Tag
  - Für 600 virtuelle Maschinen —0,724 GB/Tag
  - Für 800 virtuelle Maschinen —0,887 GB/Tag
- *Die Basisdatenträgernutzung* ist 2,4 GB
- Der*Pflege-Multiplikator* beträgt 1,25. Dieser Multiplikator berücksichtigt die Menge an Speicherplatz, die für die Pflege benötigt wird. Es wird davon ausgegangen, dass für die Pflege zusätzliche 25% des gesamten berechneten Speicherplatzes erforderlich sind.

Versionen 8.2.2 und früher In diesem Verfahren wird erläutert, wie das virtuelle Laufwerk der virtuellen Workload Balancing-Appliance für Workload Balancing-Versionen 8.2.2 und frühere Versionen erweitert wird.

> **Warnung:**
>
> Wir empfehlen, vor Durchführung dieses Verfahrens eine Momentaufnahme Ihrer Daten zu erstellen. Eine falsche Ausführung dieser Schritte kann dazu führen, dass die virtuelle Workload Balancing-Appliance beschädigt wird.

1. Fahren Sie die virtuelle Workload Balancing-Appliance herunter.
2. Wählen Sie im XenCenter Ressourcenbereich die virtuelle Workload Balancing-Appliance aus.
3. Klicken Sie auf die Registerkarte **Speicher**.
4. Wählen Sie den `vdi_xvda`-Datenträger aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
5. Wählen Sie unter `vdi_xvda` **Eigenschaften** die Option **Größe und Position** aus.
6. Erhöhen Sie die Datenträgergröße nach Bedarf und klicken Sie auf **OK**.
7. Starten Sie die virtuelle Workload Balancing Appliance und melden Sie sich bei ihr an.

8. Führen Sie den folgenden Befehl auf der virtuellen Appliance Workload Balancing aus:

```
resize2fs /dev/xvda
<!--NeedCopy-->
```

9. Führen Sie den Befehl `df –h` aus, um die neue Datenträgergröße zu bestätigen.

Installieren `resize2fs` Wenn das Tool `resize2fs` nicht auf der virtuellen Workload Balancing-Appliance installiert ist, können Sie es über die folgenden Schritte installieren.

Wenn Sie mit dem Internet verbunden sind, führen Sie den folgenden Befehl auf der virtuellen Workload Balancing-Appliance aus:

```
yum install -y --enablerepo=base,updates --disablerepo=citrix-*
    e2fsprogs
<!--NeedCopy-->
```

Wenn es keinen Internetzugang gibt:

1. Laden Sie Folgendes von herunter https://centos.pkgs.org/7/centos-x86_64/.
   - `libss-1.42.9-7.el7.i686.rpm`
   - `e2fsprogs-libs-1.42.9-7.el7.x86_64.rpm`
   - `e2fsprogs-1.42.9-7.el7.x86_64.rpm`
2. Laden Sie sie mit SCP oder einem anderen geeigneten Tool auf die Workload Balancing VM hoch.
3. Führen Sie den folgenden Befehl von der virtuellen Appliance Workload Balancing aus

```
rpm -ivh libss-\*.rpm e2fsprogs-\*.rpm
<!--NeedCopy-->
```

   Das Tool `resize2fs` ist jetzt installiert.

Versionen 8.3.0 und höher In diesem Verfahren wird erläutert, wie das virtuelle Laufwerk der virtuellen Workload Balancing-Appliance für Workload Balancing-Versionen 8.3.0 und höher mithilfe von Linux Volume Manager (LVM) erweitert wird.

> **Warnung:**
>
> Dieses Verfahren darf nur von erfahrenen Linux-Systemadministratoren befolgt werden, da eine falsche Ausführung dieser Schritte zur Beschädigung der virtuellen Workload Balancing-Appliance führen kann. Wir können nicht garantieren, dass Probleme, die sich aus der falschen Verwendung des Registrierungseditors ergeben, behoben werden können. Erstellen Sie unbedingt eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten, und fahren Sie die virtuelle Appliance herunter, bevor Sie diese Schritte ausführen. Der Workload Balancing ist

> etwa fünf Minuten lang nicht verfügbar.

Um neue Partitionen zu erstellen, physische Volumes zu manipulieren und die Größe Ihres Dateisystems zu ändern, führen Sie die folgenden Aktionen aus, während Sie als Superuser (root) angemeldet sind:

1. Sehen Sie sich die aktuellen Partitionen an:

   ```
   fdisk -l
   <!--NeedCopy-->
   ```

   Die Standardpartitionen könnten so aussehen:

   ```
   -bash-4.2# fdisk -l

   Disk /dev/xvda: 21.5 GB, 21474836480 bytes, 41943040 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk label type: dos
   Disk identifier: 0x000008b2

      Device Boot      Start         End      Blocks   Id  System
   /dev/xvda1   *        2048     1026047      512000   83  Linux
   /dev/xvda2         1026048    16777215     7875584   8e  Linux LVM

   Disk /dev/mapper/centos-root: 7159 MB, 7159676928 bytes, 13983744 sectors
   Units = sectors of 1 * 512 = 512 bytes
   ```

2. Sehen Sie sich den Stil der Datenträgerpartition an:

   ```
   parted <disk>
   <!--NeedCopy-->
   ```

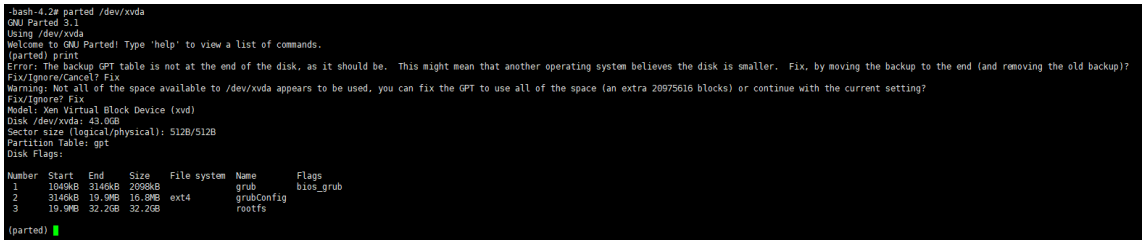
   Beispiel: Anzeigen des Partitionsstils von `/dev/xvda`:

   ```
   parted /dev/xvda
   <!--NeedCopy-->
   ```

3. Geben Sie `p` ein.

   Wenn die folgenden Fehlermeldungen auftreten, geben Sie `Fix` ein, um die jeweilige Fehlermeldung zu beheben:

   - “Error: The backup GPT table is not at the end of the disk, as it should be. This might mean that another operating system believes the disk is smaller. Fix, by moving the backup to the end (and removing the old backup)?”
   - “Warning: Not all of the space available to <`disk`> appears to be used, you can fix the GPT To use all of the space (an extra <`block number`> blocks) or continue with the current setting?”



4. Geben Sie q ein und drücken Sie zum Verlassen die **Eingabetaste**.
5. Bearbeiten Sie die Partitionen:

```
fdisk <disk>
<!--NeedCopy-->
```

   Um beispielsweise die Partitionen in Workload Balancing-Appliances zu bearbeiten:

```
fdisk /dev/xvda
<!--NeedCopy-->
```

6. Geben Sie n ein und drücken Sie die **Eingabetaste**, um eine neue Partition zu erstellen. Geben Sie p ein und drücken Sie die **Eingabetaste**, um sie zur primären Partition zu machen. Drücken Sie die **Eingabetaste** erneut, um die Standardoption, die nächste verfügbare Partition, zu verwenden (in diesem Fall ist es, wie oben angegeben, Partition Nummer 3).

   > **Hinweis:**
   >
   > Wenn noch kein zusätzlicher Speicherplatz zugewiesen wurde, wird eine Meldung angezeigt, die darauf hinweist, dass keine freien Sektoren verfügbar sind. Tippen Sie q und drücken Sie die **Eingabetaste**, um fdisk zu beenden. Ordnen Sie zuerst den gewünschten Speicherplatz über XenCenter zu und kehren Sie dann zu diesem Schritt zurück.

7. Drücken Sie zweimal die **Eingabetaste**, um den ersten und letzten Standardsektor der verfügbaren Partition zu verwenden (oder geben Sie die gewünschten Sektoren manuell an). Geben Sie t ein, um einen Partitionstyp anzugeben, wählen Sie die gewünschte Partition (in diesem Fall 3), geben Sie 8e ein und drücken Sie die **Eingabetaste**, um daraus eine Partition vom Typ LVM zu machen.

   Beispiel für eine Ausgabe:


```
Command (m for help): n
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p): p
Partition number (3,4, default 3):
First sector (16777216-41943039, default 16777216):
Using default value 16777216
Last sector, +sectors or +size{K,M,G} (16777216-41943039, default 41943039):
Using default value 41943039
Partition 3 of type Linux and of size 12 GiB is set

Command (m for help): t
Partition number (1-3, default 3):
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

8. Geben Sie p ein und drücken Sie die **Eingabetaste**, um die Details der Partition zu drucken. Die Ausgabe sollte der folgenden ähneln (beachten Sie, dass die Werte für Start- und Endblöcke je nach zugewiesenem Speicherplatz variieren können):

```
Command (m for help): p

Disk /dev/xvda: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000008b2

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     1026047      512000   83  Linux
/dev/xvda2         1026048    16777215     7875584   8e  Linux LVM
/dev/xvda3        16777216    41943039    12582912   8e  Linux LVM
```

9. Wenn etwas nicht stimmt, geben Sie q ein und drücken Sie die **Eingabetaste**, um den Vorgang zu beenden, ohne zu speichern, damit Ihre vorhandenen Partitionen nicht beeinträchtigt werden. Fangen Sie erneut mit Schritt 1 an. Wenn alles gut aussieht, geben Sie stattdessen w ein und drücken Sie die **Eingabetaste**, um die Änderungen zu schreiben.

   Nachdem Sie diese Änderungen geschrieben haben, erhalten Sie möglicherweise eine Warnung, die darauf hinweist, dass das Gerät ausgelastet war und der Kernel immer noch die alte Tabelle verwendet. Wenn das der Fall ist, führen Sie diesen Befehl aus, der die Partitionstabelle aktualisiert, bevor Sie mit dem nächsten Schritt fortfahren: `partprobe`.

   Stellen Sie sicher, dass die neue Gerätepartition (in diesem Fall `/dev/xvda4`) jetzt aufgeführt ist. Führen Sie dazu den Befehl aus: `fdisk -l`.

   Das neu erstellte Gerät sollte jetzt aufgelistet werden:


```
   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1   *        2048     1026047      512000   83  Linux
/dev/xvda2         1026048    16777215     7875584   8e  Linux LVM
/dev/xvda3        16777216    41943039    12582912   8e  Linux LVM
```

10. Wenn die Ausgabe korrekt aussieht, erstellen Sie ein Physical Volume:

```
pvcreate <new partition>
<!--NeedCopy-->
```

Beispiel:

```
pvcreate /dev/xvda4
<!--NeedCopy-->
```

11. Vergewissern Sie sich, dass das oben erstellte physische Volume jetzt aufgeführt ist:

```
pvs
<!--NeedCopy-->
```

In diesem Beispiel betrug der zusätzliche Speicherplatz 12 GB. Beispiel für eine Ausgabe:

```
-bash-4.2# pvcreate /dev/xvda3
  Physical volume "/dev/xvda3" successfully created.
-bash-4.2# pvs
  PV         VG     Fmt  Attr PSize  PFree
  /dev/xvda2 centos lvm2 a--  <7.51g 40.00m
  /dev/xvda3        lvm2 ---  12.00g 12.00g
```

12. Basierend auf der Ausgabe des vorherigen Befehls muss die Volume-Gruppe mit dem Namen centos erweitert werden:

```
vgextend <volume group> <new partition>
<!--NeedCopy-->
```

Beispiel:

```
vgextend centos /dev/xvda4
<!--NeedCopy-->
```

13. Schauen Sie sich die aktuellen Volume-Gruppen an:

```
vgs
<!--NeedCopy-->
```

14. Führen Sie den folgenden Befehl aus:

```
pvscan
<!--NeedCopy-->
```


Dies sollte /dev/xvda4 als Teil der Centos Volume-Gruppe anzeigen. Beispiel für eine Ausgabe:

```
-bash-4.2# vgextend centos /dev/xvda3
  Volume group "centos" successfully extended
-bash-4.2# vgs
  VG     #PV #LV #SN Attr   VSize  VFree
  centos   2   2   0 wz--n- 19.50g <12.04g
-bash-4.2# pvscan
  PV /dev/xvda2   VG centos          lvm2 [<7.51 GiB / 40.00 MiB free]
  PV /dev/xvda3   VG centos          lvm2 [<12.00 GiB / <12.00 GiB free]
  Total: 2 [19.50 GiB] / in use: 2 [19.50 GiB] / in no VG: 0 [0   ]
```

15. Wenn die in den vorherigen Schritten angezeigten Informationen korrekt aussehen, führen Sie diesen Befehl aus, um den Logic Volume-Pfad für das zu erweiternde logische Volume zu sehen:

```
lvdisplay
<!--NeedCopy-->
```

In diesem Beispiel lautet der Pfad /dev/centos/root:

```
--- Logical volume ---
LV Path                /dev/centos/root
LV Name                root
VG Name                centos
LV UUID                [illegible]
LV Write Access        read/write
LV Creation host, time localhost, 2017-04-26 11:
LV Status              available
# open                 1
LV Size                <6.67 GiB
Current LE             1707
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     8192
Block device           253:0
```

16. Führen Sie den folgenden Befehl aus, um die freie PE/Größe anzuzeigen (dies gibt den genauen Wert an, der beim Erweitern der Partition verwendet werden soll):

```
vgdisplay
<!--NeedCopy-->
```

Beispiel für eine Ausgabe:

```
Alloc PE / Size       1912 / <7.47 GiB
Free  PE / Size       3081 / <12.04 GiB
VG UUID               [illegible]
```


17. Erweitern Sie das Logic Volume mithilfe des freien PE/Size-Werts und des in Schritt 11 ausgegebenen Logic Volume-Pfads:

```
lvextend -l +100%FREE /dev/centos/root
<!--NeedCopy-->
```

Wenn dies erfolgreich ausgeführt wird, erweitern Sie das Dateisystem:

```
resize2fs /dev/centos/root
<!--NeedCopy-->
```

Beispiel für eine Ausgabe:

```
-bash-4.2# lvextend -l +3081 /dev/centos/root
  Size of logical volume centos/root changed from <6.67 GiB (1707 extents) to 18
.70 GiB (4788 extents).
  Logical volume centos/root successfully resized.
-bash-4.2# xfs_growfs /dev/centos/root
meta-data=/dev/mapper/centos-root isize=256    agcount=4, agsize=436992 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=1747968, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 1747968 to 4902912
```

18. Stellen Sie sicher, dass die Dateisystemgröße wie erwartet angezeigt wird:

```
df -h /*
<!--NeedCopy-->
```

```
-bash-4.2# df -h /*
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/centos-root   19G  4.1G   15G  22% /
/dev/xvda1               497M  111M  387M  23% /boot
devtmpfs                 990M     0  990M   0% /dev
```

Wenn Sie die erwarteten Zahlen sehen, haben Sie den gewünschten Speicherplatz erfolgreich zugewiesen und die Partition korrekt erweitert. Für weitere Unterstützung wenden Sie sich bitte an den XenServer-Support.

Beenden Sie den Arbeitslastausgleich

Da der Workload Balancing auf Poolebene konfiguriert ist, müssen Sie eine der folgenden Aktionen ausführen, wenn Sie die Verwaltung eines Pools beenden möchten:

Pausieren Sie den Arbeitslastausgleich. Durch das Anhalten des Arbeitslastausgleichs wird XenCenter daran gehindert, Empfehlungen für den angegebenen Ressourcenpool anzuzeigen und den

Pool zu verwalten. Das Anhalten ist für einen kurzen Zeitraum ausgelegt und ermöglicht es Ihnen, die Überwachung fortzusetzen, ohne eine Neukonfiguration vornehmen zu müssen. Wenn Sie den Workload Balancing anhalten, wird die Datenerfassung für diesen Ressourcenpool angehalten, bis Sie den Arbeitslastausgleich erneut aktivieren.

1. Wählen Sie in XenCenter den Ressourcenpool aus, für den Sie den Workload Balancing deaktivieren möchten.
2. Klicken Sie auf der Registerkarte **WLB** auf **Pause**. Auf der Registerkarte **WLB** wird eine Meldung angezeigt, die angibt, dass der Workload Balancing angehalten wurde.

> **Tipp:**
>
> Um die Überwachung fortzusetzen, klicken Sie auf der Registerkarte **WLB** auf die Schaltfläche **Fortsetzen** .

Trennen Sie den Pool vom Workload Balancing. Das Trennen der Verbindung mit der virtuellen Workload Balancing-Appliance unterbricht die Verbindung zwischen dem Pool und löscht, falls möglich, die Pool-Daten aus der Workload Balancing-Datenbank. Wenn Sie die Verbindung zum Workload Balancing trennen, sammelt der Workload Balancing keine Daten mehr im Pool.

1. Wählen Sie in XenCenter den Ressourcenpool aus, für den Sie den Workload Balancing beenden möchten.
2. Wählen Sie im Menü **Infrastruktur** die Option **Workload Balancing-Server trennen**. Das Dialogfeld **Workload Balancing Server trennen** wird angezeigt.
3. Klicken Sie auf **Trennen**, um zu verhindern, dass Workload Balancing den Pool dauerhaft überwacht

> **Tipp:**
>
> Wenn Sie den Pool von der virtuellen Workload Balancing-Appliance getrennt haben, müssen Sie erneut eine Verbindung zu einer Workload Balancing-Appliance herstellen, um den Arbeitslastausgleich in diesem Pool wieder zu aktivieren. Weitere Informationen finden Sie unter Verbinden mit der virtuellen Appliance für den Workload Balancing.

Mit aktiviertem Workload Balancing in den Wartungsmodus

Wenn Workload Balancing aktiviert ist und Sie einen Host in den Wartungsmodus versetzen, migriert XenServer die auf diesem Host laufenden VMs auf ihre optimalen Hosts, sofern verfügbar. XenServer verwendet Workload Balancing-Empfehlungen, die auf Leistungsdaten, Ihrer Platzierungsstrategie und Leistungsschwellenwerten basieren, um den optimalen Host auszuwählen.

Wenn kein optimaler Host verfügbar ist, werden im Assistenten **zum Aktivieren des**Wartungsmodus**die Worte Klicken Sie hier, um die VM zu suspendieren** angezeigt. In diesem Fall empfiehlt Workload

Balancing keine Platzierung, da kein Host mit ausreichenden Ressourcen zum Ausführen der VM vorhanden ist. Sie können diese VM entweder anhalten oder den Wartungsmodus beenden und eine VM auf einem anderen Host im selben Pool anhalten. Wenn Sie dann das Dialogfeld **Wartungsmodus aufrufen** erneut aufrufen, kann der Workload Balancing möglicherweise einen Host auflisten, der sich für die Migration eignet.

> **Hinweis:**
>
> Wenn Sie einen Host zur Wartung offline nehmen und der Workload Balancing aktiviert ist, werden die Wörter „Workload Balancing“im Assistenten zum Wechseln in den **Wartungsmodus** angezeigt.

So rufen Sie den Wartungsmodus mit aktiviertem Arbeitslastausgleich auf:

1. Wählen Sie im Bereich **Ressourcen** von XenCenter den physischen Server aus, den Sie offline nehmen möchten.
2. Wählen Sie im Menü **Server** die Option **Wartungsmodus aufrufen**.
3. Klicken **Sie im Assistenten zum Aufrufen des Wartungsmodus** auf **Wartungsmodus aufrufen**.

   Die auf dem Host laufenden VMs werden automatisch auf der Grundlage der Workload Balancing-Leistungsdaten, Ihrer Platzierungsstrategie und der Leistungsschwellenwerte auf den optimalen Host migriert.

So nehmen Sie den Server aus dem Wartungsmodus heraus:

1. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Wartungsmodus beenden**.

   Wenn Sie einen Host aus dem Wartungsmodus entfernen, stellt XenServer automatisch die ursprünglichen VMs dieses Hosts auf diesem Host wieder her.

Entfernen der virtuellen Workload Balancing-Appliance

Um die virtuelle Workload Balancing-Appliance zu entfernen, empfehlen wir, das Standardverfahren zum Löschen von VMs aus XenCenter zu verwenden.

Wenn Sie die virtuelle Workload Balancing-Appliance löschen, wird die PostgreSQL-Datenbank mit dem Workload Balancing gelöscht. Um diese Daten zu speichern, müssen Sie sie aus der Datenbank migrieren, bevor Sie die virtuelle Workload Balancing-Appliance löschen.

Verwalten der Workload Balancing-Datenbank

Die Workload Balancing-Datenbank ist eine PostgreSQL-Datenbank. PostgreSQL ist eine relationale Open-Source-Datenbank. Sie können die Dokumentation für PostgreSQL finden, indem Sie im Inter-

net suchen.

Die folgenden Informationen richten sich an Datenbankadministratoren und fortgeschrittene Benutzer von PostgreSQL, die mit Aufgaben der Datenbankverwaltung vertraut sind. Wenn Sie keine Erfahrung mit PostgreSQL haben, empfehlen wir Ihnen, sich damit vertraut zu machen, bevor Sie die Datenbankaufgaben in den folgenden Abschnitten versuchen.

Standardmäßig lautet der PostgreSQL-Benutzername `postgres`. Sie legen das Kennwort für dieses Konto während der Konfiguration des Workload Balancing fest.

Die Menge der historischen Daten, die Sie speichern können, basiert auf der Größe des virtuellen Laufwerks, das dem Workload Balancing zugewiesen ist, und dem minimal erforderlichen Speicherplatz. Standardmäßig beträgt die Größe des virtuellen Laufwerks, das dem Workload Balancing zugewiesen ist, 30 GB. In Bezug auf die Verwaltung der Datenbank können Sie den Speicherplatz steuern, den Datenbankdaten belegen, indem Sie die Datenbankpflege konfigurieren. Weitere Informationen finden Sie unter Parameter für die Datenbankpflege.

Um viele historische Daten zu speichern, z. B. wenn Sie den Poolauditlistenbericht aktivieren möchten, können Sie einen der folgenden Schritte ausführen:

- Vergrößern Sie die virtuelle Datenträgergröße, die der virtuellen Workload Balancing-Appliance zugewiesen ist. Importieren Sie dazu die virtuelle Appliance und erhöhen Sie die Größe des virtuellen Datenträgers, indem Sie die Schritte unter Datenträger der virtuellen Appliance erweitern ausführen.
- Erstellen Sie regelmäßige doppelte Backupkopien der Daten, indem Sie den Remote-Clientzugriff auf die Datenbank aktivieren und ein Drittanbieter-Datenbankverwaltungstool verwenden.

Zugriff auf die Datenbank

In der virtuellen Workload Balancing-Appliance ist eine Firewall konfiguriert. Bevor Sie auf die Datenbank zugreifen können, müssen Sie den PostgreSQL-Serverport zu den iptables hinzufügen.

1. Führen Sie in der Konsole der virtuellen Workload Balancing-Appliance den folgenden Befehl aus:

```
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
state --state NEW,ESTABLISHED -j ACCEPT
<!--NeedCopy-->
```

2. (Optional) Führen Sie den folgenden Befehl aus, damit diese Konfiguration nach dem Neustart der virtuellen Appliance beibehalten wird:

```
iptables-save > /etc/sysconfig/potables
<!--NeedCopy-->
```


Steuern der Datenbankpflege

Die Workload Balancing-Datenbank löscht automatisch die ältesten Daten, wenn die virtuelle Appliance den Mindestbetrag an Speicherplatz erreicht, den Workload Balancing für die Ausführung benötigt. Standardmäßig ist die Mindestmenge an benötigtem Speicherplatz auf 1.024 MB festgelegt.

Die Workload Balancing-Datenbank-Pflegeoptionen werden über die Datei gesteuert `wlb.conf`.

Wenn auf der virtuellen Workload Balancing-Appliance nicht mehr genügend Speicherplatz vorhanden ist, beginnt der Workload Balancing automatisch mit der Pflege historischer Daten. Das Verfahren umfasst folgende Schritte:

1. In einem vordefinierten Pflegeintervall prüft der Datensammelpunkt "Workload Balancing", ob eine Pflege erforderlich ist. Die Pflege ist erforderlich, wenn die Datenbankdaten so weit angewachsen sind, dass der einzige ungenutzte Speicherplatz der minimal erforderliche Speicherplatz ist. Verwenden Sie diese Option `GroomingRequiredMinimumDiskSizeInMB`, um den mindestens erforderlichen Speicherplatz festzulegen.

   Sie können das Pflegeintervall bei Bedarf mit ändern `GroomingIntervalInHour`. Standardmäßig prüft der Workload Balancing jedoch, ob die Pflege einmal pro Stunde erforderlich ist.

2. Wenn eine Pflege erforderlich ist, werden beim Workload Balancing zunächst die Daten vom ältesten Tag gepflegt. Der Workload Balancing prüft dann, ob jetzt genügend Speicherplatz vorhanden ist, um die Mindestanforderung an Speicherplatz zu erfüllen.

3. Wenn bei der ersten Pflege nicht genügend Speicherplatz freigegeben wurde, wiederholt der Workload Balancing die Bereinigung bis zu `GroomingRetryCounter` Mal, ohne `GroomingIntervalInHour` Stunden lang zu warten.

4. Wenn die erste oder wiederholte Pflege ausreichend Speicherplatz freigegeben hat, wartet der Workload Balancing `GroomingIntervalInHour` Stunden und kehrt zu Schritt 1 zurück.

5. Wenn die durch `GroomingRetryCounter` initiierte Pflege nicht genügend Speicherplatz freigegeben hat, wartet der Workload Balancing `GroomingIntervalInHour` Stunden und kehrt zu Schritt 1 zurück.

Parameter für die Datenbankpflege

Die Datei `wlb.conf` enthält fünf Parameter, die verschiedene Aspekte der Datenbankpflege steuern. Sie lauten wie folgt:

- `GroomingIntervalInHour`. Steuert, wie viele Stunden vergehen, bis die nächste Pflegeprüfung abgeschlossen ist. Wenn Sie beispielsweise **1**eingeben, überprüft Workload

Balancing den Speicherplatz stündlich. Wenn Sie **2**eingeben, prüft der Workload Balancing alle zwei Stunden den Speicherplatz, um festzustellen, ob die Pflege erfolgen muss.

- `GroomingRetryCounter`. Steuert, wie oft der Workload Balancing versucht, die Grooming-Datenbankabfrage erneut auszuführen.
- `GroomingDBDataTrimDays`. Steuert die Anzahl der Tage an Daten, die Workload Balancing bei jedem Versuch, Daten zu bearbeiten, aus der Datenbank löscht. Der Standardwert ist ein Tag.
- `GroomingDBTimeoutInMinute`. Steuert die Anzahl der Minuten, die die Datenbankpflege dauert, bis die Zeitüberschreitung abgelaufen ist und abgebrochen wird. Wenn die Bereinigungsabfrage länger als erwartet dauert und nicht innerhalb des Timeout-Zeitraums ausgeführt wird, wird die Bereinigungsaufgabe abgebrochen. Der Standardwert ist 0 Minuten, was bedeutet, dass die Datenbankpflege niemals zu einem Timeout kommt.
- `GroomingRequiredMinimumDiskSizeInMB`. Steuert die Mindestmenge an freiem Speicherplatz auf dem virtuellen Laufwerk, das der virtuellen Workload Balancing-Appliance zugewiesen ist. Wenn die Daten auf dem virtuellen Laufwerk wachsen, bis nur noch die minimale Datenträgergröße auf dem virtuellen Laufwerk vorhanden ist, löst der Workload Balancing die Datenbankpflege aus. Der Standardwert ist 2,048 MB.

Informationen zum Bearbeiten dieser Werte finden Sie unter Bearbeiten der Workload Balancing-Konfigurationsdatei.

Ändern Sie das Datenbankkennwort

Wir empfehlen, den Befehl `wlbconfig` zu verwenden, um das Datenbankkennwort zu ändern. Weitere Informationen finden Sie unter Ändern der Konfigurationsoptionen für den Workload Balancing. Ändern Sie das Kennwort nicht, indem Sie die Datei `wlb.conf` ändern.

Archivierung von Datenbankdaten

Um zu verhindern, dass ältere historische Daten gelöscht werden, können Sie optional Daten zur Archivierung aus der Datenbank kopieren. Um dies zu tun, müssen Sie die folgenden Aufgaben ausführen:

1. Aktiviert die Clientauthentifizierung in der Datenbank.
2. Richten Sie die Archivierung mit dem PostgreSQL-Datenbankverwaltungstool Ihrer Wahl ein.

Clientauthentifizierung für die Datenbank aktivieren

Während Sie über die Workload Balancing-Konsole eine direkte Verbindung zur Datenbank herstellen können, können Sie auch ein PostgreSQL-Datenbankverwaltungstool verwenden. Nachdem Sie ein Datenbankverwaltungstool heruntergeladen haben, installieren Sie es auf dem System, von dem aus Sie eine Verbindung zur Datenbank herstellen möchten. Sie können das Tool beispielsweise auf demselben Laptop installieren, auf dem Sie XenCenter ausführen.

Bevor Sie die Remote-Clientauthentifizierung für die Datenbank aktivieren können, müssen Sie:

1. Ändern Sie die Datenbankkonfigurationsdateien, einschließlich der Datei pg_hba.conf und postgresql.conf, um Verbindungen zuzulassen.
2. Beenden Sie die Workload Balancing-Dienste, starten Sie die Datenbank neu, und starten Sie dann die Workload Balancing-Dienste neu.
3. Konfigurieren Sie im Datenbankverwaltungstool die IP-Adresse der Datenbank (d. h. die IP-Adresse der virtuellen Workload Balancing-Appliance) und das Datenbankkennwort.

Ändern der Datenbankkonfigurationsdateien

Um die Clientauthentifizierung für die Datenbank zu aktivieren, müssen Sie die folgenden Dateien auf der virtuellen Workload Balancing-Appliance ändern: die Datei `pg_hba.conf` und die Datei `postgresql.conf`.

Bearbeiten der Datei `pg_hba.conf`:

1. Bearbeiten Sie die Datei `pg_hba.conf`. Öffnen Sie die Datei `pg_hba.conf` über die Konsole der virtuellen Workload Balancing-Appliance mit einem Editor wie VI. Beispiel:

   ```
   vi /var/lib/pgsql/9.0/data/pg_hba.conf
   <!--NeedCopy-->
   ```

2. Wenn Ihr Netzwerk IPv4 verwendet, fügen Sie die IP-Adresse des verbundenen Computers zu dieser Datei hinzu. Beispiel:

   Geben Sie im Abschnitt Konfiguration unter Folgendes ein `#IPv4 local connections`:

   - **TYPE:** host
   - **DATABASE:** all
   - **USER:** all
   - **CIDR-ADRESSE:** 0.0.0.0/0
   - **METHOD:** trust

3. Geben Sie Ihre IP-Adresse in das Feld `CIDR-ADDRESS` ein.

> **Hinweis:**
>
> Anstatt 0.0.0.0/0 einzugeben, können Sie Ihre IP-Adresse eingeben und die letzten drei Ziffern durch 0/24 ersetzen. Die abschließende "24"nach/definiert die Subnetzmaske und erlaubt nur Verbindungen von IP-Adressen innerhalb dieser Subnetzmaske.

Wenn Sie `trust` das Feld `Method` eingeben, kann sich die Verbindung authentifizieren, ohne dass ein Kennwort erforderlich ist. Wenn Sie `password` für das `Method`-Feld eingeben, müssen Sie ein Kennwort angeben, wenn Sie sich mit der Datenbank verbinden.

4. Wenn Ihr Netzwerk IPv6 verwendet, fügen Sie die IP-Adresse des verbundenen Computers zu dieser Datei hinzu. Beispiel:

   Tragen Sie unter Folgendes ein `#IPv6 local connections`:

   - **TYPE:** host
   - **DATABASE:** all
   - **USER:** all
   - **CIDR-ADRESSE:** `::0/0`
   - **METHOD:** trust

   Geben Sie die IPv6-Adressen in das Feld `CIDR-ADDRESS` ein. In diesem Beispiel öffnet `::0/0` die Datenbank für Verbindungen von beliebigen IPv6-Adressen.

5. Speichern Sie die Datei und beenden Sie den Editor.

6. Nachdem Sie die Datenbankkonfigurationen geändert haben, müssen Sie die Datenbank neu starten, um die Änderungen zu übernehmen. Führen Sie den folgenden Befehl aus:

```
service postgresql-9.0 restart
<!--NeedCopy-->
```

Bearbeiten der Datei `postgresql.conf`:

1. Bearbeiten Sie die Datei `postgresql.conf`. Öffnen Sie die Datei `postgresql.conf` über die Konsole der virtuellen Workload Balancing-Appliance mit einem Editor wie VI. Beispiel:

```
vi /var/lib/pgsql/9.0/data/postgresql.conf
<!--NeedCopy-->
```

2. Bearbeiten Sie die Datei so, dass sie auf jedem Port und nicht nur auf dem lokalen Host lauscht. Beispiel:

   a) Finde die folgende Zeile:

```
# listen_addresses='localhost'
<!--NeedCopy-->
```


b) Entfernen Sie das Kommentarsymbol (#) und bearbeiten Sie die Zeile so, dass sie wie folgt lautet:

```
listen_addresses='*'
<!--NeedCopy-->
```

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Nachdem Sie die Datenbankkonfigurationen geändert haben, müssen Sie die Datenbank neu starten, um die Änderungen zu übernehmen. Führen Sie den folgenden Befehl aus:

```
service postgresql-9.0 restart
<!--NeedCopy-->
```

Ändern des Datenbank-Wartungsfensters

Der Workload Balancing führt standardmäßig täglich um 12:05 Uhr GMT (00:05) routinemäßige Datenbankwartung durch. Während dieses Wartungsfensters erfolgt die Datenerfassung, aber die Aufzeichnung der Daten kann sich verzögern. In diesem Zeitraum sind jedoch die Workload Balancing-Benutzeroberflächensteuerelemente verfügbar, und der Workload Balancing gibt weiterhin Optimierungsempfehlungen ab.

> **Hinweis:**
>
> Um einen Verlust des Workload Balancing zu vermeiden:
>
> - Während des Wartungsfensters wird der Workload Balancing-Server neu gestartet. Stellen Sie sicher, dass Sie Ihre virtuellen Maschinen nicht gleichzeitig neu starten.
> - Wenn Sie zu anderen Zeiten alle VMs in Ihrem Pool neu starten, starten Sie den Workload Balancing-Server nicht neu.

Die Datenbankwartung umfasst die Freigabe von zugewiesenem ungenutztem Speicherplatz und das erneute Indizieren der Datenbank Die Wartung dauert etwa 6 bis 8 Minuten. In größeren Pools kann die Wartung länger dauern, je nachdem, wie lange der Workload Balancing für die Discovery dauert.

Abhängig von Ihrer Zeitzone möchten Sie möglicherweise die Zeit ändern, zu der die Wartung durchgeführt wird. In der Zeitzone Japan Standard Time (JST) erfolgt die Wartung des Workload Balancing beispielsweise um 9:05 Uhr (09:05), was zu Spitzenauslastung in einigen Organisationen führen kann. Wenn Sie eine saisonale Zeitänderung wie Sommerzeit oder Sommerzeit angeben möchten, müssen Sie die Änderung in einen von Ihnen eingegebenen Wert umwandeln.

So ändern Sie die Wartungszeit:

1. Führen Sie in der Workload Balancing-Konsole den folgenden Befehl aus einem beliebigen Verzeichnis aus:


```
crontab -e
<!--NeedCopy-->
```

Der Workload Balancing zeigt Folgendes an:

```
05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
<!--NeedCopy-->
```

Der Wert `05 0` stellt die Standardzeit für die Durchführung der Wartung durch den Workload Balancing in Minuten (05) und dann in Stunden (0) dar. (Die Sternchen stehen für den Tag, den Monat und das Jahr, in dem der Job ausgeführt wird: Bearbeiten Sie diese Felder nicht.) Der Eintrag `05 0` zeigt an, dass die Datenbankwartung jede Nacht um 12:05 Uhr oder 00:05 Uhr Greenwich Mean Time (GMT) stattfindet. Diese Einstellung bedeutet, dass, wenn Sie in New York leben, die Wartung in den Wintermonaten um 19:05 Uhr (19:05) und in den Sommermonaten um 20.05 Uhr ausgeführt wird.

> **Wichtig:**
>
> Bearbeiten Sie nicht den Tag, den Monat und das Jahr, an dem der Job ausgeführt wird (wie durch Sternchen dargestellt). Die Datenbankwartung muss täglich durchgeführt werden.

2. Geben Sie den Zeitpunkt an, zu dem die Wartung in GMT durchgeführt werden soll.
3. Speichern Sie die Datei und beenden Sie den Editor.

Workload Balancing anpassen

Der Workload Balancing bietet verschiedene Anpassungsmethoden:

- **Befehlszeilen für das Scripting**. Weitere Informationen finden Sie unter Befehle für den Arbeitslastausgleich.
- **Unterstützung für Host-Power-On-Skripte**. Sie können den Workload Balancing (indirekt) auch über das Host-Power-On-Skripting anpassen. Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

Workload Balancing aktualisieren

Das Online-Upgrade von Workload Balancing wurde aus Sicherheitsgründen veraltet. Kunden können nicht mehr mit dem yum repo upgraden. Kunden können Workload Balancing auf die neueste Version aktualisieren, indem sie die neueste virtuelle Workload Balancing-Appliance importieren, die auf der XenServer-Downloadseite heruntergeladenwerden kann.

Befehle für den Arbeitslastausgleich

Dieser Abschnitt enthält eine Referenz für die Workload Balancing-Befehle. Sie können diese Befehle vom XenServer-Host oder der XenServer-Konsole aus ausführen, um den Workload Balancing zu steuern oder die Workload Balancing-Einstellungen auf dem XenServer-Host zu konfigurieren. Dieser Anhang enthält xe-Befehle und Servicebefehle.

Führen Sie die folgenden Dienstbefehle auf der Workload Balancing-Anwendung aus. Dazu müssen Sie sich bei der virtuellen Workload Balancing-Appliance anmelden.

Melden Sie sich bei der virtuellen Workload Balancing-Appliance

Bevor Sie Dienstbefehle ausführen oder die Datei `wlb.conf` bearbeiten können, müssen Sie sich bei der virtuellen Workload Balancing-Appliance anmelden. Um dies zu tun, müssen Sie einen Benutzernamen und ein Kennwort eingeben. Sofern Sie keine zusätzlichen Benutzerkonten auf der virtuellen Appliance erstellt haben, melden Sie sich mit dem Root-Benutzerkonto an. Sie haben dieses Konto angegeben, als Sie den Konfigurations-Assistenten für den Arbeitslastausgleich ausgeführt haben (bevor Sie Ihren Pool mit dem Workload Balancing verbunden haben) Optional können Sie die Registerkarte **Konsole** in XenCenter verwenden, um sich bei der Appliance anzumelden.

Um sich bei der virtuellen Workload Balancing-Appliance anzumelden:

1. Geben Sie an der Anmeldeaufforderung den Benutzernamen des Kontos ein.
2. Geben Sie in der Kennwortaufforderung das Kennwort für das Konto ein:

> **Hinweis:**
>
> Um sich von der virtuellen Appliance Workload Balancing abzumelden, geben Sie einfach `logout` an der Eingabeaufforderung ein.

`wlb restart`

Führen Sie den Befehl `wlb restart` von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Datenerfassung, den Webdienst und die Datenanalyse für den Arbeitslastenausgleich zu beenden und dann neu zu starten.

`wlb start`

Führen Sie den Befehl `wlb start` von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Workload Balancing-Datenerfassung, den Webdienst und die Datenanalysedienste

`wlb stop`

Führen Sie den Befehl `wlb stop` von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Datenerfassung, den Webdienst und die Datenanalysedienste für den Arbeitslastausgleich

`wlb status`

Führen Sie den Befehl `wlb status` von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um den Status des Workload Balancing-Servers zu ermitteln. Nachdem Sie diesen Befehl ausgeführt haben, wird der Status der drei Workload Balancing-Dienste (Webdienst, Datenerfassungsdienst und Datenanalysedienst) angezeigt.

Ändern der Workload Balancing-Konfigurationsoptionen

Viele Workload Balancing-Konfigurationen, wie die Datenbank- und Webdienst-Konfigurationsoptionen, werden in der Datei `wlb.conf`gespeichert. Die Datei `wlb.conf` ist eine Konfigurationsdatei auf der virtuellen Workload Balancing-Appliance.

Um die am häufigsten verwendeten Optionen zu ändern, verwenden Sie den Befehl `wlb config` . Wenn Sie den Befehl `wlb config` auf der virtuellen Workload Balancing-Appliance ausführen, können Sie das Workload Balancing-Benutzerkonto umbenennen, sein Kennwort ändern oder das PostgreSQL Kennwort ändern. Nachdem Sie diesen Befehl ausgeführt haben, werden die Workload Balancing-Dienste neu gestartet.

Führen Sie den folgenden Befehl auf der virtuellen Appliance Workload Balancing aus:

```
wlb config
<!--NeedCopy-->
```

Auf dem Bildschirm werden eine Reihe von Fragen angezeigt, die Sie beim Ändern Ihres Workload Balancing-Benutzernamens und Kennworts sowie des PostgreSQL-Kennworts unterstützen Befolgen Sie die Fragen auf dem Bildschirm, um diese Elemente zu ändern.

> **Wichtig:**
>
> Überprüfen Sie alle Werte, die Sie in die Datei `wlb.conf` eingeben: Der Workload Balancing überprüft keine Werte in der Datei `wlb.conf`. Wenn die von Ihnen angegebenen Konfigurationsparameter nicht innerhalb des erforderlichen Bereichs liegen, generiert der Workload Balancing daher kein Fehlerprotokoll.

Bearbeiten der Workload Balancing-Konfigurationsdatei

Sie können die Workload Balancing-Konfigurationsoptionen ändern, indem Sie die Datei `wlb.conf` bearbeiten, die im Verzeichnis `/opt/vpx/wlb` auf der virtuellen Workload Balancing-Appliance gespeichert ist. Ändern Sie die Einstellungen in dieser Datei im Allgemeinen nur unter Anleitung von XenServer. Es gibt jedoch drei Kategorien von Einstellungen, die Sie bei Bedarf ändern können:

- **Kontoname und Kennwort für Workload Balancing**. Es ist einfacher, diese Anmeldeinformationen zu ändern, indem Sie den Befehl `wlb config` ausführen.
- **Datenbank-Kennwort**. Dieser Wert kann mit der Datei wlb.conf geändert werden. Wir empfehlen jedoch, es mit dem `wlb config` Befehl zu ändern, da dieser Befehl die Datei wlb.conf ändert und das Kennwort in der Datenbank automatisch aktualisiert. Wenn Sie stattdessen die wlb.conf-Datei ändern möchten, müssen Sie eine Abfrage ausführen, um die Datenbank mit dem neuen Kennwort zu aktualisieren.
- **Parameter für die Datenbankpflege**. Mit dieser Datei können Sie Parameter für die Datenbankpflege ändern, z. B. das Datenbankpflegeintervall, indem Sie den Anweisungen im Abschnitt Datenbankverwaltung folgen. Wenn Sie dies tun, empfehlen wir jedoch, Vorsicht walten zu lassen.

Für alle anderen Einstellungen in der `wlb.conf` Datei empfehlen wir, die Standardeinstellungen beizubehalten, es sei denn, Sie wurden angewiesen, sie zu ändern.

Bearbeiten der Datei `wlb.conf`:

1. Führen Sie an der Eingabeaufforderung auf der virtuellen Workload Balancing-Appliance Folgendes aus (unter Verwendung von VI als Beispiel):

   ```
   vi /opt/vpx/wlb/wlb.conf
   <!--NeedCopy-->
   ```

   Auf dem Bildschirm werden verschiedene Abschnitte mit Konfigurationsoptionen angezeigt.

2. Ändern Sie die Konfigurationsoptionen, und beenden Sie den Editor.

Sie müssen die Workload Balancing-Dienste nicht neu starten, nachdem Sie die Datei `wlb.conf` bearbeitet haben. Die Änderungen treten sofort nach dem Beenden des Editors in Kraft.

> **Wichtig:**
>
> Überprüfen Sie alle Werte, die Sie in die Datei `wlb.conf` eingeben: Der Workload Balancing überprüft keine Werte in der Datei `wlb.conf`. Wenn die von Ihnen angegebenen Konfigurationsparameter nicht innerhalb des erforderlichen Bereichs liegen, generiert der Workload Balancing daher kein Fehlerprotokoll.

Erhöhen Sie die Details im Workload Balancing-Protokoll

Das Workload Balancing-Protokoll enthält eine Liste von Ereignissen auf der virtuellen Workload Balancing-Appliance, einschließlich Aktionen für die Analyse-Engine, die Datenbank und das Überwachungsprotokoll. Diese Protokolldatei befindet sich an diesem Speicherort: `/var/log/wlb/LogFile.log`.

Sie können, falls gewünscht, den Detaillierungsgrad erhöhen, den das Workload Balancing-Protokoll bereitstellt. Ändern Sie dazu den Abschnitt `Trace flags` der Workload Balancing-Konfigurationsdatei (`wlb.conf`) an folgendem Speicherort: `/opt/vpx/wlb/wlb.conf`. Geben Sie 1 oder wahr ein, um die Protokollierung für eine bestimmte Ablaufverfolgung zu aktivieren, und 0 oder falsch, um die Protokollierung Um z. B. die Protokollierung für den Analysis Engine-Trace zu aktivieren, geben Sie

```
AnalEngTrace=1
<!--NeedCopy-->
```

Möglicherweise möchten Sie die Protokollierungsdetails erhöhen, bevor Sie ein Problem an den technischen Support von XenServer melden oder bei der Problembehandlung.

Option Protokollierung	Trace-Flagge	Vorteil oder Zweck
Analyse-Engine Trace	`AnalEngTrace`	Protokolliert Details der Berechnungen des Analyse-Moduls. Zeigt Details der Entscheidungen an, die die Analyse-Engine trifft, und erhält möglicherweise Einblick in die Gründe, warum der Workload Balancing keine Empfehlungen abgibt.
Datenbank-Trace	`DatabaseTrace`	Protokolliert Details zum Lesen/Schreiben von Datenbanken. Wenn Sie diese Ablaufverfolgung aktiviert lassen, wird die Größe der Protokolldatei jedoch schnell erhöht.

Option Protokollierung	Trace-Flagge	Vorteil oder Zweck
Datenerfassung Trace	`DataCollectionTrace`	Protokolliert die Aktionen zum Abrufen von Kennzahlen. Mit diesem Wert können Sie die Metriken sehen, die Workload Balancing abruft und in den Datenspeicher des Workload Balancing einfügt. Wenn Sie diese Ablaufverfolgung aktiviert lassen, wird die Größe der Protokolldatei jedoch schnell erhöht.
Datenkomprimierung Trace	`DataCompactionTrace`	Protokolliert Details darüber, wie viele Millisekunden zum Komprimieren der Metrikdaten benötigt wurden.
Datenereignis-Trace	`DataEventTrace`	Diese Ablaufverfolgung enthält Details zu Ereignissen, die Workload Balancing von XenServer abfängt.
Datenbereinigungs-Trace	`DataGroomingTrace`	Diese Ablaufverfolgung liefert Details zur Datenbankpflege.
Datenmetriken Tra	`DataMetricsTrace`	Protokolliert Details über das Parsen von Metrikdaten. Wenn Sie diese Spur eingeschaltet lassen, wird die Größe der Protokolldatei schnell erhöht.
Warteschlangenverwaltungs-Trace	`QueueManagementTrace`	Protokolliert Details über die Verarbeitung der Warteschlangenverwaltung für Daten (Diese Option ist für den internen Gebrauch bestimmt.)
Daten speichern Trace	`DataSaveTrace`	Protokolliert Details über den Pool, der in der Datenbank gespeichert wird.

Option Protokollierung	Trace-Flagge	Vorteil oder Zweck
Ablaufverfolgung des Ergebnisservers	`ScoreHostTrace`	Protokolliert Details darüber, wie der Workload Balancing zu einem Ergebnis für einen Host kommt. Dieser Trace zeigt die detaillierten Ergebnisse, die von Workload Balancing generiert werden, wenn es die Sternebewertungen für die Auswahl optimaler Hosts für die VM-Platzierung berechnet.
Ablaufverfolgung des Prüfprotokolls	`AuditLogTrace`	Zeigt die Aktion der Überwachungsprotokolldaten an, die erfasst und geschrieben werden. (Diese Option ist nur für den internen Gebrauch bestimmt und liefert keine Informationen, die im Überwachungsprotokoll erfasst werden.) Wenn Sie diese Ablaufverfolgung aktiviert lassen, wird die Größe der Protokolldatei jedoch schnell erhöht.
Ablaufverfolgung für geplante Aufgaben	`ScheduledTaskTrace`	Protokolliert Details zu geplanten Aufgaben. Wenn Ihre geplanten Modusänderungen beispielsweise nicht funktionieren, können Sie diese Ablaufverfolgung aktivieren, um die Ursache zu untersuchen.
Webdienst-Trace	`WlbWebServiceTrace`	Protokolliert Details über die Kommunikation mit der Webservice-Schnittstelle.

Zertifikate für den Workload Balancing

November 9, 2023

XenServer und Workload Balancing kommunizieren über HTTPS. Während der Konfiguration des Workload Balancing erstellt der Assistent automatisch ein selbstsigniertes Testzertifikat. Mit diesem selbstsignierten Testzertifikat kann Workload Balancing eine TLS-Verbindung zu XenServer herstellen. Standardmäßig erstellt Workload Balancing diese TLS-Verbindung mit XenServer automatisch. Sie müssen während oder nach der Konfiguration für den Workload Balancing keine Zertifikatkonfigurationen durchführen, um diese TLS-Verbindung herzustellen.

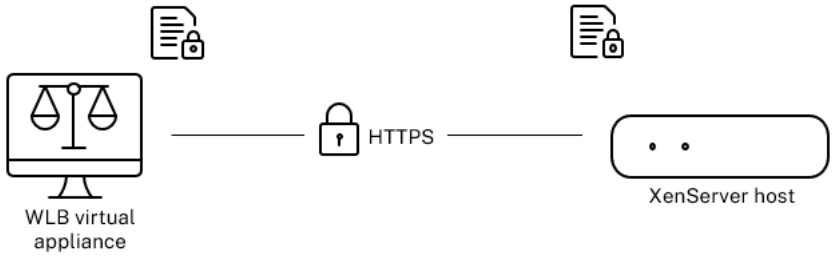
> **Hinweis:**
>
> Das selbstsignierte Zertifikat ist ein Platzhalter zur Erleichterung der HTTPS-Kommunikation und stammt nicht von einer vertrauenswürdigen Zertifizierungsstelle. Für zusätzliche Sicherheit empfehlen wir, ein Zertifikat zu verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Um ein Zertifikat von einer anderen Zertifizierungsstelle zu verwenden, z. B. ein signiertes Zertifikat von einer kommerziellen Zertifizierungsstelle, müssen Sie Workload Balancing und XenServer so konfigurieren, dass es verwendet wird.

Standardmäßig überprüft XenServer die Identität des Zertifikats nicht, bevor eine Verbindung zum Workload Balancing hergestellt wird. Um XenServer so zu konfigurieren, dass es nach einem bestimmten Zertifikat sucht, exportieren Sie das Stammzertifikat, das zum Signieren des Zertifikats verwendet wurde. Kopieren Sie das Zertifikat auf XenServer und konfigurieren Sie XenServer so, dass es überprüft, wenn eine Verbindung zu Workload Balancing hergestellt wird. XenServer fungiert in diesem Szenario als Client und Workload Balancing fungiert als Server.

Abhängig von Ihren Sicherheitszielen können Sie entweder:

- Konfigurieren Sie XenServer, um das selbstsignierte Zertifikat zu überprüfen.
- Konfigurieren Sie XenServer, um ein Zertifikat einer Zertifizierungsstelle zu überprüfen.



> **Hinweis:**
>
> Die Zertifikatsüberprüfung ist eine Sicherheitsmaßnahme, um unerwünschte Verbindungen zu verhindern. Workload Balancing-Zertifikate müssen strenge Anforderungen erfüllen, sonst ist die Zertifikatsüberprüfung nicht erfolgreich. Wenn die Zertifikatsüberprüfung fehlschlägt, lässt XenServer die Verbindung nicht zu.
>
> Damit die Zertifikatsüberprüfung erfolgreich ist, müssen Sie die Zertifikate an den spezifischen Speicherorten speichern, an denen XenServer die Zertifikate voraussichtlich findet.

Konfigurieren Sie XenServer, um das selbstsignierte Zertifikat zu überprüfen

Sie können XenServer so konfigurieren, dass überprüft wird, ob das selbstsignierte Zertifikat von XenServer Workload Balancing authentisch ist, bevor XenServer Workload Balancing die Verbindung zulässt.

> **Wichtig:**
>
> Um das selbstsignierte Zertifikat von XenServer Workload Balancing zu überprüfen, müssen Sie mit seinem Hostnamen eine Verbindung zu Workload Balancing herstellen. Führen Sie den Befehl `hostname` auf der virtuellen Appliance aus, um den Workload Balancing-Hostnamen zu ermitteln.

Gehen Sie wie folgt vor, um XenServer für die Überprüfung des selbstsignierten Zertifikats zu konfigurieren:

1. Kopieren Sie das selbstsignierte Zertifikat von der virtuellen Workload Balancing-Appliance in den Poolkoordinator. Das selbstsignierte Zertifikat von XenServer Workload Balancing wird unter gespeichert. `/etc/ssl/certs/server.pem` Führen Sie den folgenden Befehl auf dem Poolkoordinator aus:

   ```
   scp root@<wlb-ip>:/etc/ssl/certs/server.pem .
   <!--NeedCopy-->
   ```

2. Wenn Sie eine Meldung erhalten, dass die Echtheit von `wlb-ip` nicht festgestellt werden kann, geben Sie `yes` ein, um fortzufahren.

3. Geben Sie das Stammkennwort der virtuellen Workload Balancing-Appliance Das Zertifikat wird in das aktuelle Verzeichnis kopiert.

4. Installieren Sie das Zertifikat. Führen Sie den folgenden Befehl in dem Verzeichnis aus, in das Sie das Zertifikat kopiert haben:

   ```
   xe pool-certificate-install filename=server.pem
   <!--NeedCopy-->
   ```


5. Überprüfen Sie, ob das Zertifikat ordnungsgemäß installiert wurde, indem Sie den folgenden Befehl auf dem Poolkoordinator ausführen:

```
xe pool-certificate-list
<!--NeedCopy-->
```

   Wenn Sie das Zertifikat korrekt installiert haben, enthält die Ausgabe dieses Befehls das exportierte Stammzertifikat. Durch Ausführen dieses Befehls werden alle installierten TLS-Zertifikate einschließlich des von Ihnen installierten Zertifikats aufgeführt.

6. Um das Zertifikat vom Koordinator mit allen Hosts im Pool zu synchronisieren, führen Sie den folgenden Befehl auf dem Poolkoordinator aus:

```
xe pool-certificate-sync
<!--NeedCopy-->
```

   Wenn `pool-certificate-sync` Sie den Befehl auf dem Koordinator ausführen, werden die Zertifikat- und Zertifikatssperrlisten auf allen Pool-Hosts mit dem Koordinator synchronisiert. Diese Aktion stellt sicher, dass alle Hosts im Pool dieselben Zertifikate verwenden.

   Dieser Befehl liefert keine Ausgabe. Der nächste Schritt funktioniert jedoch nicht, wenn dieser nicht erfolgreich funktioniert hat.

7. Weisen Sie XenServer an, das Zertifikat zu überprüfen, bevor Sie eine Verbindung zur virtuellen Workload Balancing-Appliance herstellen. Führen Sie den folgenden Befehl auf dem Poolkoordinator aus:

```
xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
<!--NeedCopy-->
```

   > **Tipp:**
   >
   > Durch Drücken der **Tabulatortaste** wird automatisch die UUID des Pools aufgefüllt.

8. (Optional) Führen Sie die folgenden Schritte aus, um zu überprüfen, ob dieses Verfahren erfolgreich funktioniert hat:

   a) Um zu testen, ob das Zertifikat mit den anderen Hosts im Pool synchronisiert wurde, führen Sie den `pool-certificate-list` Befehl auf diesen Hosts aus.

   b) Um zu testen, ob XenServer für die Überprüfung des Zertifikats eingerichtet wurde, führen Sie den `pool-param-get` Befehl mit dem Parameter `param-name`=wlb-verify-cert aus. Beispiel:

```
xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
<!--NeedCopy-->
```


Konfigurieren Sie XenServer zur Überprüfung eines Zertifizierungsstellenzertifikats

Sie können XenServer so konfigurieren, dass ein Zertifikat überprüft wird, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Für vertrauenswürdige Autoritätszertifikate benötigt XenServer ein exportiertes Zertifikat oder eine exportierte Zertifikatskette (die Zwischen- und Stammzertifikate) in einem `.pem` Format, das den öffentlichen Schlüssel enthält.

Wenn der Workload Balancing ein Zertifikat einer vertrauenswürdigen Behörde verwenden soll, führen Sie die folgenden Aufgaben aus:

1. Beziehen Sie ein signiertes Zertifikat von der Zertifizierungsstelle.
2. Spezifizieren und wenden Sie das neue Zertifikatan.
3. Importieren Sie die Zertifikatkette in den Pool.

Bevor Sie mit diesen Aufgaben beginnen, stellen Sie sicher:

- Sie kennen die IP-Adresse für den XenServer-Poolkoordinator.
- XenServer kann den Hostnamen für den Workload Balancing auflösen. (Sie können beispielsweise versuchen, den Workload Balancing-FQDN von der XenServer-Konsole für den Poolkoordinator aus anzupingen.)

Beziehen Sie ein signiertes Zertifikat von der Zertifizierungsstelle

Um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, müssen Sie eine Certificate Signing Request (CSR) generieren. Erstellen Sie auf der virtuellen Workload Balancing-Appliance einen privaten Schlüssel und verwenden Sie diesen privaten Schlüssel, um die CSR zu generieren.

Richtlinien für die Angabe des Common Name Der Common Name (CN), den Sie beim Erstellen einer CSR angeben, muss genau mit dem FQDN Ihrer virtuellen Workload Balancing-Appliance übereinstimmen. Er muss auch mit dem FQDN oder der IP-Adresse übereinstimmen, die Sie im Feld **Adresse** des Dialogfelds Mit **WLB Server verbinden** angegeben haben.

Um sicherzustellen, dass der Name übereinstimmt, geben Sie den Common Name mithilfe einer der folgenden Richtlinien an:

- Geben Sie für den allgemeinen Namen des Zertifikats dieselben Informationen an, die Sie im Dialogfeld Mit **WLB Server verbinden** angegeben haben.

  Wenn Ihre virtuelle Workload Balancing-Appliance beispielsweise `wlb-vpx.yourdomain` benannt ist, geben Sie `wlb-vpx.yourdomain` im Dialogfeld Mit **WLB-Server verbinden** an und geben Sie beim Erstellen der CSR `wlb-vpx.yourdomain` als allgemeinen Namen an.

- Wenn Sie Ihren Pool über die IP-Adresse mit dem Workload Balancing verbunden haben, verwenden Sie den FQDN als allgemeinen Namen und die IP-Adresse als alternativen Subjektnamen (SAN). Dieser Ansatz funktioniert jedoch möglicherweise nicht in allen Situationen.

Erstellen Sie eine private Schlüsseldatei Führen Sie auf der virtuellen Workload Balancing-Appliance die folgenden Schritte aus:

1. Erstellen Sie eine private Schlüsseldatei:

```
openssl genrsa -des3 -out privatekey.pem 2048
<!--NeedCopy-->
```

2. Entferne das Kennwort:

```
openssl rsa -in privatekey.pem -out privatekey.nop.pem
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie das Kennwort falsch oder inkonsistent eingeben, erhalten Sie möglicherweise einige Meldungen, die darauf hinweisen, dass ein Benutzeroberflächenfehler vorliegt. Sie können die Nachricht ignorieren und den Befehl erneut ausführen, um die private Schlüsseldatei zu erstellen.

Generieren der Zertifikatssignierungsanfrage Führen Sie auf der virtuellen Workload Balancing-Appliance die folgenden Schritte aus:

1. Erstellen Sie die Certificate Signing Request (CSR) mit dem privaten Schlüssel:

```
openssl req -new -key privatekey.nop.pem -out csr
<!--NeedCopy-->
```

2. Befolgen Sie die Anweisungen, um die für die Generierung der CSR erforderlichen Informationen anzugeben:

   Name des Landes. Geben Sie die Ländercodes des TLS-Zertifikats für Ihr Land ein. Zum Beispiel CA für Kanada oder JM für Jamaika. Eine Liste der Ländercodes für TLS-Zertifikate finden Sie im Internet.

   Name des Bundesstaates oder der Provinz (vollständiger Name). Geben Sie den Bundesstaat oder die Provinz an, in der sich der Pool befindet. Zum Beispiel Massachusetts oder Alberta.

   Name der Lokalität. Der Name der Stadt, in der sich der Pool befindet.

   Name der Organisation. Der Name Ihres Unternehmens oder Ihrer Organisation.

Name der Organisationseinheit. Geben Sie den Namen der Abteilung ein. Das Feld ist optional.

Common Name: Geben Sie den FQDN Ihres Workload Balancing-Servers ein. Dieser Wert muss mit dem Namen übereinstimmen, den der Pool für die Verbindung mit dem Workload Balancing verwendet. Weitere Informationen finden Sie unter Richtlinien für die Angabe des allgemeinen Namens.

E-Mail-Adresse: Diese E-Mail-Adresse ist im Zertifikat enthalten, wenn Sie es generieren.

3. Geben Sie optionale Attribute an, oder klicken Sie auf die Eingabetaste, um die

   Die CSR-Anfrage wird im aktuellen Verzeichnis gespeichert und hat den Namen `csr`.

4. Zeigen Sie die CSR im Konsolenfenster an, indem Sie die folgenden Befehle in der Workload Balancing-Appliance-Konsole ausführen:

   ```
   cat csr
   <!--NeedCopy-->
   ```

5. Kopieren Sie die gesamte CSR und verwenden Sie sie, um das Zertifikat von der Zertifizierungsstelle anzufordern.

Spezifizieren und wenden Sie das neue Zertifikat an

Gehen Sie wie folgt vor, um anzugeben, dass der Arbeitslastausgleich ein Zertifikat einer Zertifizierungsstelle verwendet. Bei diesem Verfahren werden die Stammzertifikate und (falls verfügbar) Zwischenzertifikate installiert.

Führen Sie die folgenden Schritte aus, um ein neues Zertifikat anzugeben:

1. Laden Sie das signierte Zertifikat, das Stammzertifikat und, falls die Zertifizierungsstelle über eines verfügt, das Zwischenzertifikat von der Zertifizierungsstelle herunter.
2. Wenn Sie die Zertifikate nicht direkt auf die virtuelle Workload Balancing-Appliance heruntergeladen haben, kopieren Sie sie mit einer der folgenden Methoden:

   - Verwenden Sie auf einem Windows-Computer WinSCP oder ein anderes Kopierdienstprogramm.

     Für den Hostnamen können Sie die IP-Adresse eingeben und den Port auf dem Standardport belassen. Der Benutzername und das Kennwort sind normalerweise root und das Kennwort, das Sie während der Konfiguration festlegen.

   - Verwenden Sie von einem Linux-Computer zur Workload Balancing-Appliance SCP oder ein anderes Kopierdienstprogramm. Beispiel:


```
scp root_ca.pem root@wlb-ip:/path_on_your_WLB
<!--NeedCopy-->
```

3. Führen Sie auf der virtuellen Workload Balancing-Appliance den Inhalt aller Zertifikate (Stammzertifikat, Zwischenzertifikat - falls vorhanden und signiertes Zertifikat) in einer Datei zusammen. Sie können den folgenden Befehl verwenden:

```
cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
<!--NeedCopy-->
```

4. Benennen Sie das vorhandene Zertifikat und den Schlüssel mit dem Befehl move um:

```
mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
<!--NeedCopy-->
```

5. Kopieren Sie das zusammengeführte Zertifikat:

```
mv server.pem /etc/ssl/certs/server.pem
<!--NeedCopy-->
```

6. Kopieren Sie den zuvor erstellten privaten Schlüssel:

```
mv privatekey.nop.pem /etc/ssl/certs/server.key
<!--NeedCopy-->
```

7. Machen Sie den privaten Schlüssel nur von root lesbar. Verwenden Sie den Befehl `chmod`, um Berechtigungen zu korrigieren.

```
chmod 600 /etc/ssl/certs/server.key
<!--NeedCopy-->
```

8. Neustart `stunnel`:

```
killall stunnel
stunnel
<!--NeedCopy-->
```

Importieren Sie die Zertifikatkette in den Pool

Nachdem Sie die Zertifikate erhalten haben, importieren Sie sie in den XenServer-Poolkoordinator. Synchronisieren Sie die Hosts im Pool, um diese Zertifikate zu verwenden. Anschließend können Sie XenServer so konfigurieren, dass die Identität und Gültigkeit des Zertifikats jedes Mal überprüft wird, wenn Workload Balancing eine Verbindung zu einem Host herstellt.

1. Kopieren Sie das signierte Zertifikat, das Stammzertifikat und, falls die Zertifizierungsstelle über eines verfügt, das Zwischenzertifikat von der Zertifizierungsstelle auf den XenServer-Poolkoordinator.

2. Installieren Sie das Rootzertifikat auf dem Poolkoordinator:

```
xe pool-install-ca-certificate filename=root_ca.pem
<!--NeedCopy-->
```

3. Installieren Sie gegebenenfalls das Zwischenzertifikat auf dem Poolkoordinator:

```
xe pool-install-ca-certificate filename=intermediate_ca.pem
<!--NeedCopy-->
```

4. Überprüfen Sie, ob beide Zertifikate korrekt installiert sind, indem Sie diesen Befehl auf dem Poolkoordinator ausführen:

```
xe pool-certificate-list
<!--NeedCopy-->
```

   Durch Ausführen dieses Befehls werden alle installierten TLS-Zertifikate aufgeführt. Wenn die Zertifikate erfolgreich installiert wurden, werden sie in dieser Liste angezeigt.

5. Synchronisieren Sie das Zertifikat auf dem Poolkoordinator mit allen Hosts im Pool:

```
xe pool-certificate-sync
<!--NeedCopy-->
```

   Wenn `pool-certificate-sync` Sie den Befehl auf dem Koordinator ausführen, werden die Zertifikate und Zertifikatssperrlisten auf allen Poolhosts mit dem Poolkoordinator synchronisiert. Diese Aktion stellt sicher, dass alle Hosts im Pool dieselben Zertifikate verwenden.

6. Weisen Sie XenServer an, ein Zertifikat zu überprüfen, bevor Sie eine Verbindung zur virtuellen Workload Balancing-Appliance herstellen. Führen Sie den folgenden Befehl auf dem Poolkoordinator aus:

```
xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
<!--NeedCopy-->
```

   > **Tipp:**
   >
   > Durch Drücken der Tabulatortaste wird automatisch die UUID des Pools aufgefüllt.

7. Wenn Sie im Dialogfeld Mit **WLB verbinden** eine IP-Adresse angegeben haben, bevor Sie die Zertifikatsüberprüfung aktiviert haben, werden Sie möglicherweise aufgefordert, den Pool erneut mit dem Workload Balancing zu verbinden.

   Geben Sie den FQDN für die Workload Balancing-Appliance in **Adresse** im Dialogfeld Mit **WLB verbinden** genau so an, wie er im allgemeinen Namen des Zertifikats angezeigt wird. Geben Sie den FQDN ein, um sicherzustellen, dass der Common Name mit dem Namen übereinstimmt, den XenServer für die Verbindung verwendet.

Problembehandlung

- Wenn der Pool nach dem Konfigurieren der Zertifikatsüberprüfung keine Verbindung zum Workload Balancing herstellen kann, überprüfen Sie, ob der Pool eine Verbindung herstellen kann, wenn Sie die Zertifikatsüberprüfung ausschalten Sie können den Befehl `xe pool-param-set wlb-verify-cert=false uuid=uuid_of_pool` verwenden, um die Zertifikatsüberprüfung zu deaktivieren. Wenn eine Verbindung mit ausgeschalteter Überprüfung hergestellt werden kann, liegt das Problem in Ihrer Zertifikatkonfiguration. Wenn keine Verbindung hergestellt werden kann, liegt das Problem entweder in Ihren Workload Balancing-Anmeldeinformationen oder in Ihrer Netzwerkverbindung.
- Einige kommerzielle Zertifizierungsstellen stellen Tools zur Verfügung, um zu überprüfen, ob das Zertifikat korrekt installiert wurde Erwägen Sie, diese Tools auszuführen, wenn diese Verfahren das Problem nicht isolieren können. Wenn diese Tools die Angabe eines TLS-Ports erfordern, geben Sie Port 8012 oder einen anderen Port an, den Sie während der Konfiguration des Arbeitslastausgleichs festlegen
- Wenn auf der Registerkarte **WLB** ein Verbindungsfehler angezeigt wird, liegt möglicherweise ein Konflikt zwischen dem allgemeinen Namen des Zertifikats und dem Namen der virtuellen Workload Balancing-Appliance vor. Der Name der virtuellen Workload Balancing-Appliance und der allgemeine Name des Zertifikats müssen genau übereinstimmen.

Weitere Informationen finden Sie unter Problembehandlung.

---

layout: doc
description: Diagnose and gather information about issues that might arise when using Workload Balancing.—

Problembehandlung beim Workloadausgleich

Während der Workload Balancing normalerweise reibungslos abläuft, bietet diese Reihe von Abschnitten eine Anleitung für den Fall, dass Probleme auftreten.

> **Hinweise:**
>
> - Workload Balancing ist für Kunden der XenServer Premium Edition verfügbar. Weitere Informationen zur XenServer-Lizenzierung finden Sie unter Lizenzierung. Besuchen Sie die XenServer-Website, um ein Upgrade durchzuführen oder eine XenServer-Lizenz zu kaufen.

> - Workload Balancing 8.3.0 und höher sind mit XenServer 8 und Citrix Hypervisor 8.2 Cumulative Update 1 kompatibel.

Ermitteln des Status der virtuellen Workload Balancing-Appliance

Führen Sie den Befehl `systemctl status workloadbalancing` aus. Weitere Informationen finden Sie unter Befehle für den Workloadausgleich.

Allgemeine Tipps zur Fehlerbehebung

- Starten Sie die Fehlerbehebung, indem Sie die Workload Balancing-Protokolldateien (`LogFile.log` und `wlb_install_log.log`) überprüfen Sie finden diese Protokolle in der virtuellen Workload Balancing-Appliance an diesem Speicherort (standardmäßig):

  `/var/log/wlb`

  Der Detaillierungsgrad in diesen Protokolldateien kann mit der Datei `wlb.conf` konfiguriert werden. Weitere Informationen finden Sie unter Erhöhen der Details im Workload Balancing-Protokoll.

- Weitere Informationen finden Sie in den **Protokollen auf der Registerkarte XenCenter Logs** .

- Um die Build-Nummer der virtuellen Workload Balancing-Appliance zu überprüfen, führen Sie den folgenden Befehl auf einem Host in einem Pool aus, den die virtuelle Appliance überwacht:

  ```
  1  xe pool-retrieve-wlb-diagnostics | more
  2  <!--NeedCopy-->
  ```

  Die Versionsnummer des Workload Balancing wird oben in der Ausgabe angezeigt.

- Die virtuelle Workload Balancing-Appliance basiert auf dem CentOS-Betriebssystem. Wenn in der virtuellen Appliance Probleme mit CPU, Arbeitsspeicher oder Datenträger auftreten, können Sie die standardmäßigen Linux-Protokolle in `/var/log/*` verwenden, um das Problem zu analysieren.

- Verwenden Sie standardmäßige Linux-Debugging- und Leistungsoptimierungsbefehle, um das Verhalten der virtuellen Appliance Zum Beispiel `top`, `ps`, `free`, `sar` und `netstat`.

Fehlermeldungen

Beim Workload Balancing werden Fehler auf dem Bildschirm als Dialogfelder und als Fehlermeldungen auf der Registerkarte **Protokolle** in XenCenter angezeigt.

Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie das XenCenter -Ereignisprotokoll auf weitere Informationen. Weitere Informationen finden Sie in der XenCenter-Produktdokumentation.

Probleme bei der Eingabe von Workload Balancing

Wenn Sie beim Konfigurieren des Dialogfelds Mit **WLB Server verbinden** das Benutzerkonto und das Kennwort der virtuellen Appliance nicht erfolgreich eingeben können, versuchen Sie Folgendes:

- Stellen Sie sicher, dass die virtuelle Workload Balancing-Appliance importiert wurde und korrekt konfiguriert wurde und alle ihre Dienste ausgeführt werden.
- Stellen Sie sicher, dass Sie die richtigen Anmeldeinformationen eingeben. Im Dialog Mit **WLB Server verbinden** werden zwei verschiedene Anmeldeinformationen angefordert:
  - **WLB-Serveranmeldedaten**: XenServer verwendet dieses Konto für die Kommunikation mit Workload Balancing. Sie haben dieses Konto während der Konfiguration des Workloadausgleichs auf der virtuellen Appliance für den Workloadausgleich erstellt Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`.
  - **Citrix Hypervisor-Anmeldeinformationen**: Dieses Konto wird von der virtuellen Workload Balancing-Appliance verwendet, um eine Verbindung zum XenServer-Pool herzustellen. Dieses Konto wird auf dem XenServer-Poolkoordinator erstellt und hat die Rolle `pool-admin` oder `pool-operator`.
- Sie können in das Feld **Adresse** einen Hostnamen eingeben, der jedoch der vollqualifizierte Domänenname (FQDN) der virtuellen Workload Balancing-Appliance sein muss. Geben Sie nicht den Hostnamen des physischen Servers ein, der die Appliance hostet. Wenn Sie Probleme bei der Eingabe eines Computernamens haben, verwenden Sie stattdessen die IP-Adresse der Workload Balancing-Appliance.
- Stellen Sie sicher, dass der Host den richtigen DNS-Server verwendet und der XenServer-Host über seinen FQDN den Workload Balancing-Server kontaktieren kann. Um diese Prüfung durchzuführen, pingen Sie die Workload Balancing-Appliance mit ihrem FQDN vom XenServer-Host aus an. Geben Sie beispielsweise Folgendes in die XenServer-Hostkonsole ein:

```
ping wlb-vpx-1.mydomain.net
<!--NeedCopy-->
```

Probleme mit Firewalls

Der folgende Fehler wird angezeigt, wenn sich die virtuelle Workload Balancing-Appliance hinter einer Hardware-Firewall befindet und Sie die entsprechenden Firewalleinstellungen nicht konfiguriert haben: ”Beim Herstellen einer Verbindung zum Workload Balancing-Server ist ein Fehler aufgetreten: <pool name>Klicken **Initialisieren Sie WLB**, um die Verbindungseinstellungen neu zu initialisieren. “Dieser Fehler kann auch auftreten, wenn die Workload Balancing-Appliance ansonsten nicht erreichbar ist.

Wenn sich die virtuelle Workload Balancing-Appliance hinter einer Firewall befindet, öffnen Sie Port 8012.

Ebenso muss der Port, den XenServer für die Kontaktaufnahme mit Workload Balancing verwendet (standardmäßig 8012), mit der Portnummer übereinstimmen, die Sie beim Ausführen des Workload Balancing-Konfigurationsassistenten angegeben haben.

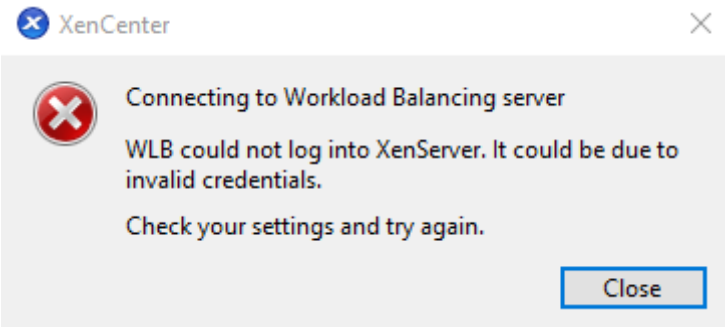
Verbindungsfehler beim Workload Balancing

Wenn Sie nach dem Konfigurieren und Herstellen einer Verbindung mit dem Workload Balancing einen Verbindungsfehler erhalten, sind die Anmeldeinformationen möglicherweise nicht mehr gültig. Um dieses Problem zu isolieren:

1. Stellen Sie sicher, dass die Anmeldeinformationen, die Sie im Dialogfeld Mit **WLB-Server verbinden** eingegeben haben, korrekt sind. Weitere Informationen finden Sie in Szenario 1 und 2.
2. Stellen Sie sicher, dass die IP-Adresse oder der FQDN für die virtuelle Workload Balancing-Appliance, die Sie im Dialogfeld Mit **WLB-Server verbinden** eingegeben haben, korrekt ist.
3. Stellen Sie sicher, dass der Benutzername, den Sie während der Workload Balancing-Konfiguration erstellt haben, mit den Anmeldeinformationen übereinstimmt, die Sie im Dialogfeld Mit **WLB-Server verbinden** eingegeben haben.
4. Wenn Sie in der Zeile Workload Balancing Status auf der Registerkarte **WLB** einen Verbindungsfehler erhalten, müssen Sie möglicherweise den Workload Balancing für diesen Pool neu konfigurieren. Klicken Sie auf der Registerkarte **WLB** auf die Schaltfläche **Verbinden** und geben Sie die Host-Anmeldeinformationen erneut ein.

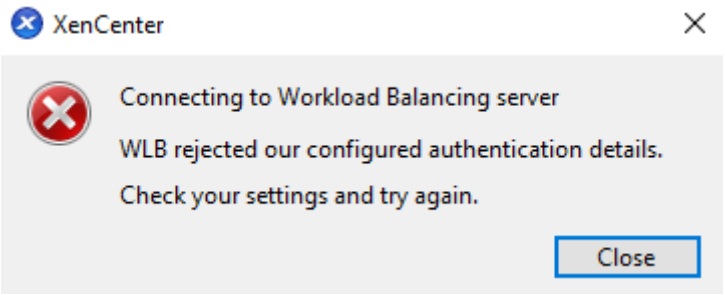
Beim Versuch, eine Verbindung von XenCenter zur virtuellen Workload Balancing-Appliance herzustellen, kann eines der folgenden Szenarien auftreten.

Szenario 1



Dies bedeutet, dass die im Feld **Citrix Hypervisor Credentials im Dialogfeld Mit**WLB-Server verbinden**eingegebenen Anmeldeinformationen** falsch sind. Um dies zu beheben, überprüfen Sie die Anmeldeinformationen oder aktivieren Sie das Kontrollkästchen **Aktuelle XenCenter-Anmeldeinformationen verwenden** .

Szenario 2



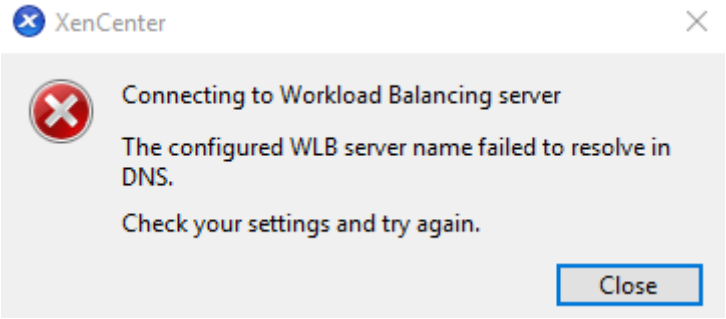
Dies bedeutet, dass beim Versuch, eine Verbindung zur virtuellen Workload Balancing-Appliance herzustellen, ein Problem mit den Anmeldeinformationen besteht, die in das Feld **WLB-Serveranmeldeinformatio** im Dialogfeld **Mit WLB-Server verbinden** eingegeben wurden (entweder der Benutzername oder das Kennwort sind falsch). Dies kann jedoch auch bedeuten, dass der Workload Balancing-Dienst nicht läuft oder dass ein Problem mit der Datenbankkonfigurationsdatei vorliegt.

Um Probleme mit den Anmeldeinformationen zu beheben, stellen Sie sicher, dass Sie den richtigen Benutzernamen und das richtige Kennwort verwenden. Der Standardbenutzername für das Feld **WLB Server Credentials** lautet `wlbuser` (nicht root). Root ist der Standard-Administratorbenutzername. Beachten Sie, dass es sich bei `wlbuser` nicht um einen tatsächlichen Benutzer mit Anmeldeberechtigungen in der Appliance handelt (existiert nicht unter `/etc/passwd`) und diese Anmeldeinformationen daher nur verwendet werden, um eine Verbindung zu Workload Balancing selbst herzustellen. Daher können sie einfach zurückgesetzt werden, indem Sie den Befehl `wlbconfig` ausführen. Informationen zum Ändern Ihrer Anmeldeinformationen finden Sie unter Ändern der Workload Balancing-Anmeldeinformationen. Um den Befehl `wlbconfig` auszuführen, müssen Sie sich als Root bei der Appliance anmelden können. Wenn das Root-Kennwort unbekannt ist, kann es mithilfe des regulären CentOS/RHEL-Kennwortwiederherstellungsverfahrens zurückgesetzt werden.

Wenn Sie Ihre Anmeldeinformationen zurückgesetzt haben, der Fehler aber weiterhin besteht:

1. Überprüfen Sie mithilfe des Befehls `systemctl status workloadbalancing`, ob der Workload Balancing-Prozess ausgeführt wird.
2. Stellen Sie sicher, dass die Datei `wlb.conf` existiert und sich im richtigen Verzeichnis befindet, indem Sie diesen Befehl ausführen: `cat /opt/vpx/wlb/wlb.conf`

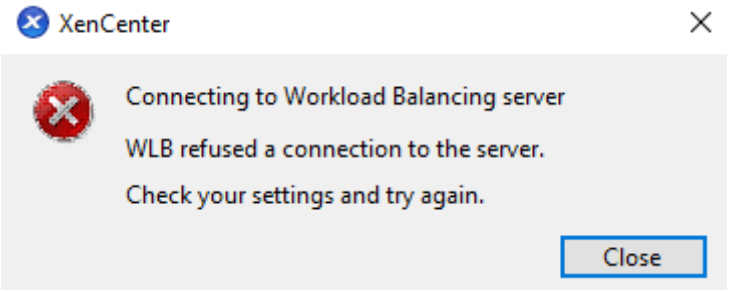
Szenario 3



Dies weist darauf hin, dass bei der Verbindung mit Workload Balancing von XenCenter aus ein Problem mit dem in den Serveradressoptionen angegebenen Port auftritt (entweder wurde der falsche Port eingegeben oder der Port hört nicht zu). Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Stellen Sie sicher, dass die Ziel-Appliance betriebsbereit ist.
2. Überprüfen Sie den Port, der im Fenster mit den Verbindungsdetails von Workload Balancing eingegeben wurde (Standard ist 8012).
3. Stellen Sie sicher, dass dieser Port in der Appliance aktiviert ist und zuhört. Verwenden Sie Befehle wie `telnet <port>` oder `iptables -L`, um festzustellen, ob der Port empfängt oder ob der Datenverkehr auf diesem Port verweigert wird.

Szenario 4



Dieser Fehler tritt auf, wenn es ein Problem mit stunnel gibt (entweder läuft es nicht oder das Zertifikat/Schlüsselpaar ist falsch). Um dieses Problem zu beheben, überprüfen Sie zunächst das Zertifikat und den Schlüssel:

1. Bestätigen Sie, dass das Zertifikat nicht abgelaufen ist, indem Sie den folgenden Befehl ausführen:

```
openssl x509 -dates -in $(grep cert\ = /etc/stunnel/stunnel.conf |
    cut -d '=' -f2) -noout
<!--NeedCopy-->
```


2. Vergleiche den Hexadezimalwert bei der Ausgabe der folgenden 2 Befehle. Wenn die Ausgabe nicht übereinstimmt, wird der falsche Schlüssel verwendet.

```
openssl x509 -modulus -in $(grep cert\ = /etc/stunnel/stunnel.conf
    |cut -d '=' -f2) -noout | openssl md5
<!--NeedCopy-->
```

und

```
 openssl rsa -modulus -in $(grep key\ = /etc/stunnel/stunnel.conf
   | cut -d '=' -f2) -noout | openssl md5
<!--NeedCopy-->
```

Wenn es keine Probleme mit dem Zertifikat und dem Schlüssel gibt, vergewissere dich, dass stunnel läuft und an Port 8012 (oder den konfigurierten Port) gebunden ist:

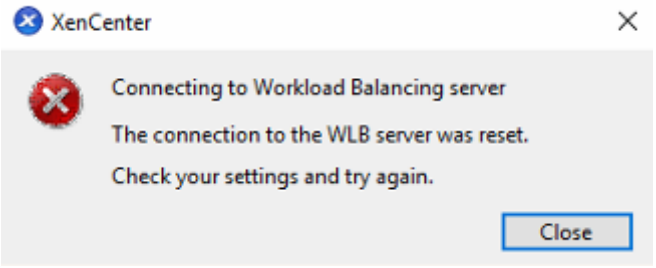
1. Führen Sie den folgenden Befehl in der CLI der WLB-Appliance aus:

```
netstat -tulpn
<!--NeedCopy-->
```

   Am Ausgang sollte 8012 (oder der benutzerdefinierte Port) Folgendes anzeigen: `status: LISTEN`.

2. Wenn der Appliance der Speicherplatz ausgeht, läuft stunnel nicht. Verwenden Sie Befehle wie `df -h` oder `du -hs /*`, um zu sehen, ob auf Ihrer Appliance genügend Speicherplatz verfügbar ist. Informationen zur Erhöhung des Speicherplatzes finden Sie unter Datenträger der virtuellen Appliance erweitern.

Szenario 5



Dieser Fehler kann auftreten, weil der Stunnelprozess beendet wurde. Wenn ein Neustart des Prozesses zu denselben Ergebnissen führt, starten Sie die virtuelle Workload Balancing-Appliance neu.

Alle anderen Fehler

Wenn Sie beim Versuch, eine Verbindung zum Workload Balancing herzustellen, auf weitere Fehler stoßen oder weitere Unterstützung bei der Durchführung der obigen Schritte benötigen, erfassen Sie die Workload Balancing-Protokolle, die Sie im Verzeichnis `/var/log/wlb` der Workload Balancing-Appliance finden.

Wenden Sie sich an den Support, um weitere Unterstützung zu erhalten.

Der Workloadausgleich funktioniert nicht mehr

Wenn der Workload Balancing nicht funktioniert (z. B. können Sie keine Änderungen an den Einstellungen speichern), überprüfen Sie die Workload Balancing-Protokolldatei auf die folgende Fehlermeldung:

```
dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
<!--NeedCopy-->
```

Dieser Fehler tritt normalerweise in Pools auf, die über eine oder mehrere problematische VMs verfügen. Wenn virtuelle Computer problematisch sind, wird möglicherweise das folgende Verhalten angezeigt:

- **Windows**. Die Windows-VM stürzt aufgrund eines Stoppfehlers (“blauer Bildschirm”) ab.
- **Linux**. Die Linux-VM reagiert möglicherweise nicht in der Konsole und wird normalerweise nicht heruntergefahren.

So umgehen Sie dieses Problem:

1. Erzwingt das Herunterfahren der VM. Um dies zu tun, können Sie auf dem Host mit der problematischen VM einen der folgenden Schritte ausführen:

   - Wählen Sie in XenCenter die VM aus und klicken Sie dann im VM-Menü auf **Force Shutdown**.
   - Führen Sie den xe-Befehl `vm-shutdown` mit dem Force-Parameter auf **`true`** aus. Beispiel:

     ```
     xe vm-shutdown force=true uuid=vm_uuid
     <!--NeedCopy-->
     ```

     Sie finden die Host-UUID auf der Registerkarte **Allgemein** für diesen Host (in XenCenter) oder indem Sie den xe-Befehl `host-list` ausführen. Sie finden die VM-UUID auf der Registerkarte **Allgemein** für die VM oder indem Sie den xe-Befehl `vm-list` ausführen. Weitere Informationen finden Sie unter Befehlszeilenschnittstelle.

2. Migrieren Sie im `xsconsole` des XenServer, das die abgestürzte VM bedient, oder in XenCenter alle VMs auf einen anderen Host und führen Sie dann den Befehl `xe-toolstack-restart` aus. (Starten Sie den Toolstack nicht neu, solange HA aktiviert ist. Wenn möglich, deaktivieren Sie HA vorübergehend, bevor Sie den Toolstack neu starten.)

Probleme beim Ändern von Workload-Balancing-Servern

Wenn Sie einen Pool mit einem anderen Workload Balancing-Server verbinden, ohne die Verbindung zum Workload Balancing zu trennen, überwachen sowohl alte als auch neue Workload Balancing-Server den Pool.

Um dieses Problem zu lösen, können Sie eine der folgenden Aktionen ausführen:

- Fahren Sie die alte virtuelle Workload Balancing Appliance herunter und löschen Sie sie
- Beenden Sie die Workload Balancing-Dienste manuell. Diese Dienste sind Analyse, Datensammler und Webdienst.

> **Hinweis:**
>
> Verwenden Sie den xe-Befehl `pool-deconfigure-wlb` nicht, um einen Pool von der virtuellen Workload Balancing-Appliance zu trennen, oder verwenden Sie den xe-Befehl `pool-initialize-wlb`, um eine andere Appliance anzugeben.

---

layout: doc
description: Convert VMware ESXi/vCenter VMs to XenServer VMs that have networking and storage configured and are ready to run in your environment.—

XenServer Conversion Manager

Verwenden Sie die virtuelle XenServer Conversion Manager-Appliance, um Ihre VMware ESXi/vCenter-VMs schnell und effizient auf XenServer zu migrieren. Sie können bis zu 10 VMware ESXi/vCenter VMs gleichzeitig parallel konvertieren. Nach der Konvertierung Ihrer VMs fährt der Conversion Manager automatisch von selbst herunter, wodurch Ressourcen auf dem Host eingespart werden.

Im Rahmen der Migration hilft Ihnen XenCenter dabei, die VMs für die Netzwerk- und Speicherkonnektivität vorzubereiten. Nachdem Sie Ihre VMs in eine XenServer-Umgebung konvertiert haben, sind sie fast betriebsbereit.

Übersicht

XenServer ermöglicht Ihnen:

- Mit einem einfachen Assistenten können Sie bis zu 10 VMware ESXi/vCenter VMs parallel konvertieren.
- Ordnen Sie Netzwerkeinstellungen zwischen VMware und XenServer zu, damit Ihre konvertierten VMs mit den richtigen Netzwerkeinstellungen betriebsbereit sind
- Wählen Sie einen Speicherort aus, an dem Ihre neuen XenServer-VMs ausgeführt werden sollen.

> **Hinweise:**
>
> - XenCenter entfernt oder ändert Ihre vorhandene VMware-Umgebung nicht. VMs werden in Ihrer XenServer-Umgebung dupliziert und nicht aus VMware entfernt.
> - Die virtuelle XenServer Conversion Manager-Appliance unterstützt die Konvertierung von VMware ESXi/vCenter-VMs mit unterschiedlichem Speicher wie Thin Provisioning, Thick Provisioning, IDE und SCSI.
> - Für die virtuelle XenServer Conversion Manager-Appliance müssen auf den Quell-VMs keine VMware Tools installiert sein. Sie können die Konvertierung auf VMware ESXi/vCenter-VMs durchführen, unabhängig davon, ob auf ihnen VMware Tools installiert sind.
> - Die virtuelle XenServer Conversion Manager-Appliance kann keine VMware ESXi/vCenter-VMs mit vier oder mehr Datenträgern in XenServer-VMs konvertieren. Ihre VMware ESXi/vCenter VMs müssen über drei oder weniger Datenträger verfügen.

XenServer verstehen

Bevor Sie Ihre Umgebung konvertieren können, sollten Sie sich mit den XenServer-Konzepten vertraut machen. Weitere Informationen finden Sie unter Technischer Überblick.

Führen Sie die folgenden Aufgaben aus, um VMware ESXi/vCenter VMs erfolgreich in XenServer zu konvertieren:

- Richten Sie eine grundlegende XenServer-Umgebung ein, einschließlich der Installation von XenServer. Weitere Informationen finden Sie unter Schnellstart und Installation.
- Erstellen Sie ein Netzwerk in XenServer und weisen Sie einer NIC eine IP-Adresse zu. Weitere Informationen finden Sie unter Schnellstart.
- Verbinden Sie sich mit Speicher. Weitere Informationen finden Sie unter Schnellstart.

Vergleichen Sie die VMware- und XenServer-Terminologie In der folgenden Tabelle ist das ungefähre XenServer-Äquivalent für allgemeine Funktionen, Konzepte und Komponenten von VMware aufgeführt:

VMware-Begriff	XenServer-Äquivalent
VMware vSphere Client	XenCenter (die Managementkonsole für XenServer)
Cluster/Ressourcenpool	Ressourcen-Pool
Datenspeicher	Speicherrepository
vMotion	Livemigration
Verteilte Ressourcenplanung (DRS)	Workload Balancing
Hochverfügbarkeit (HA)	Hochverfügbarkeit (HA)
vCenter Konverter	Virtuelles XenServer Conversion Manager-Appliance
Rollenbasierte Zugriffssteuerung (RBAC)	Rollenbasierte Zugriffssteuerung (RBAC)

Überblick über die Konvertierung

Die virtuelle XenCenter- und XenServer Conversion Manager-Appliance erstellt eine Kopie jeder Ziel-VM. Nach der Konvertierung der Ziel-VM in eine XenServer-VM mit vergleichbarer Netzwerk- und Speicherkonnektivität importiert XenCenter die VM in Ihren XenServer-Pool oder -Host. Sie können nur eine oder zwei VMs konvertieren oder Batchkonvertierungen einer gesamten Umgebung mit bis zu 10 VMware ESXi/vCenter-VMs gleichzeitig parallel durchführen.

> **Hinweis:**
>
> Bevor Sie die virtuellen Maschinen aus vSphere konvertieren, müssen Sie die virtuellen Maschinen (für die Konvertierung vorgesehen) auf vSphere herunterfahren. Die virtuelle XenServer Conversion Manager-Appliance unterstützt nicht die Konvertierung einer laufenden VM mit Speicher, der von vSphere auf XenServer kopiert wurde.
>
> Stellen Sie außerdem vor der Konvertierung sicher, dass ein Netzwerk und ein Speichercontroller in Ihrer VMware-VM vorhanden sind.

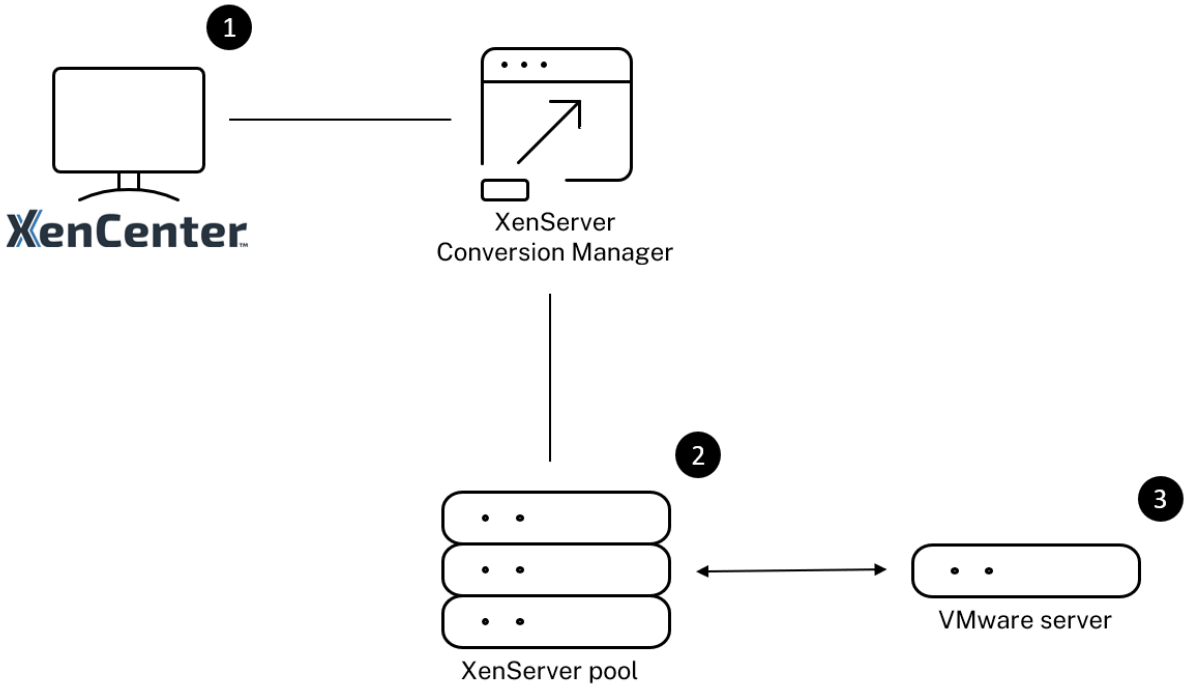
Für den Konvertierungsprozess sind vier Punkte erforderlich:

- **XenCenter** —Die XenServer-Verwaltungsoberfläche enthält einen Konvertierungsassistenten, mit dem Sie Konvertierungsoptionen festlegen und die Konvertierung steuern können. Sie können XenCenter auf Ihrem Windows-Desktop installieren. XenCenter muss in der Lage sein,

eine Verbindung zu XenServer und der virtuellen XenServer Conversion Manager-Appliance herzustellen.

- **Virtuelle XenServer Conversion Manager-Appliance** —eine vorkonfigurierte VM, die Sie in den XenServer-Host oder -Pool importieren, auf dem Sie die konvertierten VMs ausführen möchten. Die virtuelle Appliance konvertiert die Kopien der VMware ESXi/vCenter-VMs in das XenServer-Format für virtuelle Maschinen. Nach der Konvertierung werden diese Kopien in den XenServer-Pool oder -Host importiert.
- **Eigenständiger XenServer-Host oder -Pool** —die XenServer-Umgebung, in der Sie die konvertierten VMs ausführen möchten.
- **VMware-Server**: XenServer Conversion Manager benötigt eine Verbindung zu einem VMware-Server, der die VMs verwaltet, die Sie konvertieren möchten. Diese Verbindung kann zu einem vCenter Server, ESXi Server oder ESX Server bestehen. Die virtuellen Maschinen werden nicht vom VMware-Server entfernt. Stattdessen erstellt die virtuelle XenServer Conversion Manager-Appliance eine Kopie dieser VMs und konvertiert sie in das XenServer-Format für virtuelle Maschinen.

Die folgende Abbildung zeigt die Beziehungen zwischen diesen Komponenten:



> Diese Abbildung zeigt:
>
> 1. Wie XenCenter mit der virtuellen XenServer Conversion Manager-Appliance kommuniziert.
> 2. So authentifiziert sich die virtuelle XenServer Conversion Manager-Appliance beim VMware-Server.

3. Wie der VMware-Server während der Konvertierung auf die virtuelle XenServer Conversion Manager-Appliance reagiert.

Der VMware-Server kommuniziert nur dann mit der virtuellen XenServer Conversion Manager-Appliance, wenn die Appliance während der Konvertierung Umgebungsinformationen und Datenträgerdaten vom VMware-Server abfragt.

Zusammenfassung der Konvertierung von virtuellen Rechnern Sie können die virtuelle XenServer Conversion Manager-Appliance konfigurieren und mit der Konvertierung von VMs in nur wenigen einfachen Schritten beginnen:

1. Laden Sie das virtuelle XenServer Conversion Manager-Appliance von der XenServer-Downloadseite herunter.
2. Importieren Sie das virtuelle XenServer Conversion Manager-Appliance mit XenCenter in XenServer.
3. Konfigurieren Sie die virtuelle XenServer Conversion Manager-Appliance mithilfe von XenCenter.
4. Starten Sie in XenCenter den Konvertierungsassistenten und beginnen Sie mit der Konvertierung von VMs.
5. Führen Sie die Aufgaben nach der Konvertierung aus, zu denen auch die Installation von XenServer VM Tools für Windows auf Ihren Windows-VMs gehört. Bei Linux-VMs installiert der XenServer Conversion Manager während des Konvertierungsvorgangs automatisch die XenServer VM Tools für Linux.

Nach der Konvertierung Ihrer VMs fährt der Conversion Manager automatisch von selbst herunter, wodurch Ressourcen auf dem Host eingespart werden. Weitere Informationen zur Konvertierung von VMware ESXi/vCenter VMs finden Sie unter Erste Schritte mit Conversion Manager.

---

layout: doc
description: Discover the features added in the latest XenServer Conversion Manager virtual appliance.—

Neue Features in XenServer Conversion Manager

Die neueste Version der virtuellen XenServer Conversion Manager-Appliance ist Version 8.3.1. Sie können diese Version der virtuellen XenServer Conversion Manager-Appliance von der XenServer-Downloadseite herunterladen.

Wenn Sie bereits eine frühere Version der virtuellen XenServer Conversion Manager-Appliance installiert haben und ein Upgrade auf die neueste Version durchführen möchten, gibt es keinen automatischen Upgrade-Pfad. Laden Sie die neueste Version der virtuellen Appliance herunter und entfernen Sie die ältere Version von Ihrem System.

Neue Features in 8.3.1

Veröffentlicht am 1. Februar 2024

Dieses Update beinhaltet die folgende Verbesserung:

- Sie können jetzt bis zu 10 VMware ESXi/vCenter VMs gleichzeitig parallel konvertieren.

---

layout: doc
description: Install and set up the XenServer Conversion Manager virtual appliance to benefit from the Conversion Manager feature in your XenServer pools.—

Erste Schritte mit XenServer Conversion Manager

Sie können Ihre virtuellen Maschinen (VMs) von VMware ESXi/vCenter ganz einfach in nur wenigen Schritten zu XenServer konvertieren:

1. Bereiten Sie Ihre XenServer-Umgebung vor und überprüfen Sie die erforderlichen Informationen.
2. Importieren und konfigurieren Sie die virtuelle XenServer Conversion Manager-Appliance mit XenCenter.

   > **Hinweis:**
   >
   > Wenn Sie bereits eine frühere Version der virtuellen XenServer Conversion Manager-Appliance installiert haben und ein Upgrade auf die neueste Version durchführen möchten, gibt es keinen automatischen Upgrade-Pfad. Laden Sie die neueste Version der virtuellen Appliance von der XenServer-Downloadseite herunter und entfernen Sie die ältere Version von Ihrem System.

3. Starten Sie in XenCenter den Konvertierungsassistenten und beginnen Sie mit der Konvertierung Ihrer VMware ESXi/vCenter-VMs in XenServer.
4. Erledigen Sie die Aufgaben nach der Konvertierung.
5. Sehen Sie sich andere Konvertierungsaufgaben an.

Bereiten Sie Ihre Umgebung vor

Bevor Sie Ihre VMware-Umgebung konvertieren, müssen Sie den eigenständigen XenServer-Zielhost oder -Pool für die Ausführung der konvertierten VMware ESXi/vCenter-VMs erstellen und vorbereiten. Die Vorbereitung Ihrer Umgebung umfasst die folgenden Aktivitäten:

1. Definieren einer Strategie für die Konvertierung Ihrer VMware-Umgebung. Möchten Sie 1 oder 2 virtuelle Maschinen konvertieren? Möchten Sie Ihre gesamte Umgebung umwandeln? Möchten Sie zuerst einen Piloten erstellen, um sicherzustellen, dass Ihre Konfiguration korrekt ist? Führen Sie beide Umgebungen parallel aus? Möchten Sie Ihr vorhandenes Clusterdesign beibehalten, wenn Sie zu XenServer konvertieren?
2. Planen Sie Ihre Netzwerkkonfiguration. Möchten Sie eine Verbindung zu denselben physischen Netzwerken herstellen? Möchten Sie Ihre Netzwerkkonfiguration vereinfachen oder ändern?
3. Installieren Sie XenServer auf den Hosts, die Sie im Pool haben möchten. Schließen Sie im Idealfall die Netzwerkkarten der Hosts an ihre physischen Netzwerke an, bevor Sie mit der Installation beginnen.
4. Erstellen eines Pools und Durchführen einer beliebigen grundlegenden Netzwerkkonfiguration. Gehen Sie zum Beispiel wie folgt vor:
    - Konfigurieren Sie ein Netzwerk für die Verbindung mit dem VMware-Cluster auf dem XenServer-Host (wenn sich der Cluster nicht im selben Netzwerk wie der XenServer-Host befindet).
    - Konfigurieren Sie ein Netzwerk für die Verbindung mit dem Speicher-Array. Das heißt, wenn Sie IP-basierten Speicher verwenden, erstellen Sie ein XenServer-Netzwerk, das eine Verbindung zum physischen Netzwerk des Storage-Arrays herstellt.
    - Erstellen Sie einen Pool und fügen Sie diesem Pool Hosts hinzu.
5. (Für gemeinsam genutzten Speicher und XenServer-Pools.) Vorbereiten des gemeinsam genutzten Speichers, in dem Sie die virtuellen Laufwerke speichern, und Herstellen einer Verbindung zum Speicher, einem sogenannten Speicher-Repository (SR), im Pool.
6. (Fakultativ.) Obwohl dies für die Konvertierung nicht erforderlich ist, möchten Sie möglicherweise die Administratorkonten im XenServer-Pool so konfigurieren, dass sie mit diesen Konten auf dem VMware-Server übereinstimmen. Informationen zum Konfigurieren der rollenbasierten Zugriffssteuerung für Active Directory-Konten finden Sie unter Rollenbasierte Zugriffssteuerung.

Installieren Sie XenServer und erstellen Sie einen Pool

Bevor Sie VMware ESXi/vCenter VMs konvertieren können, stellen Sie sicher, dass Sie einen XenServer-Pool oder Host erstellen, auf dem Sie die konvertierten VMs ausführen möchten. Für diesen Pool muss ein Netzwerk konfiguriert sein, damit er eine Verbindung zum VMware-Server herstellen kann. Möglicherweise möchten Sie auch dieselben physischen Netzwerke im XenServer-Pool konfigurieren, die Sie im VMware-Cluster haben, oder Ihre Netzwerkkonfiguration vereinfachen. Wenn Sie die konvertierten VMs in einem Pool ausführen möchten, erstellen Sie vor der Konvertierung ein Speicherrepository und fügen Sie den freigegebenen Speicher dem Pool hinzu.

Wenn Sie mit XenServer noch nicht vertraut sind, können Sie sich unter Schnellstartüber die Grundlagen von XenServer, einschließlich der grundlegenden Installation und Konfiguration, informieren.

Überlegungen zur XenServer-Umgebung

Bevor Sie XenServer installieren und das virtuelle Gerät importieren, sollten Sie die folgenden Faktoren berücksichtigen, die Ihre Konvertierungsstrategie ändern könnten:

Wählen Sie den Host aus, auf dem Sie das virtuelle XenServer Conversion Manager-Appliance ausführen möchten. Importieren Sie die virtuelle Appliance in den eigenständigen Host oder in einen Host im Pool, auf dem Sie die konvertierten VMs ausführen.

Für Pools können Sie die virtuelle Appliance auf jedem Host im Pool ausführen, sofern der Speicher die Speicheranforderungen erfüllt.

> **Hinweis:**
>
> Es wird empfohlen, dass jeweils nur ein XenServer Conversion Manager in einem Pool ausgeführt wird.

Der für den Pool oder den Host konfigurierte Speicher, auf dem die konvertierten VMs ausgeführt werden sollen, muss bestimmte Anforderungen erfüllen. Wenn Sie Ihre neu konvertierten VMs in einem Pool ausführen möchten, müssen ihre virtuellen Datenträger im freigegebenen Speicher gespeichert werden. Wenn die konvertierten VMs jedoch auf einem einzelnen eigenständigen Host (nicht in einem Pool) ausgeführt werden, können ihre virtuellen Datenträger lokalen Speicher verwenden.

Wenn Sie die konvertierten VMs in einem Pool ausführen möchten, müssen Sie den freigegebenen Speicher zum Pool hinzufügen, indem Sie ein Speicherrepository erstellen.

Für die Konvertierung unterstützte Gastbetriebssysteme:

Sie können VMware ESXi/vCenter VMs konvertieren, auf denen die folgenden Windows-Gastbetriebssysteme ausgeführt werden:

- Windows 10 (64 Bit) Enterprise Edition
- Windows Server 2016 (64 Bit) Standardausgabe (Desktop)
- Windows Server 2019 (64 Bit) Standardausgabe (Desktop)
- Windows Server 2022 (64 Bit) Standardausgabe (Desktop)

> **Hinweis:**
>
> Nur die aufgelisteten Windows-SKUs werden für die Konvertierung unterstützt.

Die folgenden Linux-Betriebssysteme werden ebenfalls unterstützt:

- Red Hat Enterprise Linux 7.9 (64-Bit) mit der folgenden Konfiguration:
  - Dateisystem: EXT3 oder EXT4
  - Bootpartitionstyp: btrfs, lvm oder plain
- Red Hat Enterprise Linux 8.x (64-Bit) mit der folgenden Konfiguration:
  - Dateisystem: EXT3 oder EXT4
  - Bootpartitionstyp: lvm oder plain
- Ubuntu 20.04 mit der folgenden Konfiguration:
  - Dateisystem: EXT3 oder EXT4
  - Bootpartitionstyp: lvm oder regulär

Weitere Informationen zu den von XenServer unterstützten Gastbetriebssystemen finden Sie unter Unterstützung für Gastbetriebssysteme.

Erfüllen der Netzwerkanforderungen Um VMware ESXi/vCenter VMs zu konvertieren, benötigt die virtuelle XenServer Conversion Manager-Appliance Konnektivität zu einem physischen Netzwerk oder VLAN, das den VMware-Server kontaktieren kann. (In den folgenden Abschnitten wird dieses Netzwerk als “VMware-Netzwerk”bezeichnet.)

Wenn sich der VMware-Server in einem anderen physischen Netzwerk befindet als die Hosts im XenServer-Pool, fügen Sie das Netzwerk vor der Konvertierung zu XenServer hinzu.

> **Hinweis:**
>
> - Die Zeit, die für die Konvertierung Ihrer VMs benötigt wird, hängt von der physischen Entfernung zwischen Ihren VMware- und XenServer-Netzwerken sowie von der Größe der virtuellen Datenträger Ihrer VM ab. Sie können abschätzen, wie lange die Konvertierung dauern wird, indem Sie den Netzwerkdurchsatz zwischen Ihrem VMware-Server und XenServer testen.
> - Standardmäßig verwendet der XenServer Conversion Manager HTTPS, um den virtuellen

> Datenträger der VM während der VM-Konvertierung herunterzuladen. Um den Migrationsprozess zu beschleunigen, können Sie den Download-Pfad auf HTTP umstellen. Weitere Informationen finden Sie im VMware-Artikel Verbesserung der Übertragungsgeschwindigkeit von Aufgaben mit Bibliothekselementen.

Ordnen Sie Ihre vorhandene Netzwerkkonfiguration zu Die virtuelle XenServer Conversion Manager-Appliance enthält Funktionen, mit denen Sie den Umfang der manuellen Netzwerkkonfiguration reduzieren können, die nach der Konvertierung Ihrer vorhandenen VMware ESXi/vCenter-VMs auf XenServer erforderlich ist. Die virtuelle XenServer Conversion Manager-Appliance wird beispielsweise:

- Behalten Sie virtuelle MAC-Adressen auf den VMware ESXi/vCenter-VMs bei und verwenden Sie sie in den resultierenden XenServer-VMs wieder. Das Beibehalten der mit virtuellen Netzwerkadaptern verknüpften MAC-Adressen (virtuelle MAC-Adressen) kann:
  - Helfen Sie dabei, IP-Adressen in Umgebungen mit DHCP zu bewahren
  - Seien Sie nützlich für Softwareprogramme, deren Lizenzierung sich auf die virtuellen MAC-Adressen
- Ordnen Sie (virtuelle) Netzwerkadapter zu. Die virtuelle XenServer Conversion Manager-Appliance kann VMware-Netzwerke XenServer-Netzwerken zuordnen, sodass ihre virtuellen Netzwerkschnittstellen nach der Konvertierung der VMs entsprechend verbunden werden.

  Wenn Sie beispielsweise VMware “Virtual Network 4”XenServer “Network 0”zuordnen, wird jede VMware-VM, deren virtueller Adapter mit “Virtual Network 4”verbunden war, nach der Konvertierung mit “Network 0”verbunden. Die virtuelle XenServer Conversion Manager-Appliance konvertiert oder migriert keine Hypervisor-Netzwerkeinstellungen. Der Assistent ändert nur die virtuellen Netzwerkschnittstellenverbindungen einer konvertierten VM basierend auf den bereitgestellten Zuordnungen.

  > **Hinweis:**
  >
  > Sie müssen nicht alle Ihre VMware-Netzwerke den entsprechenden XenServer-Netzwerken zuordnen. Wenn Sie möchten, können Sie jedoch die von den VMs verwendeten Netzwerke ändern, die Anzahl der Netzwerke in Ihrer neuen XenServer-Konfiguration reduzieren oder konsolidieren.

  Um den größtmöglichen Nutzen aus diesen Funktionen zu ziehen, empfehlen wir Folgendes:

  - Schließen Sie vor der Installation von XenServer die Hosts an die Netzwerke auf dem Switch (d. h. die Ports) an, die Sie auf dem Host konfigurieren möchten.

- Stellen Sie sicher, dass der XenServer-Pool die Netzwerke sehen kann, die erkannt werden sollen. Schließen Sie die XenServer-Hosts insbesondere an Switch-Ports an, die auf dieselben Netzwerke zugreifen können wie der VMware-Cluster.

Es ist zwar einfacher, die XenServer-NICs an dieselben Netzwerke anzuschließen wie die NICs auf den VMware-Hosts, dies ist jedoch nicht erforderlich. Wenn Sie die NIC/Netzwerk-Zuordnung ändern möchten, können Sie eine XenServer-NIC an ein anderes physisches Netzwerk anschließen.

Bereiten Sie sich auf die Netzwerkanforderungen für virtuelle XenServer Conversion Manager-Appliances vor Wenn Sie eine Konvertierung durchführen, müssen Sie eine Netzwerkverbindung zu dem Netzwerk herstellen, in dem sich der VMware-Server befindet. Die virtuelle XenServer Conversion Manager-Appliance verwendet diese Verbindung für den Konvertierungsverkehr zwischen dem XenServer-Host und dem VMware-Server.

Um diese Netzwerkverbindung herzustellen, müssen Sie zwei Aufgaben ausführen:

- Wenn Sie das virtuelle XenServer Conversion Manager-Appliance importieren, geben Sie das Netzwerk, das Sie für den Konvertierungsverkehr hinzugefügt haben, als virtuelle Netzwerkschnittstelle an. Sie können dies tun, indem Sie **Schnittstelle 1** so konfigurieren, dass eine Verbindung zu diesem Netzwerk hergestellt wird.
- Bevor Sie den Konvertierungsassistenten ausführen, fügen Sie das Netzwerk, das VMware und XenServer verbindet, dem XenServer-Host hinzu, auf dem Sie die konvertierten VMs ausführen möchten.

Wenn Sie die virtuelle XenServer Conversion Manager-Appliance importieren, erstellt XenCenter standardmäßig eine virtuelle Netzwerkschnittstelle, die Network 0 und NIC0 (eth0) zugeordnet ist. Standardmäßig konfiguriert das XenServer-Setup NIC0 jedoch als *Verwaltungsschnittstelle, eine NIC, die für den XenServer-Verwaltungsverkehr*verwendet wird. Wenn Sie ein Netzwerk für die Konvertierung hinzufügen, sollten Sie daher möglicherweise eine andere Netzwerkkarte als NIC0 auswählen. Die Auswahl eines anderen Netzwerks kann die Leistung in stark frequentierten Pools verbessern. Weitere Informationen zur Verwaltungsschnittstelle finden Sie unter Netzwerk.

Um ein Netzwerk zu XenServer hinzuzufügen:

1. Wählen Sie im **Ressourcenbereich** in XenCenter den Pool aus, in dem Sie die virtuelle XenServer Conversion Manager-Appliance ausführen möchten.
2. Klicken Sie auf die Registerkarte **Netzwerk** .
3. Klicken Sie auf **Netzwerk hinzufügen**.
4. Wählen Sie auf der Seite **Typ auswählenExternes Netzwerk**aus, und klicken Sie auf**Weiter**.

5. Geben Sie auf der Seite **Name** einen aussagekräftigen Namen für das Netzwerk (z. B. “VMware-Netzwerk”) und eine Beschreibung ein.
6. Geben Sie auf der Seite **Interface** Folgendes an:
    - **NIC**. Die NIC, die XenServer zum Erstellen des Netzwerks verwenden soll. Wählen Sie die Netzwerkkarte aus, die an das physische oder logische Netzwerk des VMware-Servers angeschlossen ist.
    - **VLAN**. Wenn das VMware-Netzwerk ein VLAN ist, geben Sie die VLAN-ID (oder “Tag”) ein.
    - **MTU**. Wenn das VMware-Netzwerk Jumbo-Frames verwendet, geben Sie einen Wert für die Maximum Transmission Unit (MTU) zwischen 1500 und 9216 ein. Andernfalls belassen Sie den Standardwert 1500 für das MTU-Feld.

      > **Hinweis:**
      >
      > Aktivieren Sie nicht das Kontrollkästchen **Dieses Netzwerk automatisch zu neuen virtuellen Maschinen hinzufügen** .
7. Klicken Sie auf **Fertigstellen**.

Erfüllen der Speicheranforderungen Bevor Sie Batches von VMware ESXi/vCenter VMs konvertieren, müssen Sie Ihre Speicheranforderungen berücksichtigen. Konvertierte VM-Datenträger werden in einem XenServer-Speicher-Repository gespeichert.

Dieses Speicherrepository muss groß genug sein, um die virtuellen Datenträger für alle konvertierten VMs aufzunehmen, die Sie in diesem Pool ausführen möchten. Für konvertierte Maschinen, die nur auf einem eigenständigen Host ausgeführt werden, können Sie entweder lokalen oder gemeinsam genutzten Speicher als Speicherort für die konvertierten virtuellen Datenträger angeben. Für konvertierte Maschinen, die in Pools ausgeführt werden, können Sie nur freigegebenen Speicher angeben.

So erstellen Sie ein Speicherrepository:

1. Wählen Sie im **Ressourcenbereich** in XenCenter den Pool aus, in dem Sie die virtuelle XenServer Conversion Manager-Appliance ausführen möchten.
2. Klicken Sie auf die Registerkarte **Speicher**.
3. Klicken Sie auf **New SR** und befolgen Sie die Anweisungen des Assistenten. Für weitere Anweisungen drücken Sie **F1**, um die Online-Hilfe aufzurufen.

XenServer-Anforderungen Sie können mit dieser Version von XenServer Conversion Manager konvertierte VMs auf den folgenden Versionen von XenServer ausführen:

- XenServer 8
- Citrix Hypervisor 8.2 Cumulative Update 1

Anforderungen an VMware Die virtuelle XenServer Conversion Manager-Appliance kann VMware ESXi/vCenter-VMs aus den folgenden Versionen von VMware konvertieren:

- vCenter Server 6.7.x, 7.x und 8.x
- vSphere 6.7.x, 7.x und 8.x
- ESXi 6.7.x, 7.x und 8.x

> **Hinweis:**
>
> Die virtuelle XenServer Conversion Manager-Appliance kann keine VMware ESXi/vCenter-VMs mit vier oder mehr Datenträgern in XenServer-VMs konvertieren. Ihre VMware ESXi/vCenter VMs müssen über drei oder weniger Datenträger verfügen.
>
> Für Ihre VMware ESXi/vCenter-VMs müssen außerdem ein Netzwerk und ein Speichercontroller konfiguriert sein.

Bereiten Sie den Import der virtuellen Appliance vor Bevor Sie die virtuelle Appliance importieren, notieren Sie sich die folgenden Informationen und nehmen Sie gegebenenfalls die entsprechenden Änderungen an Ihrer Umgebung vor.

Laden Sie das virtuelle Gerät herunter Die virtuelle XenServer Conversion Manager-Appliance ist im XVA-Format verpackt. Sie können das virtuelle Gerät von der XenServer-Downloadseite herunterladen. Wenn Sie die Datei herunterladen, speichern Sie sie in einem Ordner auf Ihrer lokalen Datenträger (normalerweise, aber nicht unbedingt, auf dem Computer, auf dem XenCenter installiert ist). Nachdem die `.xva`-Datei auf Ihrer Datenträger ist, können Sie sie in XenCenter importieren.

Voraussetzungen für virtuelle Appliance Die virtuelle XenServer Conversion Manager-Appliance erfordert mindestens:

- Citrix Hypervisor 8.2 Kumulatives Update 1, XenServer 8
- Speicherplatz: 30 GB Speicherplatz
- Speicher: 6 GB
- Virtuelle CPU-Zuweisung: 2 vCPU

Importieren und Konfigurieren der virtuellen Appliance

Die virtuelle XenServer Conversion Manager-Appliance ist eine einzelne vorinstallierte VM, die für die Ausführung auf einem XenServer-Host konzipiert ist. Lesen Sie vor dem Importieren die Informationen und Überlegungen zu den Voraussetzungen im Abschnitt *Vorbereiten des Imports der virtuellen Appliance*.

Importieren Sie das virtuelle Gerät in XenServer

Verwenden Sie den XenCenter **Importassistenten**, um die virtuelle XenServer Conversion Manager-Appliance in den Pool oder Host zu importieren, auf dem Sie die konvertierten VMs ausführen möchten:

1. Öffnen Sie XenCenter. Klicken Sie mit der rechten Maustaste auf den Pool (oder Host), in den Sie das Paket der virtuellen Appliance importieren möchten, und wählen Sie **Importieren**.
2. Suchen Sie das virtuelle Appliance-Paket.
3. Wählen Sie den Pool oder einen *Homeserver* aus, auf dem Sie das virtuelle XenServer Conversion Manager-Appliance ausführen möchten.

   > **Hinweis:**
   >
   > Ein Homeserver ist der Host, der die Ressourcen für eine VM in einem Pool bereitstellt. Solange dies möglich ist, versucht ein XenServer, die VM auf diesem Host zu starten, bevor er es mit anderen Hosts versucht. Wenn Sie einen Host auswählen, verwendet das virtuelle XenServer Conversion Manager-Appliance diesen Host als Home-Server. Wenn Sie den Pool auswählen, wird die virtuelle Appliance automatisch auf dem am besten geeigneten Host in diesem Pool gestartet.

4. Wählen Sie ein Speicher-Repository aus, in dem der virtuelle Datenträger für die virtuelle XenServer Conversion Manager-Appliance gespeichert werden soll, und klicken Sie dann auf **Importieren**. Informationen zum Hinzufügen eines Speicherrepositorys zum Pool finden Sie im Abschnitt "Erfüllen der Speicheranforderungen". Sie können entweder lokalen oder gemeinsam genutzten Speicher wählen.
5. Stellen Sie sicher, dass das für die Konvertierung zu verwendende Netzwerk (das den VMware-Server mit dem XenServer-Host verbindet) als das Netzwerk ausgewählt ist, das der **Schnittstelle 1** ("virtuelle NIC 1") zugeordnet ist.
   - Wenn das richtige Netzwerk nicht neben Schnittstelle 1 angezeigt wird, verwenden Sie die Liste in der Spalte **Netzwerk**, um ein anderes Netzwerk auszuwählen.
   - Wenn Sie das VMware-Netzwerk nicht hinzugefügt haben, das sich in einem anderen physischen Netzwerk als dem Pool befindet, gehen Sie wie folgt vor:

a) Beenden Sie den Assistenten.
b) Fügen Sie das Netzwerk zum Pool hinzu.
c) Führen Sie den Assistenten erneut aus.

Weitere Informationen finden Sie unter **So fügen Sie XenServer ein Netzwerk hinzu**.

> **Warnung:**
>
> Konfigurieren Sie NIC0 NICHT für Ihr Kundennetzwerk. Weisen Sie NIC0 nur dem internen Verwaltungsnetzwerk "Host"zu.

6. Lassen **Sie das Kontrollkästchen VM nach dem Import starten** aktiviert und klicken Sie auf **Fertigstellen**, um die virtuelle Appliance zu importieren.
7. Nach dem Importieren der `.xva`-Datei wird die virtuelle XenServer Conversion Manager-Appliance im Bereich **Ressourcen** in XenCenter angezeigt.

Konfigurieren Sie das virtuelle XenServer Conversion Manager-Appliance

Bevor Sie die virtuelle XenServer Conversion Manager-Appliance zum Konvertieren von VMware ESXi/vCenter-VMs verwenden können, konfigurieren Sie sie auf der XenCenter-Registerkarte **Konsole**:

1. Klicken Sie nach dem Import der virtuellen XenServer Conversion Manager-Appliance auf die Registerkarte **Konsole**.
2. Lesen Sie die Lizenzvereinbarung. Um den Inhalt der Lizenzvereinbarung anzuzeigen, öffnen Sie die URL in einem Webbrowser. Drücken Sie eine beliebige Taste, um fortzufahren.
3. Geben Sie ein neues Root-Kennwort für die virtuelle XenServer Conversion Manager-Appliance ein und bestätigen Sie es. Wir empfehlen, ein sicheres Kennwort zu wählen.
4. Geben Sie einen Hostnamen für das virtuelle XenServer Conversion Manager-Appliance ein.
5. Geben Sie das Domänensuffix für die virtuelle Appliance ein. Wenn beispielsweise der vollqualifizierte Domänenname (FQDN) für die virtuelle Appliance `citrix-migrate-vm.domain4.example.com` ist, geben Sie `domain4.example.com` ein.
6. Geben Sie **y** ein, um DHCP zu verwenden, um die IP-Adresse für das virtuelle XenServer Conversion Manager-Appliance automatisch abzurufen. Andernfalls geben Sie **n** ein und geben dann eine statische IP-Adresse, eine Subnetzmaske und ein Gateway für die VM ein.
7. Überprüfen Sie den Hostnamen und die Netzwerkeinstellungen und geben Sie bei Aufforderung **y** ein. Mit diesem Schritt ist die Konfiguration der virtuellen XenServer Conversion Manager-Appliance abgeschlossen.

8. Wenn Sie die Appliance erfolgreich konfiguriert haben, wird eine Anmeldeaufforderung angezeigt. Geben Sie die Anmeldeinformationen ein und drücken Sie die Eingabetaste, um sich bei der virtuellen XenServer Conversion Manager-Appliance anzumelden.

VMware ESXi/vCenter VMs konvertieren

Wenn Sie VMware ESXi/vCenter VMs konvertieren, werden sie in den XenServer-Pool oder den eigenständigen Host importiert, auf dem Sie die virtuelle XenServer Conversion Manager-Appliance ausführen. Konvertierte VMs behalten ihre ursprünglichen VMware-Einstellungen für den virtuellen Prozessor und den virtuellen Speicher bei.

Bevor Sie mit der Konvertierung beginnen, stellen Sie sicher, dass Folgendes zutrifft:

- Sie haben die Anmeldeinformationen für den XenServer-Pool (oder den eigenständigen Host). Entweder die Anmeldeinformationen des Root-Kontos oder ein Konto für die rollenbasierte Zugriffssteuerung (RBAC) mit der konfigurierten Pool-Admin-Rolle sind zulässig.
- Sie haben die Anmeldeinformationen für den VMware-Server, der die zu konvertierenden VMs enthält. Für das Konvertierungsverfahren müssen Sie die XenServer Conversion Manager-Konsole mit dem VMware-Server verbinden.
- Die zu konvertierenden virtuellen VMware-Maschinen sind ausgeschaltet.
- Für die zu konvertierenden virtuellen VMware-Maschinen sind ein Netzwerk und ein Speichercontroller konfiguriert.
- Der XenServer-Pool (oder Host), auf dem die konvertierten VMs ausgeführt werden, ist mit einem Speicher-Repository verbunden. Das Speicherrepository muss ausreichend Speicherplatz für die konvertierten virtuellen Datenträger enthalten.
- Wenn Sie Ihre neu konvertierten VMs in einem Pool ausführen möchten, muss das Speicherrepository gemeinsam genutzter Speicher sein. Wenn die konvertierten VMs jedoch auf einem einzelnen eigenständigen Host (nicht in einem Pool) ausgeführt werden, können Sie lokalen Speicher verwenden.
- Die virtuellen Datenträger der zu konvertierenden VM sind kleiner als 2 TiB.
- Der XenServer-Pool (oder Host) verfügt über Netzwerke, die die konvertierten VMs verwenden.

So konvertieren Sie Ihre VMware ESXi/vCenter-VMs in VMs, die in einer XenServer-Umgebung ausgeführt werden können:

1. Stellen Sie sicher, dass die virtuelle Appliance auf dem XenServer-Host oder -Pool installiert ist und ausgeführt wird, in den Sie die VMs importieren möchten.
2. Gehen Sie in XenCenter zu **Pool** > **Conversion Manager**.

   Das Fenster **Conversion Manager** wird geöffnet. Warten Sie, bis der Assistent eine Verbindung zu Ihrer virtuellen Appliance herstellt.

3. Klicken Sie auf **Neue Konvertierung**.
4. Geben Sie im Assistenten für **neue Konvertierungen** die Anmeldeinformationen für den VMware-Server ein:

   - **Server**. Geben Sie die IP-Adresse oder den FQDN für den VMware-Server ein, der die VMs enthält, die Sie in XenServer konvertieren möchten.
   - **Benutzername**. Geben Sie einen gültigen Benutzernamen für diesen VMware-Server ein. Dieses Konto muss entweder ein VMware-Administratorkonto sein oder eine Root-Rolle haben.
   - **Kennwort**. Geben Sie das Kennwort für das Benutzerkonto ein, das Sie im Feld **Benutzername** angegeben haben.

   Klicken Sie auf **Weiter**. XenCenter stellt eine Verbindung zum VMware-Server her.
5. Wählen Sie auf der Seite **Virtuelle Maschinen** aus der Liste der auf dem VMware-Server gehosteten VMs aus, die Sie konvertieren möchten. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Speicher** das Speicherrepository aus, das Sie bei der Konvertierung verwenden möchten. In diesem Speicherrepository werden die VMs und virtuellen Laufwerke, die Sie erstellen, dauerhaft gespeichert.

   Auf dieser Registerkarte wird der Anteil des verfügbaren Speichers angegeben, den die virtuellen Datenträger der konvertierten VMs verbrauchen.
7. Wählen Sie auf der **Netzwerkseite** für jedes aufgelistete VMware-Netzwerk das XenServer-Netzwerk aus, dem es zugeordnet werden soll. Sie können auch auswählen, ob virtuelle MAC-Adressen beibehalten werden sollen. Klicken Sie auf **Weiter**.
8. Prüfen Sie die Optionen, die Sie für den Konvertierungsprozess konfiguriert haben. Sie können auf **Zurück** klicken, um diese Optionen zu ändern. Um mit der gezeigten Konfiguration fortzufahren, klicken Sie auf **Fertigstellen**.

   Der Konvertierungsprozess beginnt. Die Konvertierung von ESXi oder vSphere kann je nach Größe der virtuellen Datenträger mehrere Minuten dauern.

   Nach der Konvertierung Ihrer VMs fährt der Conversion Manager automatisch von selbst herunter, wodurch Ressourcen auf dem Host eingespart werden. Starten Sie eine VM, indem Sie den Host der VM auswählen und dann auf **Pool** > **Conversion Manager** klicken.

Im Fenster **Conversion Manager** werden laufende Konvertierungen und abgeschlossene Konvertierungen angezeigt.

Schritte nach der Konvertierung

Für Windows-VMs müssen Sie XenServer VM Tools für Windows installieren. Für Linux-VMs müssen Sie XenServer VM Tools für Linux nicht installieren, da der Conversion Manager sie während des Kon-

vertierungsvorgangs automatisch installiert.

Führen Sie nach der Konvertierung in XenCenter die folgenden Schritte auf Ihren neu konvertierten VMs aus:

Auf Windows-Computern:

1. Auf Windows-VMs müssen Sie je nach Microsoft-Lizenzmodell möglicherweise die Windows-Lizenz der VM reaktivieren. Diese Reaktivierung erfolgt, weil das Windows-Betriebssystem die Konvertierung als Hardwareänderung wahrnimmt.
2. Installieren Sie auf Windows-VMs die XenServer VM Tools für Windows, um Hochgeschwindigkeits-I/O für eine verbesserte Datenträger- und Netzwerkleistung zu erhalten. XenServer VM Tools für Windows ermöglichen auch bestimmte Funktionen und Features, darunter das saubere Herunterfahren, Neustarten, Anhalten und Live-Migrieren von VMs. Sie können die XenServer VM Tools für Windows von der XenServer-Downloadseiteherunterladen.

Wenn Sie mit einer VM arbeiten, auf der XenServer VM Tools nicht installiert sind, wird auf der Registerkarte **Allgemein** im Bereich **Allgemein** die Meldung "XenServer VM Tools nicht installiert" angezeigt.

> **Hinweis:**
>
> XenServer VM Tools für Windows müssen auf jeder Windows-VM installiert sein, damit die VM eine vollständig unterstützte Konfiguration hat. Windows-VMs funktionieren zwar ohne XenServer VM Tools für Windows, ihre Leistung kann jedoch beeinträchtigt werden.

VNC auf Linux-Maschinen aktivieren

Konfigurieren Sie auf Linux-VMs den VNC-Server. Weitere Informationen finden Sie unter VNC für Linux-VMs aktivieren.

> **Hinweis:**
>
> Das VNC-Kennwort muss mindestens sechs Zeichen lang sein.

Andere Konvertierungsaufgaben

Im Fenster **Conversions verwalten** können Sie andere Aufgaben im Zusammenhang mit der Konvertierung von VMs ausführen. Zu diesen Aufgaben gehören das Löschen von Jobs, das Speichern einer Zusammenfassung der Jobs, das Wiederholen von Jobs, das Abbrechen von Jobs und das Anzeigen der Protokolldatei.

Um alle Jobs zu löschen:

1. Wählen Sie **Alle löschen**.

2. Wenn Sie zur Bestätigung dieser Aktion aufgefordert werden, klicken Sie auf **Ja**, um fortzufahren

So speichern Sie eine Zusammenfassung der Jobs:

1. Klicken Sie auf **Alle exportieren**.
2. Geben Sie an, wo die CSV-Datei gespeichert wird.
3. Klicken Sie auf **Speichern**.

Um einen Job erneut zu versuchen:

1. Wählen Sie den Job aus der Liste aus.
2. Klicken Sie auf **Wiederholen**.

> **Hinweis:**
>
> Die Option **Wiederholen** ist nur für fehlgeschlagene oder abgebrochene Jobs aktiviert.

Um einen Auftrag abzubrechen:

1. Wählen Sie den Job aus der Liste aus.
2. Klicken Sie auf **Abbrechen**.

> **Hinweis:**
>
> Das Abbrechen von Jobs ist nur für Aufträge in der Warteschlange oder in der Ausführung aktiviert

So speichern Sie die Konvertierungsprotokolldatei für einen einzelnen Auftrag:

1. Wählen Sie den Job aus der Liste aus.
2. Klicken Sie im Menü “Protokolle”auf **Ausgewähltes Protokoll abrufen**.
3. Geben Sie an, wo die Protokolldatei gespeichert werden soll.

So speichern Sie die Konvertierungsprotokolldatei für alle Jobs:

1. Klicken Sie im Menü “Protokolle”auf “**Alle Protokolle abrufen**”.
2. Geben Sie an, wo die Protokolldatei gespeichert werden soll.

So zeigen Sie Konvertierungsdetails an:

1. Wählen Sie den Job aus der Liste aus.

   Die Informationen werden im Bereich **Details** angezeigt.

---

layout: doc
description: Diagnose and gather information about issues that might arise when using the XenServer Conversion Manager virtual appliance.—

Problembehandlung bei XenServer Conversion Manager

Dieser Abschnitt enthält Informationen zur Problembehandlung bei der Konvertierung und konvertierter VMs.

Probleme beim Starten einer konvertierten VM

Im Allgemeinen läuft die Konvertierung reibungslos und die virtuelle XenServer Conversion Manager-Appliance konvertiert VMs problemlos. In einigen seltenen Fällen können jedoch Fehler auftreten, wenn Sie versuchen, konvertierte VMs zu öffnen. In den folgenden Abschnitten finden Sie einige Hinweise zum Beheben von Fehlern und anderen Problemen.

Blauer Bildschirm mit Windows STOP-Code 0x0000007B

Dieser Stoppcode weist darauf hin, dass das virtuelle XenServer Conversion Manager-Appliance kein Windows-Gerät konfigurieren konnte, das für den ersten Start in XenServer wichtig ist. Speichern Sie die Protokolle und senden Sie sie an den Support, um weitere Informationen zu erhalten.

Windows Produktaktivierung

Abhängig von Ihrem Lizenzmodell wird möglicherweise eine Fehlermeldung bei der Systemaktivierung angezeigt, wenn Sie versuchen, eine Windows-VM zu starten.

Netzwerkeinstellungen in einer Windows-VM verloren

Wenn Sie eine Windows-VM von einem ESXi-Server auf XenServer importieren, können die IPv4/IPv6-Netzwerkeinstellungen verloren gehen. Um die Netzwerkeinstellungen beizubehalten, konfigurieren Sie die IPv4/IPv6-Einstellungen nach Abschluss der Konvertierung neu.

VMware SCSI-Datenträger kann nicht gestartet werden

Wenn eine VMware-VM von einer SCSI-Datenträger gestartet wird, aber auch IDE-Datenträger konfiguriert sind, wird die VM möglicherweise nicht gestartet, wenn Sie sie in XenServer konvertieren. Dieses Problem tritt auf, weil der Migrationsprozess den IDE-Datenträgern niedrigere Gerätenummern als SCSI-Datenträgern zuweist. XenServer bootet jedoch von der Datenträger, die Gerät 0 zugewiesen ist. Um dieses Problem zu beheben, ordnen Sie die Position des virtuellen Laufwerks in XenCenter neu an, sodass die VM von dem virtuellen Laufwerk, das das Betriebssystem enthält, neu gestartet wird.

So ändern Sie die Position des virtuellen Laufwerks, das das Betriebssystem enthält:

1. Wählen Sie im Bereich XenCenter **Resources** die ausgeschaltete Gast-VM aus.
2. Wählen Sie die Registerkarte **Speicher**.
3. Wählen Sie in der Liste **virtuelle Datenträger** das virtuelle Laufwerk aus, das das Betriebssystem enthält, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie im **Eigenschaftendialogfeld** des virtuellen Laufwerks auf die Registerkarte ***vm_name***, um die Geräteoptionen anzuzeigen.
5. Wählen Sie in der Liste **Geräteposition** die Option **0** aus und klicken Sie auf **OK**.

Probleme bei der Konvertierung

Wenn beim Konvertieren von VMs Probleme oder Fehler auftreten, versuchen Sie, die VMware-VM als OVF-Paket zu exportieren. Wenn Sie die VMware-VM nicht als OVF-Paket exportieren können, kann Conversion Manager diese VM nicht konvertieren. Verwenden Sie die Fehlermeldungen, die Sie erhalten, wenn Sie versuchen, die VM als OVF-Paket zu exportieren, um die Probleme mit Ihrer VMware-VM zu beheben und zu beheben. Beispielsweise müssen Sie möglicherweise ein Netzwerk oder einen Speichercontroller konfigurieren, bevor die VM als OVF-Paket exportiert oder konvertiert werden kann. Weitere Informationen zur Fehlerbehebung Ihrer VMware ESXi/vCenter VMs finden Sie in der VMware-Dokumentation.

Wenn beim Konvertieren von Linux-VMs Fehler auftreten, entfernen Sie die konvertierte VM, starten Sie die virtuelle XenServer Conversion Manager-Appliance neu und versuchen Sie es erneut.

Protokolle fehlgeschlagener Konvertierungen werden in der virtuellen XenServer Conversion Manager-Appliance gespeichert und können abgerufen werden, indem Sie im **Conversion Manager-Fensterauf Alle Protokolle abrufen** klicken. Wenn Sie den Support kontaktieren, um Probleme zu melden, empfehlen wir Ihnen, die Konvertierungsprotokolldatei und zusätzlich einen vollständigen Serverstatusbericht zur Problembehandlung bereitzustellen. Weitere Informationen finden Sie unter Erstellen eines Serverstatusberichts.

Befehlszeilenoberfläche

April 12, 2024

Mit der *xe* CLI können Sie Systemadministrationsaufgaben skripten und automatisieren. Verwenden Sie die CLI, um XenServer in eine bestehende IT-Infrastruktur zu integrieren.

Erste Schritte mit der Xe-CLI

Die xe-Befehlszeilenschnittstelle ist standardmäßig auf allen XenServer-Hosts installiert. Eine Remote-Windows-Version ist in XenCenter enthalten. Eine eigenständige Remote-CLI ist auch für Linux verfügbar.

Auf Ihrem XenServer-Host

Die xe-Befehlszeilenschnittstelle ist standardmäßig auf Ihrem Host installiert. Sie können Xe-CLI-Befehle in der dom0-Konsole ausführen. Greifen Sie auf eine der folgenden Arten auf die dom0-Konsole zu:

- Gehen Sie in XenCenter zur Registerkarte **Konsole** für den Host, auf dem Sie den Befehl ausführen möchten.
- SSH zu dem Host, auf dem Sie den Befehl ausführen möchten.

Unter Windows

Unter Windows wird der Befehl `xe.exe` zusammen mit XenCenter installiert.

Um den Befehl `xe.exe` zu verwenden, öffnen Sie eine Windows-Eingabeaufforderung und wechseln Sie in das Verzeichnis, in dem die Datei `xe.exe` ist (normalerweise `C:\Program Files (x86)\XenServer\XenCenter`). Wenn Sie das Installationsverzeichnis von `xe.exe` zu Ihrem Systempfad hinzufügen, können Sie den Befehl verwenden, ohne in das Verzeichnis wechseln zu müssen.

Unter Linux

Auf RPM-basierten Distributionen (wie Red Hat) können Sie den eigenständigen XE-Befehl von dem RPM aus installieren, das `client_install/xapi-xe-BUILD.x86_64.rpm` auf der XenServer-Haupt-Installations-ISO angegeben ist.

Verwenden Sie den folgenden Befehl, um vom RPM aus zu installieren:

```
rpm -ivh xapi-xe-BUILD.x86_64.rpm
<!--NeedCopy-->
```

Sie können Parameter in der Befehlszeile verwenden, um den XenServer-Host, den Benutzernamen und das Kennwort zu definieren, die bei der Ausführung von XE-Befehlen verwendet werden sollen. Sie haben jedoch auch die Möglichkeit, diese Informationen als Umgebungsvariable festzulegen. Beispiel:

```
export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password
    =<password>"
```



```
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Remote-XE-CLI unter Linux hängt möglicherweise beim Versuch, Befehle über eine sichere Verbindung auszuführen, und diese Befehle beinhalten die Dateiübertragung. In diesem Fall können Sie den `--no-ssl` Parameter verwenden, um den Befehl über eine unsichere Verbindung zum XenServer-Host auszuführen.

Hilfe mit xe-Befehlen erhalten

Grundlegende Hilfe für CLI-Befehle auf dem Host ist verfügbar, indem Sie Folgendes eingeben:

```
xe help command
<!--NeedCopy-->
```

Eine Liste der am häufigsten verwendeten xe-Befehle wird angezeigt, wenn Sie Folgendes eingeben:

```
xe help
<!--NeedCopy-->
```

Oder es wird eine Liste aller xe-Befehle angezeigt, wenn Sie Folgendes eingeben:

```
xe help --all
<!--NeedCopy-->
```

Grundlegende xe-Syntax

Die grundlegende Syntax aller XenServer xe CLI-Befehle lautet:

```
xe command-name argument=value argument=value
<!--NeedCopy-->
```

Jeder spezifische Befehl enthält seine eigenen Argumente, die das Format `argument=value` haben. Für einige Befehle sind Argumente erforderlich, und die meisten haben einige optionale Argumente. In der Regel geht ein Befehl von Standardwerten für einige der optionalen Argumente aus, wenn er ohne sie aufgerufen wird.

Wenn der xe-Befehl remote ausgeführt wird, werden zusätzliche Argumente für die Verbindung und Authentifizierung verwendet. Diese Argumente haben auch das Format `argument=argument_value`.

Das Argument `server` wird verwendet, um den Hostnamen oder die IP-Adresse anzugeben. Die Argumente `username` und `password` werden verwendet, um Anmeldeinformationen anzugeben.

Anstelle des Kennworts kann direkt ein Argument `password-file` angegeben werden. In diesem Fall versucht der xe-Befehl, das Kennwort aus der angegebenen Datei zu lesen, und verwendet dieses

Kennwort, um eine Verbindung herzustellen. (Alle nachfolgenden CRs und LFs am Ende der Datei werden entfernt.) Diese Methode ist sicherer als die Angabe des Kennworts direkt in der Befehlszeile.

Das optionale `port` Argument kann verwendet werden, um den Agent-Port auf dem Remote-XenServer-Host anzugeben (standardmäßig 443).

Beispiel: Auf dem lokalen XenServer-Host:

```
xe vm-list
<!--NeedCopy-->
```

Beispiel: Auf einem Remote-XenServer-Host:

```
xe vm-list username=username password=password server=hostname
<!--NeedCopy-->
```

Die Kurzschriftsyntax ist auch für Argumente für Remoteverbindungen verfügbar:

- `-u` user name
- `-pw` password
- `-pwf` password file
- `-p` Port
- `-s` server

Beispiel: Auf einem Remote-XenServer-Host:

```
xe vm-list -u myuser -pw mypassword -s hostname
<!--NeedCopy-->
```

Argumente werden auch aus der Umgebungsvariablen XE_EXTRA_ARGS in Form von kommagetrennten Schlüssel/Wert-Paaren übernommen. Um beispielsweise Befehle einzugeben, die auf einem XenServer-Remote-Host ausgeführt werden, führen Sie zunächst den folgenden Befehl aus:

```
export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=
    pass"
<!--NeedCopy-->
```

Nachdem Sie diesen Befehl ausgeführt haben, müssen Sie die XenServer-Hostparameter nicht mehr in jedem XE-Befehl angeben, den Sie ausführen.

Die Verwendung der Umgebungsvariablen XE_EXTRA_ARGS ermöglicht auch die Tabulatorvervollständigung von XE-Befehlen, wenn sie für einen Remote-XenServer-Host ausgegeben werden, der standardmäßig deaktiviert ist.

Sonderzeichen und Syntax

Um Argument-/Wertepaare in der `xe`-Befehlszeile anzugeben, schreiben Sie: `argument=value`

Verwenden Sie keine Anführungszeichen, sofern der Wert keine Leerzeichen enthält. Fügen Sie keine Leerzeichen zwischen dem Argumentnamen, dem Gleichheitszeichen (=) und dem Wert ein. Jedes Argument, das diesem Format nicht entspricht, wird ignoriert.

Für Werte, die Leerzeichen enthalten, schreiben Sie: `argument="value with spaces"`

Wenn Sie die CLI auf Ihrem XenServer-Host verwenden, verfügen Befehle über eine Funktion zur Tabulatorvervollständigung, die der Funktion in der Standard-Linux-Bash-Shell ähnelt. Wenn Sie beispielsweise `xe vm-l` eingeben und dann die **TAB-Taste** drücken, wird der Rest des Befehls angezeigt. Wenn mehrere Befehle mit `vm-l` beginnen, werden durch erneutes Drücken der **Tabulatortaste** die Möglichkeiten aufgelistet. Diese Funktion ist nützlich, wenn Objekt-UUIDs in Befehlen angegeben werden

> **Hinweis:**
>
> Die Tabulatorvervollständigung funktioniert normalerweise nicht, wenn Befehle auf einem XenServer-Remote-Host ausgeführt werden. Wenn Sie jedoch die Variable XE_EXTRA_ARGS auf dem Computer festlegen, auf dem Sie die Befehle eingeben, ist die Tab-Vervollständigung aktiviert. Weitere Informationen finden Sie unter Grundlegende XE-Syntax.

Befehlstypen

Die CLI-Befehle können in zwei Hälften aufgeteilt werden. Befehle auf niedriger Ebene befassen sich mit dem Auflisten und der Parametermanipulation von API-Objekten. Befehle auf höherer Ebene werden verwendet, um mit VMs oder Hosts auf einer abstrakteren Ebene zu interagieren.

Die Befehle auf niedriger Ebene sind:

- *class*-list
- *class*-param-get
- *class*-param-set
- *class*-param-list
- *class*-param-add
- *class*-param-remove
- *class*-param-clear

Dabei ist *class* eine dieser Optionen:

- `bond`
- `console`
- `host`

- host-crashdump
- host-cpu
- network
- patch
- pbd
- pif
- pool
- sm
- sr
- task
- template
- vbd
- vdi
- vif
- vlan
- vm

Nicht jeder Wert von *class* hat den vollständigen Satz von Befehlen für *class*-param-*action*. Einige Werte von *class* haben einen kleineren Befehlssatz.

Typen von Parametern

Die Objekte, die mit den xe-Befehlen angesprochen werden, haben Parametersätze, die sie identifizieren und ihre Zustände definieren.

Die meisten Parameter nehmen einen einzigen Wert an. Beispielsweise enthält der Parameter `name-label` einer VM einen einzelnen Zeichenfolgenwert. In der Ausgabe von Befehlen der Parameterliste gibt ein Wert in Klammern - z. B. `xe vm-param-list` - an, ob es sich bei den Parametern um Lese-/Schreibzugriff (RW) oder schreibgeschützt (RO) handelt.
Die Ausgabe von `xe vm-param-list` auf einer angegebenen VM kann die folgenden Zeilen haben:

```
user-version ( RW): 1
 is-control-domain ( RO): false
```


Der erste Parameter ist beschreibbar und hat den Wert 1. `user-version` Die zweite, `is-control-domain`, ist schreibgeschützt und hat den Wert false.

Die beiden anderen Arten von Parametern sind mehrwertig. Ein *eingestellter* Parameter enthält eine Liste von Werten. Ein *Map-Parameter* ist ein Satz von Schlüssel/Wert-Paaren. Sehen Sie sich als Beispiel die folgende Beispielausgabe von `xe vm-param-list` auf einer bestimmten VM an:

```
platform (MRW): acpi: true; apic: true; pae: true; nx: false
allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
hard_shutdown; hard_reboot; suspend
```

Der Parameter `platform` enthält eine Liste von Elementen, die Schlüssel/Wert-Paare darstellen. Auf die Schlüsselnamen folgt ein Doppelpunkt (:). Jedes Schlüssel/Wert-Paar ist durch ein Semikolon (;) vom nächsten getrennt. Das M vor dem RW zeigt an, dass dieser Parameter ein Map-Parameter ist und lesbar und beschreibbar ist. Der Parameter `allowed-operations` hat eine Liste, die aus einer Reihe von Elementen besteht. Das S vor dem RO zeigt an, dass dies ein festgelegter Parameter ist und lesbar, aber nicht beschreibbar ist.

Um nach einem Map-Parameter zu filtern oder einen Map-Parameter festzulegen, verwenden Sie einen Doppelpunkt (:), um den Map-Parameternamen und das Schlüssel/Wert-Paar zu trennen. Um beispielsweise den Wert des Schlüssels `foo` des Parameters `other-config` einer VM auf `baa` festzulegen, lautet der Befehl

```
xe vm-param-set uuid=VM uuid other-config:foo=baa
<!--NeedCopy-->
```

Parameter-Befehle auf niedriger Ebene

Es gibt mehrere Befehle für die Bedienung von Parametern von Objekten: *class*-param-get, *class*-param-set, *class*-param-add, *class*-param-remove, *class*-param-clear, and *class*-param-list. Jeder dieser Befehle benötigt einen Parameter `uuid`, um das bestimmte Objekt anzugeben. Da diese Befehle als Befehle auf niedriger Ebene betrachtet werden, müssen sie die UUID und nicht die VM-Namensbezeichnung verwenden.

- `xe class-param-list uuid=uuid`

  Listet alle Parameter und die zugehörigen Werte auf. Im Gegensatz zum Befehl *class*-list listet dieser Befehl die Werte von “teuren”Feldern auf.

- `xe class-param-get uuid=uuid param-name=parameter param-key=key`

  Gibt den Wert eines bestimmten Parameters zurück. Bei einem Map-Parameter wird durch Angabe des Parameter-Schlüssels der Wert abgerufen, der diesem Schlüssel in der Map zugeordnet ist. Wenn param-key nicht angegeben ist oder wenn der Parameter eine Menge ist, gibt der Befehl eine Zeichenfolgendarstellung des Satzes oder der Zuordnung zurück.

- `xe class-param-set uuid=uuid param=value`

  Setzt den Wert eines oder mehrerer Parameter.

- `xe class-param-add uuid=uuid param-name=parameter key=value param-key=key`

  Fügt entweder zu einer Map oder einem festgelegten Parameter hinzu. Fügen Sie für einen Map-Parameter Schlüssel/Wert-Paare hinzu, indem Sie die Schlüssel=Wert-Syntax verwenden. Wenn der Parameter ein Satz ist, fügen Sie Schlüssel mit der param-key=key-Syntax hinzu.

- `xe class-param-remove uuid=uuid param-name=parameter param-key=key`

  Entfernt entweder ein Schlüssel/Wert-Paar aus einer Map oder einen Schlüssel aus einer Menge.

- `xe class-param-clear uuid=uuid param-name=parameter`

  Löscht einen Satz oder eine Map vollständig.

Listenbefehle auf niedriger Ebene

Der Befehl *class*-list listet die Objekte vom Typ *class*auf. Standardmäßig listet dieser Befehlstyp alle Objekte auf und druckt eine Teilmenge der Parameter. Dieses Verhalten kann auf folgende Weise geändert werden:

- Es kann die Objekte so filtern, dass es nur eine Teilmenge ausgibt
- Die gedruckten Parameter können geändert werden.

Um die gedruckten Parameter zu ändern, geben Sie das Argument *params* als kommagetrennte Liste der erforderlichen Parameter an. Beispiel:

```
xe vm-list params=name-label,other-config
<!--NeedCopy-->
```

Um alle Parameter aufzulisten, verwenden Sie alternativ die Syntax:

```
xe vm-list params=all
<!--NeedCopy-->
```

Der Befehl list zeigt einige Parameter nicht an, deren Berechnung teuer ist. Diese Parameter werden beispielsweise wie folgt dargestellt:

```
allowed-VBD-devices (SRO): <expensive field>
<!--NeedCopy-->
```

Um diese Felder zu erhalten, verwenden Sie entweder die *Befehlsklasse*-param-list oder die *Klasse*-param-get

Um die Liste zu filtern, gleicht die CLI Parameterwerte mit den in der Befehlszeile angegebenen Werten ab und druckt nur Objekte, die allen angegebenen Einschränkungen entsprechen. Beispiel:

```
xe vm-list HVM-boot-policy="BIOS order" power-state=halted
<!--NeedCopy-->
```

Dieser Befehl listet nur die VMs auf, für die *sowohl* das Feld `power-state` den Wert *halted* hat als auch das Feld `HVM-boot-policy` den Wert *BIOS order*.

Sie können die Liste auch nach dem Wert von Schlüsseln in Maps oder nach dem Vorhandensein von Werten in einer Menge filtern. Die Syntax für das Filtern basierend auf Schlüsseln in Maps ist `map-name:key=value`. Die Syntax für das Filtern basierend auf Werten, die in einer Menge vorhanden sind, lautet `set-name:contains=value`.

Beim Scripting ist es eine nützliche Technik, `--minimal` an die Befehlszeile zu übergeben, wodurch `xe` nur das erste Feld in einer kommagetrennten Liste druckt. Beispielsweise gibt der Befehl `xe vm-list --minimal` auf einem Host mit drei installierten VMs die drei UUIDs der VMs an:

```
    a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-
       af10baea96b7, \
    42c044de-df69-4b30-89d9-2c199564581d
<!--NeedCopy-->
```

Secrets

XenServer bietet einen geheimen Mechanismus, um zu verhindern, dass Kennwörter im Befehlszeilenverlauf oder auf API-Objekten im Klartext gespeichert werden. XenCenter verwendet diese Funktion automatisch und kann auch über die xe CLI für jeden Befehl verwendet werden, der ein Kennwort erfordert.

> **Hinweis:**
>
> Kennwortgeheimnisse können nicht verwendet werden, um sich von einer Remoteinstanz der Xe-CLI aus bei einem XenServer-Host zu authentifizieren.

Um ein geheimes Objekt zu erstellen, führen Sie den folgenden Befehl auf Ihrem XenServer-Host aus.

```
xe secret-create value=my-password
<!--NeedCopy-->
```

Ein Secret wird erstellt und auf dem XenServer-Host gespeichert. Der Befehl gibt die UUID des geheimen Objekts aus. Beispiel: `99945d96-5890-de2a-3899-8c04ef2521db`. Fügen Sie `_secret` an den Namen des Kennwortarguments an, um diese UUID an einen Befehl zu übergeben, der ein Kennwort erfordert.

Beispiel: Auf dem XenServer-Host, auf dem Sie das Geheimnis erstellt haben, können Sie den folgenden Befehl ausführen:

```
1     xe sr-create device-config:location=sr_address device-config:type=
         cifs device-config:username=cifs_username  \
2     device-config:cifspassword_secret=secret_uuid name-label="CIFS ISO
         SR" type="iso" content-type="iso" shared="true"
3 <!--NeedCopy-->
```

Befehlsverlauf

Einige XE-Befehle, zum Beispiel `xe vm-migrate` oder `xe pool-enable-external-auth`, nehmen Secrets wie Kennwörter als Parameter. Diese können im Shell-Verlauf enden und sind während der Ausführung des Befehls in der Prozesstabelle sichtbar. Es ist daher wichtig, diese Befehle nur in vertrauenswürdigen Umgebungen auszuführen.

Für die Bash-Shell können Sie die Variable `HISTCONTROL` verwenden, um zu steuern, welche Befehle im Shell-Verlauf gespeichert werden.

xe-Befehlsreferenz

In diesem Abschnitt werden die Befehle nach den Objekten gruppiert, die der Befehl adressiert. Diese Objekte sind alphabetisch aufgelistet.

Appliance-Befehle

Befehle zum Erstellen und Ändern von VM-Appliances (auch bekannt als vApps). Weitere Informationen finden Sie unter vApps.

Geräte-Parameter

Appliance-Befehle haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die Appliance uuid	Erforderlich
`name-description`	Die Beschreibung des Geräts	Optional
`paused`		Optional
`force`	Herunterfahren erzwingen	Optional

appliance-assert-can-be-recovered

```
xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-
    uuid=vdi-uuid
<!--NeedCopy-->
```

Testet, ob Speicher zur Wiederherstellung dieser VM Appliance/vApp verfügbar ist.

appliance-create

```
xe appliance-create name-label=name-label [name-description=name-
    description]
<!--NeedCopy-->
```

Erstellt eine Appliance/vApp. Beispiel:

```
xe appliance-create name-label=my_appliance
<!--NeedCopy-->
```

Hinzufügen von virtuellen Rechnern zur Appliance:

```
xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
<!--NeedCopy-->
```

appliance-destroy

```
xe appliance-destroy uuid=appliance-uuid
<!--NeedCopy-->
```

Zerstört ein Gerät/eine vApp. Beispiel:

```
xe appliance-destroy uuid=appliance-uuid
<!--NeedCopy-->
```

appliance-recover

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
    paused=true|false]
<!--NeedCopy-->
```

Stellen Sie eine VM Appliance/vApp aus der Datenbank wieder her, die im bereitgestellten VDI enthalten ist.

appliance-shutdown

```
xe appliance-shutdown uuid=appliance-uuid [force=true|false]
<!--NeedCopy-->
```

Schließt alle virtuellen Maschinen in einer Appliance/vApp herunter. Beispiel:

```
xe appliance-shutdown uuid=appliance-uuid
<!--NeedCopy-->
```

appliance-start

```
xe appliance-start uuid=appliance-uuid [paused=true|false]
<!--NeedCopy-->
```

Startet eine Appliance/vApp. Beispiel:

```
xe appliance-start uuid=appliance-uuid
<!--NeedCopy-->
```

Befehle für die Prüfung

Mit Überwachungsbefehlen werden alle verfügbaren Datensätze der RBAC-Überwachungsdatei im Pool heruntergeladen. Wenn der optionale Parameter `since` vorhanden ist, werden nur die Datensätze von diesem bestimmten Zeitpunkt heruntergeladen.

audit-log-get-Parameter

`audit-log-get` hat die folgenden Parameter

Parametername	Beschreibung	Typ
`filename`	Schreiben Sie das Überwachungsprotokoll des Pools in den *Dateinamen*	Erforderlich
`since`	Spezifischer Datum/Uhrzeit	Optional

audit-log-get

```
xe audit-log-get [since=timestamp] filename=filename
<!--NeedCopy-->
```


Um beispielsweise Überwachungsaufzeichnungen des Pools seit einem genauen Millisekunden-Zeitstempel abzurufen, führen Sie den folgenden Befehl aus:

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z filename=/tmp/auditlog-pool-actions.out
<!--NeedCopy-->
```

Bonding-Befehle

Befehle für die Arbeit mit Netzwerkbindungen, für Ausfallsicherheit bei Failover für physische Schnittstellen. Weitere Informationen finden Sie unter Netzwerk.

Das Bond-Objekt ist ein Referenzobjekt, das *Master*- und *Member*-PIFs miteinander verbindet. Der Master-PIF ist das Bonding-Interface, das als Gesamt-PIF verwendet werden muss, um sich auf die Bindung zu beziehen. Die Mitglied-PIFs sind ein Satz von zwei oder mehr physikalischen Schnittstellen, die zu der gebundenen High-Level-Schnittstelle kombiniert wurden.

Bond-Parameter

Bonds haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Eindeutige Identifikator/Objektreferenz für die Bindung	Lesezugriff
master	UUID for the main bond PIF	Lesezugriff
members	Satz von UUIDs für die zugrunde liegenden gebundenen PIFs	Lesezugriff

bond-create

```
xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,pif_uuid_2,...
<!--NeedCopy-->
```

Erstellen Sie eine gebundene Netzwerkschnittstelle in dem Netzwerk, das aus einer Liste vorhandener PIF-Objekte angegeben ist. Der Befehl schlägt in einem der folgenden Fälle fehl:

- Wenn PIFs bereits in einer anderen Bindung sind
- Wenn bei einem Mitglied ein VLAN-Tag festgelegt ist
- Wenn sich die referenzierten PIFs nicht auf demselben XenServer-Host befinden
- Wenn weniger als 2 PIFs geliefert werden

bond-destroy

```
xe bond-destroy uuid=bond_uuid
<!--NeedCopy-->
```

Löscht eine gebundene Schnittstelle, die durch ihre UUID angegeben ist, von einem Host.

bond-set-mode

```
xe bond-set-mode uuid=bond_uuid mode=bond_mode
<!--NeedCopy-->
```

Ändern Sie den Bond-Modus.

CD-Befehle

Befehle für die Arbeit mit physischen CD/DVD-Laufwerken auf XenServer-Hosts.

CD-Parameter

CDs haben folgende Parameter:

Parametername	Beschreibung	Typ
uuid	Eindeutige Identifikator/Objektreferenz für die CD	Lesezugriff
name-**label**	Name der CD	Lese-/Schreibrechte
name-description	Beschreibungstext für die CD	Lese-/Schreibrechte
allowed-operations	Eine Liste der Vorgänge, die auf dieser CD ausgeführt werden können	Schreibgeschützter Parameter

Parametername	Beschreibung	Typ
current-operations	Eine Liste der Vorgänge, die derzeit auf dieser CD ausgeführt werden	Schreibgeschützter Parameter
sr-uuid	Die eindeutige Identifikator/Objektreferenz für das SR, zu dem diese CD gehört	Lesezugriff
sr-name-**label**	Der Name für das SR, zu dem diese CD gehört	Lesezugriff
vbd-uuids	Eine Liste der eindeutigen Kennungen für die VBDs auf VMs, die mit dieser CD verbunden sind	Schreibgeschützter Parameter
crashdump-uuids	Wird nicht auf CDs verwendet. Weil Crashdumps nicht auf CDs geschrieben werden können	Schreibgeschützter Parameter
virtual-size	Größe der CD, wie sie für virtuelle Rechner erscheint (in Byte)	Lesezugriff
physical-utilisation	Menge an physischem Speicherplatz, den das CD-Image auf dem SR belegt (in Byte)	Lesezugriff
type	Für CDs auf Benutzer setzen	Lesezugriff
sharable	Ob das CD-Laufwerk gemeinsam genutzt werden kann oder nicht. Die Standardeinstellung ist **false**.	Lesezugriff
read-only	Ob die CD schreibgeschützt ist **false**, wenn das Gerät beschreibbar ist. Stimmt immer für CDs.	Lesezugriff
storage-lock	Der Wert ist **true**, wenn dieser Datenträger auf Speicherebene gesperrt ist.	Lesezugriff
parent	Verweis auf den übergeordnete Datenträger, falls diese CD Teil einer Kette ist.	Lesezugriff

Parametername	Beschreibung	Typ
missing	Wert ist **true**, wenn der SR-Scanvorgang diese CD als nicht auf dem Datenträger vorhanden gemeldet hat	Lesezugriff
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die CD angeben	Map-Parameter lesen/schreiben
location	Der Pfad, auf dem das Gerät montiert ist	Lesezugriff
managed	Wert ist **true**, wenn das Gerät verwaltet wird	Lesezugriff
xenstore-data	In den xenstore-Baum einzufügende Daten	Schreibgeschützter Map-Parameter
sm-config	Namen und Beschreibungen der Speichermanager-Gerätekonfigurationsschlüssel	Schreibgeschützter Map-Parameter
is-a-snapshot	Wert ist **true**, wenn diese Vorlage ein CD-Snapshot ist	Lesezugriff
snapshot_of	Die UUID der CD, von der diese Vorlage ein Snapshot ist	Lesezugriff
snapshots	Die UUIDs aller Snapshots, die von dieser CD aufgenommen wurden	Lesezugriff
snapshot_time	Der Zeitstempel des Snapshot-Vorgangs	Lesezugriff

cd-list

```
xe cd-list [params=param1,param2,...] [parameter=parameter_value]
<!--NeedCopy-->
```

Listet die CDs und ISOs (CD-Image-Dateien) auf dem XenServer-Host oder -Pool auf und filtert nach dem optionalen Argument. params

Wenn das optionale Argument params verwendet wird, ist der Wert von params eine Zeichenfolge, die eine Liste von Parametern dieses Objekts enthält, die Sie anzeigen möchten. Alternativ können Sie

das Schlüsselwort verwenden `all`, um alle Parameter anzuzeigen. Wenn `params` nicht verwendet wird, zeigt die zurückgegebene Liste eine Standard-Teilmenge aller verfügbaren Parameter an.

Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten CD-Parameter sein.

Cluster-Befehle

Befehle zum Arbeiten mit Clusterpools.

Clusterpools sind Ressourcenpools, für die die Clustering-Funktion aktiviert ist. Verwenden Sie diese Pools mit GFS2-SRs. Weitere Informationen finden Sie unter Clustered-Pools.

Die Cluster- und Clusterhost-Objekte können mit den Befehlen zur Standardobjektauflistung (`xe cluster-list` und `xe cluster-host-list`) und den mit den Standardparameterbefehlen manipulierten Parametern aufgeführt werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene.
Befehle zum Arbeiten mit Clusterpools.

Cluster-Parameter

Cluster haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den Cluster	Lesezugriff
`cluster-hosts`	Eine Liste von eindeutigen Bezeichnern/Objektreferenzen für die Hosts im Cluster	Schreibgeschützter Parameter
`cluster-token`	Der geheime Schlüssel, der verwendet wird `xapi-clusterd`, wenn es auf anderen Hosts mit sich selbst spricht	Lesezugriff
`cluster-stack`	Der Technologie-Stack, der die Cluster-Funktionen bereitstellt. Mögliche Werte sind `corosync`.	Lesezugriff

Parametername	Beschreibung	Typ
allowed-operations	Listet die in diesem Zustand zulässigen Vorgänge auf. Diese Liste ist nur eine Empfehlung und der Clusterstatus hat sich möglicherweise geändert, bis ein Client dieses Feld liest.	Schreibgeschützter Parameter
current-operations	Listet die aktuell laufenden Vorgänge auf. Diese Liste ist nur eine Empfehlung und der Clusterstatus hat sich möglicherweise geändert, bis ein Client dieses Feld liest.	Schreibgeschützter Parameter
token-timeout	Das corosync-Token-Timeout in Sekunden	Lesezugriff
token-timeout-coefficient	Der corosync-Token-Timeout-Koeffizient in Sekunden	Lesezugriff
pool-auto-join	True, wenn automatisch neue Poolmitglieder dem Cluster beitreten. Dies ist auf eingestellt **true**.	Lesezugriff
cluster-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Cluster angeben.	Schreibgeschützter Map-Parameter
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Cluster angeben.	Map-Parameter lesen/schreiben

cluster-host-destroy

```
xe cluster-host-destroy uuid=host_uuid
<!--NeedCopy-->
```


Zerstören Sie einen Clusterhost und verlassen Sie effektiv den Cluster.

cluster-host-disable

```
xe cluster-host-disable uuid=cluster_uuid
<!--NeedCopy-->
```

Deaktivieren der Clustermitgliedschaft für einen aktivierten Clusterhost.

cluster-host-enable

```
xe cluster-host-enable uuid=cluster_uuid
<!--NeedCopy-->
```

Aktivieren der Clustermitgliedschaft für einen deaktivierten Clusterhost

cluster-host-force-destroy

```
xe cluster-host-force-destroy uuid=cluster_host
<!--NeedCopy-->
```

Zerstören Sie ein Clusterhostobjekt mit Nachdruck und verlassen Sie effektiv den Cluster

cluster-pool-create

```
xe cluster-pool-create network-uuid=network_uuid [cluster-stack=
    cluster_stack] [token-timeout=token_timeout] [token-timeout-
    coefficient=token_timeout_coefficient]
<!--NeedCopy-->
```

Erstellen Sie einen poolweiten Cluster.

cluster-pool-destroy

```
xe cluster-pool-destroy cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Zerstört den poolweiten Cluster. Der Pool ist weiterhin vorhanden, aber er ist nicht mehr geclustert und kann keine GFS2-SRs mehr verwenden.

cluster-pool-force-destroy

```
xe cluster-pool-force-destroy cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Erzwingen der Zerstörung des poolweiten Clusters.

cluster-pool-resync

```
xe cluster-pool-resync cluster-uuid=cluster_uuid
<!--NeedCopy-->
```

Synchronisieren Sie einen Cluster in einem Pool neu.

Befehle für die Konsole

Befehle zum Arbeiten mit Konsolen.

Die Konsolenobjekte können mit dem Standardbefehl für die Objektauflistung (`xe console-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene.

Konsolen-Parameter

Konsolen haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die Konsole	Lesezugriff
`vm-uuid`	Die eindeutige Bezeichner/Objektreferenz der VM, auf der diese Konsole geöffnet ist	Lesezugriff
`vm-name-label`	Der Name der VM, auf der diese Konsole geöffnet ist	Lesezugriff

Parametername	Beschreibung	Typ
protocol	Protokoll, das diese Konsole verwendet. Mögliche Werte sind vt100: VT100-Terminal, rfb: Remote Framebuffer-Protokoll (wie in VNC verwendet) oder rdp: Remote Desktop Protocol	Lesezugriff
location	URI für den Konsolendienst	Lesezugriff
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die Konsole angeben.	Map-Parameter lesen/schreiben

console

```
xe console
<!--NeedCopy-->
```

An einer bestimmten Konsole befestigen.

Diagnostische Befehle

Befehle zum Sammeln von Diagnoseinformationen von XenServer.

diagnostic-compact

```
xe diagnostic-compact
<!--NeedCopy-->
```

Führen Sie eine größere GC-Sammlung und Heap-Verdichtung durch.

diagnostic-db-stats

```
xe diagnostic-db-stats
<!--NeedCopy-->
```

Druckt Datenbankstatistiken.

diagnostic-gc-stats

```
xe diagnostic-gc-stats
<!--NeedCopy-->
```

GC-Statistiken drucken.

diagnostic-license-status

```
xe diagnostic-license-status
<!--NeedCopy-->
```

Hilft bei der Diagnose von poolweiten Lizenzproblemen.

diagnostic-net-stats

```
xe diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2
    ...]
<!--NeedCopy-->
```

Netzwerkstatistiken drucken.

diagnostic-timing-stats

```
xe diagnostic-timing-stats
<!--NeedCopy-->
```

Timing-Statistiken drucken.

diagnostic-vdi-status

```
xe diagnostic-vdi-status uuid=vdi_uuid
<!--NeedCopy-->
```

Fragen Sie den Sperr- und Freigabestatus eines VDI ab.

diagnostic-vm-status

```
xe diagnostic-vm-status uuid=vm_uuid
<!--NeedCopy-->
```

Fragen Sie die Hosts ab, auf denen die VM booten kann, und überprüfen Sie den Freigabe-/Sperrstatus aller VBDs.

Befehle zur Notfallwiederherstellung

Befehle zum Wiederherstellen von virtuellen Rechnern nach einer Katastrophe

drtask-create

```
xe drtask-create type=type sr-whitelist=sr-white-list device-config=
   device-config
<!--NeedCopy-->
```

Erstellt eine Disaster Recovery-Aufgabe. Um beispielsweise eine Verbindung zu einem iSCSI-SR in Vorbereitung auf die Notfallwiederherstellung herzustellen:

```
xe drtask-create type=lvmoiscsi device-config:target=target-ip-address
   \
    device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
    sr-whitelist=sr-uuid-list
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der Befehl `sr-whitelist` listet erlaubte SR-UUIDs auf. Der Befehl `drtask-create` führt nur ein SR ein und stellt eine Verbindung dazu her, das eine der zulässigen UUIDs hat

drtask-destroy

```
xe drtask-destroy uuid=dr-task-uuid
<!--NeedCopy-->
```

Zerstört eine Disaster Recovery-Aufgabe und vergisst das eingeführte SR.

vm-assert-can-be-recovered

```
xe vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Testet, ob Speicher für die Wiederherstellung dieser VM verfügbar ist.

appliance-assert-can-be-recovered

```
xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-
   uuid=vdi-uuid
<!--NeedCopy-->
```

Überprüft, ob der Speicher (der die Appliance-/vApp-Disk enthält) sichtbar ist.

appliance-recover

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
    force=true|false]
<!--NeedCopy-->
```

Stellen Sie eine Appliance/vApp aus der Datenbank wieder her, die im mitgelieferten VDI enthalten ist.

vm-recover

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true|false
    ]
<!--NeedCopy-->
```

Stellt eine VM aus der Datenbank wieder her, die im bereitgestellten VDI enthalten ist.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Ermöglicht die XAPI-Datenbankreplikation auf das angegebene (gemeinsame) SR.

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Deaktiviert die XAPI-Datenbankreplikation auf das angegebene SR.

Beispiel Verwendung

Das folgende Beispiel zeigt die DR CLI-Befehle im Kontext:

Aktivieren Sie am primären Standort die Datenbankreplikation:

```
xe sr-database-replication uuid=sr=uuid
<!--NeedCopy-->
```

Stellen Sie nach einer Katastrophe am sekundären Standort eine Verbindung zum SR her. Der Befehl `device-config` hat dieselben Felder wie `sr-probe`.


```
xe drtask-create type=lvmoiscsi \
    device-config:target=target ip address \
    device-config:targetIQN=target-iqn \
    device-config:SCSIid=scsi-id \
    sr-whitelist=sr-uuid
<!--NeedCopy-->
```

Suchen Sie in dem SR nach Datenbank-VDIs:

```
xe vdi-list sr-uuid=sr-uuid type=Metadata
<!--NeedCopy-->
```

Abfrage eines Datenbank-VDI für vorhandene virtuelle Rechner:

```
xe vm-list database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Wiederherstellen einer VM:

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
<!--NeedCopy-->
```

Zerstöre die DR-Aufgabe. Alle SRs, die durch die DR-Task eingeführt wurden und nicht von virtuellen Rechnern benötigt werden, werden vernichtet:

```
xe drtask-destroy uuid=drtask-uuid
<!--NeedCopy-->
```

Event-Befehle

Befehle zum Arbeiten mit Ereignissen.

Event-Kurse

Ereignisklassen sind in der folgenden Tabelle aufgeführt:

Name der Klasse	Beschreibung
pool	Ein Pool physischer Hosts
vm	Eine virtuelle Maschine
host	Ein physischer Host
network	Ein virtuelles Netzwerk
vif	Eine virtuelle Netzwerkschnittstelle

Name der Klasse	Beschreibung
pif	Eine physische Netzwerkschnittstelle (separate VLANs werden als mehrere PIFs dargestellt)
sr	Ein Speicherrepository
vdi	Ein virtuelles Disk-Image
vbd	Ein virtuelles Blockgerät
pbd	Die physischen Blockgeräte, über die Hosts auf SRs zugreifen

event-wait

```
xe event-wait class=class_name [param-name=param_value] [param-name=/=
   param_value]
<!--NeedCopy-->
```

Blockiert die Ausführung anderer Befehle, bis ein Objekt existiert, das die in der Befehlszeile angegebenen Bedingungen erfüllt. Das Argument `x=y` bedeutet "warte, bis Feld x den Wert y annimmt"und `x=/=y` bedeutet "warte, bis Feld x einen anderen Wert als y annimmt".

Beispiel: Warten Sie, bis eine bestimmte VM ausgeführt wird.

```
xe event-wait class=vm name-label=myvm power-state=running
<!--NeedCopy-->
```

Blockiert andere Befehle, bis eine aufgerufene VM mit dem Namen `myvm` den `power-state`-Status "running"hat.

Beispiel: Warten Sie, bis eine bestimmte VM neu gestartet wurde:

```
xe event-wait class=vm uuid=$VM start-time=/=$(xe vm-list uuid=$VM
   params=start-time --minimal)
<!--NeedCopy-->
```

Sperrt andere Befehle, bis eine VM mit UUID *$VM* neu gestartet wird. Der Befehl verwendet den Wert von `start-time`, um zu entscheiden, wann die VM neu gestartet wird.

Der Klassenname kann eine der am Anfang dieses Abschnitts aufgeführten Ereignisklassen sein. Bei den Parametern kann es sich um einen der Parameter handeln, die in der *CLI-Befehlsklasse*-param-list aufgeführt sind.

GPU Befehle

Befehle zum Arbeiten mit physischen GPUs, GPU-Gruppen und virtuellen GPUs.

Die GPU-Objekte können mit den Standardbefehlen für die Objektauflistung aufgelistet werden: `xe pgpu-listxe gpu-group-list`, und `xe vgpu-list`. Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene.

Physikalische GPU-Parameter

Physikalische GPUS (pGPUs) haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die pGPU	Lesezugriff
`vendor-name`	Der Herstellername der pGPU	Lesezugriff
`device-name`	Der vom Hersteller diesem pGPU Modell zugewiesene Name	Lesezugriff
`gpu-group-uuid`	Die eindeutige Bezeichner/Objektreferenz für die GPU-Gruppe, der diese PGPU automatisch von XenServer zugewiesen wurde. Identische pGPUs auf Hosts in einem Pool werden gruppiert	Lesezugriff
`gpu-group-name-label`	Der Name der GPU-Gruppe, der die pGPU zugewiesen ist	Lesezugriff
`host-uuid`	Die eindeutige Bezeichner/Objektreferenz für den XenServer-Host, mit dem die PGPU verbunden ist	Lesezugriff
`host-name-label`	Der Name des XenServer-Hosts, mit dem die PGPU verbunden ist	Lesezugriff
`pci-id`	PCI-Kennung	Lesezugriff
`dependencies`	Listet die abhängigen PCI-Geräte auf, die an dieselbe VM weitergegeben wurden	Map-Parameter lesen/schreiben

Parametername	Beschreibung	Typ
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die pGPU angeben	Map-Parameter lesen/schreiben
supported-VGPU-types	Liste der virtuellen GPU-Typen, die von der zugrunde liegenden Hardware unterstützt werden	Lesezugriff
enabled-VGPU-types	Liste der virtuellen GPU-Typen, die für diese pGPU aktiviert wurden	Lesen/Schreiben
resident-VGPUs	Liste der vGPUs, die auf dieser pGPU ausgeführt werden	Lesezugriff

pgpu-disable-dom0-access

```
xe pgpu-disable-dom0-access uuid=uuid
<!--NeedCopy-->
```

Deaktivieren Sie den pGPU Zugriff auf dom0.

pgpu-enable-dom0-access

```
xe pgpu-enable-dom0-access uuid=uuid
<!--NeedCopy-->
```

Ermöglichen Sie den pGPU Zugriff auf dom0.

GPU-Gruppenparameter

GPU-Gruppen haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die GPU-Gruppe	Lesezugriff
name-**label**	Der Name der GPU-Gruppe	Lese-/Schreibrechte

Parametername	Beschreibung	Typ
name-description	Der beschreibende Text der GPU-Gruppe	Lese-/Schreibrechte
VGPU-uuids	Listet die eindeutigen Bezeichner/Objektreferenzen für die virtuellen GPUs in der GPU-Gruppe auf	Schreibgeschützter Parameter
PGPU-uuids	Listet die eindeutigen Bezeichner/Objektreferenzen für die pGPUs in der GPU-Gruppe auf	Schreibgeschützter Parameter
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die GPU-Gruppe angeben	Map-Parameter lesen/schreiben
supported-VGPU-types	Vereinigung aller virtuellen GPU-Typen, die von der zugrunde liegenden Hardware unterstützt werden	Lesezugriff
enabled-VGPU-types	Vereinigung aller virtuellen GPU-Typen, die auf den zugrunde liegenden pGPUs aktiviert wurden	Lesezugriff
allocation-algorithm	Tiefen-zuerst/Breite-First-Einstellung für die Zuweisung virtueller GPUs auf pGPUs innerhalb der Gruppe	Enum-Parameter mit Lese-/Schreibzugriff

GPU-Gruppenbetrieb Befehle zum Arbeiten mit GPU-Gruppen

gpu-group-create

```
xe gpu-group-create name-label=name_for_group [name-description=
   description]
<!--NeedCopy-->
```

Erstellt eine neue (leere) GPU-Gruppe, in die pGPUs verschoben werden können.

gpu-group-destroy


```
xe gpu-group-destroy uuid=uuid_of_group
<!--NeedCopy-->
```

Zerstört die GPU-Gruppe; nur für leere Gruppen zulässig.

gpu-group-get-remaining-capacity

```
xe gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-uuid=
   uuid_of_vgpu_type
<!--NeedCopy-->
```

Gibt zurück, wie viele virtuelle GPUs des angegebenen Typs in dieser GPU-Gruppe instanziiert werden können.

gpu-group-param-set

```
xe gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
   first|depth-first
<!--NeedCopy-->
```

Ändert den Algorithmus, den die GPU-Gruppe verwendet, um virtuelle GPUs zu pGPUs zuzuweisen.

Virtuelle GPU-Parameter

Virtuelle GPUs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die virtuelle GPU	Lesezugriff
vm-uuid	Die eindeutige Bezeichner/Objektreferenz für die VM, der die virtuelle GPU zugewiesen ist	Lesezugriff
vm-name-**label**	Der Name der VM, der die virtuelle GPU zugewiesen ist	Lesezugriff
gpu-group-uuid	Die eindeutige Bezeichner/Objektreferenz für die GPU-Gruppe, in der die virtuelle GPU enthalten ist	Lesezugriff
gpu-group-name-**label**	Der Name der GPU-Gruppe, in der die virtuelle GPU enthalten ist	Lesezugriff

Parametername	Beschreibung	Typ
currently-attached	Wahr, wenn eine VM mit GPU-Passthrough läuft, andernfalls false	Lesezugriff
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die virtuelle GPU angeben	Map-Parameter lesen/schreiben
type-uuid	Die eindeutige Bezeichner/Objektreferenz für den virtuellen GPU-Typ dieser virtuellen GPU	Map-Parameter lesen/schreiben
type-model-name	Mit dem virtuellen GPU-Typ verknüpfter Modellname	Lesezugriff

Typenparameter für virtuelle GPU

> **Hinweis:**
>
> GPU-Passthrough und virtuelle GPUs sind nicht mit Live-Migration, Storage-Live-Migration oder VM Suspend kompatibel, sofern nicht unterstützte Software und Grafikkarten von GPU-Anbietern vorhanden sind. Virtuelle Rechner ohne diese Unterstützung können nicht migriert werden, um Ausfallzeiten zu vermeiden. Informationen zur Kompatibilität von NVIDIA vGPU mit Livemigration, Speicher-Livemigration und VM Suspend finden Sie unter Grafik.

Virtuelle GPU-Typen haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für den virtuellen GPU-Typ	Lesezugriff
vendor-name	Name des virtuellen GPU-Anbieters	Lesezugriff
model-name	Mit dem virtuellen GPU-Typ verknüpfter Modellname	Lesezugriff
freeze-frame	Frame-Puffergröße des virtuellen GPU-Typs in Byte	Lesezugriff

Parametername	Beschreibung	Typ
max-heads	Maximale Anzahl von Displays, die vom virtuellen GPU-Typ unterstützt werden	Lesezugriff
supported-on-PGPUs	Liste der pGPUs, die diesen virtuellen GPU-Typ unterstützen	Lesezugriff
enabled-on-PGPUs	Liste der pGPUs, für die dieser virtuelle GPU-Typ aktiviert ist	Lesezugriff
VGPU-uuids	Liste der virtuellen GPUs dieses Typs	Lesezugriff

Virtueller GPU-Betrieb

vgpu-create

```
xe vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [
   vgpu-type-uuid=uuid_of_vgpu-type]
<!--NeedCopy-->
```

Erstellt eine virtuelle GPU. Dieser Befehl hängt die VM an die angegebene GPU-Gruppe an und gibt optional den virtuellen GPU-Typ an. Wenn kein virtueller GPU-Typ angegeben ist, wird der "Passthrough"-Typ angenommen.

vgpu-destroy

```
xe vgpu-destroy uuid=uuid_of_vgpu
<!--NeedCopy-->
```

Zerstört die angegebene virtuelle GPU.

Deaktivieren von VNC für VMs mit virtueller GPU

```
xe vm-param-add uuid=uuid_of_vmparam-name=platform vgpu_vnc_enabled=
   true|false
<!--NeedCopy-->
```

Mit **false** wird die VNC-Konsole für eine VM deaktiviert, während disablevnc=1 zum Anzeigeemulator weitergeleitet wird. Standardmäßig ist VNC aktiviert.

Host-Befehle

Befehle für die Interaktion mit dem XenServer-Host.

XenServer-Hosts sind die physischen Server, auf denen die XenServer-Software ausgeführt wird. Auf ihnen laufen VMs unter der Kontrolle einer speziellen privilegierten virtuellen Maschine, die als Steuerdomäne oder Domäne 0 bekannt ist.

Die XenServer-Host-Objekte können mit den Standardbefehlen für die Objektauflistung aufgelistet werden: `xe host-listxe host-cpu-list`, und `xe host-crashdump-list`). Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene.

Host-Selektoren

Einige der hier aufgeführten Befehle haben einen gemeinsamen Mechanismus zur Auswahl eines oder mehrerer XenServer-Hosts, auf denen der Vorgang ausgeführt werden soll. Am einfachsten ist es, das Argument zu liefern `host=uuid_or_name_label`. Sie können XenServer auch angeben, indem Sie die vollständige Liste der Hosts nach den Werten der Felder filtern. Wenn Sie beispielsweise angeben, werden alle XenServer-Hosts `enabled=true` ausgewählt, deren `enabled` Feld gleich ist. **`true`** Wenn mehrere XenServer-Hosts übereinstimmen und der Vorgang auf mehreren XenServer-Hosts ausgeführt werden kann, müssen Sie angeben, ob der Vorgang ausgeführt werden `--multiple` soll. Die vollständige Liste der Parameter, die abgeglichen werden können, wird am Anfang dieses Abschnitts beschrieben. Sie können diese Befehlsliste abrufen, indem Sie den Befehl ausführen `xe host-list params=all`. Wenn keine Parameter zur Auswahl von XenServer-Hosts angegeben sind, wird der Vorgang auf allen XenServer-Hosts ausgeführt.

Host-Parameter

XenServer-Hosts haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den XenServer-Host	Lesezugriff
`name-label`	Der Name des XenServer-Hosts	Lese-/Schreibrechte
`name-description`	Die Beschreibungszeichenfolge des XenServer-Hosts	Lesezugriff

Parametername	Beschreibung	Typ
enabled	Der Wert ist **false**, falls deaktiviert. Dies verhindert, dass neue VMs auf den Hosts gestartet werden, und bereitet die Hosts auf das Herunterfahren oder Neustarten vor. Wert ist **true**, wenn der Host aktiviert ist	Lesezugriff
API-version-major	Hauptversionsnummer	Lesezugriff
API-version-minor	Kleinere Versionsnummer	Lesezugriff
API-version-vendor	Identifizierung des API-Anbieters	Lesezugriff
API-version-vendor-implementation	Einzelheiten der Implementierung des Anbieters	Schreibgeschützter Map-Parameter
logging	Protokollierungskonfiguration	Map-Parameter lesen/schreiben
suspend-image-sr-uuid	Die eindeutige Kennung/Objektreferenz für das SR, in der suspendierte Images platziert werden	Lese-/Schreibrechte
crash-dump-sr-uuid	Die eindeutige Bezeichner/Objektreferenz für das SR, in der Absturzabbilder abgelegt werden	Lese-/Schreibrechte
software-version	Liste der Versionierungsparameter und ihrer Werte	Schreibgeschützter Map-Parameter
capabilities	Liste der Xen-Versionen, die der XenServer-Host ausführen kann	Schreibgeschützter Parameter
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den XenServer-Host angeben	Map-Parameter lesen/schreiben

Parametername	Beschreibung	Typ
chipset-info	Eine Liste von Schlüssel/Wert-Paaren, die Informationen über den Chipsatz angeben	Schreibgeschützter Map-Parameter
hostname	Hostname XenServer-Hosts	Lesezugriff
address	XenServer-Host-IP-Adresse	Lesezugriff
license-server	Eine Liste von Schlüssel/Wert-Paaren, die Informationen über den Lizenzserver angeben. Der Standardanschluss für die Kommunikation mit Citrix Produkten ist 27000. Informationen zum Ändern Port Portnummern aufgrund von Konflikten finden Sie unter Portnummern ändern	Schreibgeschützter Map-Parameter
supported-bootloaders	Liste der Bootloader, die der XenServer-Host unterstützt, z. B. pygrub, eliloader	Schreibgeschützter Parameter
memory-total	Gesamtmenge an physischem RAM auf dem XenServer-Host, in Byte	Lesezugriff
memory-free	Gesamtmenge an verbleibendem physischem RAM, das virtuellen Rechnern zugewiesen werden kann, in Byte	Lesezugriff
host-metrics-live	True, wenn der Host betriebsbereit ist	Lesezugriff
logging	Der syslog_destination-Schlüssel kann auf den Hostnamen eines Syslog-Dienstes mit Remote-Listening festgelegt werden.	Map-Parameter lesen/schreiben

Parametername	Beschreibung	Typ
allowed-operations	Listet die in diesem Zustand zulässigen Vorgänge auf. Diese Liste dient nur zur Information und der Hoststatus kann sich geändert haben, bis ein Client dieses Feld liest.	Schreibgeschützter Parameter
current-operations	Listet die aktuell laufenden Vorgänge auf. Diese Liste dient nur zur Information und der Hoststatus kann sich geändert haben, bis ein Client dieses Feld liest.	Schreibgeschützter Parameter
patches	Satz von Host-Patches	Schreibgeschützter Parameter
blobs	Binärer Datenspeicher	Lesezugriff
memory-free-computed	Eine konservative Schätzung der maximalen Menge an freiem Speicher auf einem Host	Lesezugriff
ha-statefiles	Die UUIDs aller HA-State-Dateien	Lesezugriff
ha-network-peers	Die UUIDs aller Hosts, die bei einem Ausfall die VMs auf diesem Host hosten können	Lesezugriff
external-auth-type	Art der externen Authentifizierung, z. B. Active Directory.	Lesezugriff
external-auth-service-name	Der Name des externen Authentifizierungsdienstes	Lesezugriff
external-auth-configuration	Konfigurationsinformationen für den externen Authentifizierungsdienst.	Schreibgeschützter Map-Parameter

XenServer-Hosts enthalten einige andere Objekte, die ebenfalls Parameterlisten haben.

CPUs auf XenServer-Hosts haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die CPU	Lesezugriff
number	Die Nummer des physischen CPU-Kerns innerhalb des XenServer-Hosts	Lesezugriff
vendor	Die Herstellerzeichenfolge für den CPU-Namen	Lesezugriff
speed	Die CPU-Taktrate in Hz	Lesezugriff
modelname	Die Herstellerzeichenfolge für das CPU-Modell, z. B. “Intel (R) Xeon (TM) CPU 3,00 GHz”	Lesezugriff
stepping	Die CPU Revisionsnummer	Lesezugriff
flags	Die Flags der physischen CPU (eine decodierte Version des Feature-Feldes)	Lesezugriff
Utilisation	Die aktuelle CPU-Auslastung	Lesezugriff
host-uuid	Die UUID, wenn der Host, in dem sich die CPU befindet	Lesezugriff
model	Die Modellnummer der physikalischen CPU	Lesezugriff
family	Die Nummer der physischen CPU-Familie	Lesezugriff

Crash-Dumps auf XenServer-Hosts haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für den Crashdump	Lesezugriff
host	XenServer-Host, dem der Crashdump entspricht	Lesezugriff

Parametername	Beschreibung	Typ
timestamp	Zeitstempel des Datums und der Uhrzeit, zu der der Crashdump aufgetreten ist, in der Form yyyymmdd-hhmmss-ABC, wobei *ABC* die Zeitzonenanzeige ist, zum Beispiel GMT	Lesezugriff
size	Größe des Crashdump in Byte	Lesezugriff

host-all-editions

```
xe host-all-editions
<!--NeedCopy-->
```

Holen Sie sich eine Liste aller verfügbaren Editionen

host-apply-edition

```
xe host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition=
    "free" "per-socket" "xendesktop"]
<!--NeedCopy-->
```

Weist die XenServer-Lizenz einem Hostserver zu. Wenn Sie eine Lizenz zuweisen, kontaktiert XenServer den Lizenzserver und fordert den angegebenen Lizenztyp an. Wenn eine Lizenz verfügbar ist, wird sie dann vom Lizenzserver ausgecheckt.

Informationen zur Erstkonfiguration der Lizenzierung finden Sie auch unter license-server-address und license-server-port.

host-backup

```
xe host-backup file-name=backup_filename host=host_name
<!--NeedCopy-->
```

Laden Sie eine Backup der Steuerdomäne des angegebenen XenServer-Hosts auf den Computer herunter, von dem aus der Befehl aufgerufen wird. Speichern Sie es dort als Datei mit dem Namen file-name.

> **Wichtig:**
>
> Der Befehl `xe host-backup` funktioniert zwar, wenn er auf dem lokalen Host ausgeführt wird (d. h. ohne Angabe eines bestimmten Hostnamens), aber verwenden Sie ihn nicht auf diese Weise. Dadurch würde die Steuerdomänenpartition mit der Backupdatei aufgefüllt. Verwenden Sie den Befehl nur von einer remoten Maschine, die nicht auf dem Host ist, und auf der Sie Platz für die Backupdatei haben.

host-bugreport-upload

```
xe host-bugreport-upload [host-selector=host_selector_value...] [url=
    destination_url http-proxy=http_proxy_name]
<!--NeedCopy-->
```

Generieren Sie einen neuen Fehlerbericht (mit `xen-bugtool`, alle optionalen Dateien eingeschlossen) und laden Sie ihn auf die FTP-Site des Supports oder an einen anderen Ort hoch.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

Optionale Parameter sind `http-proxy`: angegebenen HTTP-Proxy verwenden und `url`: auf diese Ziel-URL hochladen. Wenn optionale Parameter nicht verwendet werden, wird kein Proxyserver identifiziert und das Ziel ist die standardmäßige FTP-Support-Site.

host-call-plugin

```
xe host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args
    =args]
<!--NeedCopy-->
```

Ruft die Funktion innerhalb des Plug-Ins auf dem angegebenen Host mit optionalen Argumenten auf.

host-compute-free-memory

```
xe host-compute-free-memory
<!--NeedCopy-->
```

Berechnet die Menge an freiem Speicher auf dem Host.

host-compute-memory-overhead


```
xe host-compute-memory-overhead
<!--NeedCopy-->
```

Berechnet den Virtualisierungsspeicher-Overhead eines Hosts.

host-cpu-info

```
xe host-cpu-info [uuid=uuid]
<!--NeedCopy-->
```

Listet Informationen über die physischen CPUs des Hosts auf.

host-crashdump-destroy

```
xe host-crashdump-destroy uuid=crashdump_uuid
<!--NeedCopy-->
```

Löschen Sie einen durch seine UUID angegebenen Host-Crashdump vom XenServer-Host.

host-crashdump-upload

```
xe host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [
    http-proxy=http_proxy_name]
<!--NeedCopy-->
```

Laden Sie einen Crashdump auf die FTP-Site des Supports oder an einem anderen Wenn optionale Parameter nicht verwendet werden, wird kein Proxyserver identifiziert und das Ziel ist die standardmäßige FTP-Support-Site. Optionale Parameter sind `http-proxy`: angegebenen HTTP-Proxy verwenden und `url`: auf diese Ziel-URL hochladen.

host-declare-dead

```
xe host-declare-dead uuid=host_uuid
<!--NeedCopy-->
```

Erklären Sie, dass der Host tot ist, ohne ihn explizit zu kontaktieren.

> **Warnung:**
>
> Dieser Aufruf ist gefährlich und kann zu Datenverlust führen, wenn der Host nicht wirklich tot ist.

host-disable

```
xe host-disable [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Deaktiviert die angegebenen XenServer-Hosts, wodurch verhindert wird, dass neue VMs auf ihnen gestartet werden. Diese Aktion bereitet die XenServer-Hosts darauf vor, heruntergefahren oder neu gestartet zu werden. Wenn nach dem Neustart des Hosts alle Bedingungen für die Aktivierung erfüllt sind (z. B. ist Speicher verfügbar), wird der Host automatisch wieder aktiviert.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-disable-display

```
xe host-disable-display uuid=host_uuid
<!--NeedCopy-->
```

Deaktiviert die Anzeige für den Host.

host-disable-local-storage-caching

```
xe host-disable-local-storage-caching
<!--NeedCopy-->
```

Deaktivieren Sie das lokale Speichercaching auf dem angegebenen Host.

host-dmesg

```
xe host-dmesg [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Ruft ein Xen `dmesg` (die Ausgabe des Kernel-Ringpuffers) von angegebenen XenServer-Hosts ab.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-emergency-ha-disable

```
xe host-emergency-ha-disable  [--force]
<!--NeedCopy-->
```


Deaktivieren Sie HA auf dem lokalen Host. Nur zur Wiederherstellung eines Pools mit einem defekten HA-Setup verwendet werden.

host-emergency-management-reconfigure

```
xe host-emergency-management-reconfigure interface=
   uuid_of_management_interface_pif
<!--NeedCopy-->
```

Konfigurieren Sie die Verwaltungsschnittstelle dieses XenServer-Hosts neu. Verwenden Sie diesen Befehl nur, wenn sich der XenServer-Host im Notfallmodus befindet. Notfallmodus bedeutet, dass der Host Mitglied in einem Ressourcenpool ist, dessen Poolkoordinator aus dem Netzwerk verschwunden ist und nach einer Reihe von Wiederholungen nicht mehr kontaktiert werden kann.

host-emergency-reset-server-certificate

```
xe host-emergency-reset-server-certificate
<!--NeedCopy-->
```

Installiert ein selbstsigniertes Zertifikat auf dem XenServer-Host, auf dem der Befehl ausgeführt wird.

host-enable

```
xe host-enable [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Aktiviert die angegebenen XenServer-Hosts, sodass neue VMs auf ihnen gestartet werden können.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standard-auswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-enable-display

```
xe host-enable-display uuid=host_uuid
<!--NeedCopy-->
```

Aktiviert die Anzeige für den Host.

host-enable-local-storage-caching

```
xe host-enable-local-storage-caching  sr-uuid=sr_uuid
<!--NeedCopy-->
```

Aktiviert das lokale Speichercaching auf dem angegebenen Host.

host-evacuate

```
xe host-evacuate [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Live migriert alle laufenden VMs auf andere geeignete Hosts in einem Pool. Deaktivieren Sie zunächst den Host mit dem Befehl `host-disable`.

Wenn der evakuierte Host der Poolkoordinator ist, muss ein anderer Host als Poolkoordinator ausgewählt werden. Verwenden Sie den Befehl `pool-designate-new-master`, um den Poolkoordinator bei deaktivierter HA zu ändern. Weitere Informationen finden Sie unter Pool-designiert-neuer-Master.

Wenn HA aktiviert ist, besteht Ihre einzige Möglichkeit darin, den XenServer-Host herunterzufahren, wodurch HA nach dem Zufallsprinzip einen neuen Poolkoordinator auswählt. Weitere Informationen finden Sie unter Host-shutdown.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-forget

```
xe host-forget uuid=host_uuid
<!--NeedCopy-->
```

Der XAPI-Agent vergisst den angegebenen XenServer-Host, ohne ihn explizit zu kontaktieren.

Verwenden Sie den Parameter `--force`, um zu vermeiden, dass Sie aufgefordert werden, zu bestätigen, dass Sie diesen Vorgang wirklich ausführen möchten.

> **Warnung:**
>
> Verwenden Sie diesen Befehl nicht, wenn HA für den Pool aktiviert ist. Deaktivieren Sie zuerst HA und aktivieren Sie sie dann erneut, nachdem Sie den Host vergessen haben.

Dieser Befehl ist nützlich, wenn der zu "vergessende"XenServer-Host tot ist. Wenn der XenServer-Host jedoch live und Teil des Pools ist, verwenden Sie `xe pool-eject` stattdessen.

host-get-server-certificate

```
xe host-get-server-certificate
<!--NeedCopy-->
```

Holen Sie sich das TLS-Zertifikat des installierten Servers.

host-get-sm-diagnostics

```
xe host-get-sm-diagnostics uuid=uuid
<!--NeedCopy-->
```

SM-Diagnoseinformationen pro Host anzeigen.

host-get-system-status

```
xe host-get-system-status filename=name_for_status_file [entries=
   comma_separated_list] [output=tar.bz2|zip] [host-selector=
   host_selector_value...]
<!--NeedCopy-->
```

Laden Sie Systemstatusinformationen in die angegebene Datei herunter. Der optionale Parameter `entries` ist eine kommagetrennte Liste von Systemstatuseinträgen, die dem vom Befehl `host-get-system-status-capabilities` zurückgegebenen XML-Fragment der Fähigkeiten entnommen wurden. Weitere Informationen finden Sie unter Host-Get-Systemstatus-Funktionen. Wenn nicht angegeben, werden alle Systemstatusinformationen in der Datei gespeichert. Der Parameter `output` kann *tar.bz2* (die Standardeinstellung) oder *zip*sein. Wenn dieser Parameter nicht angegeben ist, wird die Datei im `tar.bz2`-Format gespeichert.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben).

host-get-system-status-capabilities

```
xe host-get-system-status-capabilities [host-selector=
   host_selector_value...]
<!--NeedCopy-->
```

Ruft Systemstatus-Funktionen für die angegebenen Hosts ab. Die Funktionen werden als XML-Fragment zurückgegeben, das dem folgenden Beispiel ähnelt:

```
<?xml version="1.0" ?>
<system-status-capabilities>
```



```
    <capability content-type="text/plain" default-checked="yes" key="
        xenserver-logs"  \
        max-size="150425200" max-time="-1" min-size="150425200" min-
            time="-1" \
        pii="maybe"/>
    <capability content-type="text/plain" default-checked="yes" \
        key="xenserver-install" max-size="51200" max-time="-1" min-size
            ="10240" \
        min-time="-1" pii="maybe"/>
    ...
</system-status-capabilities>
<!--NeedCopy-->
```

Jede Capability-Entität kann die folgenden Attribute haben.

- `key` Eine eindeutige Kennung für die Funktion.
- `content-type` Kann entweder Text/Normaltext oder Anwendung/Daten sein. Zeigt an, ob eine UI die Einträge für den menschlichen Verzehr rendern kann.
- **`default`**`-checked` Kann entweder Ja oder Nein sein. Gibt an, ob eine Benutzeroberfläche diesen Eintrag standardmäßig auswählt.
- `min-size`, `max-size` Gibt einen ungefähren Bereich für die Größe dieses Eintrags in Byte an. -1 bedeutet, dass die Größe unwichtig ist.
- `min-time`, `max-time` Gibt einen ungefähren Bereich für die Zeit in Sekunden an, die zum Erfassen dieses Eintrags benötigt wird. -1 zeigt an, dass die Zeit unwichtig ist.
- `pii` Personenbezogene Daten. Zeigt an, ob der Eintrag Informationen enthält, die den Systembesitzer oder Details seiner Netzwerktopologie identifizieren können. Das Attribut kann einen der folgenden Werte annehmen:
  - `no`: In diesen Einträgen sind keine PII enthalten
  - `yes`: PII ist wahrscheinlich oder sicher in diesen Einträgen
  - `maybe`: Vielleicht möchten Sie diese Einträge auf PII überprüfen
  - `if_customized` wenn die Dateien unverändert sind, enthalten sie keine PII. Da wir jedoch die Bearbeitung dieser Dateien fördern, wurde PII möglicherweise durch eine solche Anpassung eingeführt. Dieser Wert wird insbesondere für die Netzwerkskripte in der Steuerdomäne verwendet.

  Kennwörter dürfen niemals in einen Fehlerbericht aufgenommen werden, unabhängig von einer PII-Deklaration.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben).

host-get-thread-diagnostics

```
xe host-get-thread-diagnostics uuid=uuid
<!--NeedCopy-->
```

Zeigt Diagnoseinformationen für Threads pro Host an.

host-get-vms-which-prevent-evacuation

```
xe host-get-vms-which-prevent-evacuation uuid=uuid
<!--NeedCopy-->
```

Gibt eine Liste von virtuellen Rechnern zurück, die die Evakuierung eines bestimmten Hosts verhindern, und zeigt die Gründe für jeden einzelnen an.

host-is-in-emergency-mode

```
xe host-is-in-emergency-mode
<!--NeedCopy-->
```

Gibt **true** zurück, wenn der Host, mit dem die CLI kommuniziert, im Notfallmodus ist, andernfalls **false**. Dieser CLI-Befehl funktioniert direkt auf Hosts von Poolmitgliedern, auch wenn kein Poolkoordinator vorhanden ist.

host-license-add

```
xe host-license-add [license-file=path/license_filename] [host-uuid=
   host_uuid]
<!--NeedCopy-->
```

Verwenden Sie für XenServer, um eine lokale Lizenzdatei zu analysieren und sie dem angegebenen XenServer-Host hinzuzufügen.

host-license-remove

```
xe host-license-remove [host-uuid=host_uuid]
<!--NeedCopy-->
```

Entfernen Sie alle auf einen Host angewendeten Lizenzen.

host-license-view

```
xe host-license-view [host-uuid=host_uuid]
<!--NeedCopy-->
```

Zeigt den Inhalt der XenServer-Hostlizenz an.

host-logs-download

```
xe host-logs-download [file-name=logfile_name] [host-selector=
   host_selector_value...]
<!--NeedCopy-->
```

Laden Sie eine Kopie der Protokolle der angegebenen XenServer-Hosts herunter. Die Kopie wird standardmäßig in einer Datei mit Zeitstempel namens gespeichert `hostname-yyyy-mm-dd T hh:mm:ssZ.tar.gz`. Mit dem optionalen Parameter *file-name* können Sie einen anderen Dateinamen angeben.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

> **Wichtig:**
>
> Der Befehl `xe host-logs-download` funktioniert zwar, wenn er auf dem lokalen Host ausgeführt wird (d. h. ohne Angabe eines bestimmten Hostnamens). Sie sollten ihn jedoch *nicht* auf diese Weise verwenden. Dadurch wird die Steuerdomänenpartition mit der Kopie der Protokolle überladen. Verwenden Sie den Befehl nur von einem Remote-Off-Host-Computer aus, auf dem Sie Speicherplatz für die Kopie der Protokolle haben.

host-management-disable

```
xe host-management-disable
<!--NeedCopy-->
```

Deaktiviert den Host-Agent, der auf einer externen Verwaltungsnetzwerkschnittstelle lauscht, und trennt alle verbundenen API-Clients (z. B. XenCenter). Dieser Befehl wird direkt auf dem XenServer-Host ausgeführt, mit dem die CLI verbunden ist. Der Befehl wird nicht an den Poolkoordinator weitergeleitet, wenn er auf einen XenServer-Mitgliedshost angewendet wird.

> **Warnung:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden. Nachdem dieser Befehl ausgeführt wurde, können Sie sich nicht remote über das Netzwerk mit der Steuer-

> domäne verbinden, um den Host-Agent erneut zu aktivieren.

host-management-reconfigure

```
xe host-management-reconfigure [interface=device] [pif-uuid=uuid]
<!--NeedCopy-->
```

Konfiguriert den XenServer-Host neu, sodass er die angegebene Netzwerkschnittstelle als Verwaltungsschnittstelle verwendet. Dies ist die Schnittstelle, die für die Verbindung mit dem XenCenter verwendet wird. Der Befehl schreibt den Schlüssel MANAGEMENT_INTERFACE um `/etc/xensource-inventory`.

Wenn der Gerätename einer Schnittstelle (die eine IP-Adresse haben muss) angegeben wird, bindet der XenServer-Host sofort neu. Dieser Befehl funktioniert sowohl im Normal- als auch im Notfallmodus.

Wenn die UUID eines PIF-Objekts angegeben ist, bestimmt der XenServer-Host, welche IP-Adresse an sich selbst neu gebunden werden soll. Es darf sich nicht im Notfallmodus befinden, wenn dieser Befehl ausgeführt wird.

> **Warnung:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden, und stellen Sie sicher, dass die neue Schnittstelle über Netzwerkkonnektivität verfügt. Verwenden Sie `xe pif-reconfigure` zum Einrichten. Andernfalls können nachfolgende CLI-Befehle den XenServer-Host nicht erreichen.

host-power-on

```
xe host-power-on [host=host_uuid]
<!--NeedCopy-->
```

Schaltet XenServer-Hosts mit aktivierter *Host-Power-On-Funktion* ein. Bevor Sie diesen Befehl verwenden, aktivieren Sie `host-set-power-on` auf dem Host.

host-reboot

```
xe host-reboot [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Starten Sie die angegebenen XenServer-Hosts neu. Die angegebenen Hosts müssen zuerst mit dem Befehl `xe host-disable` deaktiviert werden, andernfalls wird eine Fehlermeldung `HOST_IN_USE` angezeigt.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

Wenn die angegebenen XenServer-Hosts Mitglieder eines Pools sind, wird der Verbindungsverlust beim Herunterfahren behoben und der Pool wird wiederhergestellt, wenn die XenServer-Hosts zurückkehren. Die anderen Mitglieder und der Poolkoordinator funktionieren weiterhin.

Wenn Sie den Poolkoordinator herunterfahren, ist der Pool außer Betrieb, bis eine der folgenden Aktionen ausgeführt wird:

- Sie machen eines der Mitglieder zum Poolkoordinator
- Der ursprüngliche Poolkoordinator wird neu gestartet und ist wieder online.

  Wenn der Poolkoordinator wieder online ist, verbinden sich die Mitglieder erneut und synchronisieren sich mit dem Poolkoordinator.

host-restore

```
xe host-restore [file-name=backup_filename] [host-selector=
   host_selector_value...]
<!--NeedCopy-->
```

Stellen Sie ein Backup mit dem Namen `file-name` der XenServer-Hoststeuerungssoftware wieder her. Die Verwendung des Wortes “Wiederherstellen”bedeutet hier keine vollständige Wiederherstellung im üblichen Sinne, sondern bedeutet lediglich, dass die komprimierte Backupdatei dekomprimiert und auf die sekundäre Partition entpackt wurde. Nachdem Sie `xe host-restore` abgeschlossen haben, müssen Sie die Installations-CD starten und die Option Wiederherstellen von Backup verwenden.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-send-debug-keys

```
xe host-send-debug-keys  host-uuid=host_uuid keys=keys
<!--NeedCopy-->
```

Sendet angegebene Hypervisor-Debug-Schlüssel an den angegebenen Host.

host-server-certificate-install


```
xe host-server-certificate-install certificate=path_to_certificate_file
     private-key=path_to_private_key [certificate-chain=
    path_to_chain_file] [host=host_name | uuid=host_uuid]
<!--NeedCopy-->
```

Installieren Sie ein TLS-Zertifikat auf einem XenServer-Host.

host-set-hostname-live

```
xe host-set-hostname-live host-uuid=uuid_of_host host-name=new_hostname
<!--NeedCopy-->
```

Ändern Sie den Hostnamen des XenServer-Hosts, der von angegeben wurde `host-uuid`. Mit diesem Befehl werden sowohl der Hostname in der Steuerdomänendatenbank als auch der tatsächliche Linux-Hostname des XenServer-Hosts dauerhaft festgelegt. Der Wert von `host-name` ist *nicht* mit dem Wert des Feldes `name_label` identisch.

host-set-power-on-mode

```
xe host-set-power-on-mode host=host_uuid power-on-mode={
 "" | "wake-on-lan" | "DRAC" | "custom" }
  \
    [ power-on-config:power_on_ip=ip-address power-on-config:
       power_on_user=user power-on-config:power_on_password_secret=
       secret-uuid ]
<!--NeedCopy-->
```

Wird verwendet, um die *Host-Power-On-Funktion* auf XenServer-Hosts zu aktivieren, die mit Remote-Stromversorgungslösungen kompatibel sind. Wenn Sie den Befehl `host-set-power-on` verwenden, müssen Sie den Typ der Energieverwaltungslösung auf dem Host angeben (d. h. den Einschaltmodus). Geben Sie dann die Konfigurationsoptionen mit dem Argument power-on-config und den zugehörigen Schlüssel-Wert-Paaren an.

Geben Sie den Schlüssel `"power_on_password_secret"` an, um die Funktion “Geheimnisse” zum Speichern Ihres Kennworts zu verwenden. Weitere Informationen finden Sie unter Secrets.

host-shutdown

```
xe host-shutdown [host-selector=host_selector_value...]
<!--NeedCopy-->
```

Fahren Sie die angegebenen XenServer-Hosts herunter. Die angegebenen XenServer-Hosts müssen zuerst mit dem `xe host-disable` Befehl deaktiviert werden, andernfalls wird eine `HOST_IN_USE` Fehlermeldung angezeigt.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

Wenn die angegebenen XenServer-Hosts Mitglieder eines Pools sind, wird der Verbindungsverlust beim Herunterfahren behoben und der Pool wird wiederhergestellt, wenn die XenServer-Hosts zurückkehren. Die anderen Mitglieder und der Poolkoordinator funktionieren weiterhin.

Wenn Sie den Poolkoordinator herunterfahren, ist der Pool außer Betrieb, bis eine der folgenden Aktionen ausgeführt wird:

- Sie machen eines der Mitglieder zum Poolkoordinator
- Der ursprüngliche Poolkoordinator wird neu gestartet und ist wieder online.

  Wenn der Poolkoordinator wieder online ist, verbinden sich die Mitglieder erneut und synchronisieren sich mit dem Poolkoordinator.

Wenn HA für den Pool aktiviert ist, wird eines der Mitglieder automatisch zu einem Poolkoordinator gemacht. Wenn HA deaktiviert ist, müssen Sie den gewünschten XenServer-Host mit dem Befehl `pool-designate-new-master` manuell als Poolkoordinator festlegen. Weitere Informationen finden Sie unter Pool-designiert-neuer-Master.

host-sm-dp-destroy

```
xe host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
<!--NeedCopy-->
```

Versuch, einen Speicherdatenpfad auf einem Host zu zerstören und zu bereinigen. Wenn `allow-leak=true` angegeben wird, löscht es alle Datensätze des Datenpfads, auch wenn er nicht sauber heruntergefahren wurde.

host-sync-data

```
xe host-sync-data
<!--NeedCopy-->
```

Synchronisieren Sie die auf dem Poolkoordinator gespeicherten Daten mit dem benannten Host. Dies beinhaltet nicht die Datenbankdaten).

host-syslog-reconfigure

```
xe host-syslog-reconfigure [host-selector=host_selector_value...]
<!--NeedCopy-->
```


Konfigurieren Sie den `syslog` Daemon auf den angegebenen XenServer-Hosts neu. Mit diesem Befehl werden die Konfigurationsinformationen angewendet, die im `logging`-Hostparameter definiert sind.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein.

host-data-source-list

```
xe host-data-source-list [host-selectors=host selector value...]
<!--NeedCopy-->
```

Listen Sie die Datenquellen auf, die für einen Host aufgezeichnet werden können.

Wählen Sie die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen Hosts ausgeführt.

Datenquellen haben zwei Parameter —`standard` und `enabled`. Dieser Befehl gibt die Werte der Parameter aus:

- Wenn in einer Datenquelle `enabled` auf **`true`** festgelegt wurde, werden die Metriken derzeit in der Performance-Datenbank aufgezeichnet.
- Wenn in einer Datenquelle `standard` auf **`true`** eingestellt ist, werden die Metriken *standardmäßig*in der Performance-Datenbank aufgezeichnet. Der Wert von `enabled` ist auch für diese Datenquelle auf **`true`** festgelegt.
- Wenn für eine Datenquelle `standard` auf **`false`** eingestellt ist, werden die Metriken *nicht* standardmäßig in der Performance-Datenbank aufgezeichnet. Der Wert von `enabled` ist auch für diese Datenquelle auf **`false`** festgelegt.

Führen Sie den Befehl `host-data-source-record` aus, um die Aufzeichnung von Datenquellenmetriken in der Performance-Datenbank zu starten. Mit diesem Befehl wird `enabled` auf **`true`** festgelegt. Um aufzuhören, führe das aus `host-data-source-forget`. Mit diesem Befehl wird `enabled` auf **`false`** festgelegt.

host-data-source-record

```
xe host-data-source-record data-source=name_description_of_data_source
   [host-selectors=host_selector_value...]
<!--NeedCopy-->
```


Notieren Sie die angegebene Datenquelle für einen Host.

Bei diesem Vorgang werden die Informationen aus der Datenquelle in die Datenbank der persistenten Leistungsmetriken der angegebenen Hosts geschrieben. Aus Leistungsgründen unterscheidet sich diese Datenbank von der normalen Agentdatenbank.

Wählen Sie die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen Hosts ausgeführt.

host-data-source-forget

```
xe host-data-source-forget data-source=name_description_of_data_source
   [host-selectors=host_selector_value...]
<!--NeedCopy-->
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für einen Host und vergessen Sie alle aufgezeichneten Daten.

Wählen Sie die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen Hosts ausgeführt.

host-data-source-query

```
xe host-data-source-query data-source=name_description_of_data_source [
   host-selectors=host_selector_value...]
<!--NeedCopy-->
```

Zeigt die angegebene Datenquelle für einen Host an.

Wählen Sie die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten Host-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen Hosts ausgeführt.

Message-Befehle

Befehle zum Arbeiten mit Nachrichten. Nachrichten werden erstellt, um Benutzer über wichtige Ereignisse zu informieren, und werden in XenCenter als Warnungen angezeigt.

Die Meldungsobjekte können mit dem Standard-Objektauflistungsbefehl (`xe message-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

Message-Parameter

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die Nachricht	Lesezugriff
`name`	Der eindeutige Name der Nachricht	Lesezugriff
`priority`	Die Priorität der Nachricht. Höhere Zahlen bedeuten eine höhere Priorität	Lesezugriff
`class`	Die Nachrichtenklasse, zum Beispiel VM.	Lesezugriff
`obj-uuid`	Die UUID des betroffenen Objekts.	Lesezugriff
`timestamp`	Die Zeit, zu der die Nachricht generiert wurde.	Lesezugriff
`body`	Der Inhalt der Nachricht.	Lesezugriff

message-create

```
xe message-create name=message_name body=message_text [[host-uuid=
    uuid_of_host] | [sr-uuid=uuid_of_sr] | [vm-uuid=uuid_of_vm] | [pool-
    uuid=uuid_of_pool]]
<!--NeedCopy-->
```

Erstellt eine Nachricht.

message-destroy

```
xe message-destroy [uuid=message_uuid]
<!--NeedCopy-->
```

Zerstört eine vorhandene Nachricht. Sie können ein Skript erstellen, um alle Nachrichten zu vernichten. Beispiel:


```
# Dismiss all alerts   \
    IFS=","; for m in $(xe message-list params=uuid --minimal); do  \
    xe message-destroy uuid=$m  \
    done
<!--NeedCopy-->
```

Netzwerkbefehle

Befehle zum Arbeiten mit Netzwerken.

Die Netzwerkobjekte können mit dem Standardbefehl für die Objektauflistung (`xe network-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

Netzwerkparameter

Netzwerke haben folgende Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das Netzwerk	Lesezugriff
`name-label`	Der Name des Netzwerks	Lese-/Schreibrechte
`name-description`	Der Beschreibungstext des Netzwerks	Lese-/Schreibrechte
`VIF-uuids`	Eine Liste der eindeutigen Identifikatoren der VIFs (Virtual Network Interfaces), die von virtuellen Rechnern an dieses Netzwerk angehängt werden	Schreibgeschützter Parameter
`PIF-uuids`	Eine Liste der eindeutigen Bezeichner der PIFs (Physical Network Interfaces), die von XenServer-Hosts an dieses Netzwerk angehängt werden	Schreibgeschützter Parameter
`bridge`	Name der Bridge, die diesem Netzwerk auf dem lokalen XenServer-Host entspricht	Lesezugriff

Parametername	Beschreibung	Typ
default-locking-mode	Ein Netzwerkobjekt, das mit VIF-Objekten für die ARP-Filterung verwendet wird. Stellen Sie auf ein unlocked, um alle mit dem VIF verknüpften Filterregeln zu entfernen. Auf disabled eingestellt, damit das VIF den gesamten Datenverkehr verwirft.	Lese-/Schreibrechte
purpose	Eine Reihe von Zwecken, für die der XenServer-Host dieses Netzwerk verwendet. Stellen Sie ein nbd, um das Netzwerk zum Herstellen von NBD-Verbindungen zu verwenden.	Lese-/Schreibrechte
other-config: staticroutes	Kommagetrennte Liste formatierter *Subnetz-/Netzmasken-/Gateway*-Einträge, die die Gatewayadresse angeben, über die Subnetze weitergeleitet werden Wenn Sie beispielsweise other-config:**static**-routes auf 172.16.0.0/15/192.168.0.3,172.18.0.0/16/192.168.0.4 setzen, wird der Datenverkehr auf 172.16.0.0/15 über 192.168.0.3 und der Verkehr auf 172.18.0.0/16 über 192.168.0.4 geroutet.	Lese-/Schreibrechte
other-config: ethtoolautoneg	Auf Nein setzen, um die Autonegotiation der physikalischen Schnittstelle oder Bridge zu deaktivieren. Die Standardeinstellung ist ja.	Lese-/Schreibrechte

Parametername	Beschreibung	Typ
other-config:ethtool-rx	Auf “on”einstellen, um die Empfangsprüfsumme zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-tx	Auf “on”einstellen, um die Übertragungsprüfsumme zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-sg	Auf “on”einstellen, um Scatter Gather zu aktivieren, auf “off” zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-tso	Auf “on”einstellen, um die TCP-Segmentierungsoffload zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-ufo	Auf on setzen, um das Abladen von UDP-Fragmenten zu aktivieren, aus zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-gso	Auf “on”einstellen, um die generisches Segmentierungsoffload zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
blobs	Binärer Datenspeicher	Lesezugriff

network-create

```
xe network-create name-label=name_for_network [name-description=
    descriptive_text]
<!--NeedCopy-->
```

Erstellt ein Netzwerk.

network-destroy

```
xe network-destroy uuid=network_uuid
<!--NeedCopy-->
```


Zerstört ein vorhandenes Netzwerk.

SR-IOV-Befehle

Befehle für die Arbeit mit SR-IOV.

Die `network-sriov`-Objekte können mit dem Standardbefehl zur Objektauflistung (`xe network-sriov-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

SR-IOV-Parameter

SR-IOV hat die folgenden Parameter:

Parametername	Beschreibung	Typ
`physical-PIF`	Das PIF, um SR-IOV zu ermöglichen.	Lesezugriff
`logical-PIF`	Ein logisches SR-IOV-PIF. Benutzer können diesen Parameter verwenden, um ein SR-IOV-VLAN-Netzwerk zu erstellen.	Lesezugriff
`requires-reboot`	Wenn auf True gesetzt, wird der Host neu gestartet, um die SR-IOV-Aktivierung in Kraft zu setzen.	Lesezugriff
`remaining-capacity`	Anzahl der verbleibenden verfügbaren VFs.	Lesezugriff

`network-sriov-create`

```
xe network-sriov-create network-uuid=network_uuid pif-uuid=
   physical_pif_uuid
<!--NeedCopy-->
```

Erstellt ein SR-IOV-Netzwerkobjekt für ein bestimmtes physisches PIF und aktiviert SR-IOV auf dem physischen PIF.

network-sriov-destroy

```
xe network-sriov-destroy uuid=network_sriov_uuid
<!--NeedCopy-->
```

Entfernt ein Netzwerk-SR-IOV-Objekt und deaktiviert SR-IOV auf seinem physischen PIF.

Weisen Sie einen SR-IOV-VF zu

```
xe vif-create device=device_index mac=vf_mac_address network-uuid=
    sriov_network vm-uuid=vm_uuid
<!--NeedCopy-->
```

Weist einer VM einen VF aus einem SR-IOV-Netzwerk zu.

SDN-Controller-Befehle

Befehle zum Arbeiten mit dem SDN-Controller.

sdn-controller-forget

```
xe sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
    port=tcp_port]
<!--NeedCopy-->
```

Stellen Sie einen SDN-Controller vor.

sdn-controller-introduce

```
xe sdn-controller-forget uuid=uuid
<!--NeedCopy-->
```

Entfernen Sie einen SDN-Controller.

Tunnel-Befehle

Befehle zum Arbeiten mit Tunneln.

tunnel-create

```
xe tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
<!--NeedCopy-->
```

Erstellen Sie einen neuen Tunnel auf einem Host.

tunnel-destroy

```
xe tunnel-destroy uuid=uuid
<!--NeedCopy-->
```

Zerstöre einen Tunnel.

Patch-Befehle

Befehle zum Arbeiten mit Patches.

patch-apply

```
xe patch-apply uuid=patch_uuid host-uuid=host_uuid
<!--NeedCopy-->
```

Wendet den zuvor hochgeladenen Patch auf den angegebenen Host an.

patch-clean

```
xe patch-clean uuid=uuid
<!--NeedCopy-->
```

Löscht eine zuvor hochgeladene Patch-Datei.

patch-destroy

```
xe patch-destroy uuid=uuid
<!--NeedCopy-->
```

Entfernen Sie einen nicht angewendeten Patch-Datensatz und Dateien vom Host.

patch-pool-apply

```
xe patch-pool-apply uuid=uuid
<!--NeedCopy-->
```

Wenden Sie den zuvor hochgeladenen Patch auf alle Hosts im Pool an.

patch-pool-clean

```
xe patch-pool-clean uuid=uuid
<!--NeedCopy-->
```

Löschen Sie eine zuvor hochgeladene Patch-Datei auf allen Hosts im Pool.

patch-precheck

```
xe patch-precheck uuid=uuid host-uuid=host_uuid
<!--NeedCopy-->
```

Führen Sie die Vorprüfungen aus, die in dem zuvor auf den angegebenen Host hochgeladenen Patch enthalten sind

patch-upload

```
xe patch-upload file-name=file_name
<!--NeedCopy-->
```

Laden Sie eine Patch-Datei auf den Host hoch.

PBD-Befehle

Befehle zum Arbeiten mit PBDs (Physical Block Devices). PBDs sind die Softwareobjekte, über die der XenServer-Host auf Speicherrepositorien (SRs) zugreift.

Die PBD-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe pbd-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

PBD-Parameter

PBDs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die PBD.	Lesezugriff
sr-uuid	Das Speicherrepository, auf das die PBD verweist	Lesezugriff
device-config	Zusätzliche Konfigurationsinformationen, die dem SR-Backend-Treiber eines Hosts zur Verfügung gestellt werden	Schreibgeschützter Map-Parameter
currently-attached	True, wenn das SR an diesen Host angeschlossen ist, andernfalls False	Lesezugriff
host-uuid	UUID der physischen Maschine, auf der die PBD verfügbar ist	Lesezugriff
host	Das Host-Feld ist veraltet. Verwenden Sie stattdessen host_uuid.	Lesezugriff
other-config	Zusätzliche Informationen zur Konfiguration.	Map-Parameter lesen/schreiben

pbd-create

```
xe pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:
    key=corresponding_value]
<!--NeedCopy-->
```

Erstellen Sie eine PBD auf Ihrem XenServer-Host. Der schreibgeschützte Parameter device-config kann nur bei der Erstellung festgelegt werden.

Um eine Zuordnung von ‘path’zu ‘/tmp’hinzuzufügen, stellen Sie sicher, dass die Befehlszeile das Argument enthält device-config:path=/tmp

Eine vollständige Liste der unterstützten Schlüssel/Wert-Paare für Geräte-Konfiguration für jeden SR-Typ finden Sie unter Speicher.

pbd-destroy

```
xe pbd-destroy uuid=uuid_of_pbd
```



```
<!--NeedCopy-->
```

Zerstört die angegebene PBD.

pbd-plug

```
xe pbd-plug uuid=uuid_of_pbd
<!--NeedCopy-->
```

Versucht, die PBD an den XenServer-Host anzuschließen. Wenn dieser Befehl erfolgreich ist, werden die referenzierte SR (und die darin enthaltenen VDIs) für den XenServer-Host sichtbar.

pbd-unplug

```
xe pbd-unplug uuid=uuid_of_pbd
<!--NeedCopy-->
```

Versuchen Sie, die PBD vom XenServer-Host zu trennen.

PIF-Befehle

Befehle zum Arbeiten mit PIFs (Objekte, die die physikalischen Netzwerkschnittstellen darstellen).

Die PIF-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe pif-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

PIF-Parameter

PIFs haben folgende Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das PIF	Lesezugriff
`device machine-readable`	Name der Schnittstelle (z. B. eth0)	Lesezugriff
`MAC`	Die MAC-Adresse des PIF	Lesezugriff

Parametername	Beschreibung	Typ
other-config	Zusätzliche name:value-Paare für die PIF-Konfiguration.	Map-Parameter lesen/schreiben
physical	Wenn das stimmt, zeigt der PIF auf eine tatsächliche physische Netzwerkschnittstelle	Lesezugriff
currently-attached	Ist das PIF derzeit an diesem Host angeschlossen? **true** oder **false**	Lesezugriff
MTU	Maximale Übertragungseinheit des PIF in Byte.	Lesezugriff
VLAN	VLAN-Tag für den gesamten Datenverkehr, der über diese Schnittstelle fließt. -1 zeigt an, dass kein VLAN-Tag zugewiesen ist	Lesezugriff
bond-master-of	Die UUID der Bindung, für die dieser PIF die Hauptschnittstelle ist (falls vorhanden)	Lesezugriff
bond-slave-of	Die UUID des Bonds, zu der dieser PIF gehört (falls vorhanden)	Lesezugriff
management	Ist dieser PIF als Verwaltungsschnittstelle für die Steuerdomäne bezeichnet?	Lesezugriff
network-uuid	Die eindeutige Identifikator/Objektreferenz des virtuellen Netzwerks, an das dieser PIF angeschlossen ist	Lesezugriff
network-name-**label**	Der Name des virtuellen Netzwerks, mit dem dieser PIF verbunden ist	Lesezugriff
host-uuid	Die eindeutige Bezeichner/Objektreferenz des XenServer-Hosts, mit dem dieser PIF verbunden ist	Lesezugriff

Parametername	Beschreibung	Typ
host-name-**label**	Der Name des XenServer-Hosts, mit dem dieser PIF verbunden ist	Lesezugriff
IP-configuration-mode	Art der verwendeten Netzwerkadresskonfiguration; DHCP oder statisch	Lesezugriff
IP	Die IP-Adresse des PIF. Hier definiert, wenn der IP-Konfigurationsmodus statisch ist; undefiniert wenn DHCP	Lesezugriff
netmask	Netzmaske des PIF. Hier definiert, wenn der IP-Konfigurationsmodus statisch ist; undefiniert, wenn er von DHCP bereitgestellt wird	Lesezugriff
gateway	Gateway-Adresse des PIF. Hier definiert, wenn der IP-Konfigurationsmodus statisch ist; undefiniert, wenn er von DHCP bereitgestellt wird	Lesezugriff
DNS	DNS-Adresse des PIF. Hier definiert, wenn der IP-Konfigurationsmodus statisch ist; undefiniert, wenn er von DHCP bereitgestellt wird	Lesezugriff
io_read_kbs	Durchschnittliche Leserate in KB/s für das Gerät	Lesezugriff
io_write_kbs	Durchschnittliche Schreibrate in KB/s für das Gerät	Lesezugriff
carrier	Verbindungsstatus für dieses Gerät	Lesezugriff
vendor-id	Die dem Anbieter der NIC zugewiesene ID	Lesezugriff
vendor-name	Der Name des NIC-Anbieters	Lesezugriff
device-id	Die vom Hersteller diesem NIC-Modell zugewiesene ID	Lesezugriff

Parametername	Beschreibung	Typ
device-name	Der vom Hersteller diesem NIC-Modell zugewiesene Name	Lesezugriff
speed	Datenübertragungsrate der NIC	Lesezugriff
duplex	Duplexmodus der NIC; voll oder halb	Lesezugriff
pci-bus-path	PCI-Buspfad-Adresse	Lesezugriff
other-config: ethtoolspeed	Legt die Verbindungsgeschwindigkeit in Mbit/s fest	Lese-/Schreibrechte
other-config: ethtoolautoneg	Auf Nein setzen, um die Autonegotiation der physikalischen Schnittstelle oder Bridge zu deaktivieren. Die Standardeinstellung ist ja.	Lese-/Schreibrechte
other-config: ethtoolduplex	Legt die Duplexfähigkeit des PIF fest, entweder voll oder halb.	Lese-/Schreibrechte
other-config:ethtool-rx	Auf “on”einstellen, um die Empfangsprüfsumme zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-tx	Auf “on”einstellen, um die Übertragungsprüfsumme zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-sg	Auf “on”einstellen, um Scatter Gather zu aktivieren, auf “off” zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-tso	Auf “on”einstellen, um die TCP-Segmentierungsoffload zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:ethtool-ufo	Auf on setzen, um das Abladen von UDP-Fragmenten zu aktivieren, aus zum Deaktivieren	Lese-/Schreibrechte

Parametername	Beschreibung	Typ
other-config:ethtool-gso	Auf “on”einstellen, um die generisches Segmentierungsoffload zu aktivieren, auf “off”zum Deaktivieren	Lese-/Schreibrechte
other-config:domain	Kommagetrennte Liste zum Festlegen des DNS-Suchpfads	Lese-/Schreibrechte
other-config: bondmiimon	Intervall zwischen den Verbindungsüberprüfungen in Millisekunden	Lese-/Schreibrechte
other-config: bonddowndelay	Anzahl der Millisekunden, die gewartet werden müssen, nachdem der Link verloren gegangen ist, bevor der Link wirklich verschwunden ist. Dieser Parameter ermöglicht einen vorübergehenden Verbindungsverlust	Lese-/Schreibrechte
other-config: bondupdelay	Anzahl der Millisekunden, die nach dem Start des Links gewartet werden müssen, bevor er wirklich darüber nachgedacht wird. Ermöglicht das Hochklappen von Links. Die Standardeinstellung ist 31s, dass Switches Zeit haben, um den Datenverkehr weiterzuleiten.	Lese-/Schreibrechte
disallow-unplug	Wahr, wenn dieser PIF eine dedizierte Speicher-NIC ist, andernfalls false	Lese-/Schreibrechte

> **Hinweis:**
>
> Änderungen an den other-config-Feldern eines PIF werden erst nach einem Neustart wirksam. Verwenden Sie alternativ die Befehle xe pif-unplug und xe pif-plug, um die PIF-Konfiguration neu zu schreiben.

pif-forget

```
xe pif-forget uuid=uuid_of_pif
<!--NeedCopy-->
```

Zerstört das angegebene PIF-Objekt auf einem bestimmten Host.

pif-introduce

```
xe pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=
    interface_name
<!--NeedCopy-->
```

Erstellen Sie ein PIF-Objekt, das eine physische Schnittstelle auf dem angegebenen XenServer-Host darstellt.

pif-plug

```
xe pif-plug uuid=uuid_of_pif
<!--NeedCopy-->
```

Versuch, die angegebene physikalische Schnittstelle hochzufahren.

pif-reconfigure-ip

```
xe pif-reconfigure-ip uuid=uuid_of_pif [mode=dhcp|mode=static] gateway=
    network_gateway_address IP=static_ip_for_this_pif netmask=
    netmask_for_this_pif [DNS=dns_address]
<!--NeedCopy-->
```

Ändern Sie die IP-Adresse des PIF. Bei einer statischen IP-Konfiguration legen Sie den Parameter `mode` auf **`static`**, und die Parameter `gateway`, `IP` und `netmask` auf die entsprechenden Werte fest. Um DHCP zu verwenden, setzen Sie den Parameter `mode` auf `DHCP` und lassen Sie die statischen Parameter undefiniert.

> **Hinweis:**
>
> Die Verwendung statischer IP-Adressen auf physischen Netzwerkschnittstellen, die über das Spanning Tree Protocol mit ausgeschaltetem (oder nicht unterstütztem) STP Fast Link an einen Port eines Switches angeschlossen sind, führt zu einem Zeitraum, in dem kein Datenverkehr stattfindet.

pif-reconfigure-ipv6

```
xe pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode [gateway=
    network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=
    dns_address]
<!--NeedCopy-->
```

Konfigurieren Sie die IPv6-Adresseinstellungen auf einem PIF neu.

pif-scan

```
xe pif-scan host-uuid=host_uuid
<!--NeedCopy-->
```

Suchen Sie auf Ihrem XenServer-Host nach neuen physischen Schnittstellen.

pif-set-primary-address-type

```
xe pif-set-primary-address-type  uuid=uuid primary_address_type=
    address_type
<!--NeedCopy-->
```

Ändern Sie den von diesem PIF verwendeten primären Adresstyp.

pif-unplug

```
xe pif-unplug uuid=uuid_of_pif
<!--NeedCopy-->
```

Versuch, die angegebene physikalische Schnittstelle herunterzufahren.

Pool-Befehle

Befehle zum Arbeiten mit Pools. Ein *Pool* ist ein Aggregat aus einem oder mehreren XenServer-Hosts. Ein Pool verwendet ein oder mehrere gemeinsam genutzte Speicherrepositories, sodass die VMs, die auf einem Host im Pool ausgeführt werden, nahezu in Echtzeit zu einem anderen Host im Pool migriert werden können. Diese Migration findet statt, während die VM noch läuft, ohne dass sie heruntergefahren und wieder hochgefahren werden muss.

Jeder XenServer-Host ist in Wirklichkeit ein Pool, der standardmäßig aus einem einzigen Mitglied besteht. Wenn Ihr XenServer-Host einem Pool hinzugefügt wird, wird er als Mitglied bezeichnet. Wenn der Pool, dem der Host angehört, aus einem einzigen Mitglied besteht, wird dieses Mitglied

zum Poolkoordinator. Wenn der Pool, zu dem der Host gehört, bereits mehrere Mitglieder hat, ist eines dieser Mitglieder bereits der Poolkoordinator und bleibt es auch, wenn der neue Host dem Pool beitritt.

Das Singleton-Pool-Objekt kann mit dem Standard-Objektauflistungsbefehl (`xe pool-list`) aufgelistet werden. Seine Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

Pool-Parameter

Pools haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den Pool	Lesezugriff
`name-label`	Der Name des Pools	Lese-/Schreibrechte
`name-description`	Die Beschreibungszeichenfolge des Pools	Lese-/Schreibrechte
`master`	Die eindeutige Bezeichner/Objektreferenz des XenServer-Hosts, der als Poolkoordinator bestimmt ist	Lesezugriff
`default-SR`	Die eindeutige Bezeichner/Objektreferenz des Standard-SRs für den Pool	Lese-/Schreibrechte
`crash-dump-SR`	Die eindeutige Bezeichner/Objektreferenz des SRs, in dem alle Absturzabbilder für Poolmitglieder gespeichert werden	Lese-/Schreibrechte
`metadata-vdis`	Alle bekannten Metadaten-VDIs für den Pool	Lesezugriff
`suspend-image-SR`	Die eindeutige Bezeichner/Objektreferenz des SRs, in dem angehaltene VMs auf Poolmitgliedern gespeichert werden	Lese-/Schreibrechte

Parametername	Beschreibung	Typ
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Pool angeben	Map-Parameter lesen/schreiben
supported-sr-types	SR-Typen, die dieser Pool verwenden kann	Lesezugriff
ha-enabled	Wahr, wenn HA für den Pool aktiviert ist, false sonst	Lesezugriff
ha-configuration	Reserviert für zukünftige Verwendung.	Lesezugriff
ha-statefiles	Listet die UUIDs der VDIs auf, die von HA zur Bestimmung des Speicherzustands verwendet	Lesezugriff
ha-host-failures-to-tolerate	Die Anzahl der vor dem Senden einer Systemwarnung zu tolerierenden Host-Ausfälle	Lese-/Schreibrechte
ha-plan-exists-**for**	Die Anzahl der Hosts-Ausfälle, die gemäß den Berechnungen des HA-Algorithmus tatsächlich behandelt werden können	Lesezugriff
ha-allow-overcommit	Wahr, wenn der Pool überstimmt werden darf, andernfalls False	Lese-/Schreibrechte
ha-overcommitted	True, wenn der Pool überlastet ist	Lesezugriff
blobs	Binärer Datenspeicher	Lesezugriff
live-patching-disabled	Auf False setzen, um Live-Patching zu ermöglichen. Auf True setzen, um das Live-Patching zu deaktivieren.	Lese-/Schreibrechte
igmp-snooping-enabled	Auf True setzen, um IGMP-Snooping zu ermöglichen. Auf False setzen, um IGMP-Snooping zu deaktivieren.	Lese-/Schreibrechte

Parametername	Beschreibung	Typ
`https-only`	Auf False setzen, damit externe Clients, die die Management-API verwenden, entweder über HTTPS über Port 443 oder HTTP über Port 80 eine Verbindung zu XenServer herstellen können. Auf True setzen, um Port 80 zu blockieren und zu verlangen, dass Clients ausschließlich über HTTPS über Port 443 eine Verbindung herstellen.	Lese-/Schreibrechte
`migration-compression`	Auf True setzen, um die Komprimierung des Migrationsstreams für Ihren XenServer-Pool zu aktivieren. Auf False setzen, um die Komprimierung des Migrationsdatenstroms zu deaktivieren. Die Standardeinstellung ist False. Kann durch den Parameter `compress` des Befehls `vm-migrate` überschrieben werden.	Lese-/Schreibrechte

pool-apply-edition

```
xe pool-apply-edition edition=edition [uuid=uuid] [license-server-
    address=address] [license-server-port=port]
<!--NeedCopy-->
```

Wenden Sie eine Ausgabe im gesamten Pool an.

pool-certificate-install

```
xe pool-certificate-install filename=file_name
<!--NeedCopy-->
```


Installieren Sie ein TLS-Zertifikat, poolweit.

pool-certificate-list

```
xe pool-certificate-list
<!--NeedCopy-->
```

Listet alle installierten TLS-Zertifikate in einem Pool auf.

pool-certificate-sync

```
xe pool-certificate-sync
<!--NeedCopy-->
```

Synchronisieren Sie TLS-Zertifikate und Zertifikatssperrlisten vom Poolkoordinator mit den anderen Poolmitgliedern.

pool-certificate-uninstall

```
xe pool-certificate-uninstall name=name
<!--NeedCopy-->
```

Deinstalliert ein TLS-Zertifikat.

pool-crl-install

```
xe pool-crl-install filename=file_name
<!--NeedCopy-->
```

Installieren Sie eine TLS-Zertifikatssperrliste, poolweit.

pool-crl-list

```
xe pool-crl-list
<!--NeedCopy-->
```

Listet alle installierten TLS-Zertifikatssperrlisten auf.

pool-crl-uninstall


```
xe pool-crl-uninstall name=name
<!--NeedCopy-->
```

Deinstalliert eine TLS-Zertifikatssperrliste.

pool-deconfigure-wlb

```
xe pool-deconfigure-wlb
<!--NeedCopy-->
```

Entfernen Sie die Konfiguration für den Workloadausgleich dauerhaft.

pool-designate-new-master

```
xe pool-designate-new-master host-uuid=uuid_of_new_master
<!--NeedCopy-->
```

Weisen Sie den angegebenen XenServer-Mitgliedshost an, der Koordinator (früher "Master"genannt) eines vorhandenen Pools zu werden. Dieser Befehl führt eine geordnete Übergabe der Rolle des Poolkoordinators an einen anderen Host im Ressourcenpool durch. Dieser Befehl funktioniert nur, wenn der aktuelle Poolkoordinator online ist. Es ist kein Ersatz für die unten aufgeführten Befehle im Notfallmodus.

pool-disable-external-auth

```
xe pool-disable-external-auth [uuid=uuid] [config=config]
<!--NeedCopy-->
```

Deaktiviert die externe Authentifizierung bei allen Hosts in einem Pool.

pool-disable-local-storage-caching

```
xe pool-disable-local-storage-caching uuid=uuid
<!--NeedCopy-->
```

Deaktivieren Sie das lokale Speicher-Caching im gesamten Pool.

pool-disable-redo-log

```
xe pool-disable-redo-log
<!--NeedCopy-->
```


Deaktivieren Sie das Redo-Protokoll, falls es verwendet wird, sofern HA nicht aktiviert ist.

pool-dump-database

```
xe pool-dump-database file-name=filename_to_dump_database_into_(
   on_client)
<!--NeedCopy-->
```

Laden Sie eine Kopie der gesamten Pooldatenbank herunter und speichern Sie sie in einer Datei auf dem Client.

pool-enable-external-auth

```
xe pool-enable-external-auth  auth-type=auth_type service-name=
   service_name [uuid=uuid] [config:=config]
<!--NeedCopy-->
```

Ermöglicht die externe Authentifizierung bei allen Hosts in einem Pool. Beachten Sie, dass für einige Werte von `auth-type` bestimmte `config:`-Werte erforderlich sind.

pool-enable-local-storage-caching

```
xe pool-enable-local-storage-caching uuid=uuid
<!--NeedCopy-->
```

Aktivieren Sie das lokale Speicher-Caching im gesamten Pool.

pool-enable-redo-log

```
xe pool-ensable-redo-log sr-uuid=sr_uuid
<!--NeedCopy-->
```

Aktiviert das Redo-Protokoll auf dem angegebenen SR, falls es verwendet wird, sofern HA nicht aktiviert ist.

pool-eject

```
xe pool-eject host-uuid=uuid_of_host_to_eject
<!--NeedCopy-->
```

Weisen Sie den angegebenen XenServer-Host an, einen vorhandenen Pool zu verlassen.

pool-emergency-reset-master

```
xe pool-emergency-reset-master master-address=address_of_pool_master
<!--NeedCopy-->
```

Weisen Sie einen Poolmitgliedshost an, seine Poolkoordinator-Adresse auf den neuen Wert zurückzusetzen und zu versuchen, eine Verbindung zu diesem herzustellen. Führen Sie diesen Befehl nicht auf Poolkoordinatoren aus.

pool-emergency-transition-to-master

```
xe pool-emergency-transition-to-master
<!--NeedCopy-->
```

Weisen Sie einen XenServer-Mitgliedshost an, der Poolkoordinator zu werden (früher "Poolmaster" genannt). Der XenServer-Host akzeptiert diesen Befehl erst, nachdem der Host in den Notfallmodus übergegangen ist. Notfallmodus bedeutet, dass es sich um ein Mitglied eines Pools handelt, dessen Koordinator aus dem Netzwerk verschwunden ist und nach einer gewissen Anzahl von Wiederholungen nicht mehr kontaktiert werden kann.

Wenn das Host-Kennwort geändert wurde, seit der Host dem Pool beigetreten ist, kann dieser Befehl dazu führen, dass das Kennwort des Hosts zurückgesetzt wird. Weitere Informationen finden Sie unter (Benutzerbefehle).

pool-ha-enable

```
xe pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
<!--NeedCopy-->
```

Aktivieren Sie Hochverfügbarkeit im Ressourcenpool, indem Sie die angegebene SR-UUID als zentrales Speicher-Heartbeat-Repository verwenden.

pool-ha-disable

```
xe pool-ha-disable
<!--NeedCopy-->
```

Deaktiviert die Hochverfügbarkeitsfunktion im Ressourcenpool.

pool-ha-compute-hypothetical-max-host-failures-to-tolerate

Berechnet die maximale Anzahl von Host-Ausfällen, die in der aktuellen Pool-Konfiguration toleriert werden sollen.

pool-ha-compute-max-host-failures-to-tolerate

```
1 xe pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=
     vm_uuid] [restart-priority=restart_priority]
2 <!--NeedCopy-->
```

Berechnen Sie die maximale Anzahl von zu tolerierenden Hostausfällen mit den bereitgestellten, vorgeschlagenen geschützten VMs.

pool-initialize-wlb

```
1 xe pool-initialize-wlb wlb_url=url wlb_username=wlb_username
     wlb_password=wlb_password xenserver_username=username
     xenserver_password=password
2 <!--NeedCopy-->
```

Initialisieren Sie den Workloadausgleich für den aktuellen Pool mit dem Workload Balancing-Zielserver.

pool-join

```
1 xe pool-join master-address=address master-username=username master-
     password=password
2 <!--NeedCopy-->
```

Weisen Sie Ihren XenServer-Host an, einem vorhandenen Pool beizutreten.

pool-management-reconfigure

```
1 xe pool-management-reconfigure [network-uuid=network-uuid]
2 <!--NeedCopy-->
```

Konfiguriert die Verwaltungsschnittstelle aller Hosts im Pool neu, um die angegebene Netzwerkschnittstelle zu verwenden, die für die Verbindung mit dem XenCenter verwendet wird. Der Befehl schreibt den Schlüssel MANAGEMENT_INTERFACE in `/etc/xensource-inventory` für alle Hosts im Pool um.

Wenn der Gerätename einer Schnittstelle (die eine IP-Adresse haben muss) angegeben wird, bindet der XenServer-Poolkoordinator sofort neu. Dieser Befehl funktioniert sowohl im Normal- als auch im Notfallmodus.

Aus der angegebenen Netzwerk-UUID wird die UUID des PIF-Objekts identifiziert und dem XenServer-Host zugeordnet, der bestimmt, welche IP-Adresse an sich selbst neu gebunden werden soll. Es darf sich nicht im Notfallmodus befinden, wenn dieser Befehl ausgeführt wird.

> **Warnung:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden, und stellen Sie sicher, dass die neue Schnittstelle über Netzwerkkonnektivität verfügt. Verwenden Sie `xe pif-reconfigure` zum Einrichten. Andernfalls können nachfolgende CLI-Befehle den XenServer-Host nicht erreichen.

pool-recover-slaves

```
xe pool-recover-slaves
<!--NeedCopy-->
```

Weisen Sie den Poolkoordinator an, zu versuchen, die Adresse aller Mitglieder zurückzusetzen, die sich derzeit im Notfallmodus befinden. Dieser Befehl wird normalerweise verwendet, nachdem `pool-emergency-transition-to-master` verwendet wurde, um eines der Mitglieder als neuen Poolkoordinator festzulegen.

pool-restore-database

```
xe pool-restore-database file-name=filename_to_restore_from_on_client [
   dry-run=true|false]
<!--NeedCopy-->
```

Laden Sie ein Datenbankbackup (erstellt mit `pool-dump-database`) in einen Pool hoch. Nach Erhalt des Uploads startet sich der Poolkoordinator selbst mit der neuen Datenbank neu.

Es gibt auch eine *Testlaufoption*, mit der Sie überprüfen können, ob die Pooldatenbank wiederhergestellt werden kann, ohne den Vorgang tatsächlich auszuführen. Standardmäßig ist `dry-run` auf “false”festgelegt.

pool-retrieve-wlb-configuration

```
xe pool-retrieve-wlb-configuration
<!--NeedCopy-->
```

Ruft die Pool-Optimierungskriterien vom Workload Balancing-Server ab.

pool-retrieve-wlb-diagnostics

```
xe pool-retrieve-wlb-diagnostics [filename=file_name]
<!--NeedCopy-->
```

Ruft Diagnosen vom Workload Balancing-Server ab.

pool-retrieve-wlb-recommendations

```
xe pool-retrieve-wlb-recommendations
<!--NeedCopy-->
```

Ruft VM-Migrationsempfehlungen für den Pool vom Workload Balancing-Server ab.

pool-retrieve-wlb-report

```
xe pool-retrieve-wlb-report report=report [filename=file_name]
<!--NeedCopy-->
```

Ruft Berichte vom Workload Balancing-Server ab.

pool-secret-rotate

```
xe pool-secret-rotate
<!--NeedCopy-->
```

Rotieren Sie das Poolgeheimnis.

Das Poolgeheimnis ist ein Geheimnis, das von den XenServer-Hosts in einem Pool gemeinsam genutzt wird und es dem Host ermöglicht, seine Mitgliedschaft in einem Pool nachzuweisen. Benutzer mit der Pool-Admin-Rolle können dieses Geheimnis einsehen, wenn sie sich über SSH mit dem Host verbinden. Rotieren Sie das Poolgeheimnis, wenn einer dieser Benutzer Ihre Organisation verlässt oder seine Pooladministratorrolle verliert.

pool-send-test-post

```
xe pool-send-test-post dest-host=destination_host dest-port=
   destination_port body=post_body
<!--NeedCopy-->
```

Senden Sie den angegebenen Text mithilfe von HTTPS an den angegebenen Host und Port und drucken Sie die Antwort aus. Dies wird für das Debuggen der TLS-Schicht verwendet.

pool-send-wlb-configuration

```
xe pool-send-wlb-configuration [config:=config]
<!--NeedCopy-->
```

Legt die Pool-Optimierungskriterien für den Workload Balancing-Server fest.

pool-sync-database

```
xe pool-sync-database
<!--NeedCopy-->
```

Erzwingt die Synchronisierung der Pooldatenbank über alle Hosts im Ressourcenpool. Dieser Befehl ist im normalen Betrieb nicht erforderlich, da die Datenbank regelmäßig automatisch repliziert wird. Der Befehl kann jedoch nützlich sein, um sicherzustellen, dass Änderungen schnell repliziert werden, nachdem ein erheblicher Satz von CLI-Operationen ausgeführt wurde.

Legen Sie https-only fest

```
xe pool-param-set [uuid=pool-uuid] [https-only=true|false]
<!--NeedCopy-->
```

Aktiviert oder deaktiviert die Blockierung von Port 80 auf der Verwaltungsschnittstelle von XenServer-Hosts.

PVS Accelerator-Befehle

Befehle zum Arbeiten mit dem PVS-Beschleuniger.

pvs-cache-storage-create

```
xe pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid
    size=size
<!--NeedCopy-->
```

Konfigurieren Sie einen PVS-Cache auf einem bestimmten SR für einen bestimmten Host.

pvs-cache-storage-destroy

```
xe pvs-cache-storage-destroy uuid=uuid
<!--NeedCopy-->
```


Entferne einen PVS-Cache.

pvs-proxy-create

```
xe pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
<!--NeedCopy-->
```

Konfigurieren Sie eine VM/VIF für die Verwendung eines PVS-Proxys.

pvs-proxy-destroy

```
xe pvs-proxy-destroy uuid=uuid
<!--NeedCopy-->
```

Entfernen (oder schalten) Sie einen PVS-Proxy für diese VIF/VM aus.

pvs-server-forget

```
xe pvs-server-forget uuid=uuid
<!--NeedCopy-->
```

Vergessen Sie einen PVS-Server.

pvs-server-introduce

```
xe pvs-server-introduce addresses=adresses first-port=first_port last-
    port=last_port pvs-site-uuid=pvs_site_uuid
<!--NeedCopy-->
```

Einführung eines neuen PVS-Servers.

pvs-site-forget

```
xe pvs-site-forget uuid=uuid
<!--NeedCopy-->
```

Vergiss eine PVS-Site.

pvs-site-introduce


```
xe pvs-site-introduce name-label=name_label [name-description=
    name_description] [pvs-uuid=pvs_uuid]
<!--NeedCopy-->
```

Einführung einer neuen PVS-Site.

Storage Manager-Befehle

Befehle zum Steuern von Storage Manager-Plug-ins.

Die Storage-Manager-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe sm-list`) aufgelistet werden. Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

SM-Parameter

SMs haben folgende Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das SM-Plug-In	Lesezugriff
`name-label`	Der Name des SM-Plug-ins	Lesezugriff
`name-description`	Die Beschreibungszeichenfolge des SM-Plug-ins	Lesezugriff
`type`	Der SR-Typ, an den dieses Plug-In angeschlossen wird	Lesezugriff
`vendor`	Name des Anbieters, der dieses Plug-in erstellt hat	Lesezugriff
`copyright`	Copyright-Erklärung für dieses SM-Plug-In	Lesezugriff
`required-api-version`	Minimale SM-API-Version auf dem XenServer-Host erforderlich	Lesezugriff
`configuration`	Namen und Beschreibungen der Gerätekonfigurationsschlüssel	Lesezugriff
`capabilities`	Funktionen des SM-Plug-ins	Lesezugriff

Parametername	Beschreibung	Typ
driver-filename	Der Dateiname des SR-Treibers.	Lesezugriff

Snapshot-Befehle

Befehle zum Arbeiten mit Schnappschüssen.

snapshot-clone

```
xe snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-
    description=description]
<!--NeedCopy-->
```

Erstellen Sie eine neue Vorlage, indem Sie einen vorhandenen Snapshot klonen und, sofern verfügbar, einen schnellen Datenträgerklonvorgang auf Speicherebene verwenden.

snapshot-copy

```
xe snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-
    description=name_description] [sr-uuid=sr_uuid]
<!--NeedCopy-->
```

Erstellen Sie eine neue Vorlage, indem Sie eine vorhandene VM kopieren, ohne jedoch den schnellen Datenträgerklonvorgang auf Speicherebene zu verwenden (auch wenn diese verfügbar ist). Die Disk-Images der kopierten VM sind garantiert "vollständige Images"- also nicht Teil einer CoW-Kette.

snapshot-destroy

```
xe snapshot-destroy  [uuid=uuid] [snapshot-uuid=snapshot_uuid]
<!--NeedCopy-->
```

Zerstöre einen Schnappschuss. Dadurch bleibt der mit dem Snapshot verknüpfte Speicher intakt. Um auch Speicher zu löschen, verwenden Sie die Snapshot-Deinstallation.

snapshot-disk-list

```
xe snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-
    params=vbd_params] [vdi-params=vdi_params]
<!--NeedCopy-->
```


Listet die Datenträger der ausgewählten VM(s) auf.

snapshot-export-to-template

```
xe snapshot-export-to-template filename=file_name snapshot-uuid=
   snapshot_uuid  [preserve-power-state=true|false]
<!--NeedCopy-->
```

Exportiert einen Snapshot in den *Dateinamen*.

snapshot-reset-powerstate

```
xe snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid]
   [--force]
<!--NeedCopy-->
```

Erzwingt das Anhalten des VM-Energiezustands nur in der Datenbank des Management-Toolstack. Dieser Befehl wird verwendet, um einen Snapshot wiederherzustellen, der als "angehalten"markiert ist. Dies ist ein potenziell gefährlicher Vorgang: Sie müssen sicherstellen, dass Sie das Speicherimage nicht mehr benötigen. Sie können Ihren Snapshot nicht mehr fortsetzen.

snapshot-revert

```
xe snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
<!--NeedCopy-->
```

Setzt eine vorhandene VM in einen früheren Checkpoint- oder Snapshot-Zustand zurück.

snapshot-uninstall

```
xe snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--
   force]
<!--NeedCopy-->
```

Deinstalliert einen Schnappschuss Durch diesen Vorgang werden die VDIs zerstört, die als RW gekennzeichnet sind und nur mit diesem Snapshot verbunden sind. Um den VM-Datensatz einfach zu löschen, verwenden Sie Snapshot-Zerstören.

SR-Befehle

Befehle zur Steuerung von SRs (Speicherrepositories).

Die SR-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe sr-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

SR-Parameter

SRs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Identifikator/Objektreferenz für das SR	Lesezugriff
`name-label`	Der Name des SRs	Lese-/Schreibrechte
`name-description`	Die Beschreibungszeichenfolge des SRs	Lese-/Schreibrechte
`host`	Der Host-Name des Speicherrepository	Lesezugriff
`allowed-operations`	Liste der auf dem SR in diesem Status zulässigen Vorgänge	Schreibgeschützter Parameter
`current-operations`	Liste der Vorgänge, die derzeit auf diesem SR ausgeführt werden	Schreibgeschützter Parameter
`VDIs`	Eindeutige Bezeichner/Objektreferenz für die virtuellen Datenträger in diesem SR	Schreibgeschützter Parameter
`PBDs`	Eindeutige Identifikator/Objektreferenz für die an dieses SR angeschlossenen PBDs	Schreibgeschützter Parameter
`virtual-allocation`	Summe der Werte virtueller Größe aller VDIs in diesem Speicherrepository (in Byte)	Lesezugriff

Parametername	Beschreibung	Typ
physical-utilisation	Derzeit auf diesem SR genutzter physischer Speicherplatz in Byte. Bei Datenträgerformaten mit Thin-Provisioning ist die physische Auslastung möglicherweise geringer als die virtuelle Zuweisung	Lesezugriff
physical-size	Physische Gesamtgröße des SRs in Byte	Lesezugriff
type	Typ des SR, der zur Angabe des zu verwendenden SR-Back-End-Treibers verwendet wird	Lesezugriff
content-type	Die Art des Inhalts des SRs. Wird verwendet, um ISO-Libraries von anderen SRs zu unterscheiden. Für Speicher-Repositorys, die eine Bibliothek von ISOs speichern, muss content-type auf iso gesetzt werden. In anderen Fällen empfehlen wir, diesen Parameter entweder auf leer oder auf den Zeichenfolgenbenutzer festzulegen.	Lesezugriff
shared	Stimmt, wenn diese SR von mehreren Hosts gemeinsam genutzt werden kann. Sonst falsch.	Lese-/Schreibrechte
introduced-by	drtask (falls vorhanden), das das SR einführte	Lesezugriff
is-tools-sr	Stimmt, wenn dies die SR ist, die die Tools-ISO-VDIs enthält. Sonst falsch.	Lesezugriff

Parametername	Beschreibung	Typ
other-config	Liste der Schlüssel/Wert-Paare, die zusätzliche Konfigurationsparameter für das SR angeben	Map-Parameter lesen/schreiben
sm-config	SM-abhängige Daten	Schreibgeschützter Map-Parameter
blobs	Binärer Datenspeicher	Lesezugriff
local-cache-enabled	Wahr, wenn dieser SR als lokaler Cache für seinen Host zugewiesen ist. Sonst falsch.	Lesezugriff
tags	Benutzerspezifische Tags für Kategorisierungszwecke	Set-Parameter lesen/schreiben
clustered	Stimmt, die SR verwendet aggregierten lokalen Speicher. Sonst falsch.	Lesezugriff

sr-create

```
xe sr-create name-label=name physical-size=size type=type content-type=
    content_type device-config:config_name=value [host-uuid=host_uuid] [
    shared=true|false]
<!--NeedCopy-->
```

Erstellt eine SR auf dem Datenträger, führt sie in die Datenbank ein und erstellt eine PBD, die die SR an den XenServer-Host anhängt. Wenn auf gesetzt shared ist **true**, wird für jeden XenServer-Host im Pool eine PBD erstellt. Wenn nicht angegeben oder auf gesetzt shared ist **false**, wird eine PBD nur für den mit angegebenen XenServer-Host erstellt. host-uuid

Die genauen Parameter device-config unterscheiden sich je nach type für das Gerät. Einzelheiten zu diesen Parametern in den verschiedenen Speicher-Back-Ends finden Sie unter SR erstellen.

sr-data-source-forget

```
xe sr-data-source-forget data-source=data_source
<!--NeedCopy-->
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für ein SR und vergessen Sie alle aufgezeichneten Daten.

sr-data-source-list

```
xe sr-data-source-list
<!--NeedCopy-->
```

Listen Sie die Datenquellen auf, die für ein SR aufgezeichnet werden können.

sr-data-source-query

```
xe sr-data-source-query data-source=data_source
<!--NeedCopy-->
```

Fragen Sie den zuletzt aus einer SR-Datenquelle gelesenen Wert ab.

sr-data-source-record

```
xe sr-data-source-record  data-source=data_source
<!--NeedCopy-->
```

Notieren Sie die angegebene Datenquelle für ein SR.

sr-destroy

```
xe sr-destroy uuid=sr_uuid
<!--NeedCopy-->
```

Zerstört die angegebene SR auf dem XenServer-Host.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Ermöglicht die XAPI-Datenbankreplikation auf das angegebene (gemeinsame) SR.

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
<!--NeedCopy-->
```

Deaktiviert die XAPI-Datenbankreplikation auf das angegebene SR.

sr-forget

```
xe sr-forget uuid=sr_uuid
<!--NeedCopy-->
```

Der XAPI-Agent vergisst eine angegebene SR auf dem XenServer-Host. Wenn der XAPI-Agent ein SR vergisst, wird das SR getrennt und Sie können nicht auf VDIs darauf zugreifen, aber es bleibt auf dem Quellmedium intakt (die Daten gehen nicht verloren).

sr-introduce

```
xe sr-introduce name-label=name physical-size=physical_size type=type
    content-type=content_type uuid=sr_uuid
<!--NeedCopy-->
```

Platziert einfach einen SR-Datensatz in die Datenbank. Verwenden Sie `device-config`, um zusätzliche Parameter im Format `device-config:parameter_key=parameter_value` anzugeben, zum Beispiel:

```
xe sr-introduce device-config:device=/dev/sdb1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Dieser Befehl wird niemals im Normalbetrieb verwendet. Dieser erweiterte Vorgang kann nützlich sein, wenn ein SR nach seiner Erstellung als freigegeben neu konfiguriert werden muss oder um die Wiederherstellung nach verschiedenen Ausfallszenarien zu unterstützen.

sr-probe

```
xe sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=
    value]
<!--NeedCopy-->
```

Führt einen Scan des Back-End mit den bereitgestellten `device-config`-Schlüsseln durch. Wenn `device-config` für das SR-Backend abgeschlossen ist, gibt dieser Befehl eine Liste der SRs zurück, die auf dem Gerät vorhanden sind, falls vorhanden. Wenn die Parameter `device-config` nur teilweise sind, wird ein Back-End-spezifischer Scan durchgeführt, der Ergebnisse liefert, die Sie bei der Verbesserung der verbleibenden Parameter `device-config` anleiten. Die Scanergebnisse werden als XML-spezifisch für das Backend zurückgegeben und auf der CLI gedruckt.

Die genauen Parameter `device-config` unterscheiden sich je nach `type` für das Gerät. Einzelheiten zu diesen Parametern in den verschiedenen Speicher-Backends finden Sie unter Speicher.

sr-probe-ext

```
xe sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config]
     [sm-config:-sm_config]
<!--NeedCopy-->
```

Führen Sie eine Speichersonde durch. Die Gerätekonfigurationsparameter können beispielsweise durch device-config:devs=/dev/sdb1 angegeben werden. Im Gegensatz zu sr-probe gibt dieser Befehl Ergebnisse in demselben menschenlesbaren Format für jeden SR-Typ zurück.

sr-scan

```
xe sr-scan uuid=sr_uuid
<!--NeedCopy-->
```

Erzwingt einen SR-Scan und synchronisiert die XAPI-Datenbank mit VDIs, die im zugrunde liegenden Speichersubstrat vorhanden sind.

sr-update

```
xe sr-update uuid=uuid
<!--NeedCopy-->
```

Aktualisieren Sie die Felder des SR-Objekts in der Datenbank.

lvhd-enable-thin-provisioning

```
xe lvhd-enable-thin-provisioning  sr-uuid=sr_uuid initial-allocation=
   initial_allocation allocation-quantum=allocation_quantum
<!--NeedCopy-->
```

Ermöglichen Sie Thin-Provisioning auf einem LVHD-SR.

Subject-Befehle

Befehle zum Arbeiten mit Themen.

session-subject-identifier-list

```
xe session-subject-identifier-list
<!--NeedCopy-->
```


Gibt eine Liste aller Benutzersubjekt-IDs aller extern authentifizierten vorhandenen Sitzungen zurück.

session-subject-identifier-logout

```
xe session-subject-identifier-logout subject-identifier=
   subject_identifier
<!--NeedCopy-->
```

Melden Sie alle extern authentifizierten Sitzungen ab, die mit einer Benutzersubjekt-ID verknüpft sind.

session-subject-identifier-logout-all

```
xe session-subject-identifier-logout-all
<!--NeedCopy-->
```

Melden Sie alle extern authentifizierten Sitzungen ab.

subject-add

```
xe subject-add subject-name=subject_name
<!--NeedCopy-->
```

Fügen Sie der Liste der Themen, die auf den Pool zugreifen können, einen Betreff hinzu.

subject-remove

```
xe subject-remove subject-uuid=subject_uuid
<!--NeedCopy-->
```

Entfernt einen Betreff aus der Liste der Themen, die auf den Pool zugreifen können.

subject-role-add

```
xe subject-role-add uuid=uuid [role-name=role_name] [role-uuid=
   role_uuid]
<!--NeedCopy-->
```

Fügt einem Betreff eine Rolle hinzu.

subject-role-remove

```
xe subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
    role_uuid]
<!--NeedCopy-->
```

Entfernt eine Rolle aus einem Betreff.

secret-create

```
xe secret-create value=value
<!--NeedCopy-->
```

Erstelle ein Geheimnis.

secret-destroy

```
xe secret-destroy uuid=uuid
<!--NeedCopy-->
```

Zerstöre ein Geheimnis.

Task-Befehle

Befehle zum Arbeiten mit langwierigen asynchronen Aufgaben. Bei diesen Befehlen handelt es sich um Aufgaben wie das Starten, Stoppen und Anhalten einer virtuellen Maschine. Die Aufgaben bestehen normalerweise aus einer Reihe anderer atomarer Unteraufgaben, die zusammen den angeforderten Vorgang ausführen.

Die Aufgabenobjekte können mit dem Standardbefehl für die Objektauflistung (`xe task-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

Parameter der Aufgabe

Aufgaben haben folgende Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die Aufgabe	Lesezugriff
name-**label**	Der Name der Aufgabe	Lesezugriff
name-description	Die Beschreibungszeichenfolge der Aufgabe	Lesezugriff
resident-on	Die eindeutige Bezeichner/Objektreferenz des Hosts, auf dem die Aufgabe ausgeführt wird	Lesezugriff
status	Status der Aufgabe	Lesezugriff
progress	Wenn die Aufgabe noch aussteht, enthält dieses Feld den geschätzten Prozentsatz der Fertigstellung von 0 bis 1. Wenn die Aufgabe erfolgreich oder erfolglos abgeschlossen wurde, ist der Wert 1.	Lesezugriff
type	Wenn die Aufgabe erfolgreich abgeschlossen wurde, enthält dieser Parameter den Typ des codierten Ergebnisses. Der Typ ist der Name der Klasse, deren Referenz sich im Ergebnisfeld befindet. Andernfalls ist der Wert dieses Parameters undefined	Lesezugriff
result	Wenn die Aufgabe erfolgreich abgeschlossen wurde, enthält dieses Feld den Ergebniswert, entweder Ungültig oder eine Objektreferenz. Andernfalls ist der Wert dieses Parameters nicht definiert	Lesezugriff

Parametername	Beschreibung	Typ
error_info	Wenn die Aufgabe fehlgeschlagen ist, enthält dieser Parameter den Satz der zugehörigen Fehlerzeichenfolgen. Andernfalls ist der Wert dieses Parameters undefined	Lesezugriff
allowed_operations	Liste der in diesem Status zulässigen Vorgänge	Lesezugriff
created	Zeit, zu der die Aufgabe erstellt wurde	Lesezugriff
finished	Zeit, in der die Aufgabe abgeschlossen wurde (d. h. erfolgreich oder nicht erfolgreich). Wenn der Aufgabenstatus ausstehend ist, hat der Wert dieses Feldes keine Bedeutung	Lesezugriff
subtask_of	Enthält die UUID der Aufgaben, von denen diese Aufgabe eine Unteraufgabe ist	Lesezugriff
subtasks	Enthält die UUIDs aller Teilaufgaben dieser Aufgabe	Lesezugriff

task-cancel

```
xe task-cancel [uuid=task_uuid]
<!--NeedCopy-->
```

Weisen Sie die angegebene Aufgabe an, abzubrechen und zurückzukehren.

Template-Befehle

Befehle zum Arbeiten mit VM-Vorlagen.

Vorlagen sind im Wesentlichen VMs, bei denen der Parameter `is-a-template` auf **`true`** festgelegt ist. Eine Vorlage ist ein "Gold-Image", das alle verschiedenen Konfigurationseinstellungen enthält, um eine bestimmte VM zu instanziieren. XenServer wird mit einem Basissatz von Vorlagen geliefert,

bei denen es sich um generische "rohe"VMs handelt, mit denen eine Installations-CD eines Betriebssystemanbieters gestartet werden kann (z. B. RHEL, CentOS, SLES, Windows). Sie können VMs erstellen, sie in Standardformularen für Ihre speziellen Anforderungen konfigurieren und eine Kopie davon als Vorlagen für die zukünftige Verwendung in der VM-Bereitstellung speichern.

Die Vorlagenobjekte können mit dem Standardbefehl für die Objektauflistung (`xe template -list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

> **Hinweis:**
>
> Vorlagen können nicht direkt in VMs konvertiert werden, indem Sie den Parameter `is-a-template` auf **`false`** festlegen. Das Festlegen des Parameters `is-a-template` auf **`false`** wird nicht unterstützt und führt zu einer VM, die nicht gestartet werden kann.

Parameter der VM-Vorlage

Vorlagen haben die folgenden Parameter:

- `uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die Vorlage
- `name-label` (lesen/schreiben) den Namen der Vorlage
- `name-description` (lesen/schreiben) die Beschreibungszeichenfolge der Vorlage
- `user-version` (Lese-/Schreib-) Zeichenfolge für Ersteller von VMs und Vorlagen zum Ablegen von Versionsinformationen
- `is-a-template` (Lesen/Schreiben) true, wenn diese VM eine Vorlage ist.
  Vorlagen-VMs können niemals gestartet werden, sie werden nur zum Klonen anderer VMs verwendet. Nachdem dieser Wert auf "true"gesetzt wurde, kann er nicht auf "false"zurückgesetzt werden. Vorlagen-VMs können mit diesem Parameter nicht in virtuelle Rechner umgewandelt werden.

  Sie können eine VM in eine Vorlage konvertieren mit:

  ```
  xe vm-param-set uuid=<vm uuid> is-a-template=true
  <!--NeedCopy-->
  ```

- `is-control-domain` (schreibgeschützt) true, wenn dies eine Steuerdomäne (Domäne 0 oder eine Treiberdomäne) ist
- `power-state` (schreibgeschützt) aktueller Energiezustand. Der Wert wird für eine Vorlage immer angehalten
- `memory-dynamic-max` (schreibgeschützt) dynamischer maximaler Speicher in Byte.
  Derzeit nicht verwendet, aber wenn geändert, muss die folgende Einschränkung eingehalten

werden: memory_static_max >= memory_dynamic_max >= memory_dynamic_min >= memory_static_min.

- memory-dynamic-min (Lesen/Schreiben) dynamischer Mindestspeicher in Byte.
  Derzeit nicht verwendet, aber wenn geändert, müssen die gleichen Einschränkungen wie für memory-dynamic-max eingehalten werden.
- memory-**static**-max (Lesen/Schreiben) setzt statisch (absolut) maximalen Speicher in Byte.
  Dieses Feld ist der Hauptwert, der verwendet wird, um die Größe des Speichers zu bestimmen, der einer VM zugewiesen ist.
- memory-**static**-min (Lesen/Schreiben) setzt statisch (absolut) Mindestspeicher in Byte.
  Dieses Feld stellt den absoluten Mindestspeicher dar und memory-**static**-min muss kleiner als memory-**static**-max sein.
  Dieser Wert wird im Normalbetrieb nicht verwendet, aber die vorherige Einschränkung muss eingehalten werden.
- suspend-VDI-uuid (schreibgeschützt) der VDI, auf dem ein Suspend-Image gespeichert ist (hat keine Bedeutung für eine Vorlage)
- VCPUs-params (Zuordnungsparameter lesen/schreiben) für die ausgewählte vCPU-Richtlinie.

  Sie können das Pinning einer vCPU tunen mit:

```
xe template-param-set uuid=<template_uuid> vCPUs-params:mask
   =1,2,3
<!--NeedCopy-->
```

  Eine mit dieser Vorlage erstellte VM wird nur auf den physischen CPUs 1, 2 und 3 ausgeführt.

  Sie können auch die vCPU-Priorität (Xen-Planung) mit den Cap- und Gewicht-Parametern optimieren. Beispiel:

```
xe template-param-set uuid=<template_uuid> VCPUs-params:weight
   =512 xe template-param-set uuid=<template_uuid> VCPUs-params:
   cap=100
<!--NeedCopy-->
```

  Eine VM, die auf dieser Vorlage mit einem Gewicht von 512 basiert, erhält doppelt so viel CPU wie eine Domäne mit einem Gewicht von 256 auf einem umstrittenen Host. Die zulässigen Gewichte reichen von 1 bis 65535 und die Standardeinstellung ist 256.

  Die Obergrenze legt optional die maximale CPU-Menge fest, die eine auf dieser Vorlage basierende VM verbrauchen kann, selbst wenn der XenServer-Host CPU-Zyklen im Leerlauf hat. Die Obergrenze wird in Prozent einer physischen CPU ausgedrückt: 100 ist 1 physische CPU, 50 ist eine halbe CPU, 400 sind 4 CPUs usw. Der Standardwert 0 bedeutet, dass es keine Obergrenze gibt.

- VCPUs-max (Lesen/Schreiben) maximale Anzahl von vCPUs
- VCPUs-at-startup (Lesen/Schreiben) Startnummer der vCPUs
- actions-after-crash (Lese-/Schreib-) Aktion, die ausgeführt werden muss, wenn eine auf dieser Vorlage basierende VM abstürzt
- console-uuids (schreibgeschützte eingestellte Parameter) virtuelle Konsolengeräte
- platform (Map-Parameter lesen/schreiben) plattformspezifische Konfiguration

  Um die Emulation eines Parallelports für Gäste zu deaktivieren:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:parallel=none
  <!--NeedCopy-->
  ```

  Um die Emulation einer seriellen Port zu deaktivieren:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
  <!--NeedCopy-->
  ```

  So deaktivieren Sie die Emulation eines USB-Controllers und eines USB-Tablets:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:usb=false
  xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
  <!--NeedCopy-->
  ```

- allowed-operations (schreibgeschützt eingestellter Parameter) Liste der in diesem Zustand zulässigen Operationen
- current-operations (schreibgeschützter Set-Parameter) Liste der Vorgänge, die derzeit auf dieser Vorlage ausgeführt werden
- allowed-VBD-devices (schreibgeschützter Set-Parameter) Liste der zur Verwendung verfügbaren VBD-Identifikatoren, dargestellt durch Ganzzahlen im Bereich 0—15. Diese Liste dient nur zur Information und andere Geräte können verwendet werden (funktionieren aber möglicherweise nicht).
- allowed-VIF-devices (schreibgeschützter Set-Parameter) Liste der zur Verwendung verfügbaren VIF-Identifikatoren, dargestellt durch Ganzzahlen im Bereich 0—15. Diese Liste dient nur zur Information und andere Geräte können verwendet werden (funktionieren aber möglicherweise nicht).
- HVM-boot-policy (lesen/schreiben) die Boot-Richtlinie für Gäste. Entweder BIOS Order oder eine leere Zeichenfolge.
- HVM-boot-params (Zuordnungsparameter lesen/schreiben) Die Order-Taste steuert die Startreihenfolge der Gäste, dargestellt als Zeichenfolge, wobei jedes Zeichen eine Startmethode darstellt: d für die CD/DVD, c für den Stammdatenträger und n für den Netzwerk-PXE-Start. Die Standardeinstellung ist Gleichstrom.

- `PV-kernel` (lesen/schreiben) Pfad zum Kernel
- `PV-ramdisk` (lesen/schreiben) Pfad zum `initrd`
- `PV-args` (lesen/schreiben) Zeichenfolge von Kernel-Befehlszeilenargumenten
- `PV-legacy-args` (Lese-/Schreib) Zeichenfolge von Argumenten, um Legacy-VMs basierend auf dieser Vorlage zum Booten zu bringen
- `PV-bootloader` (lesen/schreiben) Name oder Pfad zum Bootloader
- `PV-bootloader-args` (lesen/schreiben) Zeichenfolge mit verschiedenen Argumenten für den Bootloader
- `last-boot-CPU-flags` (schreibgeschützt) beschreibt die CPU-Flags, auf denen eine auf dieser Vorlage basierende VM zuletzt gebootet wurde; nicht für eine Vorlage aufgefüllt
- `resident-on` (schreibgeschützt) der XenServer-Host, auf dem sich eine auf dieser Vorlage basierende VM befindet. Erscheint als `not in database` für eine Vorlage
- `affinity` (lesen/schreiben) der XenServer-Host, auf dem eine VM, die auf dieser Vorlage basiert, bevorzugt ausgeführt werden soll. Wird vom Befehl `xe vm-start` verwendet, um zu entscheiden, wo die VM ausgeführt werden soll.
- `other-config` (Map-Parameter mit Lese-/Schreibzugriff) Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die Vorlage angeben
- `start-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu der die Metriken für eine VM basierend auf dieser Vorlage gelesen wurden, in der Form `yyyymmddThh:mm:ss z`, wobei z die militärische Zeitzonenanzeige mit einem Buchstaben ist, z. B. Z für UTC (GMT). Legen Sie für eine Vorlage auf `1 Jan 1970 Z` (Anfang Unix/POSIX-Epoche) fest
- `install-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu der die Metriken für eine VM basierend auf dieser Vorlage gelesen wurden, in der Form `yyyymmddThh:mm:ss z`, wobei z die militärische Zeitzonenanzeige mit einem Buchstaben ist, z. B. Z für UTC (GMT). Legen Sie für eine Vorlage auf `1 Jan 1970 Z` (Anfang Unix/POSIX-Epoche) fest
- `memory-actual` (schreibgeschützt) der tatsächliche Speicher, der von einer VM basierend auf dieser Vorlage verwendet wird; 0 für eine Vorlage
- `VCPUs-number` (schreibgeschützt) die Anzahl der virtuellen CPUs, die einer VM basierend auf dieser Vorlage zugewiesen wurden; 0 für eine Vorlage
- `VCPUs-Utilization` (schreibgeschützter Map-Parameter) Liste der virtuellen CPUs und deren Gewichtung schreibgeschützter Zuordnungsparameter `os-version` Die Version des Betriebssystems für eine VM, die auf dieser Vorlage basiert. Erscheint als `not in database` für eine Vorlage

- `PV-drivers-version` (schreibgeschützter Zuordnungsparameter) die Versionen der paravirtualisierten Treiber für eine VM, die auf dieser Vorlage basieren. Erscheint als `not in database` für eine Vorlage
- `PV-drivers-detected` (schreibgeschützt) für die neueste Version der paravirtualisierten Treiber für eine auf dieser Vorlage basierende VM. Erscheint als `not in database` für eine Vorlage
- `memory` (schreibgeschützter Zuordnungsparameter) Speichermetriken, die vom Agent auf einer VM basierend auf dieser Vorlage gemeldet wurden. Erscheint als `not in database` für eine Vorlage
- `disks` (schreibgeschützter Zuordnungsparameter) Datenträgermetriken, die vom Agent auf einer VM basierend auf dieser Vorlage gemeldet wurden. Erscheint als `not in database` für eine Vorlage
- `networks` (schreibgeschützter Zuordnungsparameter) Netzwerkmetriken, die vom Agent auf einer VM basierend auf dieser Vorlage gemeldet wurden. Erscheint als `not in database` für eine Vorlage
- `other` (schreibgeschützter Zuordnungsparameter) andere Metriken, die vom Agent auf einer VM basierend auf dieser Vorlage gemeldet wurden. Erscheint als `not in database` für eine Vorlage
- `guest-metrics-last-updated` (schreibgeschützt) Zeitstempel, an dem der Gast-Agent den letzten Schreibvorgang in diese Felder ausgeführt hat. In dem Formular `yyyymmddThh:mm:ss z`, wobei z die militärische Zeitzonenanzeige mit einem Buchstaben ist, z. B. Z für UTC (GMT)
- `actions-after-shutdown` (Lesen/Schreiben) Aktion, die nach dem Herunterfahren der VM ausgeführt werden soll
- `actions-after-reboot` (Lesen/Schreiben) Aktion, die nach dem Neustart der VM ausgeführt werden soll
- `possible-hosts` (schreibgeschützt) Liste der Hosts, die die VM potenziell hosten können
- `HVM-shadow-multiplier` (Lese-/Schreib-) Multiplikator, der auf die Menge an Schatten angewendet wird, die dem Gast zur Verfügung gestellt wird
- `dom-id` (schreibgeschützt) Domänen-ID (falls verfügbar, andernfalls -1)
- `recommendations` (schreibgeschützt) XML-Spezifikation der empfohlenen Werte und Bereiche für Eigenschaften dieser VM
- `xenstore-data` (Read/Write Map-Parameter) Daten, die nach dem Erstellen der VM in die Struktur `xenstore` (`/local/domain/*domid*/vmdata`) eingefügt werden.
- `is-a-snapshot` (schreibgeschützt) True, wenn diese Vorlage ein VM-Snapshot ist

- `snapshot_of` (schreibgeschützt) die UUID der VM, von der diese Vorlage ein Snapshot ist
- `snapshots` (schreibgeschützt) die UUIDs aller Snapshots, die von dieser Vorlage erstellt wurden
- `snapshot_time` (schreibgeschützt) der Zeitstempel des zuletzt aufgenommenen VM-Snapshots
- `memory-target` (schreibgeschützt) die für diese Vorlage festgelegte Zielspeichermenge
- `blocked-operations` (Map-Parameter mit Lese-/Schreibzugriff) listet die Vorgänge auf, die mit dieser Vorlage nicht ausgeführt werden können
- `last-boot-record` (schreibgeschützt) Aufzeichnung der letzten Bootparameter für diese Vorlage im XML-Format
- `ha-always-run` (Lesen/Schreiben) True, wenn eine Instanz dieser Vorlage immer auf einem anderen Host neu gestartet wird, wenn der Host, auf dem sie ansässig ist, ausfällt. Dieser Parameter ist jetzt veraltet. Verwenden Sie stattdessen den Parameter `ha-restartpriority`.
- `ha-restart-priority` (schreibgeschützt) Neustart oder Bestleistung Lese-/Schreibblobs binärer Datenspeicher
- `live` (schreibgeschützt) nur für eine laufende VM relevant.

`template-export`

```
xe template-export template-uuid=uuid_of_existing_template filename=
    filename_for_new_template
<!--NeedCopy-->
```

Exportiert eine Kopie einer angegebenen Vorlage in eine Datei mit dem angegebenen neuen Dateinamen.

`template-uninstall`

```
xe template-uninstall template-uuid=template_uuid [--force]
<!--NeedCopy-->
```

Deinstallieren Sie eine benutzerdefinierte Vorlage. Dieser Vorgang zerstört die VDIs, die als “Eigentum”dieser Vorlage markiert sind.

Befehle aktualisieren

Der folgende Abschnitt enthält Befehle zum XenServer-Hostupdate.

das Update sobjekte können mit dem Standardbefehl für die Objektauflistung (`xe update-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

Parameter aktualisieren

XenServer-Hostupdates haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das Update	Lesezugriff
`host`	Die Liste der Hosts, auf die dieses Update angewendet wird	Lesezugriff
`host-uuid`	Die eindeutige Kennung für den abzufragenden XenServer-Host	Lesezugriff
`name-label`	Der Name des Updates	Lesezugriff
`name-description`	Die Beschreibungszeichenfolge des Updates	Lesezugriff
`applied`	Ob das Update angewendet wurde oder nicht; wahr oder falsch	Lesezugriff
`installation-size`	Die Größe des Updates in Byte	Lesezugriff
`after-apply-guidance`	Ob der XAPI-Toolstack oder der Host einen Neustart erfordert	Lesezugriff
`version`	Die Version des Updates	Lesezugriff

update-upload

```
xe update-upload file-name=update_filename
<!--NeedCopy-->
```

Laden Sie eine angegebene Update datei auf den XenServer-Host hoch. Dieser Befehl bereitet ein anzuwendendes Update vor. Bei Erfolg wird die UUID des hochgeladenen Updates gedruckt. Wenn das Update zuvor hochgeladen wurde, wird stattdessen ein Fehler `UPDATE_ALREADY_EXISTS` zurückgegeben und der Patch wird nicht erneut hochgeladen.

update-precheck

```
xe update-precheck uuid=update_uuid host-uuid=host_uuid
<!--NeedCopy-->
```

Führen Sie die im angegebenen Update enthaltenen Vorprüfungen auf dem angegebenen XenServer-Host aus.

update-destroy

```
xe update-destroy uuid=update_file_uuid
<!--NeedCopy-->
```

Löscht ein Updatesdatei, die nicht aus dem Pool angewendet wurde. Kann verwendet werden, um ein Updatesdatei zu löschen, die nicht auf die Hosts angewendet werden kann.

update-apply

```
xe update-apply host-uuid=host_uuid uuid=update_file_uuid
<!--NeedCopy-->
```

Wendet die angegebene Update datei an.

update-pool-apply

```
xe update-pool-apply uuid=update_uuid
<!--NeedCopy-->
```

Wenden Sie das angegebene Update auf alle XenServer-Hosts im Pool an.

update-introduce

```
xe update-introduce vdi-uuid=vdi_uuid
<!--NeedCopy-->
```

Einführung des Update-VDI.

update-pool-clean

```
xe update-pool-clean uuid=uuid
<!--NeedCopy-->
```

Entfernt die Dateien des Updates von allen Hosts im Pool.

Benutzer-Befehle

user-password-change

```
xe user-password-change old=old_password new=new_password
<!--NeedCopy-->
```

Ändert das Kennwort des angemeldeten Benutzers. Das alte Kennwortfeld ist nicht aktiviert, da Sie für die Verwendung dieses Befehls Supervisor-Privileg benötigen.

VBD-Befehle

Befehle zum Arbeiten mit VBDs (Virtual Block Devices).

Eine VBD ist ein Softwareobjekt, das eine VM mit dem VDI verbindet, der den Inhalt des virtuellen Laufwerks darstellt. Die VBD hat die Attribute, die den VDI mit der VM verknüpfen (ist er bootfähig, seine Lese-/Schreibmetriken usw.). Der VDI enthält Informationen zu den physikalischen Attributen des virtuellen Laufwerks (welcher SR-Typ, ob der Datenträger gemeinsam genutzt werden kann, ob das Medium schreibgeschützt oder schreibgeschützt ist usw.).

Die VBD-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe vbd-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

VBD-Parameter

VBDs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Identifikator/Objektreferenz für die VBD	Lesezugriff
`vm-uuid`	Die eindeutige Bezeichner/Objektreferenz für die VM, an die diese VBD angehängt ist	Lesezugriff
`vm-name-label`	Der Name der VM, an die diese VBD angehängt ist	Lesezugriff

Parametername	Beschreibung	Typ
vdi-uuid	Die eindeutige Bezeichner/Objektreferenz für den VDI, dem dieser VBD zugeordnet ist	Lesezugriff
vdi-name-**label**	Der Name des VDI, dem dieser VBD zugeordnet ist	Lesezugriff
empty	Wenn **true**diese VBD ein leeres Laufwerk darstellt	Lesezugriff
device	Das Gerät, das der Gast sieht, zum Beispiel hda	Lesezugriff
userdevice	Gerätenummer , die durch den Geräteparameter bei vbd-create angegeben wird, z. B. 0 für hda, 1 für hdb usw.	Lese-/Schreibrechte
bootable	True, wenn diese VBD bootfähig ist	Lese-/Schreibrechte
mode	Der Modus, mit dem die VBD montiert ist	Lese-/Schreibrechte
type	Wie die VBD der VM erscheint, zum Beispiel Datenträger oder CD	Lese-/Schreibrechte
currently-attached	Wahr, wenn die VBD an diesen Host angeschlossen ist, andernfalls false	Lesezugriff
storage-lock	True, wenn eine Sperre auf Speicherebene erworben wurde	Lesezugriff
status-code	Fehler-/Erfolgscode, der mit dem letzten Anhängevorgang verknüpft ist	Lesezugriff
status-detail	Fehler-/Erfolgsinformationen im Zusammenhang mit dem Status des letzten Anhängevorgangs	Lesezugriff
qos_algorithm_type	Der zu verwendende Priorisierungsalgorithmus	Lese-/Schreibrechte
qos_algorithm_params	Parameter für den gewählten Priorisierungsalgorithmus	Map-Parameter lesen/schreiben

Parametername	Beschreibung	Typ
qos_supported_algorithms	Unterstützte Priorisierungsalgorithmen für diese VBD	Schreibgeschützter Parameter
io_read_kbs	Durchschnittliche Leserate in kB pro Sekunde für diese VBD	Lesezugriff
io_write_kbs	Durchschnittliche Schreibrate in kB pro Sekunde für diese VBD	Lesezugriff
allowed-operations	Liste der in diesem Status zulässigen Vorgänge Diese Liste ist nur eine Empfehlung und der Serverstatus hat sich möglicherweise geändert, bis dieses Feld von einem Client gelesen wurde.	Schreibgeschützter Parameter
current-operations	Verknüpft jede der laufenden Aufgaben, die dieses Objekt verwenden (als Referenz), mit einer current_operation-Aufzählung, die die Art der Aufgabe beschreibt.	Schreibgeschützter Parameter
unpluggable	True, wenn diese VBD Hot-Unplug unterstützt	Lese-/Schreibrechte
attachable	True, wenn das Gerät angeschlossen werden kann	Lesezugriff
other-config	Zusätzliche Konfiguration	Map-Parameter lesen/schreiben

vbd-create

```
1 xe vbd-create vm-uuid=uuid_of_the_vm device=device_value vdi-uuid=
     uuid_of_vdi_to_connect_to [bootable=true] [type=Disk|CD] [mode=RW|RO
     ]
2 <!--NeedCopy-->
```

Erstellen Sie eine VBD auf einer VM.

Die zulässigen Werte für das device-Feld sind Ganzzahlen 0-15, und die Zahl muss für jede VM ein-

deutig sein. Die aktuell zulässigen Werte können im Parameter `allowed-VBD-devices` auf der angegebenen VM angezeigt werden. Dies wird als `userdevice` in den Parametern `vbd` gesehen.

Wenn `type` auf `Disk` gesetzt ist, ist `vdi-uuid` erforderlich. Der Modus kann `RO` oder `RW` für einen Datenträger sein.

Wenn `type` auf `CD` gesetzt ist, ist `vdi-uuid` optional. Wenn kein VDI angegeben ist, wird eine leere VBD für die CD erstellt. Der Modus muss `RO` für eine CD sein.

vbd-destroy

```
xe vbd-destroy uuid=uuid_of_vbd
<!--NeedCopy-->
```

Zerstört die angegebene VBD.

Wenn der Parameter `other-config:owner` für die VBD auf **`true`** eingestellt ist, wird auch der zugehörige VDI zerstört.

vbd-eject

```
xe vbd-eject uuid=uuid_of_vbd
<!--NeedCopy-->
```

Entfernen Sie das Medium aus dem Laufwerk, das durch eine VBD dargestellt wird. Dieser Befehl funktioniert nur, wenn das Medium vom Typ eines Wechselmediums ist (eine physische CD oder ein ISO). Andernfalls wird eine Fehlermeldung `VBD_NOT_REMOVABLE_MEDIA` zurückgegeben.

vbd-insert

```
xe vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
<!--NeedCopy-->
```

Legen Sie neue Medien in das durch eine VBD dargestellte Laufwerk ein. Dieser Befehl funktioniert nur, wenn das Medium vom Typ eines Wechselmediums ist (eine physische CD oder ein ISO). Andernfalls wird eine Fehlermeldung `VBD_NOT_REMOVABLE_MEDIA` zurückgegeben.

vbd-plug

```
xe vbd-plug uuid=uuid_of_vbd
<!--NeedCopy-->
```

Versuchen Sie, die VBD anzuhängen, während sich die VM im laufenden Zustand befindet.

vbd-unplug

```
xe vbd-unplug uuid=uuid_of_vbd
<!--NeedCopy-->
```

Versucht, die VBD von der VM zu trennen, während sie sich im laufenden Zustand befindet.

VDI-Befehle

Befehle für die Arbeit mit VDIs (Virtual Disk Images).

Ein VDI ist ein Softwareobjekt, das den Inhalt des virtuellen Laufwerks darstellt, das von einer VM gesehen wird. Dies unterscheidet sich von der VBD, bei der es sich um ein Objekt handelt, das eine VM an den VDI bindet. Der VDI enthält Informationen zu den physikalischen Attributen des virtuellen Laufwerks (welcher SR-Typ, ob der Datenträger gemeinsam genutzt werden kann, ob das Medium schreibgeschützt oder schreibgeschützt ist usw.). Die VBD hat die Attribute, die den VDI mit der VM verknüpfen (ist er bootfähig, seine Lese-/Schreibmetriken usw.).

Die VDI-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe vdi-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

VDI-Parameter

VDIs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den VDI	Lesezugriff
`name-label`	Der Name des VDI	Lese-/Schreibrechte
`name-description`	Die Beschreibungszeichenfolge des VDI	Lese-/Schreibrechte
`allowed-operations`	Eine Liste der in diesem Status zulässigen Vorgänge	Schreibgeschützter Parameter
`current-operations`	Eine Liste der Vorgänge, die derzeit auf diesem VDI ausgeführt werden	Schreibgeschützter Parameter
`sr-uuid`	SR, in dem sich der VDI befindet	Lesezugriff

Parametername	Beschreibung	Typ
vbd-uuids	Eine Liste von VBDs, die sich auf diesen VDI beziehen	Schreibgeschützter Parameter
crashdump-uuids	Liste der Crash-Dumps, die sich auf diesen VDI beziehen	Schreibgeschützter Parameter
virtual-size	Größe des Datenträger, wie sie der VM präsentiert wird, in Byte. Je nach Speicher-Back-End-Typ wird die Größe möglicherweise nicht genau eingehalten	Lesezugriff
physical-utilisation	Menge an physischem Speicherplatz, den der VDI auf dem SR belegt, in Byte	Lesezugriff
type	Typ des VDI, z. B. System oder Benutzer	Lesezugriff
sharable	True, wenn dieser VDI geteilt werden darf	Lesezugriff
read-only	True, wenn dieser VDI nur schreibgeschützt gemountet werden kann	Lesezugriff
storage-lock	True, wenn dieser VDI auf Speicherebene gesperrt ist	Lesezugriff
parent	Verweist auf den übergeordneten VDI, wenn dieser VDI Teil einer Kette ist	Lesezugriff
missing	True, wenn der SR-Scanvorgang diesen VDI als nicht vorhanden gemeldet hat	Lesezugriff
other-config	Zusätzliche Konfigurationsinformationen für diesen VDI	Map-Parameter lesen/schreiben
sr-name-**label**	Name des enthaltenden Speicherrepositorys	Lesezugriff
location	Informationen zum Standort	Lesezugriff
managed	True, wenn der VDI verwaltet wird	Lesezugriff

Parametername	Beschreibung	Typ
xenstore-data	Daten, die in den xenstore-Baum eingefügt werden sollen (/local/domain/0/backend/vbd/*domid*/*device-id*/smdata), nachdem der VDI angehängt wurde. Die SM-Backends setzen dieses Feld normalerweise ein vdi_attach.	Schreibgeschützter Map-Parameter
sm-config	SM-abhängige Daten	Schreibgeschützter Map-Parameter
is-a-snapshot	True, wenn dieser VDI ein VM-Speicher-Snapshot ist	Lesezugriff
snapshot_of	Die UUID des Speichers, von dem dieser VDI ein Snapshot ist	Lesezugriff
snapshots	Die UUIDs aller Snapshots dieses VDI	Lesezugriff
snapshot_time	Der Zeitstempel des Snapshot-Vorgangs, der diesen VDI erstellt hat	Lesezugriff
metadata-of-pool	Die UUID des Pools, der diesen Metadaten-VDI erstellt hat	Lesezugriff
metadata-latest	Flag, das angibt, ob der VDI die neuesten bekannten Metadaten für diesen Pool enthält	Lesezugriff
cbt-enabled	Flag, das angibt, ob Tracking geänderter Blocks für den VDI aktiviert ist	Lese-/Schreibrechte

vdi-clone

```
xe vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
<!--NeedCopy-->
```

Erstellen Sie eine neue, beschreibbare Kopie des angegebenen VDI, die direkt verwendet werden kann. Es ist eine Variante davon vdi-copy, die Hochgeschwindigkeits-Image-Klon-Funktionen verfügbar

machen kann, wo sie existieren.

Verwenden Sie den optionalen Zuordnungsparameter `driver-params`, um zusätzliche herstellerspezifische Konfigurationsinformationen an den Back-End-Speichertreiber zu übergeben, auf dem der VDI basiert. Weitere Informationen finden Sie in der Treiberdokumentation des Speicheranbieters.

vdi-copy

```
xe vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
<!--NeedCopy-->
```

Kopieren Sie einen VDI auf ein angegebenes SR.

vdi-create

```
xe vdi-create sr-uuid=uuid_of_sr_to_create_vdi_on name-label=
   name_for_the_vdi type=system|user|suspend|crashdump virtual-size=
   size_of_virtual_disk sm-config-*=storage_specific_configuration_data
<!--NeedCopy-->
```

Erstellen Sie einen VDI.

Der Parameter `virtual-size` kann in Byte oder mit den IEC-Standardsuffixen KiB, MiB, GiB und TiB angegeben werden.

> **Hinweis:**
>
> SR-Typen, die Thin Provisioning von Datenträgern unterstützen (z. B. Local VHD und NFS), erzwingen keine virtuelle Zuweisung von Datenträgern. Seien Sie vorsichtig, wenn Sie virtuellen Speicherplatz auf einem SR mehrfach zuweisen. Wenn ein zu mehrfach zugewiesenes SR voll wird, muss Speicherplatz entweder auf dem SR-Zielsubstrat oder durch Löschen nicht verwendeter VDIs in dem SR verfügbar gemacht werden.
>
> Einige SR-Typen runden den Wert `virtual-size` möglicherweise auf, um ihn durch eine konfigurierte Blockgröße teilbar zu machen.

vdi-data-destroy

```
xe vdi-data-destroy uuid=uuid_of_vdi
<!--NeedCopy-->
```

Löschen Sie die mit dem angegebenen VDI verknüpften Daten, behalten Sie jedoch die Metadaten für das Tracking geänderter Blocks bei.

> **Hinweis:**
>
> Wenn Sie Changed-Block-Tracking verwenden, um inkrementelle Backups des VDI zu erstellen, stellen Sie sicher, dass Sie den Befehl `vdi-data-destroy` verwenden, um Snapshots zu löschen, aber die Metadaten beizubehalten. Verwenden Sie `vdi-destroy` nicht für Snapshots von VDIs, bei denen das Tracking geänderter Blocks aktiviert wurde.

vdi-destroy

```
xe vdi-destroy uuid=uuid_of_vdi
<!--NeedCopy-->
```

Zerstört den angegebenen VDI.

> **Hinweis:**
>
> Wenn Sie Changed-Block-Tracking verwenden, um inkrementelle Backups des VDI zu erstellen, stellen Sie sicher, dass Sie den Befehl `vdi-data-destroy` verwenden, um Snapshots zu löschen, aber die Metadaten beizubehalten. Verwenden Sie `vdi-destroy` nicht für Snapshots von VDIs, bei denen das Tracking geänderter Blocks aktiviert wurde.
>
> Bei lokalen VHD- und NFS-SR-Typen wird Speicherplatz nicht sofort mit `vdi-destroy` freigegeben, sondern sporadisch während eines Speicherrepositoryscanvorgangs. Wenn Sie die Bereitstellung von gelöschtem Speicherplatz erzwingen müssen, rufen Sie `sr-scan` manuell auf.

vdi-disable-cbt

```
xe vdi-disable-cbt uuid=uuid_of_vdi
<!--NeedCopy-->
```

Deaktivieren Sie das Tracking geänderter Blocks für den VDI.

vdi-enable-cbt

```
xe vdi-enable-cbt uuid=uuid_of_vdi
<!--NeedCopy-->
```

Aktivieren Sie das Tracking geänderter Blocks für den VDI.

> **Hinweis:**

> Sie können die geänderte Blockverfolgung nur auf lizenzierten Instanzen von XenServer Premium Edition aktivieren.

vdi-export

```
xe vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=
    format] [base=uuid_of_base_vdi] [--progress]
<!--NeedCopy-->
```

Exportiert einen VDI in den angegebenen Dateinamen. Sie können einen VDI in einem der folgenden Formate exportieren:

- raw
- vhd

Das VHD-Format kann *sparse* sein. Wenn innerhalb des VDI nicht zugewiesene Blöcke vorhanden sind, werden diese Blöcke möglicherweise in der VHD-Datei weggelassen, wodurch die VHD-Datei kleiner wird. Sie können von allen unterstützten VHD-basierten Speichertypen (EXT3/EXT4, NFS) in das VHD-Format exportieren.

Wenn Sie den Parameter `base` angeben, exportiert dieser Befehl nur die Blöcke, die sich zwischen dem exportierten VDI und dem Basis-VDI geändert haben.

vdi-forget

```
xe vdi-forget uuid=uuid_of_vdi
<!--NeedCopy-->
```

Entfernt bedingungslos einen VDI-Record aus der Datenbank, ohne das Speicher-Backend zu berühren. Verwenden Sie im Normalbetrieb stattdessen `vdi-destroy`.

vdi-import

```
xe vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format
    =format] [--progress]
<!--NeedCopy-->
```

Importieren Sie ein VDI. Sie können einen VDI aus einem der folgenden Formate importieren:

- raw
- vhd

vdi-introduce

```
xe vdi-introduce uuid=uuid_of_vdi sr-uuid=uuid_of_sr name-label=
    name_of_new_vdi type=system|user|suspend|crashdump location=
    device_location_(varies_by_storage_type) [name-description=
    description_of_vdi] [sharable=yes|no] [read-only=yes|no] [other-
    config=map_to_store_misc_user_specific_data] [xenstore-data=
    map_to_of_additional_xenstore_keys] [sm-config=
    storage_specific_configuration_data]
<!--NeedCopy-->
```

Erstellen Sie ein VDI-Objekt, das ein vorhandenes Speichergerät darstellt, ohne tatsächlich Speicher zu ändern oder zu erstellen. Dieser Befehl wird hauptsächlich intern verwendet, um Hot-Plug-Speichergeräte automatisch einzuführen.

vdi-list-changed-blocks

```
xe vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=
    second-vdi-uuid
<!--NeedCopy-->
```

Vergleichen Sie zwei VDIs und geben Sie die Liste der Blöcke, die sich zwischen den beiden geändert haben, als Base64-codierte Zeichenfolge zurück. Dieser Befehl funktioniert nur für VDIs, bei denen das Tracking geänderter Blocks aktiviert wurde.

Weitere Informationen finden Sie unter Tracking geänderter Blocks.

vdi-pool-migrate

```
xe vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
<!--NeedCopy-->
```

Migrieren Sie einen VDI zu einem angegebenen SR, während der VDI an einen laufenden Gast angeschlossen ist. (Speicher-Livemigration)

Weitere Informationen finden Sie unter Migrieren von virtuellen Rechnern.

vdi-resize

```
xe vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
<!--NeedCopy-->
```

Ändern Sie die Größe des durch UUID angegebenen VDI.

vdi-snapshot

```
xe vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
<!--NeedCopy-->
```

Erstellt eine Lese-/Schreibversion eines VDI, die als Referenz für Backup- oder Vorlagenerstellungszwecke oder beides verwendet werden kann. Verwenden Sie den Snapshot, um eine Backup durchzuführen, anstatt Backupsoftware innerhalb der VM zu installieren und auszuführen. Die VM wird weiterhin ausgeführt, während externe Backupsoftware den Inhalt des Snapshots auf das Backupmedium streamt. In ähnlicher Weise kann ein Snapshot als "Goldenes Image"verwendet werden, auf dem eine Vorlage basiert. Eine Vorlage kann mit beliebigen VDIs erstellt werden.

Verwenden Sie den optionalen Zuordnungsparameter `driver-params`, um zusätzliche herstellerspezifische Konfigurationsinformationen an den Back-End-Speichertreiber zu übergeben, auf dem der VDI basiert. Weitere Informationen finden Sie in der Treiberdokumentation des Speicheranbieters.

Ein Klon eines Snapshots erzeugt immer einen beschreibbaren VDI.

vdi-unlock

```
xe vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
<!--NeedCopy-->
```

Versucht, die angegebenen VDIs zu entsperren. Wenn `force=true` an den Befehl übergeben wird, erzwingt es den Entsperrvorgang.

vdi-update

```
xe vdi-update uuid=uuid
<!--NeedCopy-->
```

Aktualisieren Sie die Felder des VDI-Objekts in der Datenbank.

VIF-Befehle

Befehle zum Arbeiten mit VIFs (Virtual Network Interfaces).

Die VIF-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe vif-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

VIF-Parameter

VIFs haben die folgenden Parameter:

- `uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für das VIF
- `vm-uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die VM, auf der sich dieses VIF befindet
- `vm-name-label` (schreibgeschützt) der Name der VM, auf der sich dieses VIF befindet
- `allowed-operations` (schreibgeschützter Set-Parameter) eine Liste der in diesem Zustand zulässigen Vorgänge
- `current-operations` (schreibgeschützter Set-Parameter) eine Liste der Vorgänge, die derzeit auf diesem VIF ausgeführt werden
- `device` (schreibgeschützt) Integer-Label dieses VIF, das die Reihenfolge angibt, in der VIF-Backends erstellt wurden
- `MAC` (schreibgeschützt) MAC-Adresse von VIF, wie sie der VM ausgesetzt ist
- `MTU` (schreibgeschützt) Maximale Übertragungseinheit des VIF in Byte.

  Dieser Parameter ist schreibgeschützt, Sie können jedoch die MTU-Einstellung mit dem Schlüssel `mtu` überschreiben mit dem Map-Parameter `other-config`. Um beispielsweise die MTU auf einer virtuellen Netzwerkkarte zurückzusetzen, um Jumbo-Frames zu verwenden:

  ```
  xe vif-param-set \
      uuid=<vif_uuid> \
      other-config:mtu=9000
  <!--NeedCopy-->
  ```

- `currently-attached` (schreibgeschützt) true wenn das Gerät angeschlossen ist
- `qos_algorithm_type` (lesen/schreiben) zu verwendender QoS-Algorithmus
- `qos_algorithm_params` (Map-Parameter lesen/schreiben) für den ausgewählten QoS-Algorithmus
- `qos_supported_algorithms` (schreibgeschützter Set-Parameter) unterstützte QoS-Algorithmen für dieses VIF
- `MAC-autogenerated` (schreibgeschützt) True, wenn die MAC-Adresse des VIF automatisch generiert wurde
- `other-config` (Map-Parameter lesen/schreiben) Zusätzliche `key:value`-Konfigurationspaare
- `other-config:ethtoolrx` (Lesen/Schreiben) auf on setzen, um Prüfsumme empfangen zu können, aus zum Deaktivieren

- other-config:ethtooltx (Lesen/Schreiben) auf on gesetzt, um Prüfsumme zu übertragen, aus zum Deaktivieren
- other-config:ethtoolsg (Lesen/Schreiben) auf on setzen, um Scatter Gather zu aktivieren, aus zum Deaktivieren
- other-config:ethtooltso (Lesen/Schreiben) auf on gesetzt, um TCP-Segmentierungs-Offload zu ermöglichen, aus zum Deaktivieren
- other-config:ethtoolufo (Lesen/Schreiben) auf on gesetzt, um das Abladen von UDP-Fragmenten zu ermöglichen, aus zum Deaktivieren
- other-config:ethtoolgso (Lesen/Schreiben) auf on gesetzt, um generische Segmentierungsabladung zu ermöglichen, aus zum Deaktivieren
- other-config:promiscuous (Lesen/Schreiben) entspricht einem VIF, um auf der Brücke promiskuitiv zu sein, so dass es den gesamten Verkehr über die Brücke sieht. Nützlich zum Ausführen eines Intrusion Detection Systems (IDS) oder ähnlichem in einer VM.
- network-uuid (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz des virtuellen Netzwerks, an das dieses VIF angeschlossen ist
- network-name-**label** (schreibgeschützt) der beschreibende Name des virtuellen Netzwerks, mit dem dieses VIF verbunden ist
- io_read_kbs (schreibgeschützt) durchschnittliche Leserate in KB/s für dieses VIF
- io_write_kbs (schreibgeschützt) durchschnittliche Schreibrate in KB/s für dieses VIF
- locking_mode (Lesen/Schreiben) Beeinflusst die Fähigkeit von VIFs, Datenverkehr zu/von einer Liste von MAC- und IP-Adressen zu filtern. Benötigt zusätzliche Parameter.
- locking_mode:**default** (Lesen/Schreiben) Variiert je nach Standardsperrmodus für das VIF-Netzwerk.

  Wenn der Standardsperrmodus auf eingestellt ist, wendet XenServer eine Filterregel an disabled, sodass die VIF keinen Datenverkehr senden oder empfangen kann. Wenn der Standardsperrmodus auf gesetzt ist unlocked, entfernt XenServer alle mit der VIF verknüpften Filterregeln. Weitere Informationen finden Sie unter Netzwerkbefehle.
- locking_mode:locked (Lesen/Schreiben) Im VIF ist nur Datenverkehr zulässig, der an oder von den angegebenen MAC- und IP-Adressen gesendet wird. Wenn keine IP-Adressen angegeben sind, ist kein Datenverkehr zulässig.
- locking_mode:unlocked (Lesen/Schreiben) Es werden keine Filter auf Datenverkehr angewendet, der zum oder vom VIF geht.
- locking_mode:disabled (Lesen/Schreiben) XenServer wendet eine Filterregel an, sodass die VIF den gesamten Datenverkehr verwirft.

vif-create

```
xe vif-create vm-uuid=uuid_of_the_vm device=see below network-uuid=
    uuid_of_network_to_connect_to [mac=mac_address]
<!--NeedCopy-->
```

Erstellen Sie eine VIF auf einer VM.

Entsprechende Werte für das `device`-Feld sind im Parameter `allowed-VIF-devices` auf der angegebenen VM aufgeführt. Bevor dort VIFs existieren, sind die zulässigen Werte ganze Zahlen von 0-15.

Der Parameter `mac` ist die Standard-MAC-Adresse im Format `aa:bb:cc:dd:ee:ff`. Wenn Sie es nicht spezifiziert lassen, wird eine entsprechende zufällige MAC-Adresse erstellt. Sie können auch explizit eine zufällige MAC-Adresse festlegen, indem Sie angeben `mac=random`.

vif-destroy

```
xe vif-destroy uuid=uuid_of_vif
<!--NeedCopy-->
```

Zerstöre ein VIF.

vif-move

```
xe vif-move uuid=uuid network-uuid=network_uuid
<!--NeedCopy-->
```

Verschieben Sie das VIF in ein anderes Netzwerk.

vif-plug

```
xe vif-plug uuid=uuid_of_vif
<!--NeedCopy-->
```

Versuchen Sie, das VIF anzuhängen, während sich die VM im laufenden Zustand befindet.

vif-unplug

```
xe vif-unplug uuid=uuid_of_vif
<!--NeedCopy-->
```

Versucht, das VIF während der Ausführung von der VM zu trennen.

vif-configure-ipv4

Konfigurieren Sie IPv4-Einstellungen für diese virtuelle Schnittstelle. Stellen Sie die IPv4-Einstellungen wie folgt ein:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
    gateway=gateway_address
<!--NeedCopy-->
```

Beispiel:

```
VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
   192.168.1.1")
<!--NeedCopy-->
```

Reinigen Sie die IPv4-Einstellungen wie folgt:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=none
<!--NeedCopy-->
```

vif-configure-ipv6

Konfigurieren Sie IPv6-Einstellungen für diese virtuelle Schnittstelle. Stellen Sie die IPv6-Einstellungen wie folgt ein:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
   gateway=gateway_address
<!--NeedCopy-->
```

Beispiel:

```
VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
   "fd06:7768:b9e5:8b00::1")
<!--NeedCopy-->
```

Reinigen Sie die IPv6-Einstellungen wie folgt:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=none
<!--NeedCopy-->
```

VLAN-Befehle

Befehle zum Arbeiten mit VLANs (virtuelle Netzwerke). Informationen zum Auflisten und Bearbeiten virtueller Schnittstellen finden Sie in den PIF-Befehlen, die über einen VLAN-Parameter verfügen, um zu signalisieren, dass sie über ein zugehöriges virtuelles Netzwerk verfügen. Weitere Informationen finden Sie unter PIF-Befehle. Um beispielsweise VLANs aufzulisten, verwenden Sie `xe pif-list`.

vlan-create

```
xe vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
    uuid_of_network
<!--NeedCopy-->
```

Erstellen Sie ein VLAN auf Ihrem XenServer-Host.

pool-vlan-create

```
xe pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
    uuid_of_network
<!--NeedCopy-->
```

Erstellen Sie ein VLAN auf allen Hosts in einem Pool, indem Sie festlegen, auf welcher Schnittstelle (z. B. `eth0`) sich das angegebene Netzwerk befindet (auf jedem Host) und ein neues PIF-Objekt an jedem Host entsprechend erstellen und einstecken.

vlan-destroy

```
xe vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
<!--NeedCopy-->
```

Zerstöre ein VLAN. Benötigt die UUID des PIF, das das VLAN darstellt.

VM-Befehle

Befehle zur Steuerung von virtuellen Rechnern und ihren Attributen.

VM-Selektoren

Einige der hier aufgeführten Befehle haben einen gemeinsamen Mechanismus zum Auswählen einer oder mehrerer VMs, auf denen der Vorgang ausgeführt werden soll. Der einfachste Weg ist die Angabe des Arguments `vm=name_or_uuid`. Eine einfache Möglichkeit, die UUID einer tatsächlichen VM zu erhalten, besteht beispielsweise darin, auszuführen `xe vm-list power-state=running`. (Ruft die vollständige Liste der Felder ab, die mit dem Befehl `xe vm-list params=all` abgeglichen werden können.) Wenn Sie z. B. `power-state=halted` angeben, werden VMs ausgewählt, deren Parameter `power-state` gleich `halted` ist. Wenn mehrere VMs übereinstimmen, geben Sie die Option `--multiple` zum Ausführen des Vorgangs an. Die vollständige Liste der Parameter, die abgeglichen werden können, wird am Anfang dieses Abschnitts beschrieben.

Die VM-Objekte können mit dem Standard-Objektauflistungsbefehl (`xe vm-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

VM-Parameter

Virtuelle Rechner haben die folgenden Parameter:

> **Hinweis:**
>
> Alle beschreibbaren VM-Parameterwerte können geändert werden, während die VM ausgeführt wird, aber neue Parameter werden *nicht* dynamisch angewendet und können erst angewendet werden, wenn die VM neu gestartet wurde.

- `appliance` (Lesen/Schreiben) der Appliance/vApp, zu der die VM gehört
- `uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die VM
- `name-label` (lesen/schreiben) der Name der VM
- `name-description` (lesen/schreiben) die Beschreibungszeichenfolge der VM
- `order` (Lesen/Schreiben) für das Starten/Herunterfahren der vApp und für den Start nach einem HA-Failover. VMs mit einem Ordnungswert von 0 (Null) werden zuerst gestartet, dann VMs mit einem Ordnungswert von 1 usw.
- `version` (schreibgeschützt) wie oft diese VM wiederhergestellt wurde. Wenn Sie eine neue VM mit einer älteren Version überschreiben möchten, rufen Sie `vm-recover`
- `user-version` (Lese-/Schreib-) Zeichenfolge für Ersteller von VMs und Vorlagen zum Ablegen von Versionsinformationen
- `is-a-template` (Lesen/Schreiben) False, sofern diese VM keine Vorlage ist. Vorlagen-VMs können nie gestartet werden, sie werden nur zum Klonen anderer VMs verwendet. Nachdem dieser Wert auf true gesetzt wurde, kann er nicht auf false zurückgesetzt werden. Vorlagen-VMs können mit diesem Parameter nicht in virtuelle Rechner umgewandelt werden.

  Sie können eine VM in eine Vorlage konvertieren mit:

  ```
  xe vm-param-set uuid=<vm uuid> is-a-template=true
  <!--NeedCopy-->
  ```

- `is-control-domain` (schreibgeschützt) True, wenn dies eine Steuerdomäne (Domäne 0 oder eine Treiberdomäne) ist
- `power-state` (schreibgeschützt) aktueller Energiezustand
- `start-delay` (lesen/schreiben) Die Wartezeit, bis ein Aufruf zum Starten der VM dauert, kehrt in Sekunden zurück

- `shutdown-delay` (lesen/schreiben) Die Wartezeit, bis ein Aufruf zum Herunterfahren der VM dauert, kehrt in Sekunden zurück
- `memory-dynamic-max` (Lesen/Schreiben) dynamisches Maximum in Byte
- `memory-dynamic-min` (Lesen/Schreiben) dynamisches Minimum in Byte
- `memory-static-max` (Lesen/Schreiben) statisch gesetztes (absolutes) Maximum in Byte. Wenn Sie diesen Wert ändern möchten, muss die VM heruntergefahren werden.
- `memory-static-min` (Lesen/Schreiben) statisch gesetztes (absolutes) Minimum in Byte. Wenn Sie diesen Wert ändern möchten, muss die VM heruntergefahren werden.
- `suspend-VDI-uuid` (schreibgeschützt) der VDI, auf dem ein Suspend-Image gespeichert ist
- `VCPUs-params` (Zuordnungsparameter lesen/schreiben) für die ausgewählte vCPU-Richtlinie.

  Sie können das Pinning einer vCPU mit

  ```
  xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
  <!--NeedCopy-->
  ```

  Die ausgewählte VM läuft dann nur auf den physischen CPUs 1, 2 und 3.
  Sie können auch die vCPU-Priorität (Xen-Planung) mit den Cap- und Gewicht-Parametern optimieren. Beispiel:

  ```
  xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-
     param-set uuid=<vm_uuid> VCPUs-params:cap=100
  <!--NeedCopy-->
  ```

  Eine VM mit einer Gewichtung von 512 erhält doppelt so viel CPU wie eine Domain mit einer Gewichtung von 256 auf einem konkurrierten XenServer-Host. Die zulässigen Gewichte reichen von 1 bis 65535 und die Standardeinstellung ist 256. Die Obergrenze legt optional die maximale CPU-Menge fest, die eine VM verbrauchen kann, auch wenn der XenServer-Host CPU-Zyklen im Leerlauf hat. Die Obergrenze wird in Prozent einer physischen CPU ausgedrückt: 100 ist 1 physische CPU, 50 ist eine halbe CPU, 400 sind 4 CPUs usw. Der Standardwert 0 bedeutet, dass es keine Obergrenze gibt.
- `VCPUs-max` (Lesen/Schreiben) maximale Anzahl virtueller CPUs.
- `VCPUs-at-startup` (Lesen/Schreiben) Startnummer der virtuellen CPUs
- `actions-after-crash` (Lesen/Schreiben) Aktion, die ergriffen werden muss, wenn die VM abstürzt. Für PV-Gäste sind gültige Parameter:
  - `preserve` (nur zur Analyse)
  - `coredump_and_restart` (Coredump aufzeichnen und VM neu starten)
  - `coredump_and_destroy` (Coredump aufzeichnen und VM angehalten lassen)

  - `restart` (kein Coredump und Neustart der VM)
  - `destroy` (kein Coredump und VM verlassen angehalten)

- `console-uuids` (schreibgeschützte eingestellte Parameter) virtuelle Konsolengeräte
- `platform` (Map-Parameter lesen/schreiben) plattformspezifische Konfiguration

  Deaktivieren des VDA, um Windows 10 in den Tablet-Modus zu versetzen:

```
xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
<!--NeedCopy-->
```

  So ermöglichen Sie dem VDA, Windows 10 in den Tablet-Modus zu versetzen:

```
xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
<!--NeedCopy-->
```

  Um den aktuellen Status zu überprüfen:

```
xe vm-param-get uuid=<vm_uuid> param-name=platform param-key=
   acpi_laptop_slate
<!--NeedCopy-->
```

- `allowed-operations` (schreibgeschützt eingestellter Parameter) Liste der in diesem Zustand zulässigen Operationen
- `current-operations` (schreibgeschützter Set-Parameter) eine Liste der Vorgänge, die derzeit auf der VM ausgeführt werden
- `allowed-VBD-devices` (schreibgeschützter Set-Parameter) Liste der zur Verwendung verfügbaren VBD-Identifikatoren, dargestellt durch Ganzzahlen im Bereich 0—15. Diese Liste dient nur zur Information und andere Geräte können verwendet werden (funktioniert aber möglicherweise nicht).
- `allowed-VIF-devices` (schreibgeschützter Set-Parameter) Liste der zur Verwendung verfügbaren VIF-Identifikatoren, dargestellt durch Ganzzahlen im Bereich 0—15. Diese Liste dient nur zur Information und andere Geräte können verwendet werden (funktioniert aber möglicherweise nicht).
- `HVM-boot-policy` (lesen/schreiben) die Boot-Richtlinie für Gäste. Entweder BIOS Order oder eine leere Zeichenfolge.
- `HVM-boot-params` (Zuordnungsparameter lesen/schreiben) Die Order-Taste steuert die Startreihenfolge der Gäste, dargestellt als Zeichenfolge, wobei jedes Zeichen eine Startmethode darstellt: d für die CD/DVD, c für den Stammdatenträger und n für den Netzwerk-PXE-Start. Die Standardeinstellung ist Gleichstrom.
- `HVM-shadow-multiplier` (Lese-/Schreibzugriff) Gleitkommawert, der den Schattenspeicher-Overhead steuert, der der VM gewährt werden soll. Der Standardwert ist 1,0 (der Mindestwert). Ändern Sie diesen Wert nur, wenn Sie ein fortgeschrittener Benutzer sind.

- PV-kernel (lesen/schreiben) Pfad zum Kernel
- PV-ramdisk (lesen/schreiben) Pfad zum initrd
- PV-args (lesen/schreiben) Zeichenfolge von Kernel-Befehlszeilenargumenten
- PV-legacy-args (lesen/schreiben) Zeichenfolge von Argumenten, um ältere VMs zum Booten zu bringen
- PV-bootloader (lesen/schreiben) Name oder Pfad zum Bootloader
- PV-bootloader-args (lesen/schreiben) Zeichenfolge mit verschiedenen Argumenten für den Bootloader
- last-boot-CPU-flags (schreibgeschützt) beschreibt die CPU-Flags, auf denen die VM zuletzt gebootet wurde
- resident-on (schreibgeschützt) der XenServer-Host, auf dem sich eine VM befindet
- affinity (lesen/schreiben) Der XenServer-Host, auf dem die VM bevorzugt ausgeführt wird. Wird vom Befehl xe vm-start verwendet, um zu entscheiden, wo die VM ausgeführt werden soll.
- other-config (Zuordnungsparameter mit Lese-/Schreibzugriff) Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die VM angeben.

  Das other-config-Schlüssel/Wert-Paar auto_poweron: **true** fordert beispielsweise an, die VM automatisch zu starten, nachdem ein Host im Pool gestartet wurde. Sie müssen diesen Parameter auch in Ihrem Pool unter other-config festlegen. Diese Parameter sind jetzt veraltet. Verwenden Sie stattdessen den Parameter ha-restart-priority.
- start-time (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu der die Metriken für die VM gelesen wurden. Dieser Zeitstempel hat das Format yyyymmddThh:mm:ss z, in der z der einbuchstabige militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT)
- install-time (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu der die Metriken für die VM gelesen wurden. Dieser Zeitstempel hat das Format yyyymmddThh:mm:ss z, in der z der einbuchstabige militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT)
- memory-actual (schreibgeschützt) der tatsächliche Speicher, der von einer VM verwendet wird
- VCPUs-number (schreibgeschützt) die Anzahl der virtuellen CPUs, die der VM für eine Linux-VM zugewiesen sind. Diese Nummer kann von VCPUS-max abweichen und kann geändert werden, ohne die VM mit dem Befehl vm-vcpu-hotplug neu zu starten. Weitere Informationen finden Sie unter vm-vcpu-hotplug. Windows-VMs werden immer mit der Anzahl der vCPUs ausgeführt, die in VCPUsmaxeingestellt ist, und müssen neu gestartet werden, um diesen Wert

zu ändern. Die Leistung sinkt stark, wenn Sie einen Wert einstellen VCPUs-number, der höher ist als die Anzahl der physischen CPUs auf dem XenServer-Host.

- VCPUs-Utilization (schreibgeschützter Map-Parameter) eine Liste virtueller CPUs und deren Gewicht
- os-version (schreibgeschützter Zuordnungsparameter) die Version des Betriebssystems für die VM
- PV-drivers-version (schreibgeschützter Map-Parameter) die Versionen der paravirtualisierten Treiber für die VM
- PV-drivers-detected (schreibgeschützt) Flag für die neueste Version der paravirtualisierten Treiber für die VM
- memory (schreibgeschützte Zuordnungsparameter) Speichermetriken, die vom Agent auf der VM gemeldet wurden
- disks (schreibgeschützte Zuordnungsparameter) Datenträgermetriken, die vom Agent auf der VM gemeldet wurden
- networks (schreibgeschützte Zuordnungsparameter) Netzwerkmetriken, die vom Agent auf der VM gemeldet wurden
- other (schreibgeschützter Zuordnungsparameter) andere vom Agent auf der VM gemeldete Metriken
- guest-metrics-lastupdated (schreibgeschützt) Zeitstempel, an dem der Gast-Agent den letzten Schreibvorgang in diese Felder ausgeführt hat. Der Zeitstempel hat das Format yyyymmddThh:mm:ss z, wobei z die militärische Zeitzonenanzeige mit einem Buchstaben ist, z. B. Z für UTC (GMT)
- actions-after-shutdown (Lesen/Schreiben) Aktion, die nach dem Herunterfahren der VM ausgeführt werden soll
- actions-after-reboot (Lesen/Schreiben) Aktion, die nach dem Neustart der VM ausgeführt werden soll
- possible-hosts potenzielle Hosts dieser VM schreibgeschützt
- dom-id (schreibgeschützt) Domänen-ID (falls verfügbar, andernfalls -1)
- recommendations (schreibgeschützt) XML-Spezifikation der empfohlenen Werte und Bereiche für Eigenschaften dieser VM
- xenstore-data (Map-Parameter lesen/schreiben) Daten, die nach dem Erstellen der VM in die xenstore-Struktur (/local/domain/*domid*/vm-data) eingefügt werden
- is-a-snapshot (schreibgeschützt) True, wenn diese VM ein Snapshot ist
- snapshot_of (schreibgeschützt) die UUID der VM, zu der dieser Snapshot gehört

- snapshots (schreibgeschützt) die UUIDs aller Snapshots dieser VM
- snapshot_time (schreibgeschützt) der Zeitstempel des Snapshot-Vorgangs, der diesen VM-Snapshot erstellt hat
- memory-target (schreibgeschützt) die für diese VM festgelegte Zielmenge an Arbeitsspeicher
- blocked-operations (Map-Parameter mit Lese-/Schreibzugriff) listet die Vorgänge auf, die auf dieser VM nicht ausgeführt werden können
- last-boot-record (schreibgeschützt) Aufzeichnung der letzten Bootparameter für diese Vorlage im XML-Format
- ha-always-run (Lesen/Schreiben) True, wenn diese VM immer auf einem anderen Host neu gestartet wird, wenn der Host, auf dem sie sich befindet, ausfällt. Dieser Parameter ist jetzt veraltet. Verwenden Sie stattdessen den Parameter ha-restart-priority.
- ha-restart-priority (Lesen/Schreiben) Neustart oder Bestleistung
- blobs (schreibgeschützt) binärer Datenspeicher
- live (schreibgeschützt) True, wenn die VM läuft. False, wenn HA vermutet, dass die VM nicht läuft.

vm-assert-can-be-recovered

```
xe vm-assert-can-be-recovered uuid [database] vdi-uuid
<!--NeedCopy-->
```

Testet, ob Speicher für die Wiederherstellung dieser VM verfügbar ist.

vm-call-plugin

```
xe vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
   value]
<!--NeedCopy-->
```

Ruft die Funktion innerhalb des Plug-Ins auf der angegebenen VM mit optionalen Argumenten auf (args:key=value). Um eine “value”-Zeichenfolge mit Sonderzeichen zu übergeben (z. B. neue Zeile), kann eine alternative Syntax args:key:file=local_file verwendet werden, wobei der Inhalt von local_file abgerufen und “key”als Ganzes zugewiesen wird.

vm-cd-add


```
xe vm-cd-add cd-name=name_of_new_cd device=
    integer_value_of_an_available_vbd [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Fügen Sie der ausgewählten VM eine neue virtuelle CD hinzu. Wählen Sie den Parameter `device` aus dem Wert des Parameters `allowed-VBD-devices` der VM aus.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-cd-eject

```
xe vm-cd-eject [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Werfen Sie eine CD aus dem virtuellen CD-Laufwerk aus. Dieser Befehl funktioniert nur, wenn genau eine CD an die VM angeschlossen ist. Wenn zwei oder mehr CDs vorhanden sind, verwenden Sie den Befehl `xe vbd-eject` und geben Sie die UUID der VBD an.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-cd-insert

```
xe vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Legen Sie eine CD in das virtuelle CD-Laufwerk ein. Dieser Befehl funktioniert nur, wenn genau ein leeres CD-Gerät an die VM angeschlossen ist. Wenn zwei oder mehr leere CD-Geräte vorhanden sind, verwenden Sie den Befehl `xe vbd-insert` und geben Sie die UUIDs der VBD und des VDI an, die eingefügt werden sollen.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-cd-list

```
xe vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value
    ...]
<!--NeedCopy-->
```


Listet CDs auf, die an die angegebenen VMs angeschlossen

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Sie können auch auswählen, welche VBD- und VDI-Parameter aufzulisten sind.

vm-cd-remove

```
xe vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Entfernen Sie eine virtuelle CD von den angegebenen virtuellen Rechnern.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-checkpoint

```
xe vm-checkpoint new-name-label=name_label [new-name-description=
   description]
<!--NeedCopy-->
```

Überprüfen Sie eine vorhandene VM und verwenden Sie den schnellen Datenträger-Snapshot-Betrieb auf Speicherebene, sofern verfügbar.

vm-clone

```
xe vm-clone new-name-label=name_for_clone [new-name-description=
   description_for_clone] [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Klonen Sie eine vorhandene VM und verwenden Sie den schnellen Datenträgerklonvorgang auf Speicherebene, sofern verfügbar. Geben Sie den Namen und die optionale Beschreibung für die resultierende geklonte VM mit den Argumenten **new**-name-**label** und **new**-name-description an.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-compute-maximum-memory

```
xe vm-compute-maximum-memory total=
    amount_of_available_physical_ram_in_bytes [approximate=add overhead
    memory for additional vCPUS? true|false] [vm_selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Berechnen Sie die maximale Menge an statischem Speicher, die einer vorhandenen VM zugewiesen werden kann, indem Sie die Gesamtmenge an physischem RAM als Obergrenze verwenden. Der optionale Parameter `approximate` reserviert ausreichend zusätzlichen Speicher in der Berechnung, um das spätere Hinzufügen zusätzlicher vCPUs zur VM zu berücksichtigen.

Beispiel:

```
xe vm-compute-maximum-memory vm=testvm total=`xe host-list params=
    memory-free --minimal`
<!--NeedCopy-->
```

Dieser Befehl verwendet den Wert des vom Befehl `xe host-list` zurückgegebenen Parameters `memory-free`, um den maximalen Speicher der VM `testvm` festzulegen.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-compute-memory-overhead

```
xe vm-compute-memory-overhead
<!--NeedCopy-->
```

Berechnet den Virtualisierungsspeicher-Overhead einer VM.

vm-copy

```
xe vm-copy new-name-label=name_for_copy [new-name-description=
    description_for_copy] [sr-uuid=uuid_of_sr] [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Kopieren Sie eine vorhandene VM, ohne den schnellen Datenträgerklonvorgang auf Speicherebene zu verwenden (auch wenn diese Option verfügbar ist). Bei den Disk-Images der kopierten VM handelt es sich garantiert um *vollständige Images*, d. h. sie sind nicht Teil einer Copy-on-Write-Kette (CoW).

Geben Sie den Namen und die optionale Beschreibung für die resultierende kopierte VM mit den Argumenten **new**-name-**label** und **new**-name-description an.

Geben Sie das Ziel-SR für die resultierende kopierte VM mit `sr-uuid` an. Wenn dieser Parameter nicht angegeben wird, entspricht das Ziel demselben SR, in dem die ursprüngliche VM ist.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-copy-bios-strings

```
xe vm-copy-bios-strings host-uuid=host_uuid
<!--NeedCopy-->
```

Kopieren Sie die BIOS-Strings des angegebenen Hosts auf die VM.

> **Hinweis:**
>
> Nachdem Sie eine VM zum ersten Mal gestartet haben, können Sie ihre BIOS-Zeichenfolgen nicht ändern. Stellen Sie sicher, dass die BIOS-Zeichenfolgen korrekt sind, bevor Sie die VM zum ersten Mal starten.

vm-crashdump-list

```
xe vm-crashdump-list [vm-selector=vm selector value...]
<!--NeedCopy-->
```

Listet Crashdumps auf, die mit den angegebenen VMs verknüpft sind

Wenn Sie das optionale Argument verwenden `params`, ist der Wert von params eine Zeichenfolge, die eine Liste von Parametern dieses Objekts enthält, die Sie anzeigen möchten. Alternativ können Sie das Schlüsselwort verwenden `all`, um alle Parameter anzuzeigen. Wenn `params` nicht verwendet wird, zeigt die zurückgegebene Liste eine Standardteilmenge aller verfügbaren Parameter an.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-data-source-list

```
xe vm-data-source-list [vm-selector=vm selector value...]
<!--NeedCopy-->
```

Listen Sie die Datenquellen auf, die für eine VM aufgezeichnet werden können.

Wählen Sie die VMs aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden. Weitere Informationen finden Sie unter VM-Selektoren.

Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen VMs ausgeführt.

Datenquellen haben zwei Parameter - `standard` und `enabled` -, die Sie in der Ausgabe dieses Befehls sehen können. Wenn in einer Datenquelle `enabled` auf **`true`** festgelegt wurde, werden die Metriken derzeit in der Performance-Datenbank aufgezeichnet. Wenn für eine Datenquelle `standard` auf **`true`** eingestellt ist, werden die Metriken standardmäßig in der Performance-Datenbank aufgezeichnet (und `enabled` ist auch für diese Datenquelle auf **`true`** festgelegt). Wenn für eine Datenquelle `standard` auf **`false`** eingestellt ist, werden die Metriken *nicht* standardmäßig in der Performance-Datenbank aufgezeichnet (und `enabled` sind auch für diese Datenquelle auf **`false`** festgelegt).

Führen Sie den Befehl `vm-data-source-record` aus, um die Aufzeichnung von Datenquellenmetriken in der Performance-Datenbank zu starten. Mit diesem Befehl wird `enabled` auf **`true`** festgelegt. Um aufzuhören, führe das aus `vm-data-source-forget`. Mit diesem Befehl wird `enabled` auf **`false`** festgelegt.

vm-data-source-record

```
xe vm-data-source-record data-source=name_description_of_data-source [
   vm-selector=vm selector value...]
<!--NeedCopy-->
```

Notieren Sie die angegebene Datenquelle für eine VM.

Bei diesem Vorgang werden die Informationen aus der Datenquelle in die Datenbank der persistenten Leistungsmetriken der angegebenen VMs geschrieben. Aus Leistungsgründen unterscheidet sich diese Datenbank von der normalen Agentdatenbank.

Wählen Sie die VMs aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen VMs ausgeführt.

vm-data-source-forget

```
xe vm-data-source-forget data-source=name_description_of_data-source [
   vm-selector=vm selector value...]
<!--NeedCopy-->
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für eine VM und vergessen Sie alle aufgezeichneten Daten.

Wählen Sie die VMs aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen VMs ausgeführt.

vm-data-source-query

```
xe vm-data-source-query data-source=name_description_of_data-source [vm
   -selector=vm_selector_value...]
<!--NeedCopy-->
```

Zeigt die angegebene Datenquelle für eine VM an.

Wählen Sie die VMs aus, auf denen dieser Vorgang ausgeführt werden soll, indem Sie den Standardauswahlmechanismus verwenden. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein. Wenn keine Parameter zur Auswahl von Hosts angegeben sind, wird der Vorgang auf allen VMs ausgeführt.

vm-destroy

```
xe vm-destroy uuid=uuid_of_vm
<!--NeedCopy-->
```

Zerstört die angegebene VM. Dadurch bleibt der mit der VM verknüpfte Speicher intakt. Um auch Speicher zu löschen, verwenden Sie `xe vm-uninstall`.

vm-disk-add

```
xe vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-
   selector=vm_selector_value...]
<!--NeedCopy-->
```

Fügen Sie den angegebenen virtuellen Rechnern einen Datenträger hinzu. Wählen Sie den Parameter `device` aus dem Wert des Parameters `allowed-VBD-devices` der VMs aus.

Der Parameter `disk-size` kann in Byte oder mit den IEC-Standardsuffixen KiB, MiB, GiB und TiB angegeben werden.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-disk-list

```
xe vm-disk-list [vbd-params] [vdi-params] [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Listet die an die angegebenen VMs angeschlossenen Datenträger auf. Die Parameter `vbd-params` und `vdi-params` steuern die Felder der jeweiligen Objekte, die ausgegeben werden sollen. Geben Sie die Parameter als kommagetrennte Liste oder den speziellen Schlüssel `all` für die vollständige Liste an.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-disk-remove

```
xe vm-disk-remove device=integer_label_of_disk [vm-selector=
    vm_selector_value...]
<!--NeedCopy-->
```

Entfernen Sie einen Datenträger aus den angegebenen VMs und löschen Sie ihn.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-export

```
xe vm-export filename=export_filename [metadata=true|false] [vm-
    selector=vm_selector_value...]
<!--NeedCopy-->
```

Exportieren Sie die angegebenen VMs (einschließlich Datenträgerimages) in eine Datei auf dem lokalen Computer. Geben Sie mit dem Parameter `filename` den Dateinamen an, in den die VM exportiert werden soll. Konventionell hat der Dateiname eine Erweiterung `.xva`.

Wenn der Parameter `metadata` auf **`true`** gesetzt ist, werden die Datenträger nicht exportiert. Nur die VM-Metadaten werden in die Ausgabedatei geschrieben. Verwenden Sie diesen Parameter, wenn der zugrunde liegende Speicher über andere Mechanismen übertragen wird, und ermöglicht die Neuerstellung der VM-Informationen. Weitere Informationen finden Sie unter `vm-`**`import`**.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-import

```
xe vm-import filename=export_filename [metadata=true|false] [preserve=
    true|false][sr-uuid=destination_sr_uuid]
<!--NeedCopy-->
```

Importieren Sie eine VM aus einer zuvor exportierten Datei. Wenn `preserve` auf **`true`** eingestellt ist , wird die MAC-Adresse der ursprünglichen VM beibehalten. `sr-uuid` bestimmt das Ziel-SR, in die die VM importiert werden soll. Wenn dieser Parameter nicht angegeben ist, wird das Standard-SR verwendet.

Wenn `metadata` auf **`true`** gesetzt ist, können Sie einen zuvor exportierten Satz von Metadaten ohne die zugehörigen Datenträgerblöcke importieren. Der Import nur für Metadaten schlägt fehl, wenn keine VDIs gefunden werden können (von SR benannt und `VDI.location`), sofern die Option `--force` nicht angegeben ist. In diesem Fall wird der Import trotzdem fortgesetzt. Wenn Datenträger gespiegelt oder aus dem Band verschoben werden können, ist der Import/Export von Metadaten eine schnelle Möglichkeit, VMs zwischen unzusammenhängenden Pools zu verschieben. Zum Beispiel als Teil eines Notfallwiederherstellungsplans.

> **Hinweis:**
>
> Mehrere VM-Importe werden seriell schneller ausgeführt als parallel.

vm-install

```
xe vm-install new-name-label=name [template-uuid=
    uuid_of_desired_template] [template=template_uuid_or_name] [sr-uuid=
    sr_uuid | sr-name-label=name_of_sr][copy-bios-strings-from=host_uuid
    ]
<!--NeedCopy-->
```

Installieren oder klonen Sie eine VM aus einer Vorlage. Geben Sie den Vorlagennamen mit dem Argument `template-uuid` oder `template` an. Geben Sie ein SR mit dem Argument `sr-uuid` oder `sr-name-label` an. Geben Sie mit dem Argument `copy-bios-strings-from` an, dass BIOS-gesperrte Medien installiert werden.

> **Hinweis:**
>
> Bei der Installation von einer Vorlage mit vorhandenen Datenträgern werden standardmäßig neue Datenträger in demselben SR wie diese vorhandenen Datenträger erstellt. Wo das SR dies unterstützt, sind diese Datenträger schnelle Kopien. Wenn in der Befehlszeile ein anderes SR angegeben ist, werden die neuen Datenträger dort erstellt. In diesem Fall ist ein schnelles Kopieren nicht möglich und die Datenträger sind vollständige Kopien.
>
> Bei der Installation von einer Vorlage, die keine vorhandenen Datenträger hat, werden alle neuen

> Datenträger in dem angegebenen SR oder dem Standard-SR des Pools erstellt, wenn kein SR angegeben ist.

vm-is-bios-customized

```
xe vm-is-bios-customized
<!--NeedCopy-->
```

Zeigt an, ob die BIOS-Zeichenfolgen der VM angepasst wurden.

vm-memory-dynamic-range-set

```
xe vm-memory-dynamic-range-set min=min max=max
<!--NeedCopy-->
```

Konfigurieren Sie den dynamischen Speicherbereich einer VM. Der dynamische Speicherbereich definiert weiche Unter- und Obergrenzen für den Speicher einer VM. Es ist möglich, diese Felder zu ändern, wenn eine VM läuft oder angehalten wird. Der Dynamikbereich muss innerhalb des statischen Bereichs liegen.

vm-memory-limits-set

```
xe vm-memory-limits-set static-min=static_min static-max=static_max
    dynamic-min=dynamic_min dynamic-max=dynamic_max
<!--NeedCopy-->
```

Konfigurieren Sie die Speicherbeschränkungen einer VM.

vm-memory-set

```
xe vm-memory-set memory=memory
<!--NeedCopy-->
```

Konfigurieren Sie die Speicherzuweisung einer VM.

vm-memory-shadow-multiplier-set

```
xe vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...] [
    multiplier=float_memory_multiplier]
<!--NeedCopy-->
```


Setzt den Schattenspeicher-Multiplikator für die angegebene VM.

Dies ist eine erweiterte Option, mit der die Größe des *Shadow-Speichers* geändert wird, der einer hardwareunterstützten VM zugewiesen ist.

In einigen spezialisierten Anwendungsworkloads, wie Citrix Virtual Apps, ist zusätzlicher Schattenspeicher erforderlich, um die volle Leistung zu erzielen.

Dieser Speicher wird als Overhead angesehen. Es ist von den normalen Speicherberechnungen für die Abrechnung von Speicher an eine VM getrennt. Wenn dieser Befehl aufgerufen wird, verringert sich die Menge an freiem Hostspeicher entsprechend dem Multiplikator und das Feld `HVM_shadow_multiplier` wird mit dem Wert aktualisiert, den Xen der VM zugewiesen hat. Wenn nicht genügend XenServer-Hostspeicher frei ist, wird ein Fehler zurückgegeben.

Die virtuellen Maschinen, auf denen dieser Vorgang ausgeführt werden soll, werden mithilfe des Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren.

vm-memory-static-range-set

```
xe vm-memory-static-range-set min=min max=max
<!--NeedCopy-->
```

Konfigurieren Sie den statischen Speicherbereich einer VM. Der statische Speicherbereich definiert harte Unter- und Obergrenzen für den Speicher einer VM. Es ist möglich, diese Felder nur zu ändern, wenn eine VM angehalten wird. Der statische Bereich muss den Dynamikbereich umfassen.

vm-memory-target-set

```
xe vm-memory-target-set target=target
<!--NeedCopy-->
```

Setzt das Speicherziel für eine angehaltene oder laufende VM. Der angegebene Wert muss innerhalb des Bereichs liegen, der durch die Werte memory_static_min und memory_static_max der VM definiert ist.

vm-migrate

```
xe vm-migrate [compress=true|false] [copy=true|false] [host-uuid=
    destination_host_uuid] [host=name_or_ uuid_of_destination_host] [
    force=true|false] [live=true|false] [vm-selector=vm_selector_value
    ...] [remote-master=destination_pool_master_uuid] [remote-username=
    destination_pool_username] [remote-password=
    destination_pool_password] [remote-network=
    destination_pool_network_uuid ][vif:source_vif_uuid=
    destination_network_uuid] [vdi:vdi_uuid=destination_sr_uuid]
```



```
<!--NeedCopy-->
```

Dieser Befehl migriert die angegebenen virtuellen Maschinen zwischen physischen Hosts.

Der Parameter `compress` überschreibt den `migration-compression` Pool-Parameter für `xe pool-param-set`.

Der Parameter `host` im `vm-migrate` Befehl kann entweder der Name oder die UUID des XenServer-Hosts sein. Um beispielsweise die VM auf einen anderen Host im Pool zu migrieren, wo sich die VM-Datenträger auf einem von beiden Hosts gemeinsam genutzten Speicher befinden:

```
xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid
<!--NeedCopy-->
```

So verschieben Sie VMs zwischen Hosts im selben Pool, die sich keinen Speicher teilen (Speicher-Livemigration):

```
xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
    remote-master=192.0.2.35 remote-username=username remote-password=
       password
<!--NeedCopy-->
```

Für die Speicher-Live-Migration müssen Sie den Hostnamen oder die IP-Adresse, den Benutzernamen und das Kennwort für den Poolkoordinator angeben, auch wenn Sie innerhalb desselben Pools migrieren.

Sie können das SR wählen, in der jeder VDI gespeichert wird:

```
xe vm-migrate uuid=vm_uuid remote-master=192.0.2.35 remote-username=
   username remote-password=password host-uuid=destination_host_uuid \
    vdi:vdi_1=destination_sr1_uuid \
    vdi:vdi_2=destination_sr2_uuid \
    vdi:vdi_3=destination_sr3_uuid
<!--NeedCopy-->
```

Darüber hinaus können Sie auswählen, welches Netzwerk die VM nach der Migration anhängen soll:

```
xe vm-migrate uuid=vm_uuid \
    vdi1:vdi_1_uuid=destination_sr1_uuid \
    vdi2:vdi_2_uuid=destination_sr2_uuid \
    vdi3:vdi_3_uuid=destination_sr3_uuid \
    vif:source_vif_uuid=destination_network_uuid
<!--NeedCopy-->
```

Für die poolübergreifende Migration:

```
xe vm-migrate uuid=vm_uuid remote-master=192.0.2.35 \
    remote-username=username remote-password=password \
    host-uuid=destination_host_uuid  \
    vif:source_vif_uuid=destination_network_uuid \
    vdi:vdi_uuid=destination_sr_uuid
```



```
<!--NeedCopy-->
```

Weitere Informationen zur Speicher-Livemigration, Live-Migration und Live-VDI-Migration finden Sie unter Migrieren von VMs.

> **Hinweis:**
>
> Wenn Sie ein Upgrade von einer älteren Version von XenServer oder Citrix Hypervisor durchführen, müssen Sie nach der Migration Ihrer VMs möglicherweise alle VMs herunterfahren und starten, um sicherzustellen, dass neue Virtualisierungsfunktionen übernommen werden.

Standardmäßig wird die VM angehalten, migriert und auf dem anderen Host fortgesetzt. Der Parameter `live` wählt die Livemigration aus. Die Live-Migration sorgt dafür, dass die VM während der Migration läuft, wodurch die Ausfallzeiten der virtuellen Maschine minimiert werden. Unter bestimmten Umständen, z. B. bei extrem speicherintensiven Workloads in der VM, fällt die Livemigration wieder in den Standardmodus und setzt die VM für kurze Zeit an, bevor die Speicherübertragung abgeschlossen wird.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-pause

```
xe vm-pause
<!--NeedCopy-->
```

Pausieren Sie eine laufende VM. Beachten Sie, dass dieser Vorgang den zugehörigen Speicher nicht freigibt (siehe `vm-suspend`).

vm-reboot

```
xe vm-reboot [vm-selector=vm_selector_value...] [force=true]
<!--NeedCopy-->
```

Starten Sie die angegebenen VMs neu.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Verwenden Sie das Argument `force`, um einen nicht ordnungsgemäßen Neustart zu verursachen. Wo das Herunterfahren dem Ziehen des Steckers auf einem physischen Server ähnelt.

vm-recover

```
xe vm-recover vm-uuid [database] [vdi-uuid] [force]
<!--NeedCopy-->
```

Stellt eine VM aus der Datenbank wieder her, die im bereitgestellten VDI enthalten ist.

vm-reset-powerstate

```
xe vm-reset-powerstate [vm-selector=vm_selector_value...] {
 force=true }

<!--NeedCopy-->
```

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Dies ist ein *erweiterter* Befehl, der nur verwendet wird, wenn ein Mitgliedshost in einem Pool ausfällt. Mit diesem Befehl können Sie den Poolkoordinator zwingen, den Energiezustand der VMs auf `halted` zurückzusetzen. Im Wesentlichen erzwingt dieser Befehl die Sperre der VM und der Datenträger, sodass sie als Nächstes auf einem anderen Poolhost gestartet werden kann. Für diesen Aufruf *muss* das Force-Flag angegeben werden und schlägt fehl, wenn es sich nicht in der Befehlszeile befindet.

vm-restart-device-models

```
xe vm-restart-device-models [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Starten Sie das Gerätemodell für diese VM auf dem Host neu. Während das Gerätemodell neu gestartet wird, können Sie die VM nicht stoppen, starten oder migrieren. Der Endbenutzer der VM sieht möglicherweise eine kurze Pause und setzt seine Sitzung fort.

> **Hinweis:**
>
> Damit die Aktion "Gerätemodell neu starten"auf einer Windows-VM unterstützt wird, müssen auf der VM die XenServer VM Tools für Windows installiert sein.

vm-resume

```
xe vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=
   host_uuid]
<!--NeedCopy-->
```


Setzt die angegebenen VMs fort.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Wenn sich die VM auf einem gemeinsam genutzten SR in einem Pool von Hosts befindet, verwenden Sie das Argument on, um anzugeben, auf welchem Poolmitglied sie gestartet werden soll. Standardmäßig bestimmt das System einen geeigneten Host, bei dem es sich um eines der Mitglieder des Pools handeln kann.

vm-retrieve-wlb-recommendations

```
xe vm-retrieve-wlb-recommendations
<!--NeedCopy-->
```

Rufen Sie die Empfehlungen für den Workloadausgleich für die ausgewählte VM ab.

vm-shutdown

```
xe vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
<!--NeedCopy-->
```

Fahren Sie die angegebene VM herunter.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Verwenden Sie das Argument force, um ein nicht ordnungsgemäßen Herunterfahren zu verursachen, ähnlich dem Ziehen des Steckers auf einem physischen Server.

vm-snapshot

```
xe vm-snapshot new-name-label=name_label [new-name-description+
    name_description]
<!--NeedCopy-->
```

Snapshot einer vorhandenen VM mit schnellem Datenträger-Snapshot-Betrieb auf Speicherebene, sofern verfügbar.

vm-start


```
xe vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=
    host_uuid] [--multiple]
<!--NeedCopy-->
```

Startet die angegebenen VMs.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Wenn sich die VMs auf einem gemeinsam genutzten SR in einem Pool von Hosts befinden, verwenden Sie das Argument on, um anzugeben, auf welchem Poolmitglied die VMs gestartet werden sollen. Standardmäßig bestimmt das System einen geeigneten Host, bei dem es sich um eines der Mitglieder des Pools handeln kann.

vm-suspend

```
xe vm-suspend [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Die angegebene VM aussetzen.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-uninstall

```
xe vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
<!--NeedCopy-->
```

Deinstallieren Sie eine VM und löschen Sie ihre Datenträger (die VDIs, die als RW gekennzeichnet sind und nur mit dieser VM verbunden sind) zusätzlich zu ihrem Metadatensatz. Um nur die VM-Metadaten zu löschen, verwenden Sie `xe vm-destroy`.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

vm-unpause

```
xe vm-unpause
<!--NeedCopy-->
```


Unterbrechen Sie eine angehaltene VM.

vm-vcpu-hotplug

```
xe vm-vcpu-hotplug new-vcpus=new_total_vcpu_count [vm-selector=
   vm_selector_value...]
<!--NeedCopy-->
```

Passen Sie dynamisch die Anzahl der vCPUs an, die für eine laufende Linux-VM verfügbar sind. Die Anzahl der vCPUs wird durch den Parameter begrenzt VCPUs-max. Windows-VMs werden immer mit der Anzahl der vCPUs ausgeführt, die in VCPUs-maxeingestellt ist, und müssen neu gestartet werden, um diesen Wert zu ändern.

Verwenden Sie den Parameter **new**-vcpus, um die neue *Gesamtzahl* der vCPUs zu definieren, die Sie nach der Ausführung dieses Befehls haben möchten. Verwenden Sie diesen Parameter nicht, um die Anzahl der vCPUs zu übergeben, die Sie hinzufügen möchten. Wenn Sie beispielsweise zwei vorhandene vCPUs in Ihrer VM haben und zwei weitere vCPUs hinzufügen möchten, geben Sie **new**-vcpus =4 an.

Die Linux-VM oder Windows-VMs, auf denen dieser Vorgang ausgeführt wird, werden mithilfe des Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

> **Hinweis:**
>
> Wenn Sie Linux-VMs ohne installierte XenServer VM Tools ausführen, führen Sie den folgenden Befehl auf der VM aus, root um sicherzustellen, dass die neu Hot-Plug-vCPUs verwendet werden: `# for i in /sys/devices/system/cpu/cpu[1-9]*/online; do if [ "$(cat $i)"= 0 ]; then echo 1 > $i; fi; done`

vm-vif-list

```
xe vm-vif-list [vm-selector=vm_selector_value...]
<!--NeedCopy-->
```

Listet die VIFs der angegebenen VMs auf.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden über den Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Die Selektoren arbeiten beim Filtern mit den VM-Datensätzen und *nicht* mit den VIF-Werten. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts aufgeführten VM-Parameter sein.

Geplante Snapshots

Befehle zum Steuern von VM-geplanten Snapshots und deren Attributen.

Die `vmss`-Objekte können mit dem Standardbefehl zur Objektauflistung (`xe vmss-list`) aufgelistet werden, und die Parameter können mit den Standardparameterbefehlen bearbeitet werden. Weitere Informationen finden Sie unter Parameterbefehle auf niedriger Ebene

`vmss-create`

```
xe vmss-create enabled=True/False name-label=name type=type frequency=
   frequency retained-snapshots=value name-description=description
   schedule:schedule
<!--NeedCopy-->
```

Erstellt einen Snapshot-Zeitplan im Pool.

Beispiel:

```
xe vmss-create retained-snapshots=9 enabled=true frequency=daily \
    name-description=sample name-label=samplepolicy type=snapshot \
    schedule:hour=10 schedule:min=30
<!--NeedCopy-->
```

Snapshot-Zeitpläne haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`name-label`	Name des Snapshot-Zeitplans.	Lese-/Schreibrechte
`name-description`	Beschreibung des Snapshot-Zeitplans.	Lese-/Schreibrechte
`type`	Datenträger-Snapshot oder Speicher-Snapshot	Lese-/Schreibrechte
`frequency`	Stündlich; täglich; wöchentlich	Lese-/Schreibrechte
`retained-snapshots`	Snapshots müssen beibehalten werden. Reichweite: 1-10.	Lese-/Schreibrechte
`schedule`	`schedule:days` (Montag bis Sonntag), `schedule:hours` (0 bis 23), `schedule:minutes` (0, 15, 30, 45)	Lese-/Schreibrechte

vmss-destroy

```
xe vmss-destroy uuid=uuid
<!--NeedCopy-->
```

Zerstört einen Snapshot-Zeitplan im Pool.

USB-Durchgang

USB-Passthrough wird für die folgenden USB-Versionen unterstützt: 1.1, 2.0 und 3.0.

USB-Pass-Through aktivieren/deaktivieren

```
xe pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
<!--NeedCopy-->
```

Aktivieren/Deaktivieren von USB-Passthrough.

pusb-scan

```
xe pusb-scan host-uuid=host_uuid
<!--NeedCopy-->
```

PUSB scannen und aktualisieren.

vusb-create

```
xe vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
<!--NeedCopy-->
```

Erstellt einen virtuellen USB-Stick im Pool. Starten Sie die VM, um den USB zur VM zu leiten.

vusb-unplug

```
xe vusb-unplug uuid=vusb_uuid
<!--NeedCopy-->
```

Trennen Sie den USB-Stecker von der VM.

vusb-destroy

```
xe vusb-destroy uuid=vusb_uuid
<!--NeedCopy-->
```

Entfernt die virtuelle USB-Liste von der VM.

---

layout: doc
description: Learn about the levels of support for XenServer and the logs that are available to help with troubleshooting.—

Problembehandlung

Wenn Sie technische Probleme mit dem XenServer-Host haben, soll Ihnen dieser Abschnitt helfen, das Problem nach Möglichkeit zu lösen. Wenn dies nicht möglich ist, verwenden Sie die Informationen in diesem Abschnitt, um die Anwendungsprotokolle und andere Daten zu sammeln, die dem technischen Support helfen können, das Problem zu verfolgen und zu lösen.

In den folgenden Artikeln finden Sie Informationen zur Fehlerbehebung zu bestimmten Bereichen des Produkts:

- VM-Fehlerbehebung
- Netzwerk-Fehlerbehebung
- Problembehandlung bei Clusterpools
- XenCenter Problembehandlung
- Problembehandlung beim Workload Balancing
- Problembehandlung bei Conversion Manager

Problembehandlung bei Verbindungen zwischen XenCenter und dem XenServer-Host

Wenn Sie Probleme haben, mit XenCenter eine Verbindung zum XenServer-Host herzustellen, überprüfen Sie Folgendes:

- Ist Ihr XenCenter eine ältere Version als der XenServer-Host, mit dem Sie eine Verbindung herstellen möchten?

  XenCenter 8.2.7 und früher werden mit XenServer 8-Hosts nicht unterstützt. Um Ihre XenServer 8-Hosts oder -Pools zu verwalten, benötigen Sie die neueste Version von XenCenter mit einer Version des Formulars yyyy.x.x.

  Installieren Sie die neueste Version von XenCenter, um dieses Problem zu beheben.

- Ist Ihr Führerschein aktuell?

  Sie können das Ablaufdatum für Ihren Lizenzzugriffscode auf der Registerkarte "**Allgemein** "des XenServer-Hosts im Abschnitt **Lizenzdetails** in XenCenter sehen.

  Weitere Informationen zur Lizenzierung eines Hosts finden Sie unter Lizenzierung.

- Der XenServer-Host kommuniziert mit XenCenter über HTTPS über die folgenden Ports:

  - Port 443 (eine bidirektionale Verbindung für Befehle und Antworten mithilfe der Verwaltungs-API)
  - Port 5900 für grafische VNC-Verbindungen mit paravirtualisierten Linux-VMs.

  Wenn Sie eine Firewall zwischen dem XenServer-Host und dem Computer, auf dem die Clientsoftware ausgeführt wird, aktiviert haben, stellen Sie sicher, dass sie Datenverkehr von diesen Ports zulässt. Weitere Informationen finden Sie unter Internetkonnektivität.

Sammeln Sie XenServer- und XenCenter-Protokolle

XenServer-Hostprotokolle

XenCenter kann verwendet werden, um XenServer-Hostinformationen zu sammeln.

Klicken Sie im Menü **Extras** auf **Serverstatusbericht**, um den Task **Serverstatusbericht** zu öffnen. Sie können aus einer Liste verschiedener Informationstypen auswählen (verschiedene Protokolle, Absturzabbilder usw.). Die Informationen werden kompiliert und auf den Computer heruntergeladen, auf dem XenCenter ausgeführt wird. Weitere Informationen finden Sie in der XenCenter-Dokumentation.

Standardmäßig können die für einen Serverstatusbericht gesammelten Dateien in ihrer Größe begrenzt werden. Wenn Sie Protokolldateien benötigen, die größer als die Standarddatei sind, können Sie den Befehl `xenserver-status-report -u` in der XenServer-Hostkonsole ausführen.

> **Wichtig:**
>
> XenServer-Hostprotokolle können vertrauliche Informationen enthalten.

Host-Protokollnachrichten an einen zentralen Server senden Anstatt Protokolle in das Dateisystem der Steuerdomäne schreiben zu lassen, können Sie Ihren XenServer-Host so konfigurieren, dass sie auf einen Remoteserver geschrieben werden. Auf dem Remoteserver muss der `syslogd`-Daemon laufen, um die Protokolle empfangen und korrekt aggregieren zu können. Der `syslogd`-Daemon ist ein Standardbestandteil aller Varianten von Linux und Unix, und Versionen von Drittanbietern sind für Windows und andere Betriebssysteme verfügbar.

Legen Sie den Parameter syslog_destination auf den Hostnamen oder die IP-Adresse des Remoteserver fest, auf den die Protokolle geschrieben werden sollen:


```
xe host-param-set uuid=host_uuid logging:syslog_destination=hostname
<!--NeedCopy-->
```

Führen Sie den Befehl aus:

```
xe host-syslog-reconfigure uuid=host_uuid
<!--NeedCopy-->
```

Um die Änderung durchzusetzen. (Sie können diesen Befehl auch remote ausführen, indem Sie den Parameter `host` angeben.)

XenCenter Protokolle

XenCenter hat auch ein clientseitiges Protokoll. Diese Datei enthält eine vollständige Beschreibung aller Vorgänge und Fehler, die bei der Verwendung von XenCenter auftreten. Es enthält auch eine Informationsprotokollierung von Ereignissen, die Ihnen ein Prüfprotokoll der verschiedenen aufgetretenen Aktionen liefern. Die XenCenter-Protokolldatei wird in Ihrem Profilordner unter dem folgenden Pfad gespeichert:. `%userprofile%\AppData\Roaming\XenServer\XenCenter\logs\XenCenter.log`

Um die XenCenter-Protokolldateien zu finden, z. B. wenn Sie die Protokolldatei öffnen oder per E-Mail versenden möchten, klicken Sie im XenCenter Hilfemenü auf XenCenter Log Files anzeigen**.**

Installationsprotokolle

Wenn während der Installation ein unbekannter Fehler auftritt, erfassen Sie die Protokolldatei von Ihrem Host und stellen Sie sie dem Technischen Support zur Verfügung.

Mit einer Tastatur, die direkt an den Host-Computer angeschlossen ist (nicht über eine serielle Port angeschlossen), können Sie während der Installation auf drei virtuelle Terminals zugreifen:

- Drücken Sie **Alt+F1**, um auf das XenServer-Hauptinstallationsprogramm zuzugreifen
- Drücken Sie **Alt+F2**, um auf eine lokale Shell zuzugreifen
- Drücken Sie **Alt+F3**, um auf das Ereignisprotokoll zuzugreifen

So erfassen und speichern Sie die Protokolldateien:

1. Drücken Sie **Alt+F2**, um auf die lokale Shell zuzugreifen.
2. Geben Sie Folgendes ein:

   ```
   /opt/xensource/installer/report.py
   <!--NeedCopy-->
   ```


3. Sie werden aufgefordert, auszuwählen, wo Sie die Protokolldatei speichern möchten: **NFS**, **FTP**oder **Lokale Medien**.

   Wählen Sie **NFS** oder **FTP**, um die Protokolldatei auf einen anderen Computer in Ihrem Netzwerk zu kopieren. Um dies zu tun, muss das Netzwerk ordnungsgemäß funktionieren und Sie müssen Schreibzugriff auf einen Remotecomputer haben.

   Wählen Sie **Lokales Medium** aus, um die Datei auf einem Wechselspeichergerät, z. B. einem USB-Flash-Laufwerk, auf dem lokalen Computer zu speichern.

   Sobald Sie Ihre Auswahl getroffen haben, schreibt das Programm die Protokolldatei an den von Ihnen ausgewählten Speicherort. Der Dateiname lautet `support.tar.bz2`.

---

layout: doc
description: Learn about the levels of support for XenServer—

Support

Wir bieten technischen Support für Kunden mit einer XenServer Premium Edition- oder Standard Edition-Lizenz. Um auf diesen Support zuzugreifen, können Sie online einen Support-Fall eröffnen oder sich bei technischen Problemen telefonisch an das Support Center wenden. Weitere Informationen finden Sie auf der XenServer-Supportseite.

Wenn Sie die XenServer Trial Edition (unlizenziert) verwenden, können Sie nicht auf diesen Support zugreifen, aber wir schätzen Ihr Feedback. Weitere Informationen finden Sie unter Feedback für XenServer und XenCenter geben.

> **Hinweis:**
>
> Wenn Sie XenServer 8 während der Vorschauphase installiert haben, müssen Sie Updates installieren, die am 18. März 2024 oder später veröffentlicht wurden, um Ihren Pool auf ein produktionsunterstütztes Niveau zu bringen, das Anspruch auf technischen Support hat.

Häufige Updates

XenServer 8 verwendet ein häufiges Update modell, das Funktionen, Korrekturen und Verbesserungen für Ihre Hosts bereitstellt. Wir erwarten, dass Sie diese Updates innerhalb von sechs Monaten nutzen, um den Support weiterhin nutzen zu können. Wenn die Updateversion Ihres Pools älter als sechs Monate ist, werden wir Sie bitten, das Problem auf der neuesten Updateversion zu reproduzieren.

Support-Checkliste

Dieser Abschnitt führt Sie durch mögliche Maßnahmen, die Sie ergreifen können, wenn in Ihrer XenServer-Umgebung ein Problem auftritt. Indem Sie so viele dieser Schritte wie möglich ausführen, helfen Sie uns, Ihr Problem schneller zu beheben.

Erste Schritte

Gehen Sie wie folgt vor, wenn das Problem zum ersten Mal auftritt:

1. Erfassen Sie alle möglichen Protokolle aus der Umgebung, bevor Sie irgendwelche Wiederherstellungsschritte ausführen:

   - Wenn sich das Problem auf XenServer bezieht, erfassen Sie einen Serverstatusbericht (SSR) des Hosts oder Pools, auf dem das Problem aufgetreten ist. Gehen Sie zum XenCenter **Tools-Menü** und dann zum **Serverstatusbericht**.
   - Wenn sich das Problem auf XenCenter bezieht:
     - Rufen Sie die Anwendungsprotokolldateien ab, indem Sie im XenCenter **Hilfemenü** auf **XenCenter-Protokolldateien anzeigen** gehen.
     - Erfassen Sie Screenshots der relevanten Displays.
   - Wenn sich das Problem auf eine VM bezieht, sammeln Sie alle relevanten Protokolle aus dem VM-Betriebssystem.

   Weitere Informationen zum Abrufen von Protokollinformationen finden Sie unter XenServer- und XenCenter-Protokolle sammeln.

2. Notieren Sie sich das Synchronisierungsdatum, die Synchronisierungsprüfsumme und die Updateprüfsumme für Ihren Host oder Pool. Weitere Informationen finden Sie unter Ausstehende Aufgaben anzeigen.

3. Versuchen Sie gegebenenfalls, Ihre Umgebung wieder in einen funktionierenden Zustand zu versetzen.

Selbsthilfe

Wir bieten Informationen und Anleitungen, die Ihnen helfen können, Probleme zu diagnostizieren und zu lösen, auf die Sie möglicherweise stoßen.

1. In dieser Dokumentation finden Sie Hilfe:

   - Bekannte Probleme: Dieser Artikel listet bekannte Probleme in XenServer auf und, falls zutreffend, alle Workarounds, die Sie anwenden können.

- Early Access und Normal: In diesen Artikeln sind verfügbare Updates für XenServer aufgeführt. Möglicherweise wurde kürzlich ein Fix für Ihr Problem veröffentlicht.
- Problembehandlung: Dieser Artikel ist ein Einstieg in die Informationen zur Problembehandlung in der Dokumentation.
- Lesen Sie den Abschnitt der Dokumentation zu der Funktion, bei der das Problem auftritt. Möglicherweise gibt es Einschränkungen für diese Funktion, die das Problem verursachen, oder Konfigurationsoptionen, mit denen das Problem behoben werden kann.

2. Das Citrix Knowledge Center enthält viele Artikel unseres technischen Support-Teams, in denen Lösungen für zuvor aufgetretene Probleme mit XenServer beschrieben werden.

Wenn Sie aufgrund dieser Informationen diagnostische Maßnahmen ergreifen oder Ihre Umgebungskonfiguration ändern, notieren Sie sich dies und teilen Sie uns mit, ob Sie den Support kontaktieren.

Auf die neueste Version aktualisieren

Wenn Sie bereits die neueste Version all Ihrer XenServer-Komponenten verwenden, fahren Sie mit Capture Logs fort.

Wenn Sie nicht die neueste XenServer-, XenCenter- oder verwandte Komponente ausführen, ist die Lösung für Ihr Problem möglicherweise in der neuesten Version oder dem neuesten Update-Level enthalten. Wir empfehlen, dass Sie Ihre Umgebung nach Möglichkeit auf die neueste Version aktualisieren.

1. Aktualisieren Sie Ihren Pool auf das neueste Update.
2. Aktualisieren Sie XenCenter auf die neueste Version.
3. Wenn sich das Problem auf eine Windows-VM bezieht, aktualisieren Sie die XenServer VM Tools für Windows auf die neueste Version.
4. Wenn sich das Problem auf eine Linux-VM bezieht, stellen Sie sicher, dass die neueste Version der XenServer VM Tools for Linux installiert ist. Diese Tools sind unter https://xenserver.com/downloads verfügbar.
5. Wenn sich das Problem auf Workload Balancing oder den XenServer Conversion Manager bezieht, stellen Sie sicher, dass Sie die neueste Version verwenden, die unter https://xenserver.com/downloads verfügbar ist.

Problem in der neuesten Version reproduzieren

Wenn Sie eine der Komponenten in Ihrer Umgebung aktualisiert haben, seit Sie auf das Problem gestoßen sind, versuchen Sie jetzt, das Problem zu reproduzieren.

Protokolle erfassen

- Wenn sich das Problem auf XenServer bezieht, erfassen Sie einen Serverstatusbericht (SSR) des Hosts oder Pools, auf dem das Problem aufgetreten ist. Gehen Sie zum XenCenter **Tools-Menü** und dann zum **Serverstatusbericht**.
- Wenn sich das Problem auf XenCenter bezieht:
  - Rufen Sie die Anwendungsprotokolldateien ab, indem Sie im XenCenter **Hilfemenü** auf **XenCenter-Protokolldateien anzeigen** gehen.
  - Erfassen Sie Screenshots der relevanten Displays.
- Wenn sich das Problem auf eine VM bezieht, sammeln Sie alle relevanten Protokolle aus dem VM-Betriebssystem.

Support kontaktieren

Methoden, um mit uns in Kontakt zu treten, finden Sie auf der XenServer-Supportseite.

Stellen Sie zur Unterstützung die folgenden Informationen bereit:

- Datum und Uhrzeit des Auftretens des Problems
- Pool-Updatekanal (Early Access oder Normal)
- Name des Poolkoordinators
- Datum und Uhrzeit der letzten Synchronisierung des Pools
- Synchronisierungsprüfsumme für den Poolkoordinator
- Datum und Uhrzeit der letzten Aktualisierung des Pools
- Prüfsumme für alle Hosts im Pool aktualisieren
- Alle relevanten Screenshots zur Beschreibung des Problems
- Jede Änderung oder jedes Ereignis, das das Problem ausgelöst haben könnte
- Jede bekannte Problemumgehung
- Alle diagnostischen Schritte, die Sie bereits unternommen haben
- Das SSR für den Problempool
- Falls zutreffend, die XenCenter-Protokolle

> **Hinweis:**
>
> Wenn Sie das Problem nicht in einem aktuellen Pool reproduzieren können, fügen Sie das

> SSR bei, das Sie erfasst haben, als das Problem zum ersten Mal aufgetreten ist, und erläutern Sie, warum Sie nicht alle Updates anwenden konnten.

Geben Sie Feedback für XenServer und XenCenter

Helfen Sie uns, unser Produkt zu verbessern, indem Sie uns Feedback zu den Funktionen und der Benutzerfreundlichkeit unserer neuen Version geben. Um Feedback zu geben, wenden Sie sich nicht an den technischen Support, sondern senden Sie stattdessen eine Feedback-E-Mail. Benutzer der Trial Edition können einen Bug über das Bugs-Portal melden.

Senden Sie eine Feedback-E-Mail

Senden Sie Feedback und Fragen per E-Mail an feedback@xenserver.com. Damit wir den vollständigen Kontext Ihrer Situation verstehen können, stellen Sie sicher, dass Sie die folgenden Informationen in Ihre Feedback-E-Mail aufnehmen:

- Dein voller Name
- Ihr Unternehmen oder Geschäft
- Ihr geografischer Standort
- Ihr Lizenztyp
- Die Anzahl der Hosts in Ihrer Produktionsbereitstellung
- Das Gastbetriebssystem, bei dem das Problem aufgetreten ist (Windows oder Linux)

Verwenden Sie diese E-Mail-Adresse nicht, um technischen Support anzufordern.

Einen Bug melden (Nutzer der Trial Edition)

> **Hinweis:**
>
> Wenn Sie ein Premium Edition- oder Standard Edition-Kunde sind, verwenden Sie das Bugs-Portal nicht, um Unterstützung anzufordern. Ihr Problem wird schneller behoben, indem Sie sich an den technischen Support wenden. Weitere Informationen finden Sie auf der XenServer-Supportseite.

Um einen Bug zu melden, reichen Sie ein Ticket über das XenServer 8 Bugs-Portal ein.

- Erstellen Sie ein Konto im XenServer 8 Bugs-Portal. Stellen Sie bei der Erstellung Ihres Kontos sicher, dass Sie eine gültige kontaktierbare E-Mail-Adresse verwenden. Obwohl wir uns bemühen, Ihnen auf dem Ticket zu antworten, kann es manchmal erforderlich sein, dass wir Sie direkt per E-Mail kontaktieren.

- Melden Sie einen Bug im XenServer 8 Bugs-Portal, indem Sie auf **Problem auf XenServer melden** klicken.

Probleme, die über das XenServer 8 Bugs-Portal gemeldet wurden, werden geprüft und Sie werden möglicherweise kontaktiert, wenn das Problem untersucht werden muss.

Hinweise zu Drittanbietern

September 19, 2023

Diese Version von XenServer enthält Software von Drittanbietern, die unter verschiedenen Lizenzen lizenziert ist.

Informationen zum Extrahieren der Lizenzinformationen aus Ihrem installierten XenServer-Produkt und den installierten XenServer-Komponenten finden Sie in den Anweisungen unter XenServer Open Source Licensing and Attribution.

Beachten Sie außerdem die folgenden Informationen:

- Dieses Produkt enthält Software, die vom OpenSSL Project für die Verwendung im OpenSSL Toolkit entwickelt wurde. (http://www.openssl.org/)
- Dieses Produkt enthält kryptografische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.
- XenServer High Availability wird von everRun, einer eingetragenen Marke von Stratus Technologies Bermuda, Limited, betrieben.

XenServer Open-Source-Lizenzierung und Zuordnung

April 12, 2024

Das XenServer-Produkt ist eine Zusammenstellung von Softwarepaketen. Jedes Paket unterliegt einer eigenen Lizenz. Die vollständigen Lizenzbedingungen, die für ein bestimmtes Paket gelten, finden Sie im Quell-RPM des Pakets, sofern das Paket nicht durch eine proprietäre Lizenz abgedeckt ist, die eine Weiterverbreitung der Quellen nicht zulässt. In diesem Fall wird kein Quell-RPM zur Verfügung gestellt.

Die XenServer-Distribution enthält Inhalte von CentOS Linux und CentOS Stream. Wo das CentOS-Projekt ein Copyright an den Paketen besitzt, aus denen die CentOS Linux- oder CentOS Stream-Distributionen besteht, ist dieses Copyright unter der GPLv2-Lizenz lizenziert, sofern nicht anders

angegeben. Weitere Informationen finden Sie unter https://www.centos.org/legal/licensing-policy/.

Extrahieren von Zuordnungs- und Lizenzinformationen auf einem installierten XenServer-Host

Dieser Artikel enthält eine Methode zum Extrahieren der Lizenzinformationen aus allen RPM-Paketen, die in Ihrer XenServer-Installation enthalten sind.

Übersichtsinformationen abrufen

So listen Sie alle RPMs und ihre Lizenzen auf:

1. Stellen Sie über SSH oder XenCenter eine Verbindung zu Ihrer XenServer-Hostkonsole her.
2. Führen Sie an der Konsolenbefehlszeile den folgenden Befehl aus:

```
rpm -qa --qf '%{
 name }
 -%{
 version }
 : %{
 license }
 \n'
```

Dieser Befehl listet alle installierten Komponenten und die Lizenzen auf, unter denen sie verteilt werden. Die Ausgabe hat folgende Form:

```
readline-6.2: GPLv3+
gnupg2-2.0.22: GPLv3+
libdb-5.3.21: BSD and LGPLv2 and Sleepycat
rpm-python-4.11.3: GPLv2+
sqlite-3.7.17: Public Domain
qrencode-libs-3.4.1: LGPLv2+
libselinux-2.5: Public Domain
ustr-1.0.4: MIT or LGPLv2+ or BSD
gdbm-1.10: GPLv3+
procps-ng-3.3.10: GPL+ and GPLv2 and GPLv2+ and GPLv3+ and LGPLv2+
p11-kit-trust-0.23.5: BSD
device-mapper-libs-1.02.149: LGPLv2
xenserver-release-8.2.50: GPLv2
elfutils-libs-0.170: GPLv2+ or LGPLv3+
xz-libs-5.2.2: LGPLv2+
dbus-1.10.24: (GPLv2+ or AFL) and GPLv2+
elfutils-libelf-0.170: GPLv2+ or LGPLv3+
systemd-sysv-219: LGPLv2+
jemalloc-3.6.0: BSD
<!--NeedCopy-->
```


Holen Sie sich detaillierte Informationen

Um eine vollständigere Liste von Informationen zu jeder installierten Komponente zu erhalten:

1. Stellen Sie über SSH oder XenCenter eine Verbindung zu Ihrer XenServer-Hostkonsole her.
2. Führen Sie an der Konsolenbefehlszeile den folgenden Befehl aus:

```
rpm -qai | sed '/^Name /i\\n'
```

Die Ausgabe hat folgende Form:

```
Name: host-upgrade-plugin
Version     : 2.2.6
Release     : 1.xs8
Architecture: noarch
Install Date: Wed 23 Aug 2023 01:54:25 PM UTC
Group: Unspecified
Size: 101626
License     : GPL
Signature   : RSA/SHA256, Tue 30 May 2023 10:01:44 AM UTC, Key ID
   5259d0b0f6529a4e
Source RPM  : host-upgrade-plugin-2.2.6-1.xs8.src.rpm
Build Date  : Fri 26 May 2023 03:05:49 AM UTC
Build Host  : cf27e1dd25c54cbb8cef79726ed2bf2c
Relocations : (not relocatable)
Packager    : Koji
Vendor      : Cloud Software Group, Inc.
Summary     : Host upgrade plugin
Description :
Host upgrade plugin.

Name        : m4
Version     : 1.4.16
Release     : 10.el7
Architecture: x86_64
Install Date: Wed 23 Aug 2023 01:52:31 PM UTC
Group       : Applications/Text
Size        : 525707
License     : GPLv3+
Signature   : RSA/SHA256, Tue 09 May 2023 02:53:25 PM UTC, Key ID
   5259d0b0f6529a4e
Source RPM  : m4-1.4.16-10.el7.src.rpm
Build Date  : Fri 20 Nov 2015 07:28:07 AM UTC
Build Host  : worker1.bsys.centos.org
Relocations : (not relocatable)
Packager    : CentOS BuildSystem <http://bugs.centos.org>
Vendor      : CentOS
URL         : http://www.gnu.org/software/m4/
Summary     : The GNU macro processor
Description :
A GNU implementation of the traditional UNIX macro processor.  M4
   is
```



```
39 useful for writing text files which can be logically parsed, and
      is used
40 by many programs as part of their build process.  M4 has built-in
41 functions for including files, running shell commands, doing
      arithmetic,
42 etc.  The autoconf program needs m4 for generating configure
      scripts, but
43 not for running configure scripts.
44 <!--NeedCopy-->
```

Holen Sie sich mehr Informationen

In den meisten Fällen sind weitere Informationen zu jeder Komponente und der vollständige Lizenztext entweder in /usr/share/doc/ oder /usr/share/licensesinstalliert.

Sie können beispielsweise weitere Informationen über die Komponente jemalloc-3.6.0 finden, indem Sie den folgenden Befehl ausführen:

```
1 ls -l /usr/share/doc/jemalloc-3.6.0/
2
3 total 120
4 -rw-r--r--. 1 root root   1703 Mar 31  2014 COPYING
5 -rw-r--r--. 1 root root 109739 Mar 31  2014 jemalloc.html
6 -rw-r--r--. 1 root root   1084 Mar 31  2014 README
7 -rw-r--r--. 1 root root     50 Mar 31  2014 VERSION
```

Für einige von CentOS vertriebene Komponenten ist der Lizenztext jedoch nicht im XenServer-Produkt installiert. Um den Lizenztext für diese Komponenten anzuzeigen, können Sie in die Quell-RPMs schauen. Wir stellen die Quell-RPMs für den XenServer-Host an den folgenden Orten zur Verfügung:

- Für die erste Produktversion werden die Quelldateien auf der XenServer-Downloadseitebereitgestellt.
- Für alle Updates oder Hotfixes der ersten Version werden aktualisierte Quelldateien im entsprechenden Artikel auf der Citrix Support-Sitebereitgestellt.

Der Name der Quelldatei für eine bestimmte Komponente wird durch den Wert “Source RPM”in der detaillierten Informationsausgabe angegeben. Beispiel:

```
1 Source RPM : m4-1.4.16-10.el7.src.rpm
2 <!--NeedCopy-->
```

Mehrfache Lizenzen

Einige Komponenten des XenServer-Produkts enthalten mehrere Lizenzen. procps-ng-3.3.10 enthält zum Beispiel die folgenden Teile:

- einige Teile, die mit der ursprünglichen GPL (oder einer späteren Version) lizenziert sind
- einige Teile, die mit der GPL Version 2 lizenziert sind (nur)
- einige Teile, die mit der GPL Version 2 (oder einer späteren Version) lizenziert sind
- einige Teile, die mit der GPL Version 3 (oder einer späteren Version) lizenziert sind
- einige Teile, die mit der LGPL Version 2 (oder einer späteren Version) lizenziert sind

Prüfen Sie in diesem Fall die Dokumentation in `/usr/share/doc/procps-ng-3.3.10` auf weitere Informationen oder, falls erforderlich, das entsprechende Quellen-RPM.

Andere XenServer-Komponenten

Zusätzliche Packungen

Zusätzliche Pakete werden auf dem XenServer-Host installiert. Wenn Sie zusätzliche Pakete auf Ihrem Host installiert haben, sind deren RPM-Informationen enthalten, wenn Sie die Schritte im vorherigen Abschnitt dieses Artikels ausführen.

Die Quelldateien für Zusatzpakete finden Sie auch auf der XenServer-Downloadseite.

XenCenter

Führen Sie die folgenden Schritte aus, um Informationen zu in XenCenter enthaltenen Komponenten von Drittanbietern anzuzeigen:

1. Gehen Sie in XenCenter zu **Hilfe > Über XenCenter**.
2. Klicken Sie auf **Rechtliche Hinweise anzeigen**.

XenServer VM-Tools für Windows

Die XenServer VM Tools für Windows bestehen aus den folgenden Komponenten:

- Der Management Agent, der durch eine proprietäre Lizenz abgedeckt ist.
- Die Windows I/O-Treiber, die von der BSD2-Lizenzabgedeckt sind. Copyright Cloud Software Group, Inc.

  Lizenzinformationen sind in der INF-Datei für jeden Treiber enthalten. Wenn die Treiber von Windows Update oder dem Management-Agent-Installationsprogramm auf Ihrem Windows-System installiert werden, werden die INF-Dateien als gespeichert `C:\Windows\INF\OEM*.inf`. Das Management-Agent-Installationsprogramm speichert auch die INF-Dateien in `C:\Program Files\XenServer\XenTools\Drivers\***.inf`.

Die Quelle wurde für XenServer VM Tools für Windows nicht bereitgestellt.

XenServer VM Tools für Linux

Die XenServer VM Tools für Linux sind durch die BSD2-Lizenzabgedeckt. Copyright Cloud Software Group, Inc.

Die auf der Produkt-Downloadseite bereitgestellte Archivdatei enthält die Lizenzdatei und die Quelldateien für die Tools.

Virtuelle Appliances

Die folgenden virtuellen Appliances werden als optionale Komponenten für Ihre XenServer-Umgebung bereitgestellt:

- Virtuelles XenServer Conversion Manager-Appliance
- Virtuelle Appliance für den Workloadausgleich

Diese virtuellen Appliances basieren ebenfalls auf CentOS. Sie können dieselben Befehle wie für den XenServer-Host verwenden, um einen Überblick und detaillierte Informationen zu den in den virtuellen Appliances enthaltenen Open-Source-Paketen zu erhalten.

Führen Sie in der Konsole der virtuellen Appliance die folgenden Befehle aus:

- Für Übersichtsinformationen: `rpm -qa --qf '%{ name } -%{ version } : %{ license } \n'`
- Für ausführliche Informationen: `rpm -qai | sed '/^Name /i\\n'`

Darüber hinaus verwenden die virtuelle XenServer Conversion Manager-Appliance und die virtuelle Workload Balancing-Appliance dynamisch einige Komponenten von Drittanbietern.

- Für das virtuelle XenServer Conversion Manager-Appliance befinden sich die Lizenzdateien für diese Komponenten im folgenden Pfad: `/opt/vpxxcm/conversion`.
- Für die virtuelle Workload Balancing-Appliance befinden sich die Lizenzdateien für diese Komponenten unter dem folgenden Pfad: `/opt/vpx/wlb`.

Quelldateien für die virtuellen Appliances finden Sie auf der XenServer-Downloadseite.

Data Governance

April 12, 2024

Dieser Artikel enthält Informationen zur Erfassung, Speicherung und Aufbewahrung von Protokollen durch XenServer.

XenServer ist eine Servervirtualisierungsplattform, mit der der Kunde eine Bereitstellung virtueller Maschinen erstellen und verwalten kann. XenCenter ist die Management-Benutzeroberfläche für XenServer. XenServer und XenCenter können Kundendaten im Rahmen der Bereitstellung der folgenden Funktionen sammeln und speichern:

- **Telemetrie** —Die Telemetriefunktion überträgt grundlegende Lizenzinformationen über einen XenServer-Pool. XenServer sammelt diese grundlegenden Lizenzdaten, soweit dies für seine legitimen Interessen, einschließlich der Einhaltung der Lizenzbestimmungen, erforderlich ist.
- **Serverstatusberichte** —Ein Serverstatusbericht kann bei Bedarf generiert und auf Citrix Insight Services hochgeladen oder dem Support zur Verfügung gestellt werden. Der Serverstatusbericht enthält Informationen, die Ihnen bei der Diagnose von Problemen in Ihrer Umgebung helfen können.
- **Automatische Updates für den Management Agent** —**Der Management Agent** wird innerhalb von VMs ausgeführt, die auf einem XenServer-Host oder -Pool gehostet werden. Wenn der Server oder Pool lizenziert ist, kann der Management Agent nach Updates für sich selbst und für die I/O-Treiber in der VM suchen und diese anwenden. Im Rahmen der Suche nach Updates sendet die automatische Update funktion eine Webanfrage an die Cloud Software Group, die die VM identifizieren kann, auf der der Management Agent ausgeführt wird.
- **XenCenter nach Updates suchen** —Dieses Feature bestimmt, ob Hotfixes, kumulative Updates oder neue Releases für die XenServer-Hosts und Pools verfügbar sind, die XenCenter verwaltet. Im Rahmen der Suche nach Updates sendet diese Funktion eine Webanfrage an Citrix, die Telemetrie umfasst. Diese Telemetrie ist nicht benutzerspezifisch und wird verwendet, um die Gesamtzahl der XenCenter-Instanzen weltweit zu schätzen.
- **XenCenter E-Mail-Warnungen** XenCenter kann so konfiguriert werden, dass E-Mail-Benachrichtigungen gesendet werden, wenn Warnungsschwellenwerte überschritten werden. Um diese E-Mail-Warnungen zu senden, sammelt und speichert XenCenter die Ziel-E-Mail-Adresse.

Telemetrieinformationen, die von der Cloud Software Group empfangen werden, werden gemäß unseren Vereinbarungenbehandelt.

Telemetrie

Die XenServer-Telemetriefunktion sammelt grundlegende Lizenzinformationen zu Ihren XenServer-Pools.

Wenn Sie XenServer installieren, sammelt Ihr Poolkoordinator Telemetriedaten und lädt sie wöchentlich in eine Microsoft Azure Cloud-Umgebung in den USA hoch. Diese Daten identifizieren keine Personen oder Kunden und werden sicher über HTTPS auf Port 443 an `https://telemetry`

`.ops.xenserver.com/` gesendet. Es werden keine anderen Informationen als die vier unten aufgeführten Elemente gesammelt oder übertragen.

Der Zugriff auf diese Daten ist auf Mitglieder der Teams für Betrieb und Produktmanagement von XenServer beschränkt.

Telemetrieinformationen, die von der Cloud Software Group empfangen werden, werden gemäß unseren Vereinbarungenbehandelt.

Telemetrie gesammelt

Für jeden XenServer-Pool sammelt der Poolkoordinator die folgenden Daten:

Erfasste Daten	Beschreibung
UUID	Eine zufällige eindeutige ID für die Telemetriedaten dieses Pools. Diese UUID ist nicht identisch mit der Pool-UUID oder einem anderen vorhandenen Bezeichner. Es wird nicht in Serverstatusberichten gesammelt.
Produktversion	Die Version von XenServer, die in diesem Pool installiert ist.
Sockets (pro Host)	Die Anzahl der Sockets, die dieser Host hat.
Edition (pro Host)	Der Lizenztyp auf diesem Host.

Diese Daten identifizieren keine Personen oder Kunden und enthalten keine personenbezogenen Daten.

Telemetriedaten anzeigen

Die Daten, die XenServer übermittelt, sind bei Ihrem Poolkoordinator angemeldet. `/var/telemetry/telemetry.data` Diese Datei wird nicht in den Serverstatusprotokollen gesammelt.

Serverstatusberichte

Während des Betriebs sammelt und protokolliert ein XenServer-Host verschiedene Informationen auf dem Server, auf dem XenServer installiert ist. Diese Protokolle können als Teil eines Serverstatusberichts gesammelt werden.

Ein Serverstatusbericht kann bei Bedarf generiert werden. Sie können diese Berichte auf Citrix Insight Services hochladen oder sie dem Support zur Verfügung stellen. Der Serverstatusbericht enthält Informationen, die Ihnen bei der Diagnose von Problemen in Ihrer Umgebung helfen können.

Serverstatusberichte, die zu Citrix Insight Services hochgeladen werden, werden in Amazon S3-Umgebungen in den USA gespeichert.

XenServer und XenCenter sammeln Informationen aus den folgenden Datenquellen:

- XenCenter
- XenServer-Hosts und -Pools
- Gehostete virtuelle Maschinen

Sie können auswählen, welche Datenelemente in den Serverstatusberichten enthalten sind. Sie können auch alle Serverstatusberichte löschen, die auf Ihr MyCitrix-Konto in Citrix Insight Services hochgeladen wurden.

Citrix Insight Services implementiert keine automatische Datenspeicherung für vom Kunden hochgeladene Serverstatusberichte. Der Kunde legt die Datenaufbewahrungsrichtlinie fest. Sie können sich dafür entscheiden, alle Serverstatusberichte zu löschen, die in Ihr MyCitrix-Konto auf Citrix Insight Services hochgeladen wurden.

Erfasste Daten

Ein Serverstatusbericht kann die folgenden Protokolldateien enthalten:

Typ des Protokolls	Enthält PII?
`device-model`	Ja
`fcoe`	Ja
`firstboot`	Ja
`network-status`	Ja
`process-list`	Ja
`xapi`	Ja
`xenserver-databases`	Ja
`control-slice`	vielleicht
`disk-info`	vielleicht
`hardware-info`	vielleicht
`high-availability`	vielleicht

Typ des Protokolls	Enthält PII?
host-crashdump-logs	vielleicht
kernel-info	vielleicht
loopback-devices	vielleicht
message-switch	vielleicht
multipath	vielleicht
system-logs	vielleicht
v6d	vielleicht
xapi-clusterd	vielleicht
xapi-debug	vielleicht
xcp-rrdd-plugins	vielleicht
xen-info	vielleicht
xenopsd	vielleicht
xenserver-config	vielleicht
xenserver-install	vielleicht
xenserver-logs	vielleicht
xha-liveset	vielleicht
yum	Wenn angepasst
network-config	Wenn angepasst
cron	Wenn angepasst
blobs	no
block-scheduler	no
boot-loader	no
conntest	no
CVSM	no
pam	no
system-services	no
tapdisk-logs	no
VM-snapshot-schedule	no
xapi-subprocess	no

Typ des Protokolls	Enthält PII?
`xen-bugtool`	no
`xenserver-domains`	no

Automatische Updates des Management Agents

Der Management Agent wird innerhalb von VMs ausgeführt, die auf einem XenServer-Host oder -Pool gehostet werden. Wenn der Host oder Pool lizenziert ist, kann der Management Agent nach Updates für sich selbst und die I/O-Treiber in der VM suchen und diese anwenden. Im Rahmen der Suche nach Updates sendet die automatische Update funktion eine Webanfrage an uns, mit der die VM identifiziert werden kann, auf der der Management Agent ausgeführt wird.

Die Webprotokolle, die aus den Anforderungen der Funktion für automatische Updates des Management Agents erfasst werden, befinden sich in einer Microsoft Azure Cloud-Umgebung in den USA. Diese Protokolle werden dann auf einen Protokollverwaltungsserver im Vereinigten Königreich kopiert.

Die Webanforderungen, die von der Funktion für automatische Updates des Management Agents gestellt werden, werden über HTTPS gestellt. Webprotokolldateien werden sicher zum Protokollverwaltungsserver übertragen.

Sie können auswählen, ob Ihre VM die automatische Updatefunktion des Management Agents verwendet. Wenn Sie die automatische Updatefunktion des Management Agents verwenden möchten, können Sie auch festlegen, ob die Webanforderung die Informationen zur Identifizierung des virtuellen Rechners enthält.

Webprotokolle mit Informationen aus Webanforderungen, die von der Funktion für automatische Updates des Management Agents und der XenCenter Funktion zur Suche nach Updates gestellt wurden, können auf unbestimmte Zeit aufbewahrt werden.

Erfasste Daten

Die Webanforderungen für automatische Updates des Management Agents können die folgenden Datenpunkte enthalten:

Erfasste Daten	Beschreibung	Verwendungszweck
IP-Adresse	Die IP-Adresse der VM, auf der der Management Agent installiert ist	

Erfasste Daten	Beschreibung	Verwendungszweck
Teilweise VM-UUID	Die ersten vier Zeichen der eindeutigen Benutzer-ID für die VM, auf der der Management Agent installiert ist	

XenCenter sucht nach Updates

Dieses Feature bestimmt, ob Hotfixes, kumulative Updates oder neue Releases für die XenServer-Hosts und -Pools verfügbar sind, die XenCenter verwaltet. Im Rahmen der Suche nach Updates sendet diese Funktion eine Webanfrage an die Cloud Software Group, die Telemetrie beinhaltet. Diese Telemetrie identifiziert Benutzer nicht persönlich und wird verwendet, um die Gesamtzahl der XenCenter-Instanzen weltweit zu schätzen.

Die Webprotokolle, die aus den Anfragen der XenCenter-Funktion "Nach Updates suchen"erfasst wurden, befinden sich in einer Microsoft Azure Cloud-Umgebung in den USA. Diese Protokolle werden dann auf einen Protokollverwaltungsserver im Vereinigten Königreich kopiert.

Die Webanfragen der XenCenter-Funktion "Nach Updates suchen"werden über HTTPS gestellt. Webprotokolldateien werden sicher zum Protokollverwaltungsserver übertragen.

Die XenCenter Funktion zum Suchen nach Updates ist standardmäßig aktiviert. Sie können diese Funktion deaktivieren.

Erfasste Daten

Die Webanfragen der Funktion "Nach Updates suchen"enthalten die folgenden Datenpunkte:

Erfasste Daten	Beschreibung	Verwendungszweck
IP-Adresse	Die IP-Adresse der XenCenter-Hostmaschine	
XenCenter Version	Die Version von XenCenter, die die Anfrage stellt	

XenCenter E-Mail-Warnungen

XenCenter kann so konfiguriert werden, dass E-Mail-Benachrichtigungen gesendet werden, wenn Warnschwellenwerte überschritten werden. Um diese E-Mail-Warnungen zu senden, sammelt und speichert XenCenter die Ziel-E-Mail-Adresse.

Die E-Mail-Adresse, die XenCenter zum Senden von E-Mail-Warnungen verwendet, ist auf dem Computer gespeichert, auf dem Sie XenCenter installiert haben.

Sie können in XenCenter konfigurierte E-Mail-Warnungen löschen, um die gespeicherten E-Mail-Informationen zu entfernen.

XenCenter behält die E-Mail-Informationen, die zum Bereitstellen von E-Mail-Warnungen für die gesamte Lebensdauer der E-Mail-Benachrichtigung verwendet werden. Wenn Sie die konfigurierte E-Mail-Warnung löschen, werden die Daten entfernt.

Erfasste Daten

Um E-Mail-Benachrichtigungen bereitzustellen, speichert XenCenter die folgenden Datenpunkte:

Erfasste Daten	Beschreibung	Verwendungszweck
E-Mail-Adresse	Die E-Mail-Adresse für Benachrichtigungen	Um Warn- und Benachrichtigungs-E-Mails zu senden an
SMTP-Server	Der zu verwendende SMTP-Server	Um die E-Mail-Benachrichtigungen an den Empfänger weiterzuleiten