Citrix Hypervisor 8.0

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Citrix Dokumentation maschinell übersetzt. Citrix hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Citrix Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Citrix gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Citrix kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Aktuelle Version von Citrix Hypervisor 8.1

January 22, 2020

Die Technologie, die Sie von XenServer, dem Hochleistungs-Hypervisor, der für virtuelle App- und Desktop-Workloads optimiert ist und auf dem Xen Project-Hypervisor basiert, ist jetzt Citrix Hypervisor.

Citrix Hypervisor 8.1 ist die neueste Version der aktuellen Version von Citrix Hypervisor. Diese Dokumentation enthält Funktionen und Konfigurationen in dieser neuesten Version. Weitere Informationen zu den neuen Features in Citrix Hypervisor 8.1 finden Sie unter Neue Features.

Frühere Versionen

Dokumentation zu unterstützten früheren Versionen finden Sie unter:

- Citrix Hypervisor 8.0 CR
- XenServer 7.1 LTSR
- XenServer 7.0

Die Dokumentation für Citrix Hypervisor- und XenServer Releases, die nicht mehr unterstützt werden, wird im Bereich Legacy-Dokumentation archiviert.

Die Citrix Hypervisor Produktlebenszyklusstrategie für aktuelle und langfristige Serviceversionen wird unter beschrieben Lebenszyklus-Meilensteine für Citrix Hypervisor.

Informationen zu Citrix Hypervisor

Citrix Hypervisor ist die komplette Servervirtualisierungsplattform von Citrix. Das Citrix Hypervisor Paket enthält alles, was Sie benötigen, um eine Bereitstellung virtueller x86-Computer zu erstellen und zu verwalten, die auf Xen ausgeführt werden, dem Open-Source-Paravirtualisierender Hypervisor mit nahezu nativer Leistung. Citrix Hypervisor ist für virtuelle Windows- und Linux-Server optimiert.

Citrix Hypervisor wird direkt auf Serverhardware ausgeführt, ohne dass ein zugrunde liegendes Betriebssystem erforderlich ist. Dies führt zu einem effizienten und skalierbaren System. Citrix Hypervisor kann Elemente von der physischen Maschine (z. B. Festplatten, Ressourcen und Ports) abstrahieren und sie den *virtuellen Maschinen* zuweisen, die auf dem Computer ausgeführt werden.

Eine virtuelle Maschine (VM) ist ein Computer, der vollständig aus Software besteht, der sein eigenes Betriebssystem und Anwendungen wie ein physischer Computer ausführen kann. Eine VM verhält sich genau wie ein physischer Computer und enthält eine eigene virtuelle (softwarebasierte) CPU, RAM, Festplatte und NIC.

Mit Citrix Hypervisor können Sie VMs erstellen, VM-Festplatten-Snapshots erstellen und VM-Workloads verwalten. Eine umfassende Liste der wichtigsten Citrix Hypervisor-Funktionen finden Sie unter https://www.citrix.com/products/citrix-hypervisor/.

XenCenter

XenCenter ist ein Windows-GUI-Client, der eine umfassende Benutzererfahrung bei der Verwaltung mehrerer Citrix Hypervisor-Server und Ressourcenpools sowie der damit verbundenen virtuellen Infrastruktur bietet. Weitere Informationen finden Sie unter XenCenter Dokumentation.

Kopiert!
Failed!

Neue Features

October 16, 2019

Über diese Version

Die Technologie, die Sie von XenServer, dem Hochleistungs-Hypervisor, der für virtuelle App- und Desktop-Workloads optimiert ist und auf dem Xen Project-Hypervisor basiert, ist jetzt Citrix Hypervisor.

Citrix Hypervisor 8.0 ist eine aktuelle Version (CR). Mit dem Modell „Aktuelle Version“ können Kunden neue Features zum frühestmöglichen Zeitpunkt nutzen. Eine aktuelle Version steht im Gegensatz zur Long Term Service Release (XenServer 7.1 LTSR), die Stabilität in Bezug auf die Funktionsgruppe garantiert.

Citrix Hypervisor 8.0 ist in den folgenden Editionen verfügbar:

- Premium Edition (zuvor Enterprise Edition)
- Standard Edition
- Express Edition (bisher Free Edition)

Informationen zu den Funktionen, die in jeder Edition verfügbar sind, finden Sie imCitrix Hypervisor Feature-Matrix.

Neue Funktionen und Verbesserungen in Citrix Hypervisor 8.0

Citrix Hypervisor 8.0 bietet erweiterte Funktionen und Funktionen für Anwendungsfälle, Desktop- und Servervirtualisierung. Alle Citrix Hypervisor 8.0 Funktionen stehen allen lizenzierten Citrix Virtual

Apps and Desktops (ehemals XenApp und XenDesktop) Kunden zur Verfügung.

Plattformaktualisierung

Die Citrix Hypervisor Plattform wurde aktualisiert, um die folgende Software zu verwenden:

- Kernel-Version: Linux 4.14
- Xen Hypervisor-Version: 4.11
- Steuerdomäne Betriebssystemversion: CentOS 7.5

Im Rahmen des Updates auf die Kernel-Version hat sich die Speichermenge erhöht, die der Steuerdomäne (dom0) zugewiesen wurde. Weitere Informationen finden Sie unter Speichernutzung.

Die Kernel-Gerätetreiber wurden ebenfalls auf neuere Versionen aktualisiert. Einige Hardware, die in früheren Versionen unterstützt wurde, funktioniert möglicherweise nicht mit den neueren Treibern. Überprüfen Sie die Hardwarekompatibilitätslistevor dem Upgrade auf Citrix Hypervisor 8.0.

Darüber hinaus wurden die folgenden mit Citrix Hypervisor bereitgestellten Appliances aktualisiert, um CentOS 7.5 als Basisbetriebssystem zu verwenden:

- Citrix Hypervisor Konvertierungsmanager
- Virtuelle Appliance für den Arbeitslastausgleich
- Virtuelle Demo-Linux-Appliance

Änderungen an der Unterstützung des Gastbetriebssystems

Die Gruppe der Gastbetriebssysteme, die von Citrix Hypervisor unterstützt werden, wurde aktualisiert. Weitere Informationen finden Sie unter Unterstützung für Gastbetriebssysteme

Hinzugefügt

Citrix Hypervisor unterstützt jetzt die folgenden zusätzlichen Gastvorlagen:

- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Desktop 15
- CentOS 7.6
- Oracle Linux 7.6
- Red Hat Enterprise Linux 7.6
- Scientific Linux 7.6
- CentOS 6.10
- Oracle Linux 6.10
- Red Hat Enterprise Linux 6.10
- Scientific Linux 6.10
- Windows Server 2019

Entfernt

Wir haben die Unterstützung für die folgenden Gastvorlagen entfernt:

- Debian 6 Squeeze
- Ubuntu 12.04
- 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
- Legacy-Windows

> **Hinweis:**
>
> Mit dem Entfernen der Legacy-Windows Vorlage entfernen wir auch die älteren Windows-Treiber aus dem Citrix VM Tools-ISO.

Sie können vorhandene VMs weiterhin mit diesen Betriebssystemen verwenden. Citrix unterstützt diese VMs jedoch nicht mehr.

Änderungen an der Prozessorunterstützung

Die folgenden Prozessoren werden jetzt in Citrix Hypervisor 8.0 unterstützt:

- Xeon 82xx/62xx/52xx/42xx/32xx Cascadelake-SP

Die folgenden Legacy-Prozessoren werden in Citrix Hypervisor 8.0 nicht mehr unterstützt:

- Opteron 13xx Budapest
- Opteron 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

Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste.

Erstellen von VDIs größer als 2 TiB (Premium Edition)

Sie können jetzt virtuelle Laufwerk-Images erstellen, die größer als 2 TiB auf GFS2 SRs sind.

Online-LUN-Größe für GFS2 SRs (Premium Edition)

Sie können jetzt die Größe der LUNs für GFS2 SRs ändern.

Unterstützung für Festplatten- und Speicher-Snapshots für VGPU-fähige VMs (Premium Edition)

Wenn ein Festplatten- und Speicher-Snapshot einer VGPU-fähigen VM verwendet wird, schließt der Status der VM den vGPU Status ein. Dieser vGPU Status wird wiederhergestellt, wenn die VM aus dem Snapshot fortgesetzt wird.

Webbasierte Hilfe für XenCenter und Citrix Hypervisor Conversion Manager

[Dokumentation fürXenCenter[]undCitrix Hypervisor Konvertierungs-Manager[]ist ab sofort online auf der Citrix Produktdokumentation()Website.]

Diese Online-Dokumentation ersetzt die Hilfe im Produkt. Wenn Sie nun **F1** in der Benutzeroberfläche drücken oder auf die kontextbezogene Hilfe zugreifen möchten, wird der entsprechende Artikel in Ihrem Standardbrowser geöffnet. Diese Artikel stehen auch als PDF zur Offline-Anzeige zur Verfügung. Verwenden Sie die Schaltfläche **PDF anzeigen** , um die PDF herunterzuladen.

Diese webbasierten Artikel bieten Ihnen die genauesten und aktuellsten Inhalte.

Experimentelle Funktionen

Citrix Hypervisor 8.0 enthält die folgende experimentelle Funktion:

- Gast-UEFI-Boot

Weitere Informationen finden Sie unter Experimentelle Funktionen.

Installationsoptionen

Citrix Hypervisor 8.0 kannCitrix Hypervisor Produkt Download-Seiteim folgenden Paket heruntergeladen werden:

- Citrix Hypervisor 8.0 Basisinstallations-ISO. Verwenden Sie diese Datei, um eine Neuinstallation von Citrix Hypervisor 8.0 zu erstellen oder um ein Upgrade von XenServer 7.6, 7.5, 7.1 Kumulatives Update 2 oder 7.0 durchzuführen.

Diese Version von Citrix Hypervisor ist nicht als Update verfügbar.

> **Hinweis:**
>
> - Wenn Sie XenCenter zum Aktualisieren Ihrer Hosts verwenden, aktualisieren Sie die XenCenter-Installation auf die neueste Version, die auf der Downloadseite von Citrix Hypervisor 8.0 bereitgestellt wird, bevor Sie beginnen.
> - Aktualisieren Sie den Poolmaster immer, bevor Sie andere Hosts in einem Pool aktualisieren.
> - Stellen Sie sicher, dass Sie XenServer 7.1 auf kumulative Update 2 aktualisieren, bevor Sie ein Upgrade auf Citrix Hypervisor 8.0 durchführen.

Überprüfen Sie vor Beginn der Installation dieSystemanforderungenundInstallations- und Bereitstellungsszenarien.

Wechsel vom Long Term Service Release zum aktuellen Release

Wenn Sie einen XenServer LTSR ausführen, aber die neuen Funktionen nutzen möchten, können Sie sich entscheiden, in den Citrix Hypervisor CR-Stream zu wechseln. Wenn Sie die Citrix Hypervisor or-Versionen aus dem CR-Stream verwenden, müssen Sie regelmäßig neue CRs übernehmen, um weiterhin Unterstützung zu erhalten.

Wechseln Sie zu dieser aktuellen Version, indem Sie ein Upgrade von XenServer 7.1 Kumulatives Update 2 LTSR durchführen.

Wechsel von der aktuellen Version in den langfristigen Serviceabruf

Wenn Sie einen Citrix Hypervisor CR ausführen, stattdessen jedoch zu einer Version von Citrix Hypervisor mit einem garantierten und stabilen Funktionsumfang wechseln möchten, können Sie zu einem XenServer LTSR wechseln. Die neueste XenServer LTSR steht auf der Seite zum Download des Citrix Hypervisor Produkts zum Download zur Verfügung.

Wechseln Sie zum neuesten LTSR, indem Sie eine Neuinstallation von XenServer 7.1 Kumulatives Update 2 LTSR erstellen.

Weitere Hinweise zu LTSRs und CRs finden Sie unterCitrix Virtual Apps, Citrix Virtual Desktops und Citrix Hypervisor Wartungsoptionen.

Lizenzierung

Kunden müssen ihren Citrix License Server auf Version 11.14 oder höher aktualisieren, um alle lizenzierten Citrix Hypervisor 8.0 nutzen zu können.

Weitere Informationen zur Citrix Hypervisor 8.0 Lizenzierung finden Sie unterLizenzierung.

Hardwarekompatibilität

Die neuesten Ergänzungen und Hinweise zu allen Fragen zur Hardwarekompatibilität finden Sie im Citrix HypervisorHardwarekompatibilitätsliste.

Wenn Sie über VMs mit angeschlossenen virtuellen GPUs verfügen, lesen SieHardwarekompatibilitätslistesowohl die Dokumentation als auch die GPU-Herstellerdokumentation, um sicherzustellen, dass unterstützte Treiber verfügbar sind, bevor Sie auf die neueste Version von Citrix aktualisieren. Hypervisor.

Interoperabilität mit Citrix Produkten

Citrix Hypervisor 8.0 ist mit Citrix XenApp und XenDesktop 7.15 CU3 (LTSR), Citrix Virtual Apps and Desktops 7 1903 sowie Citrix Virtual Apps und Desktops 7 1906 kompatibel.

Citrix Hypervisor 8.0 ist mit Citrix Provisioning 7.15 CU3 und 1903 interoperabel.

Citrix Hypervisor 8.0 ist mit Citrix Cloud kompatibel.

Citrix Produktnamen wechseln mit der Vereinheitlichung unseres Produktportfolios. Weitere Informationen finden Sie unter https://www.citrix.com/about/citrix-product-guide/.

Lokalisierungsunterstützung

Die lokalisierte Version von XenCenter (vereinfachtes Chinesisch und Japanisch) ist ebenfalls in dieser Version verfügbar.

Produktdokumentation

Informationen zum Zugriff auf die Citrix Hypervisor 8.0 Produktdokumentation finden Sie unter Citrix Hypervisor 8.0 — Produktdokumentation. Häufig gestellte Fragen zu Citrix Hypervisor finden Sie unterTechnische Übersicht.

Die Dokumentation kann nach der ersten Veröffentlichung aktualisiert oder geändert werden. Wir empfehlen Ihnen, regelmäßig denCitrix Produktdokumentationzu besuchen, um mehr über Updates zu erfahren.

Kopiert!
Failed!

Experimentelle Funktionen

October 16, 2019

Experimentelle Funktionen sind nicht für den Einsatz in Produktionsumgebungen geeignet. Citrix bietet keine Garantie, dass die experimentellen Funktionen in einer GA-Version von Citrix Hypervisor verfügbar sind.

Gast-UEFI-Boot

Citrix Hypervisor ermöglicht jetzt das Starten neuer Versionen von Windows Gastbetriebssystemen im UEFI-Modus. UEFI-Boot bietet eine umfassendere Schnittstelle für die Interaktion der Gastbetriebssysteme mit der Hardware, was die Startzeiten für Windows VM erheblich reduzieren kann.

> **Hinweis:**
>
> Gast-UEFI-Boot ist ein experimentelles Feature. Sie können UEFI-fähige VMs auf Hosts erstellen, die sich in einer Produktionsumgebung befinden. UEFI-fähige VMs dürfen jedoch nicht für Produktionszwecke verwendet werden. Möglicherweise müssen Sie die VMs neu erstellen, wenn Sie den Host auf eine neuere Version von Citrix Hypervisor aktualisieren.

Citrix Hypervisor unterstützt UEFI-Boot auf neu erstellten VMs mit Windows 10 (64-Bit), Windows Server 2016 (64-Bit) und Windows Server 2019 (64-Bit). Beim Erstellen einer VM müssen Sie den Startmodus angeben. Es ist nicht möglich, den Startmodus einer VM nach dem ersten Booten der VM zu ändern.

Berücksichtigen Sie Folgendes, wenn Sie UEFI-Boot auf VMs aktivieren:

- Stellen Sie sicher, dass die UEFI-fähige VM über mindestens zwei vCPUs verfügt.
- Sie können eine UEFI-fähige VM, die auf Citrix Hypervisor erstellt wurde, als OVA-, OVF- oder XVA-Datei importieren oder exportieren. Das Importieren einer UEFI-fähigen VM aus OVF- oder OVF-Paketen, die auf anderen Hypervisoren erstellt wurden, wird nicht unterstützt.
- UEFI-fähige VMs werden von Citrix Machine Creation Services nicht unterstützt.
- GPU-Pass-Through wird nicht unterstützt.
- PVS wird nicht unterstützt.
- Der sichere UEFI-Boot wird nicht unterstützt.
- Verwenden Sie das UEFI-Einstellungsmenü, um die Bildschirmauflösung der XenCenter Konsole zu ändern. Ausführliche Anweisungen finden Sie unter Ändern der Bildschirmauflösung.

UEFI-Boot aktivieren

Sie können XenCenter oder die XE CLI verwenden, um den GUEFI-Boot zu aktivieren.

Verwenden von XenCenter

Wenn Sie eine VM mit dem Assistenten für **neue VM** erstellen, wählen Sie auf der Seite **Installationsmedien** die Option **UEFI-Boot** aus.

> **Hinweis:**
>
> Die Option **UEFI-Boot** wird ausgegraut angezeigt, wenn die ausgewählte VM-Vorlage den UEFI-Boot nicht unterstützt.

Verwenden der XE CLI

Wenn Sie eine VM erstellen, führen Sie den folgenden Befehl aus, bevor Sie die VM zum ersten Mal starten:

```
xe vm-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
```

Wo,`UUID` ist die UUID der VM und`MODE` ist entweder 'BIOS' oder 'UEFI'. Wenn Sie den Modus nicht angeben, wird standardmäßig „BIOS" verwendet.

Führen Sie den folgenden Befehl aus, um eine UEFI-fähige VM aus einer Vorlage zu erstellen:

```
UUID=$(xe vm-clone name-label='Windows 10 (64-bit)'
new-name-label='Windows 10 (64-bit)(UEFI)') xe template-param-set
   uuid=<UUID> HVM-boot-params:firmware=<MODE>
```

Ändern der Bildschirmauflösung

So ändern Sie die Bildschirmauflösung der XenCenter Konsole auf einer UEFI-fähigen VM:

1. Öffnen Sie die **Windows Einstellungen**
2. Klicken Sie auf die Schaltfläche **Aktualisieren und Sicherheit**
3. Drücken Sie unter der Registerkarte Wiederherstellung die Schaltfläche **Jetzt neu starten** .
4. Navigieren Sie zu **Problembehandlung** > **Erweiterte Optionen** > **UEFI-Firmware-Einstellungen** .
5. Drücken Sie **Neu starten**. Beim Neustart wird das UEFI-Einstellungsmenü geladen.
6. Navigieren Sie zu **Device Manager** > **OVMF-Plattformkonfiguration** . Dies zeigt die aktuelle Bildschirmauflösung an.
7. Drücken **Sie die Eingabetaste** , um die Optionen zur 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.

Kopiert!
Failed!

Behobene Probleme

October 16, 2019

Dieser Artikel listet Probleme in früheren Versionen auf, die in dieser Version behoben wurden.

Allgemein

- Wenn Sie einen neuen Host zu einem Clusterpool mit einem VLAN im Clusternetzwerk hinzufügen, wird möglicherweise die Fehlermeldung „Dieser Server benötigt eine (und nur eine) IP-Adresse im Netzwerk, die für das Clustering verwendet wird“ angezeigt. Dies gilt auch, wenn Sie das VLAN über einem gebundenen Clusternetzwerk verfügen. (CA-306864)
- Weisen Sie Dom0 nicht mehr als 32 GB Arbeitsspeicher zu, da ansonsten intermittierende VM-Einfrieren auftreten können, häufig während des Boots von VMs. (CA-236674)
- In Citrix Virtual Desktop Director wurden VM-Konsolen für XenServer 7.5 und XenServer 7.6 nicht angezeigt. (CA-309048)
- Die Webkonsole des Distributed Virtual Switch Controller wird in Firefox, Google Chrome und Microsoft Edge-Browsern nicht ordnungsgemäß geladen. (CA-298945)
- Wenn die virtuelle Demo Linux Appliance zum ersten Mal startet, ruft sie ihre IP-Adresse von einem DHCP-Server ab, selbst wenn Sie angegeben haben, dass sie eine statische IP-Adresse verwendet. (CA-292640)

Grafik

- In XenServer 7.6 funktionieren die RRDs für NVIDIA vGPUs nicht und Diagramme dieser Leistungsmetriken können nicht in XenCenter angezeigt werden. (CA-300751)

Gäste

- Bei der Behebung eines Problems mit Windows 10 1803 VMs wurde ein Leistungsproblem eingeführt. Das Leistungsproblem wurde jetzt behoben. (CA-303359)
- Bei einer VM, die aus der Vorlage „Andere Installationsmedien“ erstellt wurde, startet QEMU nicht und die VM hängt in folgenden Fällen:
  - Wenn Sie die virtuelle Maschine live von einem XenServer 7.5 oder früheren Host auf einen XenServer 7.6-Host migrieren
  - Wenn Sie die VM auf einem XenServer 7.5 oder früheren Host anhalten und versuchen, die VM auf einem XenServer 7.6-Host fortzusetzen

  In diesem Fall wird kein Fehler angezeigt, und die VM wird möglicherweise fälschlicherweise ausgeführt, wenn sie in XenCenter angezeigt wird. (CA-309144)
- VM-Metadatensicherungen können zeitweise fehlschlagen, wenn der VDI für die Pool-Backup-Metadaten voll ist. Die Standardgröße der Pool-Backup-Metadaten VDI wurde auf 500 MB erhöht. (CA-311705)

XenCenter

- Wenn Sie mit XenCenter 7.6 ein Update von einem Drittanbieter mit der Anleitung nach dem Anwenden anwenden`restarthost`, wird der Host am Ende des Prozesses nicht neu gestartet. (CA-298913)
- In XenCenter 7.6 und früheren Versionen hat XenCenter die Erstellung von VDIs nicht verhindert, die größer als die maximal unterstützte Größe sind. (XSI-465)

Kopiert!
Failed!

Bekannte Probleme

October 16, 2019

Dieser Artikel enthält Hinweise und kleinere Probleme in Citrix Hypervisor 8.0 und alle möglichen Problemumgehungen.

Allgemein

- Der CPU-Featuresatz eines Pools kann sich ändern, während eine VM läuft. (Zum Beispiel, wenn ein neuer Host zu einem vorhandenen Pool hinzugefügt wird oder wenn die VM zu einem Host in einem anderen Pool migriert wird.) Wenn sich der CPU-Featuresatz eines Pools ändert, verwendet die VM weiterhin den Featuresatz, der beim Start angewendet wurde. Um die VM so zu aktualisieren, dass sie den neuen Featuresatz des Pools verwendet, müssen Sie die VM ausschalten und dann starten. Beim Neustart der VM, z. B. durch Klicken auf „Neustart“ in XenCenter, wird der Funktionssatz der VM nicht aktualisiert. (CA-188042)
- Die Erhöhung der Speichermenge dom0 in Citrix Hypervisor 8.0 kann dazu führen, dass für die Ausführung von VMs etwas weniger Arbeitsspeicher verfügbar ist. Auf einigen Hardware können Sie möglicherweise nicht dieselbe Anzahl von VMs mit Citrix Hypervisor 8.0 ausführen wie auf derselben Hardware mit einer früheren Version von XenServer. (CP-29627)
- Wenn Sie versuchen, die serielle Konsole für die Verbindung mit einem Citrix Hypervisor or-Server zu verwenden, verweigert die serielle Konsole möglicherweise die Annahme von Tastatureingaben. Wenn Sie warten, bis die Konsole zweimal aktualisiert wird, akzeptiert die Konsole Tastatureingaben. (CA-311613)
- Wenn Sie bei der Verwendung eines Clusterpools dasselbe Netzwerk für die Clusterbildung verwenden wie für die Verwaltung oder den Speicher, kann eine moderate Last dazu führen, dass sich der gesamte Cluster selbst durchsetzt. (CA-312476)

Grafik

- Wenn Sie eine VM, an der eine AMD MxGPU angeschlossen ist, zwangsweise herunterfahren oder das Gastbetriebssystem abnormal heruntergefahren wird, kann es zu Speicherbeschädigungen bei Ihrem Citrix Hypervisor or-Server kommen. Führen Sie ein kooperatives Herunterfahren durch, um sicherzustellen, dass die Hardware während des Herunterfahrens korrekt bereinigt wird. (CA-297891)
- Wenn Sie parallel viele VMs mit angeschlossenen AMD MxGPU-Geräten starten, schlagen einige VMs möglicherweise mit einem VIDEO_TDR_FAILURE fehl. Dies kann auf eine Hardware-Beschränkung zurückzuführen sein. (CA-305555)
- In seltenen Fällen können VMs mit angeschlossenen NVIDIA-VGPUs beim Start der VM in einem gelben Zustand stecken bleiben. Dies wird wahrscheinlich dadurch verursacht, dass einer der VGPUs „Kompatibilitätsmetadaten“ gesetzt hat, wenn dies nicht sollte. Um die Metadaten zu entfernen, halten Sie die VM an und setzen Sie sie fort. (CA-312226)

Gäste

- Auf Citrix Hypervisor Hosts, die den`bnxt_en` Treiber verwenden, können Oracle 6.x-VMs beim Herstellen einer Verbindung mit einem Netzwerk abstürzen. Stellen Sie sicher, dass der`bnxt_en` Treiber auf dem neuesten Stand ist, indem Sie die folgende Treiberdiskette installieren:Treiberdiskette für Broadcom bnxt_en-1.8.29 - Für XenServer 7.x CR (CA-288010)
- In seltenen Fällen kann das Aussetzen oder Migrieren einer Linux-VM mit ausstehenden XenStore-Transaktionen aufgrund eines Problems im Linux-Kernel der VM hängen. Wenn Ihr VM dieses Problem auftritt, zwingen Sie die VM, herunterzufahren, und starten Sie sie neu. (CP-30551)

Internationalisierung

- Nicht-ASCII-Zeichen, z. B. Zeichen mit Akzenten, können in der Host-Konsole nicht verwendet werden. (CA-40845)
- In einer Windows VM mit installierten Citrix VM-Tools kann das Kopieren und Einfügen von Doppelbyte-Zeichen fehlschlagen, wenn die Standarddesktopkonsole in XenCenter verwendet wird. Die eingefügten Zeichen werden als Fragezeichen (?) angezeigt.
  Um dieses Problem zu umgehen, können Sie stattdessen die Remotedesktopkonsole verwenden. (CA-281807)

Speicher

- Wenn Sie GFS2 SRs verwenden und zwei Server in Ihrem Clusterpool haben, kann der Cluster Quorum und Fencing während des Upgrades auf Citrix Hypervisor 8.0 verlieren. Um diese Situation zu vermeiden, entfernen oder fügen Sie einen Server aus dem Cluster hinzu, um sicherzustellen, dass während des Upgradevorgangs entweder ein oder drei Server im Pool vorhanden sind. (CA-313222)
- Wenn Sie das GFS2-Feature zuvor als experimentelles Feature auf XenServer 7.5 verwendet und nicht auf XenServer 7.6 aktualisiert haben, führen Sie beim Aktualisieren von XenServer 7.5 auf Citrix Hypervisor 8.0 die folgenden Schritte aus:

  1. Exportieren Sie alle Daten, die Sie von diesen SRs behalten möchten.
  2. Lösen Sie vor dem Upgrade alle GFS2 SRs von Ihrem Pool ab und zerstören Sie sie.
  3. Deaktivieren Sie das Clustering in Ihrem Pool.
  4. Schließen Sie das Update für Citrix Hypervisor 8.0 ab.
  5. Führen Sie nach Abschluss der Aktualisierung den folgenden Befehl auf allen Hosts in Ihrem Pool aus:


```
```
rm /var/opt/xapi-clusterd/db
```
```

1. Führen Sie den folgenden Befehl auf dem Poolmaster aus:

   ```
   systemctl restart xapi-clusterd
   ```

2. Achten Sie beim Erstellen einer GFS2 SR für Ihren aktualisierten Pool darauf, dass Sie **Format** und nicht **erneut anfügen** auswählen. Sie können eine GFS2 SR, die mit XenServer 7.5 erstellt wurde, nicht erneut an einen Citrix Hypervisor 8.0-Pool anhängen. (CP-29465)

- Ein GFS2 SR kann aufgrund eines asynchronen Plugs des Clusterspeichers eine falsche Warnung „Fehler beim Anhängen von Speicher beim Serverstart“ auslösen. Überprüfen Sie den SR-Status in XenCenter, um festzustellen, ob die Warnung falsch positiv war. (CA-311625)
- Wenn Sie eine GFS2 SR verwenden, stellen Sie sicher, dass Sie Massenspeicher-Multipathing für maximale Ausfallsicherheit aktivieren. Wenn das Speicher-Multipathing nicht aktiviert ist, wird das Schreiben von Dateisystemblockieren möglicherweise nicht rechtzeitig abgeschlossen. (CA-312678)

XenCenter

- Das Ändern der Schriftgröße oder dpi auf dem Computer, auf dem XenCenter ausgeführt wird, kann dazu führen, dass die Benutzeroberfläche falsch angezeigt wird. Die Standardschriftgröße beträgt 96 dpi; Windows 8 und Windows 10 beziehen sich auf diese Schriftgröße als 100%. (CA-45514) (AUTO-1940)
- Wenn XenCenter unter Windows Server 2008 SP2 installiert ist, kann es keine Verbindung zu einem Citrix Hypervisor Host mit der Meldung „Der sichere SSL/TLS-Kanal konnte nicht erstellt werden“. Um dieses Problem zu beheben, stellen Sie sicher, dass eines der folgenden Windows Updates auf dem Windows Server 2008 SP2-System installiert ist: KB4056564 oder KB4019276. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/4019276. (CA-298456)
- Manchmal können Sie mit der XenCenter Massenspeicher-Livemigration oder dem Assistenten zum Importieren von OVF/OVA nicht fortfahren, und die Schaltfläche **Weiter** bleibt deaktiviert. Starten Sie in diesem Fall XenCenter neu, und wiederholen Sie den Vorgang. (CA-314346)

Kopiert!
Failed!

Veraltete und Entfernungen

October 16, 2019

Die Ankündigungen in diesem Artikel sollen Ihnen erweiterte Informationen zu Plattformen, Citrix Produkten und Funktionen vermitteln, die schrittweise abgeschafft werden, damit Sie zeitnah Geschäftsentscheidungen treffen können. Citrix überwacht die Kundenverwendung und das Feedback, um festzustellen, wann sie zurückgezogen werden. Ankündigungen können sich in nachfolgenden Versionen ändern und beinhalten möglicherweise nicht alle veralteten Funktionen oder Funktionen. Weitere Informationen zur Produktlebenszyklusunterstützung finden Sie imProduktlebenszyklus-Support-RichtlinieArtikel.

Verwerfungen

In den folgenden Informationen werden die Hardware, Plattformen, Citrix Produkte und Features aufgeführt, die in Citrix Hypervisor 8.0 veraltet sind. Veraltete Artikel werden nicht sofort entfernt. Citrix unterstützt sie weiterhin in dieser Version, aber sie werden in einer zukünftigen aktuellen Version entfernt.

- Die folgenden Legacy-Treiber:
  - qla4xxx
  - qla3xxx
  - netxen_nic
  - qlge
  - Qlcnic

Einige Hardware, die in früheren Versionen unterstützt wurde, funktioniert möglicherweise nicht, jetzt sind diese Treiber veraltet. Überprüfen Sie die Hardwarekompatibilitätslistevor dem Upgrade auf Citrix Hypervisor 8.0.

Umzüge

In den folgenden Informationen werden die Hardware, Plattformen, Citrix Produkte und Features aufgeführt, die in Citrix Hypervisor 8.0 entfernt werden. Entfernte Elemente werden entweder entfernt oder werden in Citrix Hypervisor nicht mehr unterstützt.

- XenCenter er-Installationsprogramm im Lieferumfang des Citrix Hypervisor Installationsmediums. Laden SieDownload-Seitestattdessen das XenCenter er-Installationsprogramm von herunter.
- XenCenter Verbindungen zu XenServer Hosts ab Version 6.x.

- Unterstützung für die Nutanix Integration.
- Unterstützung für die folgenden Legacy-Prozessoren:
  - Opteron 13xx Budapest
  - Opteron 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

  Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste.
- Unterstützung für qemu-trad. Es ist nicht mehr möglich, qemu-trad durch Einstellung zu verwenden`platform-device-model=qemu-trad`. Alle mit dem qemu-trad-Geräteprofil erstellten VMs werden automatisch auf qemu-upstream-compat-Profil aktualisiert.
- Unterstützung für die folgenden Gastvorlagen, die Betriebssysteme verwenden, die von ihren Anbietern nicht mehr unterstützt werden:
  - Debian 6 Squeeze
  - Ubuntu 12.04
  - Legacy-Windows

    Mit dem Entfernen der Legacy-Windows Vorlage entfernen wir auch die älteren Windows-Treiber aus dem Citrix VM Tools-ISO.
- Unterstützung für die folgenden Gastvorlagen:
  - 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

Kopiert!
Failed!

Systemanforderungen

October 16, 2019

Citrix Hypervisor benötigt mindestens zwei separate physische x86-Computer: einer ist der Citrix Hypervisor or-Server und der andere, um die XenCenter Anwendung oder die Citrix Hypervisor-Befehlszeilenschnittstelle (CLI) auszuführen. Der Citrix Hypervisor-Servercomputer ist ausschließlich der Ausführung von Citrix Hypervisor und dem Hosten von VMs gewidmet und wird nicht für andere Anwendungen verwendet.

> **Warnhinweis:**
>
> Die direkte Installation von Drittanbietersoftware in der Steuerungsdomäne des Citrix Hypervisor wird nicht unterstützt. Die Ausnahme gilt für Software, die als ergänzendes Paket bereitgestellt und von Citrix explizit unterstützt wird.

Verwenden Sie zum Ausführen von XenCenter jedes allgemeine Windows -System, das die Hardwareanforderungen erfüllt. Dieses Windows -System kann verwendet werden, um andere Anwendungen auszuführen.

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

Systemanforderungen für Citrix Hypervisor Server

Obwohl Citrix Hypervisor normalerweise auf Serverhardware bereitgestellt wird, ist Citrix Hypervisor auch mit vielen Modellen von Workstations und Laptops kompatibel. Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste (HCL).

Im folgenden Abschnitt werden die empfohlenen Citrix Hypervisor Hardwarespezifikationen beschrieben.

Der Citrix Hypervisor or-Server muss eine 64-Bit-x86-Serverklasse sein, die dem Hosten von VMs gewidmet ist. Citrix Hypervisor erstellt eine optimierte und gehärtete Linux-Partition mit einem XEN-fähigen Kernel. Dieser Kernel steuert die Interaktion zwischen den virtualisierten Geräten, die von VMs gesehen werden, und der physischen Hardware.

Citrix Hypervisor kann Folgendes verwenden:

- Bis zu 5 TB RAM
- Bis zu 16 physische Netzwerkkarten
- Bis zu 288 logische Prozessoren pro Host.

> **Hinweis:**
>
> Die maximale Anzahl der unterstützten logischen Prozessoren unterscheidet sich je nach CPU. Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste (HCL).

Die Systemanforderungen für den Citrix Hypervisor -Server sind:

CPUs

Mindestens ein 64-Bit-x86-CPUs, mindestens 1,5 GHz, 2 GHz oder schnellere Multicore-CPU empfohlen.

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

> **Hinweis:**
>
> Um Windows VMs oder neuere Versionen von Linux auszuführen, aktivieren Sie Hardware-Unterstützung für die Virtualisierung auf dem Citrix Hypervisor or-Server. Virtualisierungsunterstützung ist eine Option im BIOS. Möglicherweise ist die Virtualisierungsunterstützung für Ihr BIOS deaktiviert. Weitere Informationen finden Sie in der BIOS-Dokumentation.

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

RAM

2 GB Minimum, 4 GB oder mehr empfohlen

Festplattenspeicher

- Lokal angeschlossener Speicher (PATA, SATA, SCSI) mit mindestens 46 GB Speicherplatz, 70 GB Festplattenspeicher empfohlen
- SAN über HBA (nicht über Software) bei der Installation mit Multipath-Boot von SAN.

Eine detaillierte Liste kompatibler Speicherlösungen finden Sie imHardwarekompatibilitätsliste (HCL).

Netzwerk

100 Mbit/s oder schnellere NIC. Eine oder mehrere Gbit- oder 10-Gbit-NICs werden für schnellere P2V- und Export/Importdatenübertragungen und VM-Livemigration empfohlen.

Es wird empfohlen, mehrere Netzwerkkarten für Redundanz zu verwenden. Die Konfiguration von NICs unterscheidet sich je nach Speichertyp. Weitere Informationen finden Sie in der Herstellerdokumentation.

Citrix Hypervisor erfordert ein IPv4-Netzwerk für Verwaltung und Speicherverkehr.

> **Hinweise:**
>
> - Stellen Sie sicher, dass die Zeiteinstellung im BIOS Ihres Servers auf die aktuelle Uhrzeit in UTC eingestellt ist.
> - In einigen Supportfällen ist der Zugriff auf die serielle Konsole für Debug-Zwecke erforderlich. Beim Einrichten der Citrix Hypervisor Konfiguration wird empfohlen, den Zugriff auf die serielle Konsole zu konfigurieren. Prüfen Sie bei Hosts, die keinen physischen seriellen Port haben oder wenn keine geeignete physische Infrastruktur verfügbar ist, ob Sie ein eingebettetes Verwaltungsgerät konfigurieren können. Zum Beispiel Dell DRAC oder HP iLO. Weitere Hinweise zum Einrichten des seriellen Konsolenzugriffs finden Sie unterCTX228930 - Konfigurieren des seriellen Konsolenzugriffs auf XenServer und höher.

XenCenter -Systemanforderungen

XenCenter hat die folgenden Systemanforderungen:

- **Betriebssystem:**
  - Windows 10
  - Windows 8.1
  - Windows 7 SP1
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2 (siehe Hinweis)
  - Windows Server 2016
- **.NET Framework:** Version 4.6
- **CPU-Geschwindigkeit:** mindestens 750 MHz, 1 GHz oder schneller empfohlen
- **RAM:** mindestens 1 GB, 2 GB oder mehr empfohlen
- **Festplattenspeicher:** mindestens 100 MB
- **Netzwerk:** 100 Mbit/s oder schneller NIC
- **Bildschirmauflösung:** 1024 x 768 Pixel, Minimum

XenCenter ist mit allen unterstützten Versionen von Citrix Hypervisor kompatibel.

> **Hinweis:**
>
> Wenn XenCenter unter Windows Server 2008 SP2 installiert ist, stellen Sie sicher, dass

> eines der folgenden Windows-Updates auf dem Windows Server 2008 SP2-System installiert ist: KB4056564 oder KB4019276. Weitere Informationen finden Sie unter http://support.microsoft.com/kb/4019276.

Unterstützte Gastbetriebssysteme

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

Anforderungen an den Pool

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

Hardwareanforderungen

Alle Server in einem Citrix Hypervisor Ressourcenpool müssen über breit kompatible CPUs verfügen, d. h.:

- Der CPU-Hersteller (Intel, AMD) muss auf allen CPUs auf allen Servern identisch sein.
- Um virtuelle HVM-Maschinen ausführen zu können, müssen alle CPUs die Virtualisierung aktiviert haben.

Sonstige Anforderungen

Zusätzlich zu den zuvor ermittelten Hardwarevoraussetzungen gibt es weitere Konfigurationsvoraussetzungen für einen Server, der einem Pool beitritt:

- Sie muss über eine konsistente IP-Adresse verfügen (eine statische IP-Adresse auf dem Server oder eine statische DHCP-Lease). Diese Anforderung gilt auch für Server, die gemeinsam genutzten NFS- oder iSCSI-Speicher bereitstellen.
- Seine Systemuhr muss mit dem Poolmaster synchronisiert werden (z. B. über NTP).
- Es kann kein Mitglied eines vorhandenen Ressourcenpools sein.
- Es dürfen keine ausgeführten oder angehaltenen VMs oder aktive Vorgänge auf ihren VMs ausgeführt werden, z. B. herunterfahren oder exportieren. Fahren Sie alle VMs auf dem Server herunter, bevor Sie sie einem Pool hinzufügen.
- Es kann kein freigegebener Speicher bereits konfiguriert sein.

- Es kann keine gebundene Management-Schnittstelle haben. Konfigurieren Sie die Verwaltungsschnittstelle neu und verschieben Sie sie auf eine physische Netzwerkkarte, bevor Sie den Server zum Pool hinzufügen. Nachdem der Server dem Pool beigetreten ist, können Sie die Verwaltungsschnittstelle erneut konfigurieren.
- Es muss dieselbe Version von Citrix Hypervisor auf derselben Patch-Ebene ausgeführt werden wie Server, die sich bereits im Pool befinden.
- Es muss mit den gleichen Zusatzpaketen konfiguriert werden wie die Server, die sich bereits im Pool befinden. Zusätzliche Packs werden verwendet, um Add-On-Software in der Citrix Hypervisor or-Steuerdomäne dom0 zu installieren. Um eine inkonsistente Benutzererfahrung in einem Pool zu verhindern, müssen auf allen Servern im Pool dieselben Zusatzpakete bei derselben Revision installiert sein.
- Es muss über dieselbe Citrix Hypervisor-Lizenz verfügen wie die Server, die sich bereits im Pool befinden. Sie können die Lizenz von Poolmitgliedern ändern, nachdem Sie dem Pool beigetreten sind. Der Server mit der niedrigsten Lizenz bestimmt die Funktionen, die allen Mitgliedern im Pool zur Verfügung stehen.

Citrix Hypervisor or-Server in Ressourcenpools können unterschiedliche physische Netzwerkschnittstellen enthalten und lokale Speicher-Repositorys unterschiedlicher Größe aufweisen. In der Praxis ist es oft schwierig, mehrere Server mit genau denselben CPUs zu erhalten, und daher sind kleinere Abweichungen zulässig. Wenn in Ihrer Umgebung Hosts mit unterschiedlichen CPUs im selben Ressourcenpool vorhanden sein sollen, können Sie mithilfe der CLI einen Pool gemeinsam verbinden. Hinweise zum Erzwingen des Verbindungsvorgangs finden Sie unterHosts und Ressourcenpools.

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

Homogenes Schwimmbecken

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

Heterogene Pools

Heterogene Pool-Erstellung wird durch die Verwendung von Technologien in Intel (FlexMigration) und AMD (Extended Migration) CPUs ermöglicht, die *CPU-Maskierung* oder *-Nivellierung* ermöglichen. *Mit diesen Features kann eine CPU so konfiguriert werden, dass sie eine andere Marke, ein Modell oder einen*

anderen Feature-Satz bereitstellt, als sie tatsächlich tut. Diese Funktionen ermöglichen es Ihnen, Pools von Hosts mit unterschiedlichen CPUs zu erstellen, aber dennoch sicher Live-Migrationen zu unterstützen.

Hinweise zum Erstellen heterogener Pools finden Sie unterHosts und Ressourcenpools.

Kopiert!
Failed!

Konfigurationsgrenzen

October 16, 2019

Verwenden Sie die folgenden Konfigurationsbeschränkungen als Richtlinie, wenn Sie Ihre virtuelle und physische Umgebung für Citrix Hypervisor auswählen und konfigurieren. Die folgenden getesteten und empfohlenen Konfigurationslimits werden für Citrix Hypervisor vollständig unterstützt.

- Grenzwerte für virtuelle Maschinen
- Grenzwerte für Citrix Hypervisor or-Server
- Ressourcenpool-Grenzwerte

Faktoren wie Hardware und Umgebung können sich auf die unten aufgeführten Einschränkungen auswirken. Weitere Informationen zu unterstützter Hardware finden Sie auf derHardwarekompatibilitätsliste. Wenden Sie sich an die dokumentierten Grenzwerte Ihrer Hardwarehersteller, um sicherzustellen, dass Sie die unterstützten Konfigurationsgrenzen für Ihre Umgebung nicht überschreiten.

Grenzwerte für virtuelle Maschinen (VM)

Artikel	Begrenzen
Berechnen	
Virtuelle CPUs pro VM (Linux)	32 (siehe Anmerkung 1)
Virtuelle CPUs pro VM (Windows)	32
Speicherkapazität	
RAM pro VM	1,5 TiB (siehe Anmerkung 2)

Artikel	Begrenzen
Lagerhaltung	
Virtual Disk Images (VDI) (einschließlich CD-ROM) pro VM	255 (siehe Anmerkung 3)
Virtuelle CD-ROM-Laufwerke pro VM	1
Virtuelle Datenträgergröße (NFS)	2 TiB minus 4 GiB
Virtuelle Datenträgergröße (LVM)	2 TiB minus 4 GiB
Virtuelle Datenträgergröße (GFS2)	16 TiB
Vernetzung	
Virtuelle Netzwerkkarten pro VM	7 (siehe Anmerkung 4)

Hinweise:

1. Überprüfen Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten.
2. Die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, variiert. Das Festlegen des Speichers auf eine Ebene, die größer ist als das vom Betriebssystem unterstützte Limit kann zu Leistungsproblemen innerhalb Ihres Gastes führen. Einige 32-Bit-Windows Betriebssysteme können über den PAE-Modus (Physical Address Extension) mehr als 4 GiB RAM unterstützen. Die Grenze für virtuelle 32-Bit-PV-Maschinen beträgt 64 GiB. Weitere Informationen finden Sie in der Dokumentation Ihres Gastbetriebssystems und Unterstützung für Gastbetriebssysteme.
3. Die maximale Anzahl der unterstützten VDIs hängt vom Gastbetriebssystem ab. Überprüfen Sie die Dokumentation Ihres Gastbetriebssystems, um sicherzustellen, dass Sie die unterstützten Grenzwerte nicht überschreiten.
4. Mehrere Gastbetriebssysteme haben eine untere Grenze, andere Gäste benötigen die Installation der Citrix VM-Tools, um dieses Limit zu erreichen.

Grenzwerte für Citrix Hypervisor or-Server

Artikel	Begrenzen
Berechnen	
Logische Prozessoren pro Host	288 (siehe Anmerkung 1)

Artikel	Begrenzen
Gleichzeitige VMs pro Host	1000 (siehe Anmerkung 2)
Gleichzeitige geschützte VMs pro Host mit aktiviertem HA	500
Virtuelle GPU-VMs pro Host	128 (siehe Anmerkung 3)
Speicherkapazität	
RAM pro Host	5 TB (siehe Anmerkung 4)
Lagerhaltung	
Gleichzeitige aktive virtuelle Laufwerke pro Host	4096
Vernetzung	
Physische Netzwerkkarten pro Host	16
Physische Netzwerkkarten pro Netzwerkanleihe	4
Virtuelle Netzwerkkarten pro Host	512
VLANs pro Host	800
Netzwerkanleihen pro Host	4
Grafikfunktionen	
GPUs pro Host	12 (Siehe Anmerkung 5)

Hinweise:

1. Die maximale Anzahl der unterstützten logischen physischen Prozessoren unterscheidet sich von der CPU. Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste.
2. Die maximale Anzahl der unterstützten VMS/Host hängt von der Arbeitslast der virtuellen Maschine, der Systemauslastung, der Netzwerkkonfiguration und bestimmten Umgebungsfaktoren ab. Wir behalten uns das Recht vor zu bestimmen, welche spezifischen

Umweltfaktoren die maximale Funktionsfähigkeit eines Systems beeinflussen. Für Systeme mit mehr als 500 VMs empfehlen wir, der Control Domain (Dom0) 8 GB RAM zuzuweisen. Hinweise zum Konfigurieren von Dom0-Speicher finden Sie unter CTX134951 - Konfigurieren von dom0-Speicher in XenServer 6.2 und höher.

3. Für NVIDIA vGPU sind 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. Informationen zu den aktuell unterstützten Grenzwerten finden Sie im Hardwarekompatibilitätsliste.
4. Wenn ein Host über einen oder mehrere 32-Bit-Paravirtualisierte Gäste (Linux VMs) verfügt, wird auf dem Host maximal 128 GB RAM unterstützt.
5. Diese Zahl könnte sich ändern. Informationen zu den aktuell unterstützten Grenzwerten finden Sie im Hardwarekompatibilitätsliste.

Ressourcenpool-Grenzwerte

Artikel	Begrenzen
Berechnen	
VMs pro Ressourcenpool	4096
Hosts pro Ressourcenpool	64 (Siehe Anmerkung 1)
Vernetzung	
VLANs pro Ressourcenpool	800
Aktive Hosts pro serverübergreifendem privates Netzwerk	64
Serverübergreifende private Netzwerke pro Ressourcenpool	16
Virtuelle Netzwerkkarten pro serverübergreifendem privates Netzwerk	16
Serverübergreifende private Netzwerkkarten für virtuelle Netzwerkkarten pro Ressourcenpool	256
Hosts pro vSwitch-Controller	64

Artikel	Begrenzen
Virtuelle Netzwerkkarten pro vSwitch-Controller	1024
VMs pro vSwitch-Controller	1024
Disaster Recovery	
Integrierte Speicher-Repositories für die Standortwiederherstellung pro Ressourcenpool	8
Lagerhaltung	
Pfade zu einer LUN	8
Multipathed LUNs pro Host	256 (Siehe Anmerkung 2)
Multipathed LUNs pro Host (von Speicher-Repositories verwendet)	256 (Siehe Anmerkung 2)
VDIs pro SR (NFS, SMB, EXT, GFS2)	20000
VDIs pro SR (LVM)	1000
Live-Migration von Massenspeicher	
(Nicht-CD-ROM) VDIs pro VM	6
Snapshots pro VM	1
Gleichzeitige Übertragungen	3
XenCenter	
Gleichzeitige Vorgänge pro Pool	25

Hinweise:

1. Cluster-Pools, 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. Hinweise zum Erhöhen des HA-Timeouts finden Sie unterCTX139166 - Ändern der Timeout-

> Einstellungen für hohe Verfügbarkeit.

Kopiert!
Failed!

Unterstützung für Gastbetriebssysteme

October 16, 2019

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

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Fest-plattenspeicher
Windows 7 SP1, Windows 8.1, Windows 10 (32-Bit)	HVM	1 GB	4 DE	24 GB (40 GB oder mehr empfohlen)
Windows 7 SP1 (64 Bit)	HVM	2 GB	192 DE	24 GB (40 GB oder mehr empfohlen)
Windows 8.1 (64 Bit)	HVM	2 GB	512 DE	24 GB (40 GB oder mehr empfohlen)
Windows 10 (64 Bit)	HVM	2 GB	1,5 TB	24 GB (40 GB oder mehr empfohlen)
Windows Server 2008 SP2 (32-bit)	HVM	512 MB	64 DE	24 GB (40 GB oder mehr empfohlen)
Windows Server 2008 SP2 (64 Bit)	HVM	512 MB	1 TB	24 GB (40 GB oder mehr empfohlen)
Windows Server 2008 R2 SP1	HVM	512 MB	1,5 TB	24 GB (40 GB oder mehr empfohlen)

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Festplattenspeicher
Windows Server 2012, Windows Server 2012 R2 (64 Bit)	HVM	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows Server 2016, Windows Server Core 2016 (64-bit)	HVM	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
Windows Server 2019, Windows Server Core 2019 (64-bit)	HVM	1 GB	1,5 TB	32 GB (40 GB oder mehr empfohlen)
CentOS 5.x (32-Bit)	PV	512 MB	16 GB	8 GB
CentOS 5.0—5.7 (64-Bit)	PV	512 MB	16 GB	8 GB
CentOS 5.8—5.11 (64-Bit)	PV	512 MB	128 GB	8 GB
CentOS 6.0, 6.1 (32-Bit)	PV	1 GB	8 GB	8 GB
CentOS 6.0, 6.1 (64-Bit)	PV	512 MB	32 GB	8 GB
CentOS 6.2—6.10 (32-Bit)	PV	512 MB	16 GB	8 GB
CentOS 6.2—6.10 (64-Bit)	PV	1 GB	128 GB	8 GB
CentOS 7.x (64-Bit)	HVM	2 GB	1,5 TB	10 GB
Red Hat Enterprise Linux 5.x (32-Bit)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 5.0—5.7 (64-Bit)	PV	512 MB	16 GB	8 GB

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Festplattenspeicher
Red Hat Enterprise Linux 5.8—5.11 (64-Bit)	PV	512 MB	128 GB	8 GB
Red Hat Enterprise Linux 6.0, 6.1 (32-Bit)	PV	512 MB	8 GB	8 GB
Red Hat Enterprise Linux 6.0, 6.1 (64-bit)	PV	1 GB	32 GB	8 GB
Red Hat Enterprise Linux 6.2-6.10 (32-Bit)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 6.2-6.10 (64-Bit)	PV	1 GB	128 GB	8 GB
Red Hat Enterprise Linux 7.x (64-Bit)	HVM	2 GB	1,5 TB	10 GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (32 Bit)	PV	1 GB	16 GB	8 GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (64 Bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64 Bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12 SP3 (64 Bit)	HVM	1 GB	1,5 TB	8 GB

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Festplattenspeicher
SUSE Linux Enterprise Server 15 (64 Bit)	HVM	1 GB	1,5 TB	8 GB
SUSE Linux Enterprise Desktop 11 SP3 (64 Bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64 Bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12 SP3 (64 Bit)	HVM	1 GB	1,5 TB	8 GB
SUSE Linux Enterprise Desktop 15 (64 Bit)	HVM	1 GB	1,5 TB	8 GB
Oracle Linux 5.0—5.7, 5.10, 5.11 (32-Bit)	PV	512 MB	64 DE	8 GB
Oracle Linux 5.8, 5.9 (32-Bit)	PV	512 MB	16 GB	8 GB
Oracle Linux 5.x (64-Bit)	PV	512 MB	128 GB	8 GB
Oracle Linux 6.x (32-Bit)	PV	512 MB	8 GB	8 GB
Oracle Linux 6.0, 6.1 (64-Bit)	PV	1 GB	32 GB	8 GB
Oracle Linux 6.2—6.10 (64-Bit)	PV	1 GB	128 GB	8 GB

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Festplattenspeicher
Oracle Linux 7.x (64-Bit)	HVM	2 GB	1,5 TB	10 GB
Scientific Linux 6.6—6.10 (32-Bit)	PV	512 MB	16 GB	8 GB
Scientific Linux 6.6—6.10 (64-Bit)	PV	1 GB	128 GB	8 GB
Scientific Linux 7.x (64-bit)	HVM	2 GB	1,5 TB	10 GB
Debian Wheezy 7 (32-Bit)	PV	512 MB	64 DE	8 GB
Debian Wheezy 7 (64-bit)	PV	512 MB	128 GB	8 GB
Debian Jessie 8 (32-Bit)	HVM	128 MB	64 DE	8 GB
Debian Jessie 8 (64-bit)	HVM	128 MB	1,5 TB	8 GB
Debian Stretch 9 (32-Bit)	HVM	256 MB	64 DE	10 GB
Debian Stretch 9 (64-bit)	HVM	256 MB	1,5 TB	10 GB
Ubuntu 14.04 (32-Bit)	HVM	512 MB	64 DE	8 GB
Ubuntu 14.04 (64-bit)	HVM	512 MB	1,5 TB	8 GB
Ubuntu 16.04 (32-Bit)	HVM	512 MB	64 DE	10 GB
Ubuntu 16.04 (64-bit)	HVM	512 MB	1,5 TB	10 GB
Ubuntu 18.04 (64-bit)	HVM	512 MB	1,5 TB	10 GB

Betriebssystem	Virtualisierungsmodus	Minimaler Arbeitsspeicher	Maximaler Arbeitsspeicher	Minimaler Festplattenspeicher
CoreOS-Stable (64-Bit) [Die neueste getestete Version ist 1911.4.0]	HVM	2 GB	512 DE	8 GB
NeoKylin Linux Advanced Server 6.5 (64-bit)	PV	1 GB	128 GB	8 GB
NeoKylin Linux Advanced Server 7.2 (64-bit)	HVM	1 GB	1,5 TB	10 GB

Wichtig:

- RHEL, OL und CentOS 5.x Gastbetriebssysteme mit dem ursprünglichen Kernel können unter Citrix Hypervisor 8.0 nicht gestartet werden. Bevor Sie versuchen, Citrix Hypervisor or-Server auf 8.0 zu aktualisieren, aktualisieren Sie den Kernel auf Version 5.4 (2.6.18-164.el5xen) oder höher.
- Einzelne Versionen der Betriebssysteme können auch ihre eigenen Höchstgrenzen für die unterstützte Speicherkapazität festlegen (z. B. aus Lizenzgründen).
- Überschreiten Sie bei der Konfiguration des Gastspeichers nicht die maximale Menge an physischem Speicher, die Ihr Betriebssystem adressieren kann. Wenn Sie ein Speichermaximum festlegen, das größer als das vom Betriebssystem unterstützte Limit ist, kann es zu Stabilitätsproblemen innerhalb Ihres Gastes kommen.

Hinweise:

- Verwenden Sie die folgende Methode, um eine VM einer neueren Nebenversion von RHEL zu erstellen, als in der vorherigen Tabelle aufgeführt ist:
  - Installieren Sie die VM von den neuesten unterstützten Medien für die Hauptversion
  - Verwenden Sie`yum update` zum Aktualisieren der VM auf die neuere Nebenversion

  Dieser Ansatz gilt auch für RHEL-basierte Betriebssysteme wie CentOS und Oracle Linux.
- Einige 32-Bit-Windows Betriebssysteme unterstützen mehr als 4 GB RAM im PAE-Modus (Physical Address Extension). Um eine VM mit mehr als 4 GB RAM neu zu konfigurieren, ver-

> wenden Sie die xe-CLI, nicht XenCenter, da die CLI keine Obergrenzen für auferlegt`memory-static-max`.

Langfristiger Gast-Support

Citrix Hypervisor enthält eine Langzeit-Gast-Support-Richtlinie (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

Kopiert!
Failed!

Schnellstart

October 16, 2019

Dieser Artikel beschreibt die Installation und Konfiguration von Citrix Hypervisor und dessen grafische Windows-basierte Benutzeroberfläche XenCenter. Nach der Installation werden Sie durch das Erstellen virtueller Windows Maschinen (VMs) und anschließende Erstellen benutzerdefinierter VM-Vorlagen, mit denen Sie mehrere, ähnliche VMs schnell erstellen können. Schließlich wird in diesem Artikel beschrieben, wie Sie einen Hostpool erstellen, der die Grundlage für die Migration ausgeführter VMs zwischen Hosts mithilfe der Livemigration bildet.

Dieser Artikel konzentriert sich auf die grundlegendsten Szenarien und zielt darauf ab, Sie schnell einzurichten.

Dieser Artikel richtet sich in erster Linie an neue Benutzer von Citrix Hypervisor und XenCenter. Sie richtet sich an Benutzer, die Citrix Hypervisor mithilfe von XenCenter verwalten möchten. Informationen zum Verwalten von Citrix Hypervisor mithilfe der Linux-basierten xe-Befehle über die Befehlszeilenschnittstelle (CLI) von Citrix Hypervisor finden Sie unterBefehlszeilenschnittstelle.

Terminologie und Abkürzungen

- *Host*: Ein physischer Computer, auf dem Citrix Hypervisor ausgeführt wird
- *Virtual Machine (VM)*: ein Computer, der vollständig aus Software besteht, der sein eigenes Betriebssystem und Anwendungen wie ein physischer Computer ausführen kann. Eine VM verhält sich genau wie ein physischer Computer und enthält eine eigene virtuelle (softwarebasierte) CPU, RAM, Festplatte und NIC.

- *Pool*: eine einzelne verwaltete Entität, die mehrere Citrix Hypervisor or-Server und ihre VMs miteinander verbindet
- *Storage Repository (SR)*: ein Speichercontainer, in dem virtuelle Laufwerke gespeichert sind

Hauptkomponenten

Citrix Hypervisor

Citrix Hypervisor ist eine vollständige Servervirtualisierungsplattform mit allen Funktionen, die zum Erstellen und Verwalten einer virtuellen Infrastruktur erforderlich sind. Citrix Hypervisor ist für virtuelle Windows s- und Linux-Server optimiert.

Citrix Hypervisor wird direkt auf Serverhardware ausgeführt, ohne dass ein zugrunde liegendes Betriebssystem erforderlich ist. Dies führt zu einem effizienten und skalierbaren System. Citrix Hypervisor abstrahiert Elemente von der physischen Maschine (z. B. Festplatten, Ressourcen und Ports) und weist sie den darauf ausgeführten virtuellen Maschinen (VMs) zu.

Mit Citrix Hypervisor können Sie VMs erstellen, VM-Festplatten-Snapshots erstellen und VM-Workloads verwalten.

XenCenter

XenCenter ist eine grafische Windows-basierte Benutzeroberfläche. Mit XenCenter können Sie Citrix Hypervisor or-Server, Pools und gemeinsam genutzten Speicher verwalten. Verwenden Sie XenCenter zum Bereitstellen, Verwalten und Überwachen von VMs auf Ihrem Windows Desktopcomputer.

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

Installieren von Citrix Hypervisor und XenCenter

In diesem Abschnitt richten Sie eine Mindestinstallation von Citrix Hypervisor ein.

Was du lernen wirst

Sie werden lernen, wie Sie:

- Installieren von Citrix Hypervisor auf einem einzigen physischen Host
- Installieren von XenCenter auf einem Windows Computer
- Verbinden von XenCenter und Citrix Hypervisor, um die Infrastruktur für das Erstellen und Ausführen virtueller Maschinen (VMs) zu bilden.

Anforderungen

Um zu beginnen, benötigen Sie die folgenden Elemente:

- Ein physischer Computer als Citrix Hypervisor -Server
- Ein Windows Computer zum Ausführen der XenCenter Anwendung
- Installationsdateien für Citrix Hypervisor und XenCenter

Der Citrix Hypervisor-Servercomputer ist ausschließlich der Ausführung von Citrix Hypervisor und dem Hosten von VMs gewidmet und wird nicht für andere Anwendungen verwendet. Bei dem Computer, auf dem XenCenter ausgeführt wird, kann es sich um jeden Allzweck-Windows Computer handeln, der die Hardwareanforderungen erfüllt. Mit diesem Computer können Sie auch andere Anwendungen ausführen. Weitere Informationen finden Sie unter Systemvoraussetzungen.

Sie können die Installationsdateien von herunterladenCitrix Hypervisor Downloads.

Installieren des Citrix Hypervisor -Servers

Allen Hosts ist mindestens eine IP-Adresse zugeordnet. Um eine statische IP-Adresse für den Host zu konfigurieren (statt DHCP zu verwenden), müssen Sie die statische IP-Adresse zur Hand haben, bevor Sie mit diesem Verfahren beginnen.

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

So installieren Sie den Citrix Hypervisor or-Server:

1. Brennen Sie die Installationsdateien für Citrix Hypervisor auf eine CD.

   > **Hinweis:**
   >
   > Hinweise zur Verwendung von HTTP, FTP oder NFS als Installationsquelle finden Sie unterInstallieren von Citrix Hypervisor.

2. Sichern Sie die zu behaltenden Daten. Bei der Installation von Citrix Hypervisor werden Daten auf allen Festplatten überschrieben, die Sie für die Installation auswählen.
3. Legen Sie die Installations-CD in das DVD-Laufwerk des Hostcomputers ein.
4. Starten Sie den Hostcomputer neu.
5. Starten Sie vom DVD-Laufwerk (falls erforderlich, finden Sie in der Dokumentation des Hardwareherstellers Informationen zum Ändern der Startreihenfolge).
6. Wählen Sie nach den ersten Startmeldungen und dem Bildschirm **Willkommen bei Citrix Hypervisor** das Tastaturlayout für die Installation aus.

7. Wenn der Bildschirm **Willkommen bei Citrix Hypervisor Setup** angezeigt wird, wählen Sie **OK** aus.
8. Lesen und akzeptieren Sie die Citrix Hypervisor EULA.

   > **Hinweis:**
   >
   > Wenn Sie eine **Systemhardwarwarwarnung** sehen und vermuten, dass Unterstützung für Hardwarevirtualisierungsunterstützung auf Ihrem System verfügbar ist, wenden Sie sich an den Hardwarehersteller, um BIOS-Upgrades zu erhalten.

9. Select **OK** , um eine Neuinstallation durchzuführen.
10. Wenn Sie mehrere Festplatten haben, wählen Sie einen primären Datenträger für die Installation aus. Select **OK**aus.

    Wählen Sie die Datenträger aus, die Sie für die Speicherung virtueller Maschinen verwenden möchten. Wählen Sie **OK**.
11. Select **Lokale Medien** als Installationsquelle aus.
12. Select **Verifizierung überspringen**und dann **OK**aus.

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

13. Erstellen und bestätigen Sie ein Stammkennwort, mit dem die XenCenter Anwendung eine Verbindung mit dem Citrix Hypervisor or-Server herstellt.
14. Richten Sie die Verwaltungsschnittstelle ein, die für die Verbindung mit XenCenter verwendet werden soll.

    Wenn Ihr Computer über mehrere Netzwerkkarten verfügt, wählen Sie die Netzwerkkarte aus, die Sie für den Verwaltungsdatenverkehr verwenden möchten (normalerweise die erste Netzwerkkarte).
15. Konfigurieren Sie die Management-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 den DNS manuell konfigurieren, geben Sie die IP-Adressen Ihrer primären (erforderlich), sekundären (optional) und tertiären (optional) DNS-Server in die dafür vorgesehenen Felder ein.
17. Select Ihre Zeitzone aus.
18. Geben Sie an, wie der Server die lokale Zeit bestimmen soll: mit NTP oder manueller Zeiteingabe. Wählen Sie **OK**.

Bei Verwendung von NTP können Sie angeben, ob DHCP den Zeitserver festlegt. Alternativ können Sie mindestens einen NTP-Servernamen oder eine IP-Adresse in die folgenden Felder eingeben.

19. Select **Citrix Hypervisor installieren aus**.
20. Wenn Sie das Datum und die Uhrzeit manuell festlegen möchten, werden Sie dazu aufgefordert.
21. Wenn Sie von CD installieren, wird im nächsten Bildschirm gefragt, ob Sie zusätzliche Packs von einer CD installieren möchten. Wählen Sie **Nein** , um fortzufahren.
22. Aus dem Bildschirm **Installation abgeschlossen** , werfen Sie die Installations-CD aus dem Laufwerk aus, und wählen Sie dann ***OK,** um den Server neu zu starten.

    Nach dem Neustart des Servers zeigt Citrix Hypervisor **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 von XenCenter

XenCenter wird normalerweise auf Ihrem lokalen System installiert. Sie können das XenCenter er-Installationsprogramm von derCitrix Download-Site

So installieren Sie XenCenter:

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

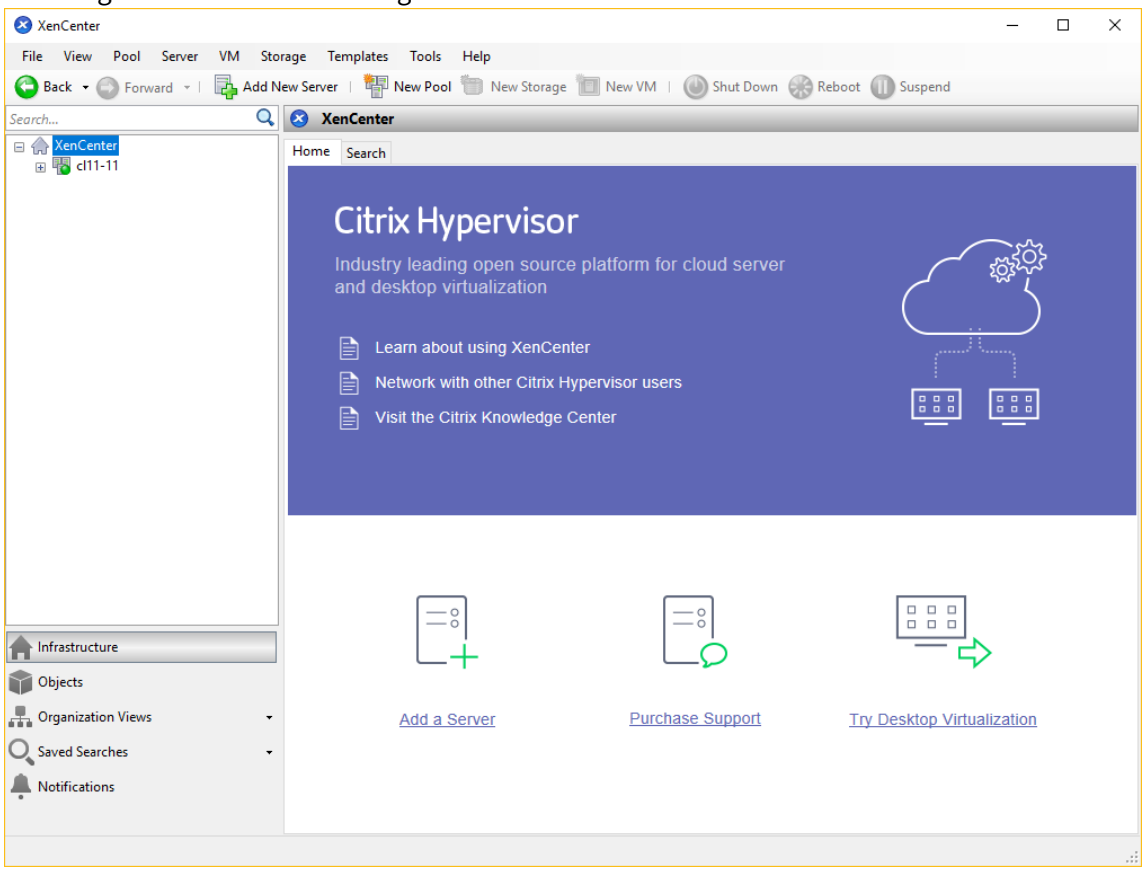
Verbinden von XenCenter mit dem Citrix Hypervisor or-Server

Mit diesem Verfahren können Sie XenCenter einen Host hinzufügen.

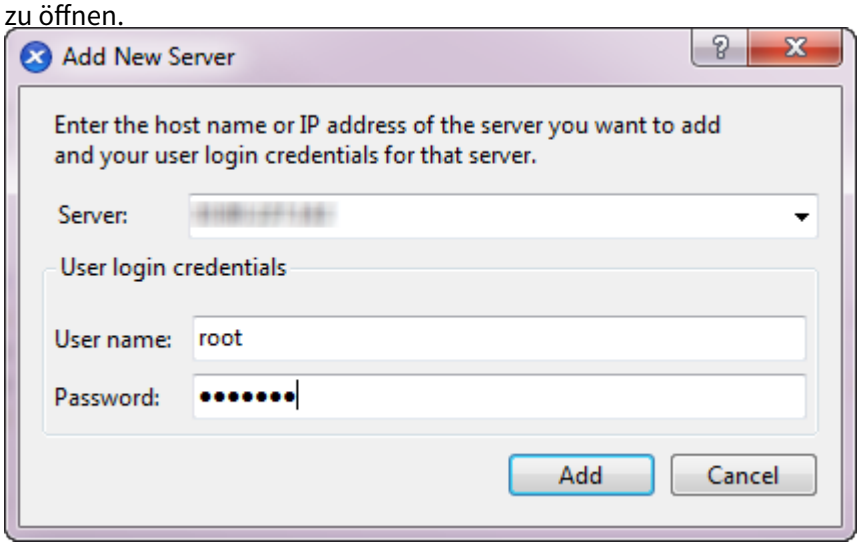
So verbinden Sie XenCenter mit dem Citrix Hypervisor or-Server:

1. Starten Sie XenCenter.

Das Programm öffnet sich zur Registerkarte **Startseite**.



2. Klicken Sie auf das Symbol **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 Stammbenutzernamen und das Kennwort ein, die Sie während der Citrix Hypervisor Installation festgelegt haben. Wählen Sie **Hinzufügen**.

> **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 der Hostverbindungsinformationen und das automatische Wiederherstellen von Serververbindungen festlegen.

Lizenz für Citrix Hypervisor

Sie können Citrix Hypervisor ohne Lizenz (Free Edition) verwenden. Diese Edition bietet jedoch eine eingeschränkte Reihe von Funktionen.

Wenn Sie über eine Citrix Hypervisor-Lizenz verfügen, wenden Sie sie jetzt an.

Weitere Informationen finden Sie unter Lizenzierung.

Erstellen eines Pools von Citrix Hypervisor -Servern

Ein Ressourcenpool besteht aus mehreren Citrix Hypervisor or-Serverinstallationen, die als eine einzelne verwaltete Entität miteinander verbunden sind.

Mit Ressourcenpools können Sie mehrere Hosts und deren verbundenen gemeinsam genutzten Speicher als eine einzige einheitliche Ressource anzeigen. Sie können VMs flexibel im Ressourcenpool bereitstellen, basierend auf Ressourcenanforderungen und Geschäftsprioritäten. Ein Pool kann bis zu 64 Hosts enthalten, auf denen dieselbe Version der Citrix Hypervisor or-Software auf derselben Patch-Ebene und mit allgemein kompatibler Hardware ausgeführt wird.

Ein Host im Pool wird als *Poolmaster*festgelegt. Der Poolmaster stellt einen einzigen Ansprechpartner für den gesamten Pool bereit und leitet die Kommunikation an andere Mitglieder des Pools nach Bedarf weiter. Jedes Mitglied eines Ressourcenpools enthält alle Informationen, die erforderlich sind, um die Rolle des Masters bei Bedarf zu übernehmen. Der Poolmaster ist der erste Host, der für den Pool im XenCenter Ressourcenbereich aufgeführt ist. Sie können die IP-Adresse des Poolmasters finden, indem Sie den Poolmaster auswählen und auf die Registerkarte **Suchen** klicken.

In einem Pool mit gemeinsam genutztem Speicher können Sie VMs auf einem *beliebigen* Pool-Mitglied starten, das über ausreichenden Arbeitsspeicher verfügt, und die VMs dynamisch zwischen Hosts verschieben. Die VMs werden während der Ausführung und mit minimaler Ausfallzeit verschoben. Wenn ein einzelner Citrix Hypervisor or-Server 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. Bei einem HA-aktivierten Pool wird automatisch ein neuer Poolmaster nominiert, wenn der Master heruntergefahren wird.

> **Hinweis:**
>
> Eine Beschreibung der heterogenen Pooltechnologie finden Sie unterHosts und Ressourcenpools.

Was du lernen wirst

Sie werden lernen, wie Sie:

- Erstellen eines Pools von Hosts
- Einrichten eines Netzwerks für den Pool
- Bond-NICs
- Einrichten des gemeinsam genutzten Speichers für den Pool

Während Citrix Hypervisor viele gemeinsam genutzte Speicherlösungen unterstützt, konzentriert sich dieser Abschnitt auf zwei gängige Typen: NFS und iSCSI.

Anforderungen

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

- Ein zweiter Citrix Hypervisor or-Server mit ähnlichem Prozessortyp.
  Verbinden Sie diesen Host mit Ihrer XenCenter Anwendung.
- Ein Speicher-Repository für IP-basierten Speicher

Um einen schnellen Einstieg zu erhalten, konzentriert sich dieser Abschnitt auf die Erstellung *homogener* Pools. Innerhalb eines homogenen Pools müssen alle Hosts über kompatible Prozessoren verfügen und dieselbe Version von Citrix Hypervisor unter derselben Citrix Hypervisor-Produktlizenz ausführen. Eine vollständige Liste der Anforderungen an homogene Pools finden Sie unterSystemanforderungen.

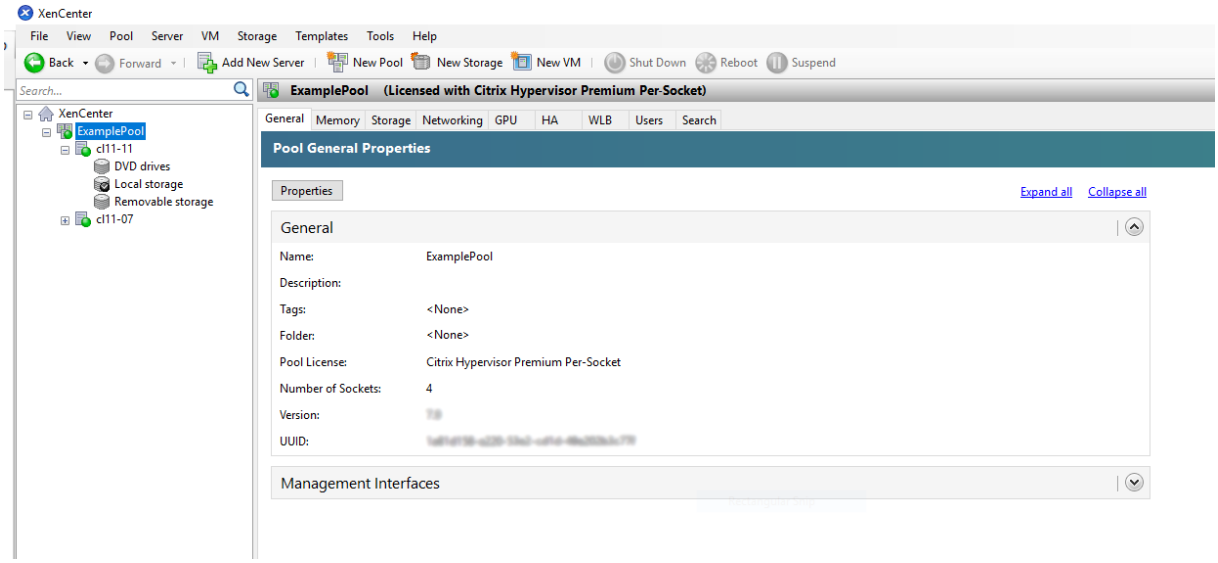
Erstellen eines Pools

So erstellen Sie einen Pool:

1. Klicken Sie auf der Symbolleiste auf die Schaltfläche **Neuer Pool** .
   

2. Geben Sie einen Namen und eine optionale Beschreibung für den neuen Pool ein.
3. Nominieren Sie den Poolmaster, indem Sie einen Host aus der **Master-Liste** auswählen.
4. Select in der Liste **Weitere Mitglieder** den zweiten Host aus, der in den neuen Pool platziert werden soll.

5. Klicken Sie auf **Pool erstellen**.
   Der neue Pool wird im Bereich **Ressourcen** angezeigt.



Einrichten von Netzwerken für den Pool

Wenn Sie Citrix Hypervisor installieren, erstellen Sie eine Netzwerkverbindung, normalerweise auf der ersten Netzwerkkarte im Pool, in der Sie eine IP-Adresse angegeben haben (während der Citrix Hypervisor Installation).

Möglicherweise müssen Sie Ihren Pool jedoch mit VLANs und anderen physischen Netzwerken verbinden. Dazu müssen Sie diese Netzwerke dem Pool hinzufügen. Sie können Citrix Hypervisor so konfigurieren, dass jede Netzwerkkarte mit einem physischen Netzwerk und zahlreichen VLANs verbunden wird.

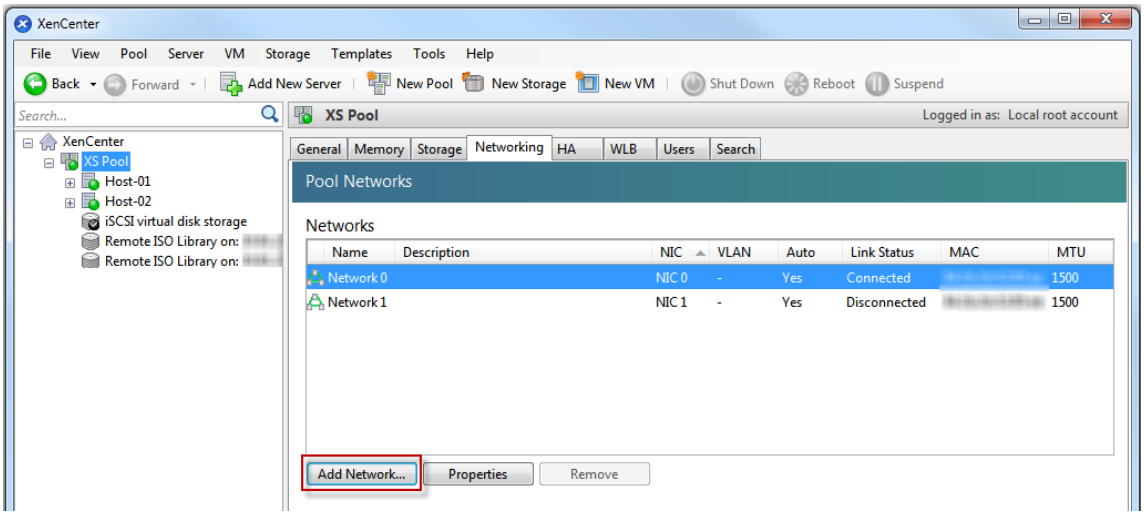
Stellen Sie vor dem Erstellen von Netzwerken sicher, dass die Verkabelung auf jedem Host im Pool übereinstimmt. Schließen Sie die Netzwerkkarten auf jedem Host an dieselben physischen Netzwerke wie die entsprechenden Netzwerkkarten auf den anderen Poolmitgliedern an.

> **Hinweis:**
>
> Wenn die Netzwerkkarten bei der Installation von Citrix Hypervisor nicht an die Netzwerkkarten auf dem Host angeschlossen wurden:
>
> - Schließen Sie die NICs ein
> - Wählen Sie in XenCenter **<your host> > Registerkarte Netzwerkkarten
> - Klicken Sie auf **Erneut scannen** , damit sie angezeigt werden.

Weitere Informationen zum Konfigurieren von Citrix Hypervisor Netzwerken finden Sie in der *XenCenter Hilfe* und Vernetzung .

So fügen Sie Citrix Hypervisor ein Netzwerk hinzu:

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. Select auf der Seite **Typ auswählen** die Option **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:** Select die Netzwerkkarte aus, die Citrix Hypervisor zum Senden und Empfangen von Daten aus dem Netzwerk verwenden soll.
   - **VLAN:** Wenn das Netzwerk ein VLAN ist, geben Sie die VLAN-ID (oder „Tag“) ein.
   - **MTU:** Wenn das Netzwerk Jumbo-Frames verwendet, geben Sie einen Wert für die Maximum Transmission Unit (MTU) zwischen 1500 und 9216 ein. Andernfalls belassen Sie die MTU-Box auf den Standardwert 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 **Fertig stellen**.

Bonding NICs

NIC-Bonding kann Ihren Server widerstandsfähiger machen, indem zwei oder mehr physische Netzwerkkarten verwendet werden, als ob es sich um einen einzigen, leistungsstarken Kanal handelt. Dieser Abschnitt bietet nur einen sehr kurzen Überblick über das Bonding, auch *NIC-Teaming*genannt. Bevor

Sie Bindungen für den Einsatz in einer Produktionsumgebung konfigurieren, empfehlen wir Ihnen, ausführlichere Informationen zum Bonding zu lesen. Weitere Informationen finden Sie unter Vernetzung.

Citrix Hypervisor unterstützt die folgenden Bond-Modi: Aktiv/Aktiv, Aktiv/Passiv (Aktiv/Backup) und LACP. Active/Active bietet Lastausgleich und Redundanz für VM-basierten Datenverkehr. Bei anderen Arten von Datenverkehr (Speicher und Verwaltung) kann aktiv/aktiv kein Lastenausgleich des Datenverkehrs erfolgen. Daher sind LACP oder Multipathing eine bessere Wahl für Speicherdatenverkehr. Hinweise zum Multipathing finden Sie unterSpeicher. Weitere Hinweise zum Kleben finden Sie unterVernetzung.

LACP-Optionen sind nur sichtbar oder verfügbar, wenn Sie den vSwitch 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 unterVernetzung.

So binden Sie NICs an:

1. Stellen Sie sicher, dass die Netzwerkkarten, die Sie miteinander verbinden möchten (die Bond-Slaves), nicht verwendet werden: Schließen Sie alle VMs mit virtuellen Netzwerkschnittstellen mithilfe der Bond-Slaves herunter, bevor Sie die Bindung erstellen. Nachdem Sie die Bindung erstellt haben, müssen Sie die virtuellen Netzwerkschnittstellen erneut mit einem geeigneten Netzwerk verbinden.
2. Select den Server im **Ressourcenbereich** aus, öffnen Sie die Registerkarte **Netzwerkkarten** , und klicken Sie auf **Anleihe erstellen** .
3. Select 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 zu erhalten, können Sie entweder zwei, drei oder vier Netzwerkkarten verbinden, wenn vSwitch der Netzwerkstapel ist. Sie können jedoch nur zwei Netzwerkkarten binden, wenn Linux-Brücke der Netzwerkstapel ist.
4. Wählen Sie unter **Anleihemodus** die Art der Anleihe aus:
   - Select **Aktiv-Aktiv** , um eine aktive Anleihe zu konfigurieren. Der Datenverkehr wird zwischen den gebundenen NICs ausgeglichen. Wenn eine Netzwerkkarte innerhalb der Bindung ausfällt, leitet der Netzwerkverkehr des Hostservers automatisch über die zweite Netzwerkkarte.
   - Select **Aktiv-Passiv** , um eine aktive und passive Bindung zu konfigurieren. Der Datenverkehr wird nur über eine der gebundenen NICs geleitet. In diesem Modus wird die zweite Netzwerkkarte nur aktiv, wenn die aktive Netzwerkkarte ausfällt, z. B. wenn sie die Netzwerkverbindung verliert.

- Select **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 NICs vorhanden sind: Da der Lastausgleich nicht optimal ist, da der Datenverkehr nicht auf Netzwerkkarten aufgeteilt werden kann.
- Select **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 Netzwerkkarten zuweisen. 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-aktive und aktiv-passive Bonding-Modi sowohl für die vSwitch- als auch für die Linux-Brücke verfügbar sind. Hinweise zu Netzwerkstacks finden Sie unterVernetzung.

5. Um Jumbo-Frames zu verwenden, stellen Sie die Maximum Transmission Unit (MTU) auf einen Wert zwischen 1500 und 9216 ein.
6. Aktivieren Sie das Kontrollkästchen, damit das neue gebundene Netzwerk automatisch allen neuen VMs hinzugefügt wird, die mit dem Assistenten für neue VM erstellt wurden.
7. Klicken Sie auf **Erstellen** , um die NIC-Bindung zu erstellen und das Dialogfeld zu schließen.

   XenCenter verschiebt Verwaltungs- und sekundäre Schnittstellen automatisch von Bond-Slaves in den Bond-Master, wenn die neue Bindung erstellt wird. Ein Server mit seiner Management-Schnittstelle auf einer Anleihe ist nicht berechtigt, einem Pool beizutreten. Bevor der Server einem Pool beitreten kann, müssen Sie die Verwaltungsschnittstelle neu konfigurieren und wieder auf eine physische Netzwerkkarte verschieben.

Einrichten des gemeinsam genutzten Speichers für den Pool

Um die Hosts in einem Pool mit einem Remotespeicher-Array zu verbinden, erstellen Sie eine Citrix Hypervisor SR. Der SR ist der Speichercontainer, in dem die virtuellen Laufwerke einer VM gespeichert sind. SRs sind persistente Objekte auf der Festplatte, die unabhängig von Citrix Hypervisor vorhanden sind. SRs können auf verschiedenen Arten von physischen Speichergeräten vorhanden sein, sowohl intern als auch extern. Zu diesen Typen gehören lokale Festplattengeräte und freigegebene Netzwerkspeicher.

Sie können eine Citrix Hypervisor SR für verschiedene Speichertypen konfigurieren, darunter:

- NFS
- Software-iSCSI
- Hardware-HBA
- SMB
- Fibre-Channel
- Software FCoE

In diesem Abschnitt werden zwei Arten von gemeinsam genutzten SRs für einen Hostpool eingerichtet: NFS und iSCSI. Bevor Sie eine SR erstellen, konfigurieren Sie Ihr NFS- oder iSCSI-Speicher-Array. Setup unterscheidet sich je nach Art der Speicherlösung, die Sie verwenden. Weitere Informationen finden Sie in der Dokumentation Ihres Herstellers. Führen Sie im Allgemeinen vor Beginn die folgende Einrichtung für Ihre Speicherlösung aus:

- **iSCSI SR**: Sie müssen ein Volume und eine LUN auf dem Speicher-Array erstellt haben.
- **NFS SR**: Sie müssen das Volume auf dem Speichergerät erstellt haben.
- **Hardware-HBA**: Sie müssen die erforderliche Konfiguration vorgenommen haben, um die LUN verfügbar zu machen, bevor Sie den Assistenten „Neues Speicher-Repository“ ausführen.
- **Software FCoE SR**: Sie müssen die erforderliche Konfiguration manuell abgeschlossen haben, um eine LUN für den Host verfügbar zu machen. Dieses Setup umfasst die Konfiguration der FCoE-Fabric und die Zuweisung von LUNs für den öffentlichen World Wide Name (PWWN) Ihres SAN.

Wenn Sie eine 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 Speicherdatenverkehr. Um eine andere Netzwerkkarte für den Speicherdatenverkehr 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 im selben Subnetz wie der Speichercontroller, falls zutreffend
- Die IP-Adresse befindet sich in einem anderen Subnetz als die IP-Adresse, die Sie bei der Installation von Citrix Hypervisor angegeben haben
- Die IP-Adresse befindet sich nicht im selben Subnetz wie andere Verwaltungsschnittstellen.

So weisen Sie einer NIC 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.

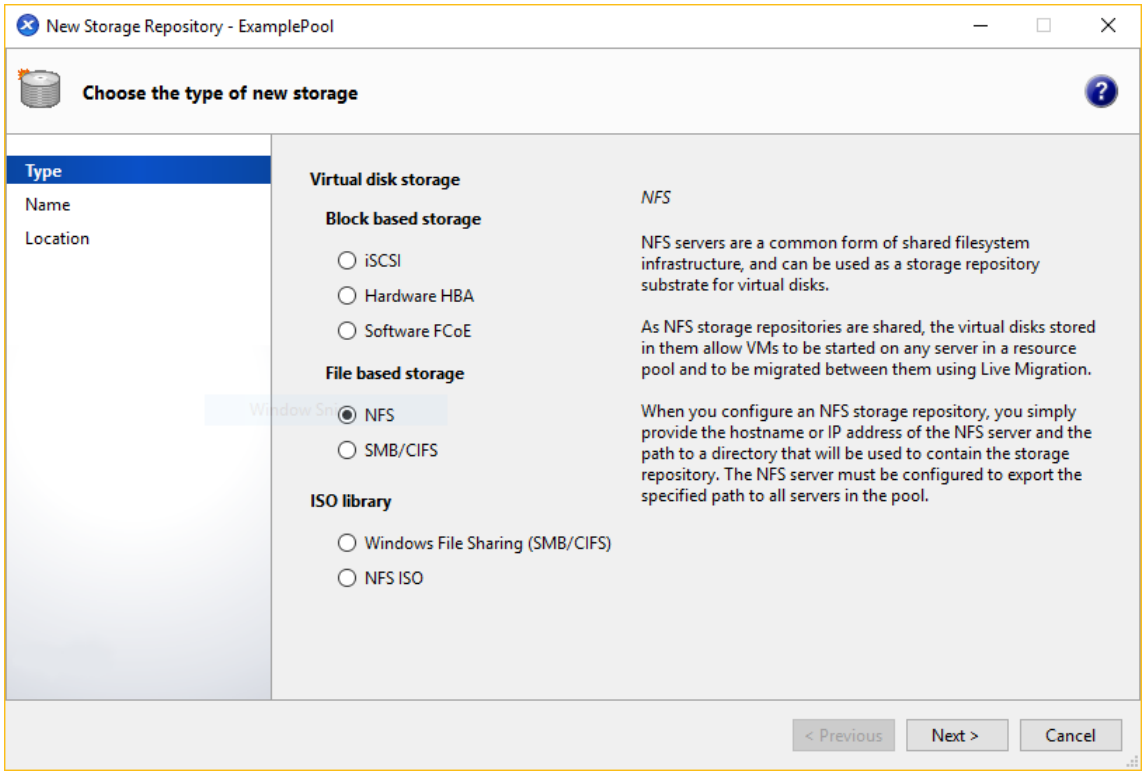
2. Wählen Sie im **Ressourcenbereich** von XenCenter den Pool (oder den eigenständigen Server) aus. Klicken Sie auf die Registerkarte **Netzwerk** , und klicken Sie dann auf die Schaltfläche **Konfigurieren** .
3. Klicken **Sie im Dialogfeld IP-Adresse konfigurieren** im linken Bereich auf **IP-Adresse hinzufügen** .
4. Geben Sie der neuen Schnittstelle einen aussagekräftigen Namen (z. B. *yourstoragearray_network*). Select das **Netzwerk** aus, das der Netzwerkkarte zugeordnet ist, die Sie für den Speicherdatenverkehr 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 befinden wie der Speichercontroller, mit dem die Netzwerkkarte verbunden ist.

> **Hinweis:**
>
> Wenn Sie einer NIC eine IP-Adresse zuweisen, muss sie sich in einem anderen Subnetz befinden als alle anderen Netzwerkkarten mit IP-Adressen im Pool. Dies schließt die primäre Verwaltungsschnittstelle ein.

So erstellen Sie ein neues freigegebenes NFS- oder iSCSI-Speicher-Repository:

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

   Der Assistent **Neues Speicher-Repository** wird geöffnet.



2. Wählen Sie unter Virtueller Festplattenspeicher NFS oder iSCSI als Speichertyp aus. Klicken Sie auf Weiter, um fortzufahren.
3. Wenn Sie NFS wählen:
   a) Geben Sie einen Namen für die neue SR und den Namen der Freigabe ein, in der sie sich befindet. Klicken Sie auf **Scannen** , damit der Assistent nach vorhandenen NFS-SRs am angegebenen Speicherort sucht.

      > **Hinweis:**
      >
      > Der NFS-Server muss so konfiguriert sein, dass er den angegebenen Pfad in alle Citrix Hypervisor or-Server im Pool exportiert.

   b) Klicken Sie auf **Fertig stellen**.

      Der neue SR wird im **Ressourcenbereich** im Pool angezeigt.
4. Wenn Sie iSCSI wählen:
   a) Geben Sie einen Namen für den neuen SR und dann die IP-Adresse oder den DNS-Namen des iSCSI-Ziels ein.

      > **Hinweis:**
      >
      > Das iSCSI-Speicherziel muss so konfiguriert sein, dass jeder Citrix Hypervisor or-Server 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.

> **Warnhinweis:**
>
> Das iSCSI-Ziel und alle Server im Pool müssen über *eindeutige* IQNs verfügen.

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

> **Warnhinweis:**
>
> Jedes einzelne iSCSI-Speicher-Repository muss sich vollständig auf einer einzelnen LUN befinden und darf nicht mehr als eine LUN umfassen. Alle Daten, die auf der ausgewählten LUN vorhanden sind, werden zerstört.

e) Klicken Sie auf **Fertig stellen**.

Der neue SR wird im **Ressourcenbereich** im Pool angezeigt.

Die neue freigegebene SR wird jetzt zum Standard-SR für den Pool.

Erstellen von virtuellen Maschinen

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

Citrix Hypervisor bietet auch eine einfache Möglichkeit, Batches virtueller Maschinen von VMware zu konvertieren. Weitere Informationen finden Sie unter Konvertierungs-Manager.

Dieser Abschnitt konzentriert sich auf einige Methoden zum Erstellen von Windows VMs. Um schnell zu beginnen, verwenden die Verfahren die einfachste Einrichtung von Citrix Hypervisor: ein einzelner Citrix Hypervisor-Server mit lokalem Speicher (nachdem Sie XenCenter mit dem Citrix Hypervisor-Server verbunden haben, wird der Speicher automatisch auf dem lokalen Datenträger des Hosts konfiguriert).

In diesem Abschnitt wird außerdem veranschaulicht, wie Sie die Livemigration für die Livemigration von VMs zwischen Hosts im Pool verwenden.

Nachdem Sie erläutert haben, wie Sie Ihre neue VM erstellen und anpassen, wird in diesem Abschnitt veranschaulicht, wie Sie diese vorhandene VM in eine VM-Vorlage konvertieren. Eine VM-Vorlage behält Ihre Anpassung bei, sodass Sie jederzeit VMs mit denselben (oder ähnlichen) Spezifikationen erstellen können. Außerdem wird die Zeit für die Erstellung mehrerer VMs reduziert.

Sie können auch eine VM-Vorlage aus einem Snapshot einer vorhandenen VM erstellen. Ein Snapshot ist ein Datensatz einer laufenden VM zu einem Zeitpunkt. Sie speichert die Speicher-, Konfigurations- und Netzwerkinformationen der ursprünglichen VM, was sie für Sicherungszwecke nützlich macht. Snapshots bieten eine schnelle Möglichkeit, VM-Vorlagen zu erstellen. In diesem Abschnitt wird veranschaulicht, wie Sie einen Snapshot einer vorhandenen VM erstellen und dann diesen Snapshot in eine VM-Vorlage konvertieren. Schließlich wird in diesem Abschnitt beschrieben, wie VMs aus einer VM-Vorlage erstellt werden.

Was du lernen wirst

Sie werden lernen, wie Sie:

- Erstellen einer Windows 8.1-VM
- Installieren von Citrix VM-Tools
- Migrieren einer ausgeführten 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 von Ihnen eingestellte Citrix Hypervisor Pool
- XenCenter
- Installationsdateien für Windows 8.1

Erstellen einer Windows 8.1 (32-Bit) -VM

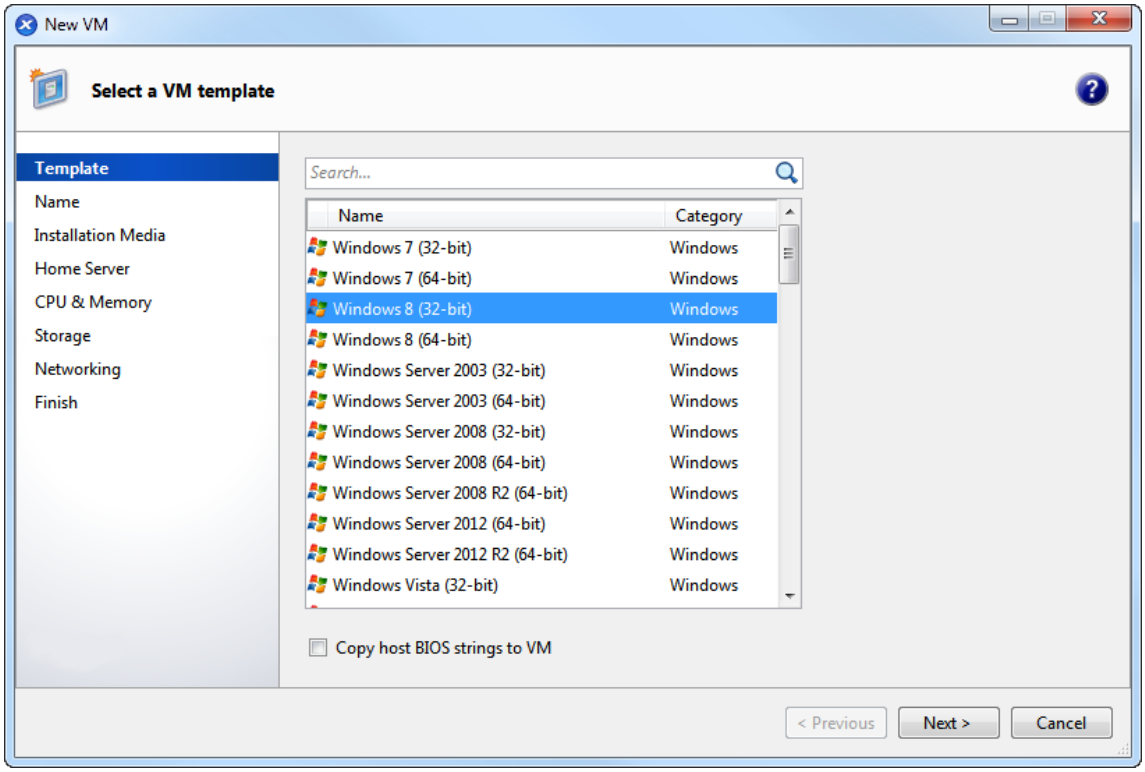
> **Hinweis:**
>
> Das folgende Verfahren enthält ein Beispiel für die Erstellung von Windows 8.1 (32-Bit-) VM. Die Standardwerte können je nach verwendetem Betriebssystem variieren.

So erstellen Sie eine Windows VM:

1. Klicken Sie auf 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. Select eine VM-Vorlage aus, 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 enthält die Vorlagen, die von Citrix Hypervisor derzeit unterstützt werden.

   > **Hinweis:**
   >
   > Wenn das Betriebssystem, das Sie auf Ihrer neuen VM installieren, nur mit der ursprünglichen Hardware kompatibel ist, aktivieren Sie das Kontrollkästchen **Host-BIOS-Zeichenfolgen in VM kopieren** . Verwenden Sie diese Option beispielsweise für eine Betriebssystem-Installations-CD, die mit einem bestimmten Computer verpackt wurde.

3. Geben Sie einen Namen für die neue VM und eine optionale Beschreibung ein.

4. Wählen Sie die Quelle des Betriebssystemmediums aus, das auf der neuen VM installiert werden soll.

   Die Installation von einer CD/DVD ist die einfachste Möglichkeit, um loszulegen. Wählen Sie die Standardinstallationsquellenoption (DVD-Laufwerk), legen Sie den Datenträger in das DVD-Laufwerk des Citrix Hypervisor or-Servers ein und wählen Sie **Weiter** , um fortzufahren.

   Mit Citrix Hypervisor können Sie außerdem 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 die spezifischen ISO-Medien des Betriebssystems aus der Liste auswählen.

5. Die VM wird auf dem installierten Host ausgeführt. Wählen Sie **Weiter**, um fortzufahren.
6. Zuweisen von Prozessor- und Speicherressourcen.

   Für eine Windows 8.1-VM ist der Standardwert 1 virtuelle CPU, 1 Socket mit 1 Core pro Socket und 2 GB RAM. Sie können die Standardeinstellungen bei Bedarf ändern. Klicken Sie auf **Weiter**, um fortzufahren.

   > **Hinweis:**
   >
   > Jedes Betriebssystem hat unterschiedliche Konfigurationsanforderungen, die sich in den Vorlagen widerspiegeln.

7. Weisen Sie eine Grafikprozesseinheit (GPU) zu.

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

   > **Hinweis:**
   >
   > Die GPU-Virtualisierung ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.

8. Konfigurieren Sie den Speicher für die neue VM.

   Klicken Sie auf **Weiter** , um die Standardzuweisung (24 GB) und -konfiguration auszuwählen, oder Sie möchten:

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

   b) Fügen Sie ein neues virtuelles Laufwerk hinzu, indem Sie **Hinzufügen**auswählen.

   > **Hinweis:**
   >
   > Wenn Sie einen Pool von Citrix Hypervisor or-Servern 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 NIC, oder Sie können:

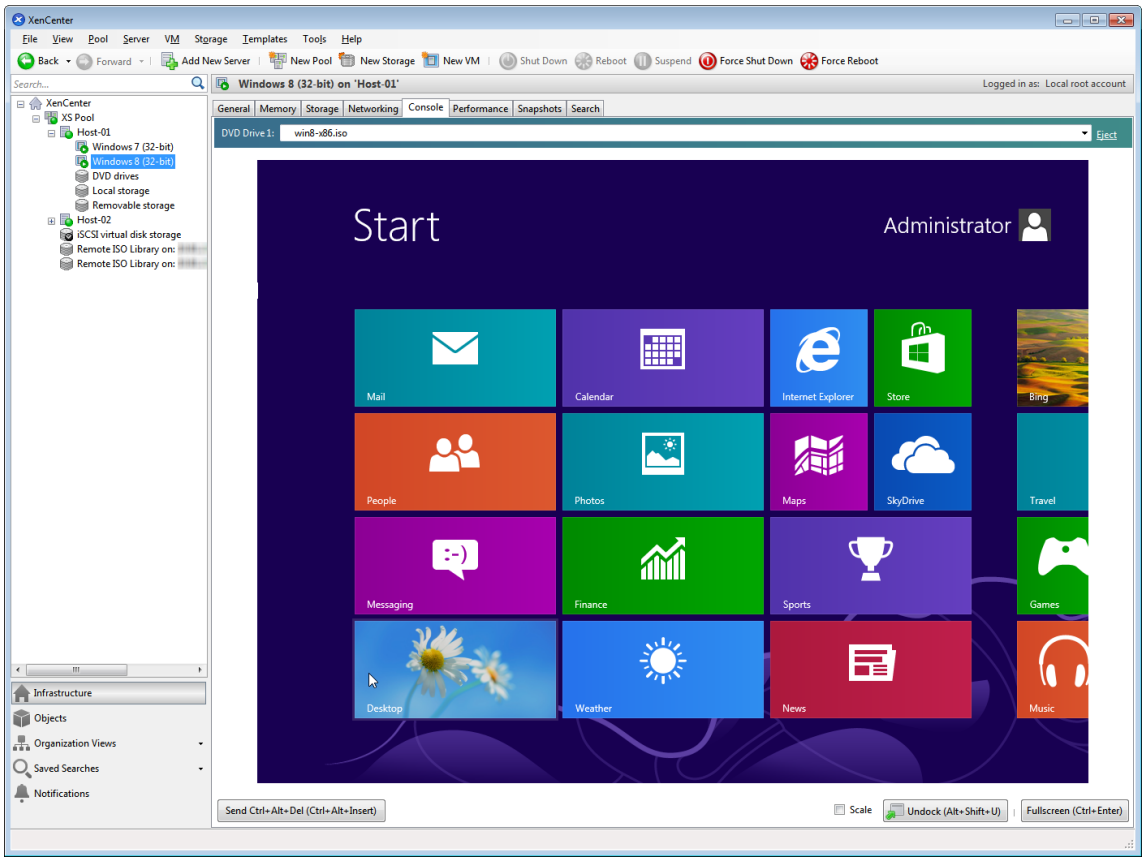
   a) Ändern Sie die physische Netzwerk-, MAC-Adresse oder QoS-Priorität (Quality of Service) des virtuellen Laufwerks, indem Sie auf **Eigenschaften** klicken.

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

Citrix Hypervisor verwendet die virtuelle Netzwerkschnittstelle, um eine Verbindung mit dem physischen Netzwerk auf dem Host herzustellen. Stellen Sie sicher, dass Sie das Netzwerk auswählen, das dem Netzwerk entspricht, das die virtuelle Maschine benötigt. Informationen zum Hinzufügen eines physischen Netzwerks finden Sie unterEinrichten von Netzwerken für den Pool

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

Im **Ressourcenbereich** wird unter dem Host ein Symbol für Ihre neue VM 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 Betriebssysteminstallationsbildschirmen und treffen Sie Ihre Auswahl.
12. Nachdem die Installation des Betriebssystems abgeschlossen und die VM neu gestartet wurde, installieren Sie die Citrix VM-Tools.

Installieren von Citrix VM-Tools

Citrix VM-Tools bieten leistungsstarke E/A-Dienste ohne den Aufwand herkömmlicher Geräteemulation. Citrix VM Tools bestehen aus E/A-Treibern (auch als paravirtualisierte Treiber oder PV-Treiber bezeichnet) und dem Management Agent. Citrix VM Tools müssen auf jeder VM installiert sein, damit die VM über eine vollständig unterstützte Konfiguration verfügt. Eine VM funktioniert ohne sie, aber die Leistung wird behindert. Citrix VM-Tools ermöglichen auch bestimmte Funktionen und Funktionen, einschließlich sauberes Herunterfahren, Neustart, Anhalten und Live-Migrieren von VMs.

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

So installieren Sie Citrix VM-Tools:

1. Select die VM im Ressourcenbereich aus, klicken Sie mit der rechten Maustaste, und klicken Sie dann im Kontextmenü auf **Citrix VM-Tools installieren** . Alternativ klicken Sie im Menü VM auf **Citrix VM Tools installieren**.

   Oder

   Klicken Sie auf der Registerkarte **Allgemein** der VM auf **E/A-Treiber und Verwaltungs-Agent installieren** .

   > **Hinweis:**
   >
   > Wenn Sie Citrix VM Tools auf Ihrer VM installieren, installieren Sie sowohl E/A-Treiber (PV-Treiber) als auch den Management Agent

2. Wenn die automatische Wiedergabe für das CD/DVD-Laufwerk der VM aktiviert ist, wird die Installation nach wenigen Augenblicken automatisch gestartet. Der Prozess installiert die E/A-Treiber und den Management Agent und startet die VM nach Bedarf neu.

3. Wenn die automatische Wiedergabe nicht aktiviert ist, zeigt das Citrix VM Tools-Installationsprogramm die Installationsoptionen an. Klicken Sie auf **Citrix VM-Tools installieren**, um mit der Installation fortzufahren. Die Citrix VM Tools ISO (`guest-tools.iso`) ist auf dem CD/DVD-Laufwerk der VM eingehängt.

4. Klicken Sie auf **Setup.exe ausführen** , um die Installation von Citrix VM Tools zu starten, und 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. Es wird jedoch empfohlen, das Citrix VM Tools-Paket zu installieren, um den Management Agent zu installieren und eine unterstützte Konfiguration

> zu verwalten. Die folgenden Funktionen sind nur für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben:
>
> - Möglichkeit zum Empfangen von E/A-Treibern von Windows Update
> - Automatische Aktualisierung des Management Agents

Nachdem Sie die Citrix VM-Tools installiert haben, können Sie Ihre VM anpassen, indem Sie Anwendungen installieren und andere Konfigurationen ausführen. 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 VMs zu erstellen. Weitere Informationen finden Sie unter Erstellen von VM-Vorlagen.

Migrieren von ausgeführten VMs zwischen Hosts in einem Pool

Mit der Livemigration können Sie eine ausgeführte VM von einem Host auf einen anderen im selben Pool verschieben und praktisch ohne Unterbrechung des Dienstes. Wo Sie eine VM migrieren möchten, hängt davon ab, wie Sie die VM und den Pool konfigurieren.

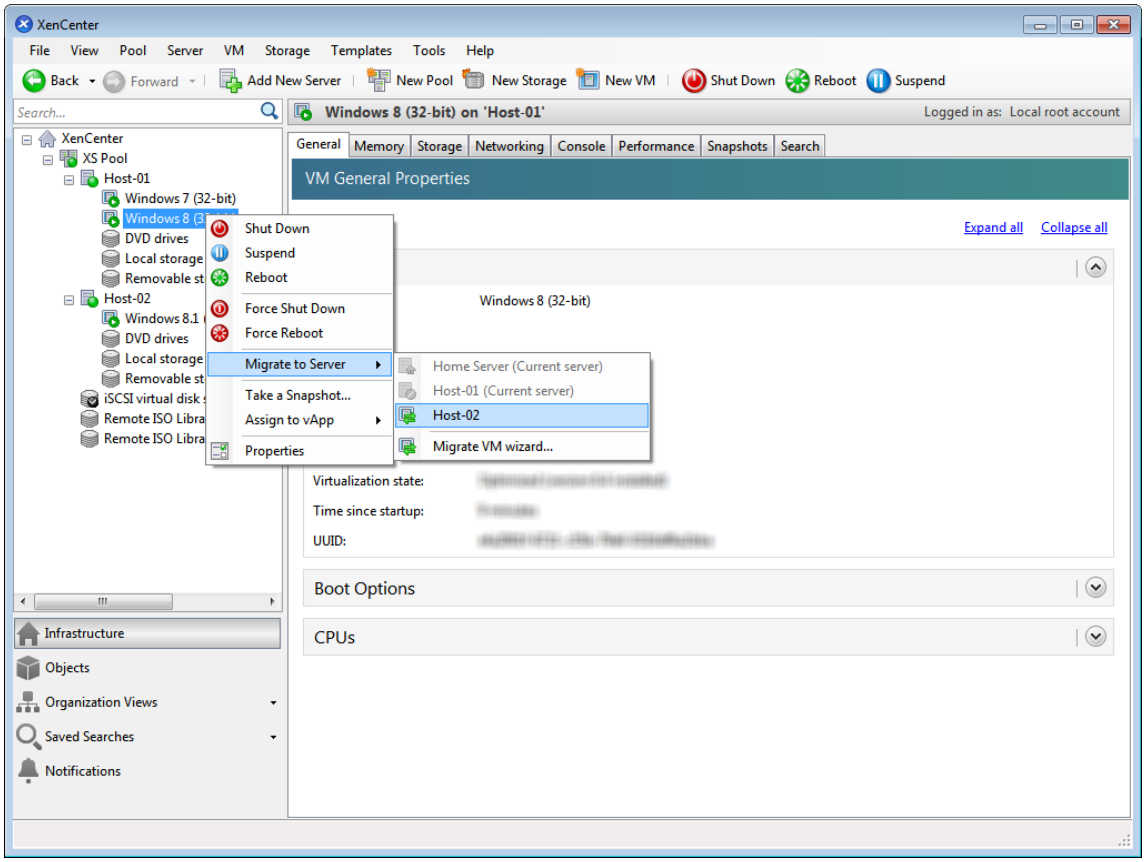
So migrieren Sie eine ausgeführte VM:

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 besitzt.

2. Klicken Sie mit der rechten Maustaste auf das VM Symbol, zeigen Sie **auf Zu 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 von 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 neue, ähnliche VMs schnell zu erstellen. In diesem Abschnitt wird veranschaulicht, wie neue VMs aus diesen Vorlagen erstellt werden.

Bevor Sie eine Vorlage aus einem vorhandenen VM- oder VM-Snapshot erstellen, wird empfohlen, das Windows DienstprogrammSysprep auf der ursprünglichen VM auszuführen. Im AllgemeinenSysprep bereitet das Ausführen ein Betriebssystem für das Klonen und Wiederherstellen von Festplatten vor. Windows Betriebssysteminstallationen enthalten viele eindeutige Elemente pro Installation (einschließlich Sicherheitskennungen und Computernamen). Diese Elemente müssen eindeutig bleiben und nicht auf neue VMs kopiert werden. Wenn kopiert, werden Verwirrung und Probleme wahrscheinlich auftreten. Das AusführenSysprep vermeidet diese Probleme, indem es die Generierung neuer, eindeutiger Elemente für die neuen VMs ermöglicht.

> **Hinweis:**
>
> Die Ausführung ist für grundlegende Bereitstellungen oder TestumgebungenSysprep möglicherweise nicht so notwendig wie für Produktionsumgebungen.

Weitere InformationenSysprepdazu finden Sie in der Windows Dokumentation. Die detaillierte Vorgehensweise zum Ausführen dieses Dienstprogramms kann je nach installierter Windows Version variieren.

Erstellen einer VM-Vorlage aus einer vorhandenen VM

So erstellen Sie eine VM-Vorlage von einer vorhandenen VM:

> **Warnhinweis:**
>
> Wenn Sie eine Vorlage von einer vorhandenen VM erstellen, ersetzt die neue Vorlage die ursprüngliche VM. Die VM ist nicht mehr vorhanden.

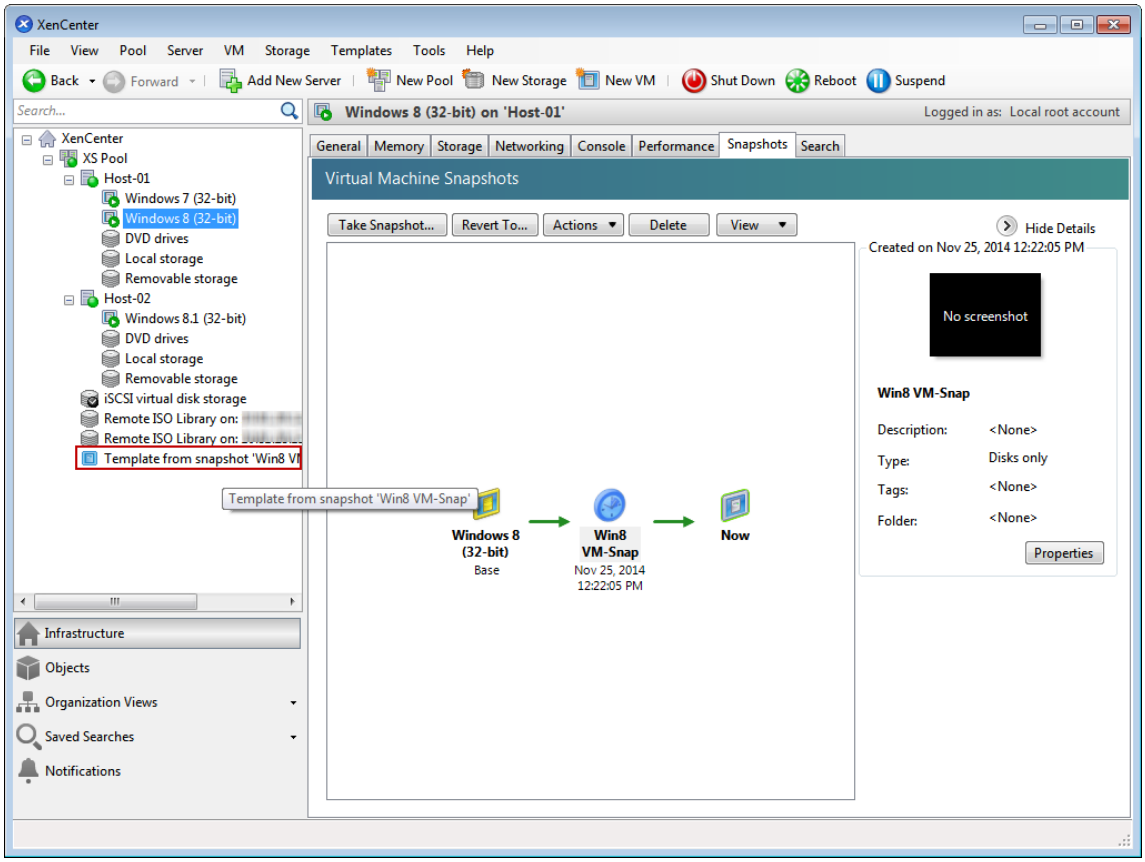
1. Fahren Sie die VM herunter, die Sie konvertieren möchten.
2. Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf die VM, und wählen Sie **In Vorlage konvertieren** aus.
3. Klicken Sie zum Bestätigen auf **Konvertieren** .

   Nachdem Sie die Vorlage erstellt haben, wird die neue VM-Vorlage im **Ressourcenbereich** 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 **Snapshot erstellen** .
2. Geben Sie einen Namen und eine optionale Beschreibung des neuen Snapshots ein. Klicken Sie auf **Snapshot erstellen**.
3. Sobald der Snapshot abgeschlossen ist und das Symbol auf der Registerkarte **Snapshots** angezeigt wird, wählen Sie das Symbol aus.



4. Wählen Sie in der Liste **Aktionen** die Option **Als Vorlage speichern** .
5. Geben Sie einen Namen für die Vorlage ein, und klicken Sie dann auf **Erstellen**.

Erstellen von VMs aus einer VM-Vorlage

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

1. Klicken Sie im Bereich XenCenter **Ressourcen** mit der rechten Maustaste auf die Vorlage, und wählen Sie **Neuer VM-Assistent** aus.

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

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

   > **Hinweis:**
   >
   > Wenn der Assistent Sie zur Eingabe einer Betriebssysteminstallationsmedienquelle auffordert, wählen Sie die Standardeinstellung aus, und fahren Sie fort.

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

Wenn Sie eine Vorlage verwenden, die von einer vorhandenen VM erstellt wurde, können Sie auch **Schnellerstellen**auswählen. Diese Option führt Sie nicht durch den Assistenten für **neue VM** .

Stattdessen erstellt diese Option sofort eine neue VM mit allen Konfigurationseinstellungen, die in Ihrer Vorlage angegeben sind, und stellt sie bereit.

Kopiert!
Failed!

Technische Übersicht

October 16, 2019

Citrix Hypervisor ist eine branchenführende Open-Source-Plattform für kostengünstige Desktop-, Server- und Cloud-Virtualisierungsinfrastrukturen. Mit Citrix Hypervisor können Unternehmen jeder Größe oder Art Rechenressourcen konsolidieren und in virtuelle Workloads für die heutigen Rechenzentrumsanforderungen umwandeln. Mittlerweile stellt sie einen nahtlosen Weg für das Verschieben von Arbeitslasten in die Cloud sicher.

Die wichtigsten Funktionen von Citrix Hypervisor sind:

- Konsolidierung mehrerer virtueller Maschinen (VMs) auf einem physischen Server
- Reduzierung der Anzahl separater Disk-Images, die verwaltet werden sollen
- Einfache Integration in vorhandene Netzwerk- und Speicherinfrastrukturen
- Ermöglichen Sie die Planung der Null-Ausfallzeitwartung durch Live-Migration von VMs zwischen Citrix Hypervisor Hosts
- Sicherstellen der Verfügbarkeit von VMs durch Verwendung hoher Verfügbarkeit zum Konfigurieren von Richtlinien, die VMs auf einem anderen Server neu starten, falls eine fehlschlägt
- Erhöhte Portabilität von VM-Images, da ein VM-Image auf einer Reihe von Bereitstellungsinfrastrukturen funktioniert

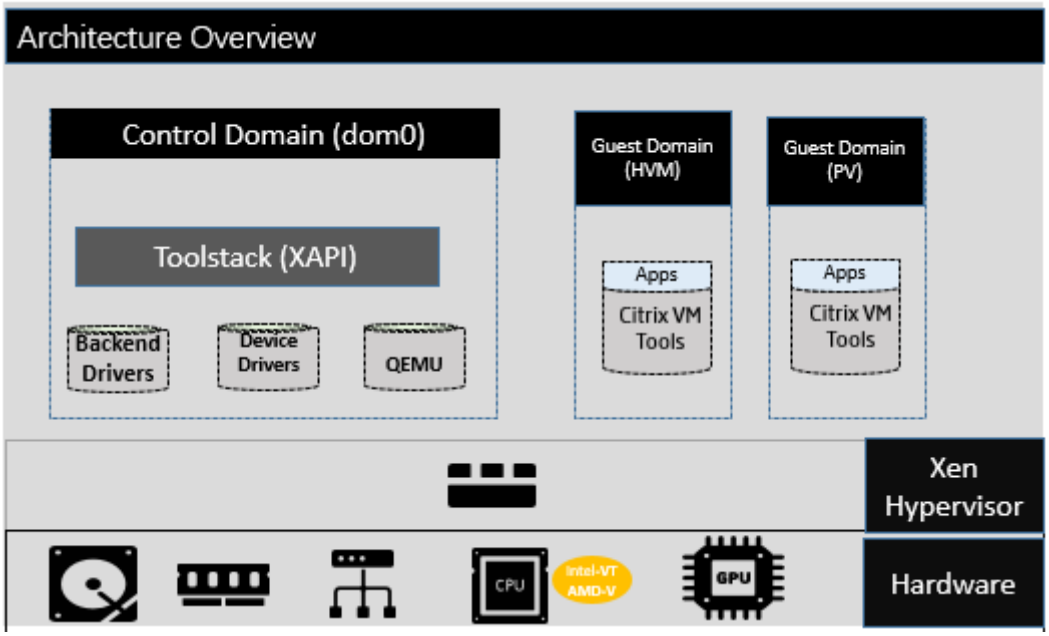
Virtualisierung und Hypervisor

Virtualisierung, oder genauer, 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. Dies ist eine Möglichkeit, die physischen Ressourcen, die auf modernen leistungsstarken Servern verfügbar sind, vollständig zu nutzen, wodurch die Gesamtbetriebskosten (TCO) für Serverbereitstellungen gesenkt werden.

Ein Hypervisor ist die grundlegende Abstraktionsschicht der Software. Der Hypervisor führt Low-Level-Aufgaben wie die CPU-Planung durch und ist für die Speicherisolation für residierende VMs verantwortlich. Der Hypervisor abstrahiert die Hardware für die VMs. Der Hypervisor hat keine Kenntnisse über Netzwerke, externe Speichergeräte, Video usw.

Schlüsselkomponenten

In diesem Abschnitt erfahren Sie mehr über die Funktionsweise von Citrix Hypervisor. In der folgenden Abbildung finden Sie die wichtigsten Komponenten von Citrix Hypervisor:



Hardware

Die Hardwareschicht enthält die physischen Serverkomponenten wie CPU, Arbeitsspeicher, Netzwerk und Festplattenlaufwerke.

Sie benötigen ein Intel VT- oder AMD-V 64-Bit-x86-basiertes System mit mindestens einem CPUs, um alle unterstützten Gastbetriebssysteme auszuführen. Weitere Informationen zu Citrix Hypervisor Host-Systemanforderungen finden Sie unter Systemanforderungen.Eine
vollständige Liste der zertifizierten Hardware und Systeme von Citrix Hypervisor finden Sie in derHardwarekompatibilitätsliste(HCL).

Xen Hypervisor

Der Xen Project Hypervisor ist ein Open-Source-Hypervisor Typ 1 oder Bare-Metal-Hypervisor. Es ermöglicht, dass viele Instanzen eines Betriebssystems oder verschiedener Betriebssysteme parallel auf einem einzigen Computer (oder Host) ausgeführt werden. Xen Hypervisor wird als Grundlage für viele verschiedene kommerzielle und Open-Source-Anwendungen verwendet, wie zum Beispiel: Servervirtualisierung, Infrastructure as a Service (IaaS), Desktop-Virtualisierung, Sicherheitsanwendungen, Embedded und Hardware-Appliances.

Citrix Hypervisor basiert auf dem Xen Project-Hypervisor mit zusätzlichen Funktionen und Unterstützung von Citrix. Citrix Hypervisor 8.0 verwendet Version 4.11 des Xen Hypervisors.

Steuerdomäne

Die **Steuerdomäne**, auch Domäne 0 oder dom0 genannt, ist eine sichere, privilegierte Linux-VM, auf der der Citrix Hypervisor Verwaltungstoolstack namens XAPI ausgeführt wird. Diese Linux-VM basiert auf einer CentOS 7.5-Distribution. Neben der Bereitstellung von Citrix Hypervisor Verwaltungsfunktionen führt dom0 auch die physischen Gerätetreiber für Netzwerke, Speicher usw. aus. Die Steuerdomäne kann mit dem Hypervisor sprechen, um ihn anzuweisen, Gast-VMs zu starten oder zu stoppen.

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 Citrix Hypervisor Ressourcenpools.
XAPI stellt die öffentlich dokumentierte Verwaltungs-API bereit, die von allen Tools zur Verwaltung von VMs und Ressourcenpools verwendet wird. Weitere Informationen finden Sie unter https://developer-docs.citrix.com.

Gastdomäne (VMs)

Gastdomänen sind vom Benutzer erstellte virtuelle Maschinen, die Ressourcen von dom0 anfordern. Die Gastdomäne in Citrix Hypervisor unterstützt vollständige Virtualisierung (HVM), Paravirtualisierung (PV) und PV auf HVM. Eine detaillierte Liste der unterstützten Distributionen finden Sie unterUnterstützte Gäste, virtuelle Arbeitsspeicher und Datenträgergrößenbeschränkungen.

Vollständige Virtualisierung

Die vollständige Virtualisierung oder hardwaregestützte Virtualisierung nutzt Virtualisierungserweiterungen von der Host-CPU, um Gäste zu virtualisieren. Vollständig virtualisierte Gäste benötigen keine Kernelunterstützung. Der Gast wird als Hardware-Virtual Machine (HVM) bezeichnet. HVM erfordert Intel VT- oder AMD-V-Hardware-Erweiterungen für Arbeitsspeicher und privilegierte Vorgänge. Citrix Hypervisor verwendet Quick Emulator (QEMU), um PC-Hardware zu emulieren, einschließlich BIOS, IDE-Festplattencontroller, VGA-Grafikadapter, USB-Controller, Netzwerkadapter usw. Um die Leistung hardwaresensitiver Vorgänge wie Festplatten- oder Netzwerkzugriff zu verbessern, werden HVM-Gäste mit den Citrix Hypervisor Tools installiert. Weitere Informationen finden Sie unter PV auf HVM.

HVM wird häufig verwendet, wenn ein Betriebssystem wie Microsoft Windows virtualisiert wird, wo es unmöglich ist, den Kernal zu ändern, um es virtualisierungsbewusst zu machen.

Paravirtualisierung (PV)

Paravirtualisierung ist eine effiziente und leichte Virtualisierungstechnik, die ursprünglich vom Xen Projekt eingeführt und später von anderen Virtualisierungsplattformen übernommen wurde. PV erfordert keine Virtualisierungserweiterungen von der Host-CPU. PV-Gäste benötigen jedoch einen PV-fähigen Kernel und PV-Treiber, so dass die Gäste den Hypervisor kennen und ohne virtuelle emulierte Hardware effizient arbeiten können. PV-fähige Kernel existieren für Linux, NetBSD, FreeBSD und Open Solaris. Eine Liste der unterstützten Verteilungen im PV-Modus finden Sie unterPV-Linux-Distributionen.

Für einen PV-Gast leitet Xen Hypervisor die E/A-Vorgangsanforderungen an die Steuerdomäne weiter. Der Gast kennt den Hypervisor und sendet privilegierte Anweisungen an den Hypervisor.

PV auf HVM

PV on HVM ist eine Mischung aus Paravirtualisierung und vollständiger Hardware-Virtualisierung. Das primäre Ziel ist es, die Leistung der HVM-Gäste durch die Verwendung speziell optimierter paravirtualisierter Treiber zu steigern. In diesem Modus können Sie die Vorteile der x86-Virtual-Container-Technologien in neueren Prozessoren nutzen, um die Leistung zu verbessern. Netzwerk- und Speicherzugriff von diesen Gästen wird immer noch im PV-Modus betrieben, wobei Treiber verwendet werden, die zu den Kerneln bauen.

Windows und einige Linux-Distributionen sind im PV-Modus auf HVM-Modus in Citrix Hypervisor verfügbar. Eine Liste der unterstützten Linux-Distributionen mit PV auf HVM finden Sie unterHVM-Linux-Distributionen.

Citrix VM-Tools

Citrix VM-Tools oder Gästetools bieten leistungsstarke E/A-Dienste ohne den Aufwand herkömmlicher Geräteemulation. Citrix VM-Tools bestehen aus E/A-Treibern (auch als paravirtualisierte Treiber oder PV-Treiber bezeichnet) und dem Management Agent.

Die E/A-Treiber enthalten Front-End-Speicher- und Netzwerktreiber sowie Low-Level-Verwaltungsschnittstellen. Diese Treiber ersetzen die emulierten Geräte und bieten einen Hochgeschwindigkeitstransport zwischen VMs und der Citrix Hypervisor Produktfamilie.

Der Management Agent, auch als Gast-Agent bezeichnet, ist für Verwaltungsfunktionen der virtuellen Maschine auf hoher Ebene verantwortlich. Es bietet vollständige Funktionalität für XenCenter (für Windows VMs), einschließlich stillgezogene Snapshots.

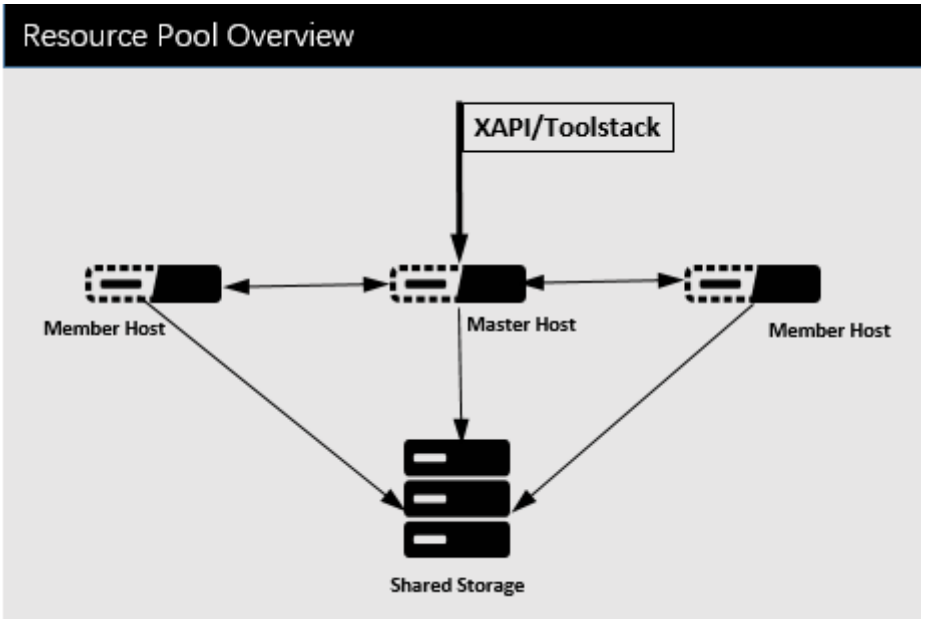
> **Hinweise:**
>
> - Citrix VM Tools müssen auf jeder Windows VM installiert sein, damit die VM über eine vollständig unterstützte Konfiguration verfügt. Eine VM funktioniert ohne die Citrix VM-Tools, aber die Leistung wird erheblich beeinträchtigt, wenn die E/A-Treiber (PV-Treiber) nicht installiert sind.
> - Bei Windows VMs werden Citrix VM-Tools als Windows Gasttools bezeichnet, zu denen Windows-PV-Treiber und der Verwaltungs-Agent gehören.
> - Für Linux-VMs sind PV-Treiber bereits im Xen Kernel enthalten.

Weitere Informationen finden Sie unter Citrix VM-Tools.

Schlüsselkonzepte

Ressourcenpool

Mit Citrix Hypervisor können Sie mehrere Server und den verbundenen gemeinsam genutzten Speicher als eine Einheit mithilfe von Ressourcenpools verwalten. Mit Ressourcenpools können Sie virtuelle Maschinen auf verschiedenen Citrix Hypervisor Hosts verschieben und ausführen. Außerdem können alle Server ein gemeinsames Framework für Netzwerk und Speicher gemeinsam nutzen. Ein Pool kann bis zu 64 Server enthalten, auf denen dieselbe Version der Citrix Hypervisor or-Software auf derselben Patch-Ebene und mit allgemein kompatibler Hardware ausgeführt wird. Weitere Informationen finden Sie unter Hosts und Ressourcenpools.



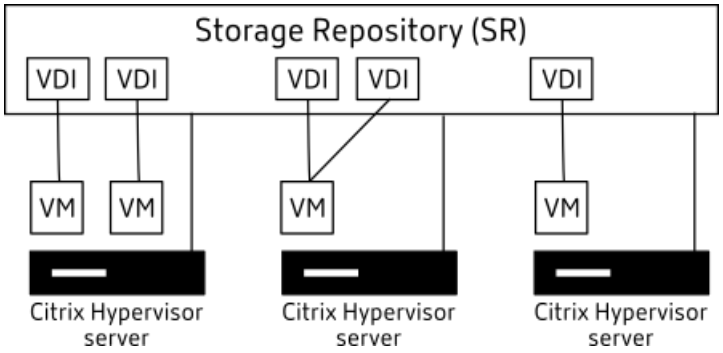
Citrix Hypervisor Ressourcenpool verwendet eine Master-/Slave-Architektur, die von XAPI implementiert wird. XAPI-Aufrufe werden vom Poolmaster an Pool-Mitglieder weitergeleitet. Pool-Mitglieder

machen DB-RPCs gegen den Poolmaster. Der Master-Host ist für die Koordination und Sperre von Ressourcen innerhalb des Pools verantwortlich und verarbeitet alle Steuerungsvorgänge. Mitgliedshosts sprechen mit dem Master über HTTP und XMLRPC, aber sie können miteinander kommunizieren (über denselben Kanal) zu:

- Übertragen von VM-Speicherabbildern (VM-Migration)
- Spiegelnde Festplatten (Speichermigration)

Speicher-Repository

Citrix Hypervisor or-Speicherziele werden als Speicher-Repositories (SRs) bezeichnet. In einem Speicher-Repository werden Virtual Disk Images (VDIs) gespeichert, die den Inhalt eines virtuellen Laufwerks enthalten.
SRs sind flexibel und bieten integrierte Unterstützung für IDE-, SATA-, SCSI- und SAS-Laufwerke, die lokal verbunden sind und iSCSI-, NFS-, SAS- und Fibre-Channel remote verbunden sind. Die SR- und VDI-Abstraktionen ermöglichen erweiterte Speicherfunktionen wie Thin Provisioning, VDI-Snapshots und schnelles Clonen auf Speicherzielen, die sie unterstützen, verfügbar gemacht werden.



Jeder Citrix Hypervisor Host kann mehrere SRs und verschiedene SR-Typen gleichzeitig verwenden. Diese SRs können zwischen Hosts geteilt oder für bestimmte Hosts dediziert werden. Gemeinsamer Speicher wird zwischen mehreren Hosts innerhalb eines definierten Ressourcenpools gepoolt. Ein gemeinsam genutzter SR muss für jeden Host im Pool auf das Netzwerk zugegriffen werden. Alle Hosts in einem einzelnen Ressourcenpool müssen über mindestens eine gemeinsam genutzte SR verfügen. Gemeinsamer Speicher kann nicht zwischen mehreren Pools freigegeben werden.

Weitere Hinweise zum Arbeiten mit SRs finden Sie unterKonfigurieren des Speichers.

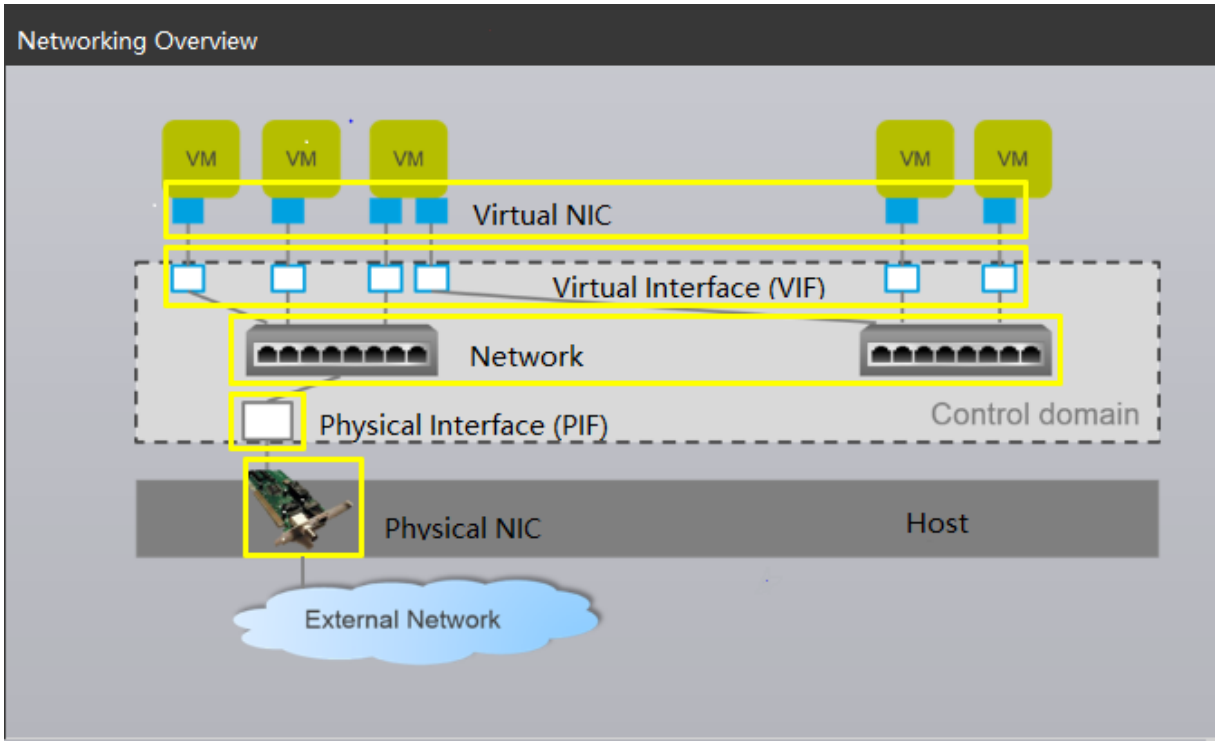
Vernetzung

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

- Ein **PIF**, bei dem es sich um ein Softwareobjekt handelt, das in dom0 verwendet wird und eine physische Netzwerkkarte auf einem Host darstellt. PIF-Objekte haben einen Namen und eine

Beschreibung, eine UUID, die Parameter der Netzwerkkarte, die sie darstellen, sowie das Netzwerk und den Server, 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, der zum Weiterleiten des Netzwerkdatenverkehrs auf einem Netzwerkhost verwendet wird. Netzwerkobjekte verfügen über einen Namen und eine Beschreibung, eine UUID und die Sammlung von VIFs und PIFs, die mit ihnen verbunden sind.



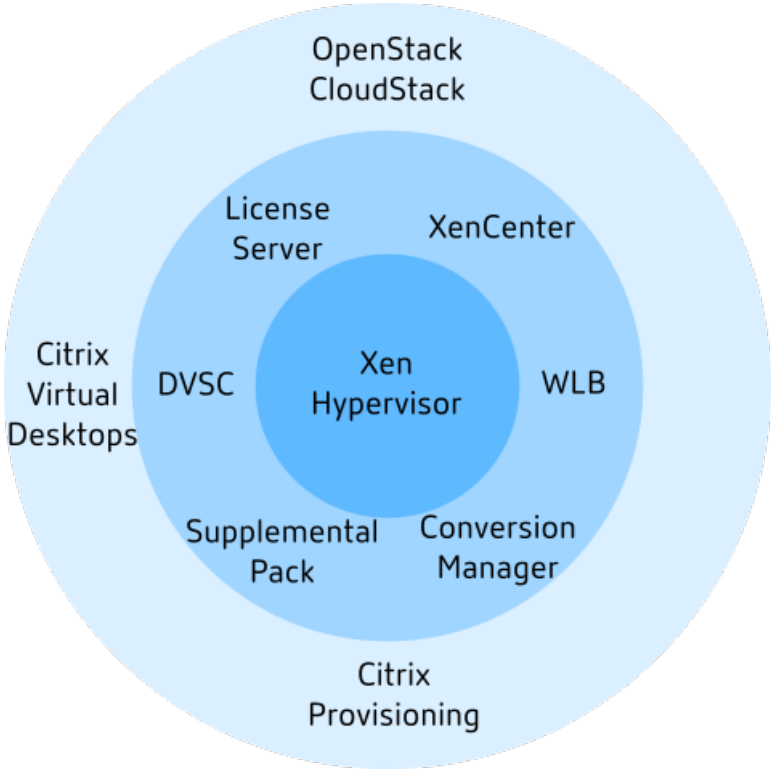
Citrix Hypervisor Verwaltungs-APIs ermöglichen folgende Vorgänge:

- Konfiguration von Netzwerkoptionen
- Kontrolle über die Netzwerkkarte, die für Verwaltungsvorgänge verwendet werden soll
- Erstellung von erweiterten Netzwerkfunktionen wie Virtual Local Area Networks (VLANs) und NIC-Anleihen

Weitere Informationen zum Verwalten von Netzwerken auf XenServer finden Sie unterVernetzung.

Ähnliche Add-ons und Anwendungen

Während Xen Hypervisor auf der Kernebene arbeitet, stehen Citrix Hypervisor spezifische Add-Ons für hypervisor-agnostische Anwendungen und Dienste zur Verfügung, um die Virtualisierung zu vervollständigen.



- **XenCenter**

  Ein Windows-GUI-Client für die VM-Verwaltung, basierend auf der Management-API implementiert. XenCenter bietet eine umfassende Benutzererfahrung, um mehrere Citrix Hypervisor Hosts,
  Ressourcenpools und die gesamte damit verbundene virtuelle Infrastruktur zu verwalten.

- **Arbeitslastausgleich (WLB)**

  Eine Appliance, die Ihren Pool ausgleicht, indem virtuelle Maschinen auf die bestmöglichen Server für ihre Arbeitslast in einem Ressourcenpool verlagert werden. Weitere Informationen finden Sie unter Workload Balancing (/de-de/citrix-hypervisor/vswitch-controller.html).

- **Distributed Virtual Switch Controller (DVSC)**

  Eine Debian-basierte Appliance, die zum Erstellen von Open Flow-Regeln verwendet wird, die XAPI-fähig sind. Die Implementierung besteht aus folgenden Komponenten:

  - Ein virtualisierungsorientierter Switch (der vSwitch), der auf jedem Citrix Hypervisor und dem vSwitch Controller ausgeführt wird.
  - Ein zentralisierter Server, der das Verhalten jedes einzelnen vSwitches verwaltet und koordiniert, um das Erscheinungsbild eines einzelnen vSwitches bereitzustellen.

  Weitere Informationen finden Sie unter vSwitch und Controller.

- **Citrix Lizenzserver**

Eine Linux-basierte Appliance, die XenCenter kontaktiert, um eine Lizenz für den angegebenen Server anzufordern.

- **Citrix Hypervisor Conversion Manager (XCM)**

  Eine virtuelle Appliance mit einer Konsole, die es Benutzern ermöglicht, vorhandene virtuelle VMware Maschinen in virtuelle Citrix Hypervisor Maschinen mit vergleichbarer Netzwerk- und Speicherkonnektivität zu konvertieren. Weitere Informationen finden Sie unter Konvertierungs-Manager.

- **Ergänzungspaket für gemessene Stiefel**

  Ein ergänzendes Paket, mit dem Kunden wichtige Komponenten ihrer Citrix Hypervisor Hosts beim Booten messen können, und APIs bereitgestellt werden, mit denen Remote-Bescheinigungslösungen diese Messungen sicher erfassen können. Weitere Informationen finden Sie unterErgänzungspaket für gemessene Stiefel.

- **Citrix Provisioning**

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

- **Citrix Virtual Desktops**

  Ein VDI-Produkt (Virtual Desktop Infrastructure), das auf Windows Desktops spezialisiert ist. Citrix Virtual Desktops verwenden XAPI, um Citrix Hypervisor in einer Konfiguration mit mehreren Host-Pools zu verwalten. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops.

- **OpenStack/CloudStack**

  Open-Source-Software für den Aufbau öffentlicher und privater Clouds. Verwendet die Verwaltungs-API zur Steuerung von XenServer. Weitere Informationen finden Sie unterhttps://www.openstack.org/ undhttps://cloudstack.apache.org/

Kopiert!
Failed!

Technische FAQs

October 16, 2019

Hardware

Was sind die Mindestsystemanforderungen für die Ausführung von Citrix Hypervisor?

Die Mindestsystemanforderungen für diese Version finden Sie unterSystemanforderungen.

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

Ja. Für die Ausführung aller CPUs ist entweder ein Intel VT- oder AMD-V 64-Bit-x86-basiertes System mit mindestens einem CPUs erforderlichunterstützte Gastbetriebssysteme.

Weitere Hinweise zu Hostsystemanforderungen finden Sie unterSystemanforderungen.

Benötige ich ein System mit Hardware-Virtualisierungsunterstützung?

Um Windows Betriebssysteme oder HVM Linux-Gäste ausführen zu können, benötigen Sie ein 64-Bit-x86-Prozessor basiertes System, das entweder Intel VT- oder AMD-V-Hardware-Virtualisierungstechnologie im Prozessor und im BIOS unterstützt.

Weitere Informationen zu HVM Linux-Gästen finden Sie unterLinux-VMs.

Welche Systeme sind für den Betrieb von Citrix Hypervisor zertifiziert?

Eine vollständige Liste der zertifizierten Citrix Hypervisor Systeme finden Sie imHardwarekompatibilitätsliste (HCL).

Unterstützt Citrix Hypervisor AMD Rapid Virtualization Indexing und Intel Extended Page Tables?

Ja. Citrix Hypervisor unterstützt AMD Rapid Virtualization Indexing und Intel Extended Page Tables. Die Rapid Virtualization Indexing bietet eine Implementierung der Technologie für verschachtelte Tabellen, die zur weiteren Verbesserung der Leistung des Xen Hypervisors verwendet wird. Extended Page Tables bieten eine Implementierung von hardwareunterstütztem Paging, das zur weiteren Verbesserung der Leistung des Xen Hypervisors verwendet wird.

Kann Citrix Hypervisor auf Notebook- oder Desktop-Systemen ausgeführt werden?

Citrix Hypervisor wird auf vielen Notebook- oder Desktop-Systemen ausgeführt, die den minimalen CPU-Anforderungen entsprechen. Citrix unterstützt jedoch nur Systeme, die zertifiziert und im aufgeführt sindHardwarekompatibilitätsliste (HCL). Kunden können für Demonstrations- und Testzwecke

auf nicht unterstützten Systemen ausgeführt werden. Einige Funktionen wie Energieverwaltungsfunktionen funktionieren jedoch nicht.

Produktgrenzen

> **Hinweis:**
>
> Eine vollständige Liste der unterstützten Grenzwerte von Citrix Hypervisor finden Sie unterKonfigurationsbeschränkungen.

Wie hoch ist die maximale Speichergröße, die Citrix Hypervisor auf einem Hostsystem verwenden kann?

Citrix Hypervisor Hostsysteme können bis zu 5 TB physischen Speicher belegen.

Wie viele Prozessoren kann Citrix Hypervisor verwenden?

Citrix Hypervisor unterstützt bis zu 288 logische Prozessoren pro Host. Die maximale Anzahl der unterstützten logischen Prozessoren unterscheidet sich je nach CPU.

Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste (HCL).

Wie viele virtuelle Maschinen können gleichzeitig auf Citrix Hypervisor ausgeführt werden?

Die maximale Anzahl der für die Ausführung auf einem Citrix Hypervisor Host unterstützten virtuellen Maschinen (VMs) beträgt 1000. Für Systeme mit mehr als 500 VMs empfiehlt Citrix, Dom0 8 GB RAM zuzuweisen. Hinweise zum Konfigurieren von Dom0-Speicher finden Sie unter CTX134951 - Konfigurieren von dom0-Speicher in XenServer 6.2 und höher.

Für ein bestimmtes System hängt die Anzahl der VMs, die gleichzeitig und mit akzeptabler Leistung ausgeführt werden können, von den verfügbaren Ressourcen und der VM-Arbeitslast ab. Citrix Hypervisor skaliert automatisch die Speichermenge, die der Control Domain (Dom0) zugewiesen ist, basierend auf dem verfügbaren physischen Speicher.

> **Hinweis:**
>
> Wenn mehr als 50 VMs pro Host vorhanden sind und der physische Speicher des Hosts weniger als 48 GB beträgt, empfiehlt es sich, diese Einstellung außer Kraft zu setzen. Weitere Informationen finden Sie unter Speichernutzung.

Wie viele physische Netzwerkschnittstellen unterstützt Citrix Hypervisor?

Citrix Hypervisor unterstützt bis zu 16 physische NIC-Ports. Diese NICs können gebunden werden, um bis zu 8 logische Netzwerkanleihen zu erstellen. Jede Bindung kann bis zu 4 NICs umfassen.

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

Citrix Hypervisor unterstützt bis zu 32 vCPUs pro VM. Die Anzahl der unterstützten vCPUs variiert je nach Gastbetriebssystem.

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

Wie viel Arbeitsspeicher kann Citrix Hypervisor einer VM zuweisen?

Citrix Hypervisor unterstützt bis zu 1,5 TB pro Gast. Die Größe des Speichers, der unterstützt werden kann, variiert je nach Gastbetriebssystem.

> **Hinweis:**
>
> Die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, variiert. Wenn Sie den Speicher auf eine Ebene festlegen, die größer ist als das vom Betriebssystem unterstützte Limit kann es zu Leistungsproblemen innerhalb Ihres Gastes kommen. Einige 32-Bit-Windows Betriebssysteme können über den PAE-Modus (Physical Address Extension) mehr als 4 GB RAM unterstützen. Die Grenze für virtuelle 32-Bit-PV-Maschinen beträgt 64 GB. Weitere Informationen finden Sie in der Dokumentation Ihres Gastbetriebssystems und unterstützte Gastbetriebssysteme.

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

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

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

Wie viele virtuelle Netzwerkschnittstellen kann Citrix Hypervisor einer VM zuweisen?

Citrix Hypervisor kann bis zu 7 virtuelle Netzwerkkarten pro VM zuweisen. Die Anzahl der unterstützten virtuellen Netzwerkkarten variiert je nach Gastbetriebssystem.

Ressourcenfreigabe

Wie werden Verarbeitungsressourcen zwischen VMs aufgeteilt?

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

Wie wählt Citrix Hypervisor aus, welche physischen Prozessoren er der VM zuweist?

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

Wie werden Datenträger-E/A-Ressourcen auf die VMs aufgeteilt?

Citrix Hypervisor verwendet eine Fair-Share-Ressourcenaufteilung für Datenträger-E/A-Ressourcen zwischen VMs. Sie können auch eine VM mit höherer oder niedrigerer Priorität auf Datenträger-E/A-Ressourcen bereitstellen.

Wie werden Netzwerk-E/A-Ressourcen auf die VMs aufgeteilt?

Citrix Hypervisor verwendet eine Fair Share-Ressourcenaufteilung für Netzwerk-E/A-Ressourcen zwischen den VMs. Sie können auch Grenzwerte für die Bandbreiteneinschränkung pro VM mithilfe des Open vSwitch steuern.

Gastbetriebssysteme

Kann Citrix Hypervisor 32-Bit-Betriebssysteme als Gäste ausführen?

Ja. Weitere Informationen finden Sie unter Unterstützte Gastbetriebssysteme.

Kann Citrix Hypervisor 64-Bit-Betriebssysteme als Gäste ausführen?

Ja. Weitere Informationen finden Sie unter Unterstützte Gastbetriebssysteme.

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

Eine Liste der unterstützten Windows Gastbetriebssysteme finden Sie unterUnterstützte Gastbetriebssysteme.

Welche Versionen von Linux können als Gäste auf Citrix Hypervisor ausgeführt werden?

Eine Liste der unterstützten Linux-Gastbetriebssysteme finden Sie unterUnterstützte Gastbetriebssysteme.

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

Citrix unterstützt nur Betriebssysteme unter Betriebssystemanbieterunterstützung. Obwohl nicht unterstützte Betriebssysteme weiterhin funktionieren, bitten wir Sie möglicherweise, ein Upgrade auf ein unterstütztes Betriebssystemservicepack durchzuführen, bevor wir Probleme untersuchen können.

Für Betriebssystemversionen, die nicht unterstützt werden, stehen möglicherweise keine entsprechenden Treiber zur Verfügung. Ohne die Treiber funktionieren diese Betriebssystemversionen nicht mit optimierter Leistung.

Es ist oft möglich, andere Linux-Distributionen zu installieren. Citrix kann jedoch nur die unter aufgeführten Betriebssysteme unterstützenUnterstützte Gastbetriebssysteme. Wir bitten Sie möglicherweise, zu einem unterstützten Betriebssystem zu wechseln, bevor Probleme untersucht werden können.

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

Citrix Hypervisor unterstützt keine BSD-basierten Gastbetriebssysteme für allgemeine Virtualisierungsbereitstellungen. FreeBSD-VMs, die auf Citrix Hypervisor ausgeführt werden, sind jedoch für die Verwendung in bestimmten Citrix Produkten zertifiziert.

Was sind die Citrix VM-Tools?

Die Citrix VM-Tools sind Softwarepakete für Windows und Linux-basierte Gastbetriebssysteme. Bei Windows Betriebssystemen enthalten die Citrix VM-Tools leistungsstarke E/A-Treiber (PV-Treiber) und den Management Agent. Bei Linux-basierten Betriebssystemen enthalten die Citrix VM-Tools einen Gast-Agent, der dem Citrix Hypervisor Host zusätzliche Informationen über die VM bereitstellt. Weitere Informationen finden Sie unter Citrix VM-Tools.

XenCenter

Muss ich XenCenter auf einem Windows Computer ausführen?

Ja. Die XenCenter Verwaltungskonsole wird unter einem Windows Betriebssystem ausgeführt. Informationen zu
den Systemanforderungen finden Sie unterSystemanforderungen

Wenn Sie Windows nicht ausführen möchten, können Sie Citrix Hypervisor Hosts und -Pools mithilfe der xe-CLI oder mithilfe der xsconsole, einer
Systemkonfigurationskonsole, verwalten.

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

Ja. Sie können XenCenter Anmeldeanforderungen so einrichten, dass Active Directory für alle Editionen von Citrix Hypervisor verwendet wird.

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

Ja. Die rollenbasierte Zugriffssteuerungsfunktion in Kombination mit der Active Directory Authentifizierung kann den Zugriff für Benutzer in XenCenter einschränken.

Kann ich eine einzelne XenCenter Konsole verwenden, um eine Verbindung mit mehreren Citrix Hypervisor Hosts herzustellen?

Ja. Sie können eine einzelne XenCenter Konsole verwenden, um eine Verbindung mit mehreren Citrix Hypervisor Hostsystemen herzustellen.

Kann ich XenCenter verwenden, um eine Verbindung mit mehreren Hosts herzustellen, auf denen verschiedene Versionen von Citrix Hypervisor ausgeführt werden?

Ja. XenCenter ist abwärtskompatibel mit mehreren Hostsystemen, auf denen verschiedene Versionen von Citrix Hypervisor ausgeführt werden, die derzeit unterstützt werden.

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

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

Wie kann ich auf die Konsole der Linux-basierten VM zugreifen?

Die Registerkarte Konsole in XenCenter bietet Zugriff auf die textbasierten und grafischen Konsolen von VMs, auf denen Linux-basierte Betriebssysteme ausgeführt werden. Bevor Sie eine Verbindung mit der grafischen Konsole einer Linux-VM herstellen können, stellen Sie sicher, dass der VNC-Server und ein X-Display-Manager auf der VM installiert und ordnungsgemäß konfiguriert sind.

Mit XenCenter können Sie auch eine Verbindung zu Linux-VMs über SSH herstellen, indem Sie die Option SSH-Konsole öffnen auf der Registerkarte Konsole der VM verwenden.

Wie kann ich auf die Konsole einer Windows-basierten VM zugreifen?

XenCenter bietet Zugriff auf die emulierten Grafiken für eine Windows VM. Wenn XenCenter Remotedesktopfunktionen auf der VM erkennt, stellt XenCenter eine Schnellverbindungsschaltfläche bereit, um einen integrierten RDP-Client zu starten, der eine Verbindung mit der VM herstellt. Oder Sie können sich direkt mit Ihren Gästen verbinden, indem Sie externe Remotedesktop-Software verwenden.

Befehlszeilenschnittstelle (CLI)

Enthält Citrix Hypervisor eine CLI?

Ja. Alle Editionen von Citrix Hypervisor verfügen über eine vollständige Befehlszeilenschnittstelle (CLI) — bekannt als`xe`.

Kann ich direkt auf dem Host auf die Citrix Hypervisor CLI zugreifen?

Ja. Sie können auf die CLI zugreifen, indem Sie einen Bildschirm und eine Tastatur verwenden, die direkt mit dem Host verbunden ist, oder über einen Terminalemulator, der mit dem seriellen Port des Hosts verbunden ist.

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

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

Kann ich die Citrix Hypervisor CLI mit meinen Active Directory Benutzerkonten verwenden?

Ja. Sie können sich mit Active Directory für alle Editionen von Citrix Hypervisor anmelden.

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

Ja. Sie können den Benutzerzugriff auf die Citrix Hypervisor CLI einschränken.

VMs

Können VMs, die mit VMware oder Hyper-V erstellt wurden, auf Citrix Hypervisor ausgeführt werden?

Ja. Sie können VMs mit dem branchenüblichen OVF-Format exportieren und importieren.

Sie können VMs auch in Batches mit Citrix Hypervisor Conversion Manager konvertieren. Tools von Drittanbietern sind ebenfalls verfügbar. Weitere Informationen finden Sie unter Konvertierungs-Manager.

Welche Arten von Installationsmedien kann ich verwenden, um ein Gastbetriebssystem zu installieren?

Sie können ein Gastbetriebssystem installieren, indem Sie:

- Eine CD im CD-ROM-Laufwerk des Hosts
- Ein virtuelles CD-ROM-Laufwerk mit Technologien wie iLO oder 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. Alle VM, die auf Citrix Hypervisor erstellt wurden, können geklont oder in eine VM-Vorlage konvertiert werden. Eine VM-Vorlage kann dann verwendet werden, um weitere VMs zu erstellen.

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

Ja. VMs, die aus älteren Versionen von Citrix Hypervisor exportiert wurden, können in eine neuere Version importiert werden.

Kann ich eine VM von der Open-Source-Version von Xen in Citrix Hypervisor konvertieren?

Nr.

Bietet Citrix Hypervisor Festplatten-Snapshot-Funktionen für VMs?

Ja. Citrix Hypervisor unterstützt Snapshotting in allen Editionen. Weitere Informationen finden Sie unter VM-Snapshots.

Speicher

Welche Arten von lokalen Speicher können mit Citrix Hypervisor verwendet werden?

Citrix Hypervisor unterstützt lokalen Speicher wie SATA und SAS.

Welcher SAN-/NAS-Speichertyp kann mit Citrix Hypervisor verwendet werden?

Citrix Hypervisor unterstützt Fibre Channel-, FCoE-, hardwarebasierte iSCSI- (HBA), iSCSI-, NFS- und SMB-Speicher-Repositories. Weitere Informationen finden Sie unterSpeicherund imHardwarekompatibilitätsliste.

Unterstützt Citrix Hypervisor softwarebasiertes iSCSI?

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

Welche Version von NFS ist für den Remotespeicher erforderlich?

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

Kann ich softwarebasiertes NFS verwenden, das auf einem Allzweckserver ausgeführt wird, für freigegebenen Remote-Massenspeicher?

Ja. Obwohl Citrix empfiehlt, ein dediziertes NAS-Gerät mit NFSv3 oder NFSv4 mit nicht-flüchtiger Hochgeschwindigkeits-Caching zu verwenden, um akzeptable E/A-Leistung zu erreichen.

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

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

Kann ich einen Citrix Hypervisor Host mit UEFI booten?

Ja. Citrix Hypervisor unterstützt das Starten von BIOS und UEFI.

Unterstützt Citrix Hypervisor Multipath I/O (MPIO) für Speicherverbindungen?

Ja. Citrix empfiehlt die Verwendung von Multipath für belastbare Speicherverbindungen.

Unterstützt Citrix Hypervisor eine softwarebasierte RAID-Implementierung?

Nein. Citrix Hypervisor unterstützt kein Software-RAID.

Unterstützt Citrix Hypervisor HOSTRAID- oder FakerAid-Lösungen?

Nein. Citrix Hypervisor unterstützt keine proprietären RAID-ähnlichen Lösungen wie HostRAID oder FakerAid.

Unterstützt Citrix Hypervisor Thin Cloning vorhandener VMs?

Ja. Thin Cloning ist auf lokalen Datenträgern verfügbar, die als EXT3 formatiert sind, zusätzlich zu NFS- und SMB-Speicher-Repositories.

Unterstützt Citrix Hypervisor Distributed Replicated Block Device (DRBD) -Speicher?

Nein. Citrix Hypervisor unterstützt DRBD nicht.

Unterstützt Citrix Hypervisor ATA over Ethernet?

Nein. Citrix Hypervisor unterstützt keinen ATA-über-Ethernet-basierten Speicher.

Vernetzung

Kann ich private Netzwerke erstellen, die Gruppen von VMs isolieren?

Ja. Sie können ein privates Netzwerk auf einem einzelnen Host für residierende VMs erstellen. Mit der vSwitch Controller Appliance können Sie auch private Netzwerke erstellen, die mehrere Hosts mit oder ohne Verschlüsselung umfassen.

Unterstützt Citrix Hypervisor mehrere physische Netzwerkverbindungen?

Ja. Sie können mehrere physische Netzwerke herstellen, die an verschiedene Netzwerkschnittstellen auf dem physischen Hostsystem angeschlossen sind.

Können VMs eine Verbindung zu mehreren Netzwerken herstellen?

Ja. VMs können eine Verbindung zu jedem Netzwerk herstellen, das für den Host verfügbar ist.

Unterstützt Citrix Hypervisor IPv6?

Gast-VMs, die auf Citrix Hypervisor gehostet werden, können eine beliebige Kombination von IPv4- und IPv6-konfigurierten Adressen verwenden.

Citrix Hypervisor unterstützt jedoch die Verwendung von IPv6 in der Steuerdomäne (Dom0) nicht. IPv6 kann nicht für das Hostverwaltungsnetzwerk oder das Speichernetzwerk verwendet werden. IPv4 muss verfügbar sein, damit der Citrix Hypervisor Host verwendet werden kann.

Unterstützt Citrix Hypervisor VLANs auf einer physischen Netzwerkschnittstelle?

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

Übergeben virtuelle Citrix Hypervisor Netzwerke den gesamten Netzwerkverkehr an alle VMs?

Nein. Citrix Hypervisor verwendet Open vSwitch (OVS), der als Layer 2-Switch fungiert. Eine VM sieht nur den Datenverkehr für diese VM. Darüber hinaus ermöglicht die Unterstützung für mehrere Mandanten in Citrix Hypervisor ein höheres Maß an Isolation und Sicherheit.

Unterstützen die virtuellen Netzwerkschnittstellen und Netzwerke den Promiscuous-Modus?

Ja. Virtuelle Netzwerkschnittstellen können für den Promiscuous-Modus konfiguriert werden, sodass Sie den gesamten Datenverkehr auf einem virtuellen Switch anzeigen können. Weitere Informationen zur Konfiguration des Promiscuous-Modus finden Sie in den folgenden Knowledge Center-Artikeln:

- CTX116493 - Aktivieren des Promiscuous-Modus auf einer physischen Netzwerkkarte
- CTX121729 - Konfigurieren einer promiscuous virtuellen Maschine in XenServer

Darüber hinaus ermöglicht der Open vSwitch die Konfiguration von RSPAN zur Erfassung des Netzwerkverkehrs.

Unterstützt Citrix Hypervisor das Verbinden oder das Verbinden von physischen Netzwerkschnittstellen?

Ja. Citrix Hypervisor unterstützt physische Netzwerkschnittstellenbindung für Failover und Link-Aggregation mit optionaler LACP-Unterstützung. Weitere Informationen finden Sie unter Vernetzung.

Speicher

Wie viel Arbeitsspeicher wird durch die Ausführung von Citrix Hypervisor belegt?

Drei Komponenten tragen zum Speicherbedarf eines Citrix Hypervisor Hosts bei.

1. Der Xen Hypervisor
2. Die Control Domain auf dem Host (dom0)
3. Der Citrix Hypervisor Absturzkernel

Die zum Ausführen von dom0 erforderliche Speichermenge wird automatisch angepasst. Die Menge des zugewiesenen Speichers basiert auf der Menge des physischen Speichers auf dem Host, wie in der folgenden Tabelle dargestellt:

Hostspeicher (GB)	Zugewiesener Domänenspeicher steuern (MB)
<24	752
24–47	2048

Hostspeicher (GB)	Zugewiesener Domänenspeicher steuern (MB)
48–63	3072
64–1024	4096

> **Hinweis:**
>
> Die Speichermenge, die der Control Domain zugewiesen ist, kann über die in der obigen Tabelle angegebenen Beträge hinaus erhöht werden. Sie müssen diese Zuweisung jedoch nur unter Anleitung von Citrix Support erhöhen.

In XenCenter meldet das Feld Xen auf der Registerkarte Speicher den Speicher, der von der Steuerdomäne, vom Xen-Hypervisor selbst und vom Citrix Hypervisor Crash-Kernel verwendet wird. Der vom Hypervisor verwendete Arbeitsspeicher ist für Hosts mit mehr Arbeitsspeicher größer.

Weitere Informationen finden Sie unter Speichernutzung

Optimiert Citrix Hypervisor die Speicherauslastung des virtuellen Rechners?

Ja. Citrix Hypervisor verwendet Dynamic Memory Control (DMC), um den Speicher ausgeführter VMs automatisch anzupassen. Durch diese Anpassungen wird die Menge an Arbeitsspeicher, die jeder VM zugewiesen wird, zwischen festgelegten Mindest- und Maximalspeicherwerten beibehalten, was die Leistung garantiert und eine höhere VM-Dichte ermöglicht.

Weitere Informationen finden Sie unter VM-Speicher.

Ressourcenpools

Was ist ein Ressourcenpool?

Ein Ressourcenpool ist eine Sammlung von Citrix Hypervisor Hosts, die als Einheit verwaltet werden. In der Regel verwendet ein Ressourcenpool eine gewisse Menge an Netzwerkspeicher, damit VMs schnell von einem Host auf einen anderen innerhalb des Pools migriert werden können. Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

Benötigt Citrix Hypervisor einen dedizierten Host zur Verwaltung eines Ressourcenpools?

Nein. Ein einzelner Host im Pool muss als Poolmaster angegeben werden. Der Poolmaster steuert alle administrativen Aktivitäten, die für den Pool erforderlich sind. Dieses Design bedeutet, dass es keinen externen Single Point of Failure gibt. Wenn der Poolmaster fehlschlägt, arbeiten andere Hosts

im Pool weiter, und die residenten VMs werden weiterhin normal ausgeführt. Wenn der Poolmaster nicht wieder online sein kann, stuft Citrix Hypervisor einen der anderen Hosts im Pool zum Master auf, um die Kontrolle über den Pool wiederherzustellen.

Dieser Prozess wird mit der Funktion „Hochverfügbarkeit“ automatisiert. Weitere Informationen finden Sie unter Hohe Verfügbarkeit.

Wo werden die Konfigurationsdaten für einen Ressourcenpool gespeichert?

Eine Kopie der Konfigurationsdaten wird auf jedem Host im Ressourcenpool gespeichert. Wenn der aktuelle Poolmaster fehlschlägt, können diese Daten alle Hosts im Ressourcenpool zum neuen Poolmaster werden.

Welche Konfigurationstypen können auf Ressourcenpoolebene vorgenommen werden?

Shared Remotespeicher- und Netzwerkkonfigurationen können auf Ressourcenpool-Ebene vorgenommen werden. Wenn eine Konfiguration im Ressourcenpool gemeinsam genutzt wird, propagiert das Mastersystem automatisch Konfigurationsänderungen an alle Mitgliedssysteme.

Werden neue Hostsysteme zu einem Ressourcenpool automatisch mit freigegebenen Einstellungen konfiguriert?

Ja. Alle neuen Hostsysteme, die einem Ressourcenpool hinzugefügt werden, erhalten automatisch dieselben Konfigurationen für den freigegebenen Speicher und die Netzwerkeinstellungen.

Kann ich verschiedene CPU-Typen im selben Citrix Hypervisor Ressourcenpool verwenden?

Ja. Citrix empfiehlt, dass der gleiche CPU-Typ im gesamten Pool verwendet wird (homogener Ressourcenpool). Es ist jedoch möglich, dass Hosts mit unterschiedlichen CPU-Typen einem Pool beitreten (heterogen), sofern die CPUs vom selben Anbieter stammen.

Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

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

Live-Migration (ehemals XenMotion)

Kann ich eine laufende VM von einem Host auf einen anderen verschieben?

Mit der Live-Migration können Sie ausgeführte VMs verschieben, wenn Hosts denselben Speicher (in einem Pool) gemeinsam nutzen.

Darüber hinaus ermöglicht die Massenspeicher-Livemigration die Migration zwischen Hosts, die keinen Speicher gemeinsam nutzen. VMs können innerhalb oder über Pools hinweg migriert werden.

Hohe Verfügbarkeit

Bietet Citrix Hypervisor Funktionen für hohe Verfügbarkeit?

Ja. Wenn High Availability (HA) aktiviert ist, überwacht Citrix Hypervisor kontinuierlich den Zustand der Hosts in einem Pool. Wenn HA erkennt, 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 Citrix Hypervisor High Availability lokalen Speicher?

Nein. Wenn Sie HA verwenden möchten, ist gemeinsam genutzter Speicher erforderlich. Mit diesem freigegebenen Speicher können VMs verlagert werden, wenn ein Host ausfällt. HA ermöglicht jedoch, dass VMs, die auf dem lokalen Speicher gespeichert sind, für den automatischen Neustart markiert werden, wenn der Host nach einem Neustart wiederhergestellt wird.

Kann ich HA verwenden, um den Neustart wiederhergestellten VMs automatisch zu sequenzieren?

Ja. Mit der HA-Konfiguration können Sie die Reihenfolge definieren, in der VMs gestartet werden. Mit dieser Funktion können VMs, die voneinander abhängig sind, automatisch sequenziert werden.

Performance-Metriken

Sammeln die Citrix Hypervisor Verwaltungstools Leistungsinformationen?

Ja. Citrix Hypervisor bietet eine detaillierte Überwachung der Leistungsmetriken. Diese Metriken umfassen CPU, Arbeitsspeicher, Festplatte, Netzwerk, C-State/P-Statusinformationen und Speicher. Gegebenenfalls sind diese Metriken auf Host- und VM-Basis verfügbar. Leistungsmetriken sind direkt verfügbar (als

Round-Robin-Datenbanken verfügbar) oder können in XenCenter oder anderen Anwendungen von Drittanbietern auf grafische Weise aufgerufen und angezeigt werden. Weitere Informationen finden Sie unter Überwachen und Verwalten Ihrer Bereitstellung.

Wie werden Performance-Metriken von Citrix Hypervisor erfasst?

Die Daten für die Performance-Metriken von Citrix Hypervisor 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 Echtzeit-Leistungsmetriken auf der Registerkarte Leistung für jede ausgeführte VM sowie für den Citrix Hypervisor Host an. Sie können die angezeigten Metriken anpassen.

Speichert und zeigt XenCenter historische Leistungsmetriken an?

Ja. Citrix Hypervisor hält Performance-Metriken aus dem letzten Jahr (mit abnehmender Granularität). XenCenter bietet eine Visualisierung dieser Metriken in grafischen Echtzeitdarstellungen.

Installation

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

Nein. Citrix Hypervisor wird direkt auf Bare-Metal-Hardware installiert, wodurch die Komplexität, Overhead und Performance-Engpässe eines zugrunde liegenden Betriebssystems vermieden werden.

Kann ich eine vorhandene Citrix Hypervisor XenServer Installation auf eine neuere Version aktualisieren?

Ja. Wenn Sie bereits eine unterstützte Version von Citrix Hypervisor oder XenServer installiert haben, können Sie anstelle einer Neuinstallation auf eine neuere Version von Citrix Hypervisor aktualisieren oder aktualisieren. Weitere Informationen finden Sie unter Update und Aktualisieren.

Kann ich ein Upgrade von einer nicht unterstützten Version von Citrix Hypervisor oder XenServer Installation auf diese Version durchführen?

Wenn Ihre vorhandene Version von Citrix Hypervisor oder XenServer nicht mehr unterstützt wird, können Sie nicht direkt auf die neueste Version von Citrix Hypervisor aktualisieren oder aktualisieren.

- Für XenServer und 6.5 Service Pack 1 können Sie zuerst ein Upgrade auf XenServer 7.1 kumulative Update 2 durchführen und dann von XenServer 7.1 kumulative Update 2 auf Citrix Hypervisor 8.0 aktualisieren.
- Für andere 6.x-Versionen von XenServer können Sie kein Upgrade auf die neueste Version durchführen und müssen eine Neuinstallation von Citrix Hypervisor 8.0 erstellen.
- Für aktuelle Versionen von XenServer 7.x ohne Support können Sie kein Upgrade auf die neueste Version durchführen und eine Neuinstallation von Citrix Hypervisor 8.0 erstellen.

Alle anderen Upgrade-Pfade für diese nicht unterstützten Versionen werden nicht unterstützt.

Wie viel lokaler Speicher benötigt Citrix Hypervisor für die Installation auf dem physischen Hostsystem?

Citrix Hypervisor benötigt mindestens 46 GB lokalen Speicher auf dem physischen Hostsystem.

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

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

Läuft der Xen Hypervisor unter Linux?

Nein. Xen ist ein Hypervisor des Typs 1, der direkt auf der Host-Hardware ausgeführt wird („Bare Metal“). Nachdem der Hypervisor geladen wurde, startet er die privilegierte Verwaltungsdomäne — die Control Domain, die eine minimale Linux-Umgebung enthält.

Wo erhält Citrix Hypervisor seine Gerätetreiberunterstützung?

Citrix Hypervisor verwendet die vom Linux-Kernel verfügbaren Gerätetreiber. Daher wird Citrix Hypervisor auf einer Vielzahl von Hardware- und Speichergeräten ausgeführt. Citrix empfiehlt jedoch, zertifizierte Gerätetreiber zu verwenden.

Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste.

Lizenzierung

Wie lizenziere ich Citrix Hypervisor?

Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unterLizenzierung

Technischer Support

Bietet Citrix direkten technischen Support für Citrix Hypervisor?

Ja. Weitere Informationen finden Sie unter Citrix Support und Services.

Kann ich technischen Support für Citrix Hypervisor und andere Citrix Produkte in einem einzigen Support-Vertrag erhalten?

Ja. Citrix stellt Verträge über den technischen Support bereit, mit denen Sie Supportvorfälle auf Citrix Hypervisor und anderen Citrix Produkten öffnen können.

Weitere Informationen finden Sie unter Citrix Support und Services.

Muss ich gleichzeitig mit dem Kauf von Citrix Hypervisor einen Vertrag für den technischen Support von Citrix erwerben?

Nein. Sie können einen Vertrag über den technischen Support von Citrix entweder am Point of Sale oder zu einem anderen Zeitpunkt erwerben.

Gibt es alternative Kanäle für technischen Support für Citrix Hypervisor?

Ja. Für den technischen Support für Citrix Hypervisor stehen mehrere alternative Kanäle zur Verfügung. Sie können auch unsere Foren nutzenCitrix Support Knowledge Center, besuchen oder mit autorisierten Citrix Hypervisor Partnern abschließen, die technischen Support-Services anbieten.

Bietet Citrix technischen Support für das Open-Source-Xen en-Projekt?

Nein. Citrix bietet keinen technischen Support für das Open-Source-Xen en-Projekt. Weitere Informationen finden Sie unterhttp://www.xen.org/.

Kann ich einen technischen Support-Vorfall mit Citrix öffnen, wenn ein nicht technisches Problem auftritt?

Nein. Beheben Sie nicht technische Probleme mit Citrix Hypervisor über den Citrix Customer Service. Beispielsweise Probleme mit Softwarewartung, Lizenzierung, Administrationsunterstützung und Auftragsbestätigung.

Kopiert!
Failed!

Lizenzierung

October 16, 2019

Citrix Hypervisor 8.0 ist in den folgenden Editionen verfügbar:

- Premium Edition (zuvor Enterprise Edition)
- Standard Edition
- Express Edition (bisher Free Edition)

Die **Standard Edition** ist unser kommerzielles Einstiegsangebot. Es verfügt über eine Reihe von Funktionen für Kunden, die eine robuste und leistungsstarke Virtualisierungsplattform wünschen, aber die Premium-Funktionen der Premium Edition nicht benötigen. In der Zwischenzeit möchten sie weiterhin von der umfassenden Citrix Support und Wartung profitieren.

Die **Premium Edition** ist unser Premium-Angebot, das für Desktop-, Server- und Cloud-Workloads optimiert ist. Neben den Funktionen der Standard Edition bietet die Premium Edition folgende Funktionen:

- Automatische Windows VM-Treiberaktualisierungen
- Automatische Aktualisierung des Management Agents
- Unterstützung für SMB-Speicher
- Direkte Inspektion von APIs
- Dynamischer Arbeitslastausgleich
- GPU-Virtualisierung mit NVIDIA GRID, AMD MxGPU und Intel GVT-G
- Konversionsdienstprogramme für VMware vSphere zu Citrix Hypervisor
- Intel Secure Measured Boot (TXT)
- Exportieren von Pool-Ressourcendaten
- In-Memory-Lese-Caching
- PVS-Beschleuniger
- Automatisierte Updates mit XenCenter
- Live-Patching von Citrix Hypervisor

- Aktivierung für Citrix Virtual Desktops Tablet-Modus
- Blockverfolgung geändert
- IGMP-Snooping
- USB-Durchgang
- SR-IOV-Netzwerkunterstützung
- Thin Provisioning für gemeinsam genutzte Blockspeichergeräte

Premium Edition wurde in früheren Versionen von Citrix Hypervisor als Enterprise Edition bezeichnet. Der Name der Edition wurde geändert, um sich an andere Citrix Produkte anzupassen, aber die Funktionen und Funktionen der Edition haben sich nicht geändert.

Kunden, die Citrix Virtual Apps oder Citrix Virtual Desktops erworben haben, haben Anspruch auf Citrix Hypervisor, der alle für Premium Edition aufgeführten Funktionen umfasst.

Die **Express Edition** bietet einen reduzierten Funktionsumfang und ist nicht für Citrix Support und Wartung qualifiziert. Express Edition erfordert keine Lizenz. Hosts, auf denen die Express Edition von Citrix Hypervisor ausgeführt wird, werden in XenCenter als „Nicht lizenziert“ bezeichnet.

Express Edition wurde in früheren Versionen von Citrix Hypervisor als Free Edition bezeichnet. Der Name der Edition wurde geändert, um sich an andere Citrix Produkte anzupassen, aber die Funktionen und Funktionen der Edition haben sich nicht geändert.

Weitere Informationen finden Sie unter Citrix Hypervisor Feature-Matrix.

Citrix Hypervisor verwendet denselben Lizenzierungsprozess wie andere Citrix Produkte und erfordert daher eine gültige Lizenz auf einem Lizenzserver. Sie können den Lizenzserver von herunterladenCitrix Lizenzierung. Citrix Hypervisor (außer über die Lizenzen für Citrix Virtual Apps and Desktops) wird *pro Socket-Basis* lizenziert. Die Zuweisung von Lizenzen wird zentral verwaltet und durch einen eigenständigen, physischen oder virtuellen Citrix Lizenzserver in der Umgebung durchgesetzt. Nach der Anwendung einer Pro-Socket-Lizenz wird Citrix Hypervisor als *Citrix Hypervisor Pro-Socket-Edition angezeigt. *

> **Hinweis:**
>
> Gemischte Pools von lizenzierten und nicht lizenzierten Hosts verhalten sich so, als wären alle Hosts nicht lizenziert.

Nicht lizenzierte Hosts unterliegen Einschränkungen. Weitere Informationen finden Sie unter Weitere Fragen.

Übersicht über Lizenzierungsschritte

Sie benötigen die folgenden Elemente, um Citrix Hypervisor Premium Edition oder Standard Edition zu lizenzieren:

- Eine Citrix Hypervisor-Lizenz

- Ein Citrix Lizenzserver
- Ein Citrix Hypervisor -Server
- XenCenter

Die folgenden Schritte geben einen Überblick über den Prozess:

1. Installieren Sie Citrix License Server, oder importieren Sie die virtuelle Citrix License Server Appliance in einen Citrix Hypervisor or-Server.
2. Lizenzdatei herunterladen
3. Hinzufügen der Lizenzdatei zum Citrix Lizenzserver
4. Geben Sie mithilfe von XenCenter die Lizenzserverdetails ein und wenden Sie sie auf Hosts im Ressourcenpool an.

Weitere Informationen zur Citrix Lizenzierung finden Sie imCitrix Lizenzierungsdokumentation.

Lizenzierung von Citrix Hypervisor

F: Wo kann ich eine Citrix Hypervisor-Lizenz erwerben?

A: Sie können eine Citrix Hypervisor-Lizenz bei erwerbenhttp://citrix.com/buy.

F: Wie kann ich eine Citrix Hypervisor-Lizenz anwenden?

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

- Ein Windows -Server, auf dem die Citrix License Server-Software
  oder
- Die virtuelle Citrix License Server Appliance.

Wenn Sie einem Citrix Hypervisor or-Server eine Lizenz zuweisen, kontaktiert Citrix Hypervisor den angegebenen Citrix Lizenzserver und fordert eine Lizenz für die angegebenen Server an. Wenn erfolgreich, wird eine Lizenz ausgecheckt und der Lizenzmanager zeigt Informationen über die Lizenz an, unter der die Hosts lizenziert sind.

Anweisungen zum Anwenden einer Citrix Hypervisor-Lizenz auf eine virtuelle Citrix License Server Appliance finden Sie unterCTX200159 — Anwenden einer Citrix Hypervisor or-Lizenzdatei auf Citrix License Server Virtual Appliance (CLSVA).

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

A: Citrix Hypervisor ist auf Basis *pro CPU-Sockel* lizenziert. Damit ein Pool als lizenziert gilt, müssen alle Citrix Hypervisor or-Server im Pool lizenziert sein. Citrix Hypervisor zählt nur befüllte CPU-Sockets.

Mit dem Citrix License Server können Sie die Anzahl der verfügbaren Lizenzen anzeigen, die im *Dashboard der License Administration Console*angezeigt werden.

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

A: Nein, nur befüllte CPU-Sockets 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 VMs oder deren Daten.

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

A. Wenn Ihre Lizenz noch nicht abgelaufen ist und der Lizenzserver nicht verfügbar ist, erhalten Sie eine *Nachfrist* von 30 Tagen auf der zuvor angewendeten Lizenzstufe.

F: Ich führe ein Upgrade von einer früheren Citrix Hypervisor Version mit einer Pro-Socket-Lizenz auf Citrix Hypervisor 8.0 durch. Muss ich etwas tun?

A: Nein. Sie können Ihre Hosts mit den zuvor erworbenen Pro-Socket-Lizenzen auf Citrix Hypervisor 8.0 Premium Edition upgraden, vorausgesetzt der Customer Success Services ist mindestens bis zum 27. März 2019 gültig.

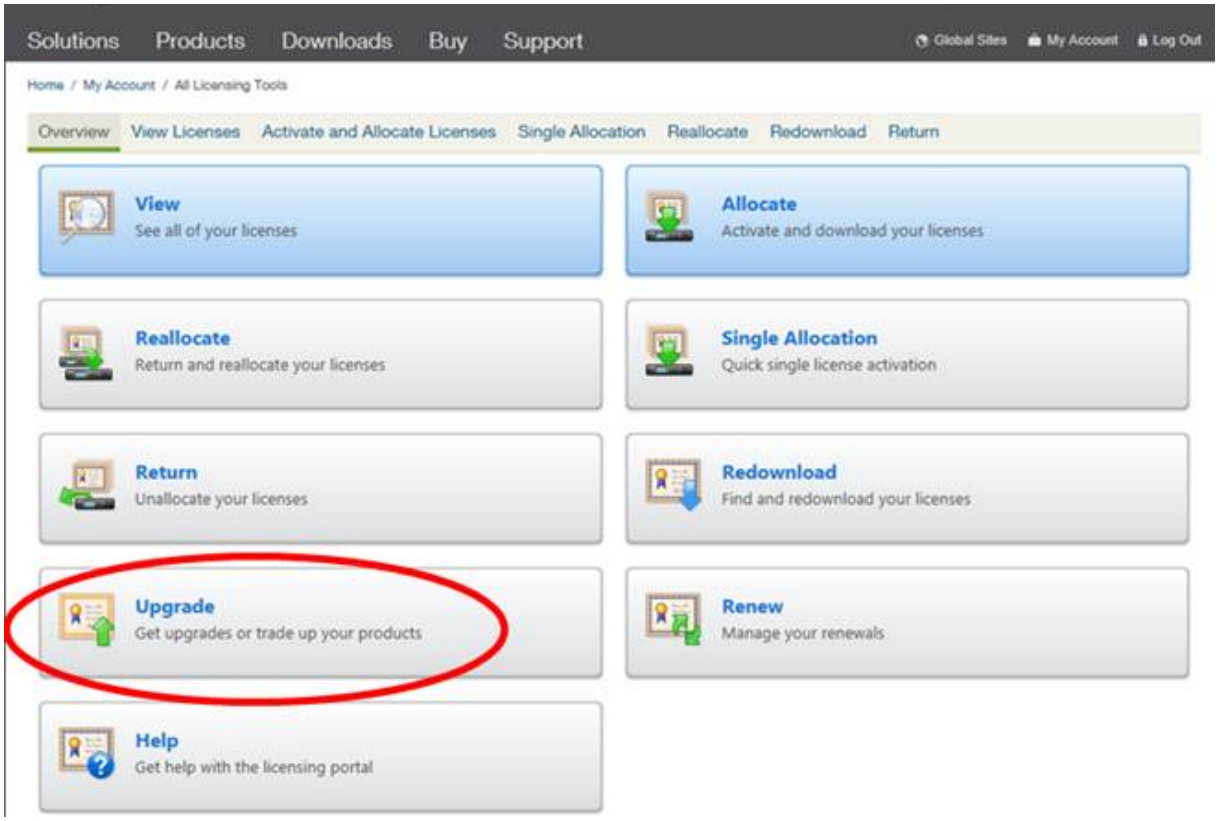
Wenn Sie Ihre Customer Success Services nach dem ursprünglichen Kauf erneuert haben, müssen Sie möglicherweise die Lizenzdatei auf dem Lizenzserver aktualisieren, um sicherzustellen, dass die Berechtigung für die Customer Success Services angezeigt wird.

F: Ich gehe von der nicht lizenzierten XenServer 7.6 auf Citrix Hypervisor 8.0 um. Muss ich irgendetwas tun?

A: Nein. Sie können Ihre Hosts auf Citrix Hypervisor 8.0 aktualisieren oder aktualisieren. Sie erhalten weiterhin keine Supportberechtigung und Premium-Funktionen (einschließlich Rolling Pool Upgrade) sind erst verfügbar, wenn eine entsprechende Lizenz beantragt wurde.

F: Ich bin ein Kunde von Citrix Virtual Apps and Desktops, der von XenServer 7.6 auf Citrix Hypervisor 8.0 wechselt. Muss ich irgendetwas tun?

A: Nein. Kunden von Citrix Virtual Apps oder Citrix Virtual Desktops können nahtlos auf Citrix Hypervisor 8.0 aktualisieren. Ihre vorhandene installierte Citrix Virtual Apps oder Citrix Virtual Desktops Lizenz gewährt Ihnen Anspruch auf Citrix Hypervisor, ohne dass weitere Änderungen erforderlich sind.



F: Ich bin ein Citrix Service Provider, der für Citrix Virtual Apps and Desktops lizenziert ist. Kann ich diese Lizenz für Citrix Hypervisor verwenden, wenn ich ein Upgrade auf Citrix Hypervisor 8.0 mache?

A: Ja. Citrix Hypervisor 8.0 unterstützt Ihre Lizenz. Mit dieser Lizenz können Sie alle Premium-Funktionen der Premium Edition von Citrix Hypervisor nutzen. Um diese Lizenz auf Ihre Pools anzuwenden, aktualisieren Sie zuerst alle Hosts im Pool, um Citrix Hypervisor 8.0 auszuführen.

F: Ich bin Kunde mit einem Citrix Virtual Apps and Desktops Service-Abonnement. Habe ich das Recht, Citrix Hypervisor 8.0 zu verwenden?

A: Ja. Wenn Sie über ein Citrix Virtual Apps and Desktops Service-Abonnement verfügen, das die Verwendung lokaler Desktops und Apps ermöglicht, sind Sie berechtigt, Citrix Hypervisor zum Hosten

dieser Desktops und Apps zu verwenden.

Laden Sie eine Lizenz über das Lizenzierungsverwaltungs-Tool herunter. Installieren Sie diese Lizenz auf Ihrem Lizenzserver, um den lokalen Citrix Hypervisor mit Ihrem Citrix Virtual Apps and Desktops Service-Abonnement zu verwenden.

Mit dieser Lizenz können Sie alle die gleichen Premium-Funktionen wie eine lokale Citrix Virtual Apps and Desktops Berechtigung nutzen. Um diese Lizenz auf Ihre Pools anzuwenden, aktualisieren Sie zuerst alle Hosts im Pool, um Citrix Hypervisor 8.0 auszuführen.

F: Welche Einschränkungen bestehen bei der Verwendung der erweiterten Virtualisierungsverwaltungsfunktionen von Citrix Hypervisor Premium Edition, die im Rahmen von Citrix Virtual Apps and Desktops bereitgestellt werden?

A: Jede Edition von Citrix Virtual Apps and Desktops hat Zugriff auf erweiterte Virtualisierungsverwaltungsfunktionen von Citrix Hypervisor Premium Edition. Eine vollständige Liste aller Funktionen, die durch eine Citrix Virtual Apps oder Citrix Virtual Desktops -Lizenz aktiviert werden, finden Sie in der Citrix Hypervisor Feature-Matrix.

Citrix Hypervisor Berechtigungen ermöglichen die Virtualisierung jeder Infrastruktur, die für die Bereitstellung von Citrix Virtual Apps oder Citrix Virtual Desktops Feature-Komponenten erforderlich ist. Auf diese Funktionen muss ausschließlich von lizenzierten Benutzern oder Geräten von Citrix Virtual Apps oder Citrix Virtual Desktops zugegriffen werden.

Zusätzliche Infrastrukturunterstützungsserver wie Microsoft-Domänencontroller und SQL-Server sind ebenfalls von dieser Berechtigung abgedeckt, sofern sie im gleichen Citrix Hypervisor Ressourcenpool bereitgestellt werden wie die Citrix Virtual Apps s- oder Citrix Virtual Desktops Infrastruktur, die von dieser Lizenz abgedeckt wird, und diese werden nur zur Unterstützung der Citrix Virtual Apps oder Citrix Virtual Desktops Infrastruktur verwendet.

Die Citrix Hypervisor Berechtigung in der Citrix Virtual Apps- oder Citrix Virtual Desktop-Lizenz kann nicht für Citrix Hypervisor Pools verwendet werden, die keine Citrix Virtual Apps oder Citrix Virtual Desktops oder Virtual Delivery Agents (VDAs) hosten. Sie können diese Berechtigung auch nicht zum Hosten von virtuellen Maschinen verwenden, die nicht von den oben genannten Berechtigungen abgedeckt sind. Citrix Hypervisor muss für diese Anwendungen separat erworben werden.

Citrix Lizenzserver

F: Welche Lizenzserver kann ich mit Citrix Hypervisor verwenden?

A: Sie können entweder die Citrix License Server-Software Version 11.14 oder höher (auf einem Server mit Microsoft Windows) oder die virtuelle Linux-basierte Citrix License Server-Appliance verwenden.

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

A: Informationen zum Importieren einer Lizenzdatei finden Sie imLizenzierungsdokumentation.

- Installieren von Lizenzen mithilfe von Citrix Licensing Manager
- Importieren von Lizenzdateien mithilfe der Licensing Administration Console
- Installieren von Lizenzdateien über die Befehlszeile

F: Kann ich den Lizenzserver auf meinem Citrix Hypervisor Pool ausführen?

A: Ja. Sie können die Citrix License Server-Software auf einer Windows VM installieren oder die virtuelle Linux-basierte Citrix License Server-Appliance importieren. Zur Vereinfachung der Bereitstellung ist die Citrix Lizenzserver-Software auf dieser virtuellen Appliance vorinstalliert und kann als VM im Citrix Hypervisor Pool ausgeführt werden.

Citrix Hypervisor arbeitet mit einer „Gnade“ -Lizenz, bis der Lizenzserver gestartet werden kann. Dieses Verhalten bedeutet, dass nach der Lizenzierung der Citrix Hypervisor or-Server in Ihrem Pool und dem Neustart des Hosts, auf dem der Citrix Lizenzserver ausgeführt wird, eine Kulanzfrist auf diesen Host angewendet wird, bis die Appliance neu gestartet wird.

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

A: Ja.

F: Kann ich Lizenzen für andere Citrix Produkte auf einer virtuellen Citrix License Server-Appliance oder auf der unter Windows installierten Citrix License Server-Software installieren?

A: Ja, Sie können andere Citrix Produkte mit der virtuellen Citrix License Server-Appliance oder über die unter Windows installierte Citrix License Server-Software lizenzieren. Weitere Informationen finden SieLizenzierungauf derCitrix ProduktdokumentationWebsite.

Lizenzieren eines Citrix Hypervisor Pools

F: Wie kann ich eine Lizenz auf alle Hosts anwenden, die XenCenter verwenden?

A: Gehen Sie folgendermaßen vor, um eine Lizenz anzuwenden:

1. Klicken Sie im Menü **Extras** auf **Lizenz-Manager** .

2. Select 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, und geben Sie den Hostnamen oder die IP-Adresse des Lizenzservers ein.

F: Kann ich eine Lizenz ohne XenCenter anwenden?

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|desktop-plus|
        desktop|standard-per-socket  \
2
3        license-server-address=<licenseserveraddress> host-uuid=<
            uuidofhost>  \
4
5        license-server-port=<licenseserverport>
```

Um einen Pool zu lizenzieren, verwenden Sie den Befehl pool-apply-edition. Zum Beispiel:

```
1    xe pool-apply-edition edition=enterprise-per-socket|desktop-plus|
        desktop|standard-per-socket  \
2
3        license-server-address=<licenseserveraddress> pool-uuid=<
            uuidofpool>  \
4
5        license-server-port=<licenseserverport>
```

F: Wie kann ich den Lizenzstatus meiner Hosts und Pools ermitteln?

A: XenCenter zeigt den Lizenztyp eines Servers oder Pools an.

Um den Lizenztyp eines Servers oder Pools anzuzeigen, wählen Sie diesen Server oder Pool in der Strukturansicht aus. XenCenter zeigt den Lizenzstatus in der Titelleiste für diesen Server oder Pool nach dem Server- oder Poolnamen an.

Gemischte Pools von lizenzierten und nicht lizenzierten Hosts verhalten sich so, als wären alle Hosts nicht lizenziert. In der Strukturansicht zeigt XenCenter nicht lizenzierte Pools mit einem Warndreiecksymbol an.

Weitere Fragen

F: Wie erhalte ich eine Lizenz für die Bewertung von Citrix Hypervisor?

A: Für die Evaluierung von Citrix Hypervisor benötigen Sie keine Lizenz. Sie können Citrix Hypervisor in einem nicht lizenzierten Zustand verwenden. Sie haben jedoch keinen Zugriff auf Premium-Funktionen. Darüber hinaus sind Sie nicht für Citrix Support oder Wartung berechtigt.

Sie können eine Testlizenz erhalten, um die Premium Edition-Funktionen zu testen. Weitere Informationen finden Sie unter Erste Schritte.

F: Kann ich Citrix Hypervisor ohne Lizenz verwenden?

A: Ja. Wenn Sie Citrix Hypervisor in einem nicht lizenzierten Zustand (Express Edition) verwenden, sind Sie nicht für Citrix Support oder Wartung berechtigt. Darüber hinaus sind die folgenden Funktionen eingeschränkt und erfordern eine Lizenz:

- Pools mit mehr als drei Hosts

> **Hinweis:**
>
> Diese Einschränkung wirkt sich nicht auf vorhandene Pools aus, die drei oder mehr Hosts enthalten, bis Sie versuchen, einen anderen Host zum Pool hinzuzufügen

- Hohe Verfügbarkeit
- Dynamische Speichersteuerung
- Storage Motion
- Rollenbasierte Zugriffssteuerung
- GPU-Passthrough
- Site Recovery Manager
- Active Directory Integration
- Upgrade des rollenden Pools

Sie können eine Testlizenz für Citrix Hypervisor Premium Edition erhalten. Weitere Informationen finden Sie unter Erste Schritte mit Citrix Hypervisor.

Weitere Informationen

- Weitere Hinweise zur Citrix Hypervisor 8.0 Version finden Sie unter*Citrix Hypervisor 8.0 — Versionshinweise*.

- Informationen zum Zugriff auf die Citrix Hypervisor 8.0 Produktdokumentation finden Sie unter Citrix Hypervisor 8.0 — Produktdokumentation.
- Eine Übersicht über das Citrix Hypervisor Produkt finden Sie unterTechnische Übersicht.
- CTX200159 — Anwenden einer Citrix Hypervisor or-Lizenzdatei auf Citrix License Server Virtual Appliance (CLSVA).
- Beheben Sie nicht technische Probleme mit Citrix Hypervisor, einschließlich Support für das Customer Success Services Programm, Lizenzierung, administrative Unterstützung und Auftragsbestätigung durchCitrix Kundenservice.

Kopiert!
Failed!

Installieren

October 16, 2019

Dieser Abschnitt enthält Verfahren, die Sie durch die Installation, Konfiguration und den ersten Betrieb von Citrix Hypervisor führen. Es enthält auch Informationen zur Problembehandlung bei Problemen, die während der Installation auftreten können, und verweist auf zusätzliche Ressourcen.

Diese Informationen richten sich in erster Linie an Systemadministratoren, die Citrix Hypervisor or-Server auf physischen Servern einrichten möchten.

Citrix Hypervisor wird direkt auf Bare-Metal-Hardware installiert, wodurch die Komplexität, Overhead und Performance-Engpässe eines zugrunde liegenden Betriebssystems vermieden werden. Es verwendet die vom Linux-Kernel verfügbaren Gerätetreiber. Daher kann Citrix Hypervisor auf einer Vielzahl von Hardware- und Speichergeräten ausgeführt werden. Stellen Sie jedoch sicher, dass Sie zertifizierte Gerätetreiber verwenden.

Weitere Informationen finden Sie unter Hardwarekompatibilitätsliste (HCL).

> **Wichtig:**
>
> Der Citrix Hypervisor or-Server muss auf einem dedizierten 64-Bit-x86-Server installiert sein. Installieren Sie kein anderes Betriebssystem in einer Dual-Boot-Konfiguration mit dem Citrix Hypervisor or-Server. Diese Konfiguration wird nicht unterstützt.

Bevor Sie beginnen

Berücksichtigen Sie vor der Installation von Citrix Hypervisor 8.0 die folgenden Faktoren:

- Welchen Release-Stream von Citrix Hypervisor möchten Sie verwenden?
- Was ist die geeignete Installationsmethode?
- Was sind die Systemanforderungen?

Citrix Hypervisor Release-Streams

Citrix Hypervisor Versionen befinden sich in einem der folgenden Release-Streams: Aktuelle Version (CR) oder Long Term Service Release (LTSR). Citrix Hypervisor 8.0 ist eine aktuelle Version. Wenn Sie auswählen, ob eine Version von Citrix Hypervisor aus dem CR-Stream oder dem LTSR-Stream installiert werden soll, sollten Sie Folgendes beachten:

- Wie oft möchten Sie Ihre Version von Citrix Hypervisor aktualisieren?
- Bevorzugen Sie einen stabilen Featuresatz oder den neuesten Featuresatz?

Aktueller Release

Aktuelle Versionen von Citrix Hypervisor ermöglichen es Ihnen, neue Funktionen so bald wie möglich zu nutzen. Jedes Quartal werden neue Versionen von Citrix Hypervisor aus dem CR-Stream veröffentlicht. Wenn Sie sich im CR-Stream befinden, müssen Sie regelmäßig neue CRs übernehmen, um weiterhin Unterstützung zu erhalten. Die meisten in Citrix Hypervisor CR erkannten Probleme werden in einer nachfolgenden aktuellen Version behoben. Sicherheitsprobleme werden in Hotfixes behoben, die auf die CR angewendet werden können.

Wenn XenServer 7.6 oder 7.5 installiert ist, müssen Sie zu Citrix Hypervisor 8.0 wechseln, um weiterhin Unterstützung zu erhalten.

Langfristige Service-Freigabe

Langfristige Service-Releases von Citrix Hypervisor, ehemals XenServer, garantieren Stabilität in Bezug auf den Featuresatz in Citrix Hypervisor. Neue Versionen von Citrix Hypervisor aus dem LTSR-Stream werden alle zwei Jahre veröffentlicht und werden bis zu 10 Jahre lang unterstützt. Alle Probleme in Citrix Hypervisor LTSR werden in Hotfixes oder kumulativen Updates behoben, die auf Citrix Hypervisor LTSR angewendet werden können.

Wenn Sie derzeit XenServer 7.1 Kumulative Update 2 LTSR installiert haben, können Sie auf den aktuellen Datenstrom von Citrix Hypervisor aktualisieren, um die neuen Funktionen zu nutzen.

Installationsmethoden

Citrix Hypervisor 8.0 kann auf eine der folgenden Arten installiert werden:

- Als Neuinstallation
- Als Upgrade auf eine frühere unterstützte Version von Citrix Hypervisor

Vorhandene Version von Citrix Hypervisor oder XenServer	So erhalten Sie Citrix Hypervisor 8.0	Zu verwendende ISO-Datei
Keine	Neuinstallation	Basisinstallation ISO
7.6, 7.5, 7.1 Kumulatives Update 2, 7.0	Aktualisieren	Basisinstallation ISO

> **Hinweis: *
>
> Das Upgrade wird nur vom neuesten kumulativen Update der LTSR unterstützt. Wenn Ihre vorhandene XenServer Version 7.1 oder 7.1 kumulatives Update 1 ist, wenden Sie zuerst 7.1 kumulative Update 2 an, bevor Sie ein Upgrade auf Citrix Hypervisor 8.0 durchführen.

Es gibt keinen unterstützten direkten Upgradepfad von Versionen von XenServer auf Citrix Hypervisor 8.0. Führen Sie stattdessen eine Neuinstallation durch.

Neuinstallation

Wenn Sie eine Neuinstallation von Citrix Hypervisor 8.0 erstellen:

- Verwenden Sie die **Citrix Hypervisor 8.0 Basisinstallations-ISO-Datei**.

  Sie können diese Datei von derCitrix Download-Site

- [Überprüfen Sie die Informationen inSystemvoraussetzungenLizenzierung von Citrix Hypervisor[], undInstallieren von Citrix Hypervisor und XenCenter()vor der Installation von Citrix Hypervisor .]

Update

Aufgrund des von Citrix Hypervisor 8.0 bereitgestellten Plattformupdates können Sie den Aktualisierungsmechanismus nicht verwenden, um aus früheren aktuellen XenServer Versionen zu wechseln. Verwenden Sie stattdessen den Upgrade-Mechanismus.

Aktualisieren

Wenn Sie ein Upgrade von XenServer 7.1 Kumulatives Update 2 oder 7.0 auf Citrix Hypervisor 8.0 durchführen:

- Verwenden Sie die **Citrix Hypervisor 8.0 Basisinstallations-ISO-Datei**.

  Sie können diese Datei von der herunterladenCitrix Download-Site.

- Überprüfen Sie die Informationen inSystemvoraussetzungenundUpgrade von einer vorhandenen Versionvor dem Upgrade von Citrix Hypervisor.

Speicherorte installieren

Installieren Sie den Citrix Hypervisor or-Server mithilfe einer der folgenden Methoden:

- Von einer CD

  Sie können das Installationsprogramm (ISO-Dateiformat) herunterladen und auf eine CD brennen.

  Um das Installationsprogramm herunterzuladen, besuchen Sie dieCitrix DownloadsSeite.

  Die Hauptinstallationsdatei enthält die grundlegenden Pakete, die zum Einrichten von Citrix Hypervisor auf Ihrem Host erforderlich sind.

- Richten Sie einen netzwerkfähigen TFTP-Server zum Starten ein.

  Weitere Informationen zum Einrichten eines TFTP-Servers zum Starten des Installationsprogramms über das Netzwerk finden Sie unterNetzwerk-Boot-Installation.

- Installieren von Citrix Hypervisor auf einem Remote-Datenträger auf einem SAN, um den Start von SAN zu aktivieren

  Weitere Informationen finden Sie unter Starten von SAN.

Ergänzungspakete

Sie können jedes erforderliche Zusatzpaket nach der Installation von Citrix Hypervisor installieren. Laden Sie das Ergänzungspaket (Dateiname.iso) an einen bekannten Speicherort auf Ihrem Computer herunter und installieren Sie das Ergänzungspaket auf die gleiche Weise wie ein Update.

Weitere Informationen finden Sie unter Ergänzungspakete und der DDK-Leitfaden.

Upgrades

Das Installationsprogramm stellt die Option zum Upgrade vor, wenn eine zuvor installierte Version von Citrix Hypervisor erkannt wird. Der Upgrade-Prozess folgt dem Erstinstallationsprozess, mehrere Setup-Schritte werden jedoch umgangen. Die vorhandenen Einstellungen werden beibehalten, einschließlich Netzwerkkonfiguration, Systemzeit usw.

> **Wichtig:**
>
> Das Upgrade erfordert eine sorgfältige Planung und Aufmerksamkeit. Ausführliche Informationen zum Aktualisieren einzelner Citrix Hypervisor or-Server und -Pools finden Sie unterUpgrade

> von einer vorhandenen Version.

Installieren des Citrix Hypervisor -Servers

> **Tipp:**
>
> Während der Installation schnell zum nächsten Bildschirm wechseln, indem Sie F12 drücken. Verwenden Sie Tabulatortaste, um zwischen Elementen zu wechseln, und Raum oder Eingabetaste, um auszuwählen. Drücken Sie F1, um allgemeine Hilfe zu erhalten.
>
> **Warnhinweis:**
>
> Bei der Installation von Citrix Hypervisor werden Daten auf allen Festplatten überschrieben, die Sie für die Installation auswählen. Sichern Sie die Daten, die Sie beibehalten möchten, bevor Sie fortfahren.

So installieren oder aktualisieren Sie den Citrix Hypervisor or-Server:

1. Starten Sie den Computer von der Installations-CD oder, falls zutreffend, Netzwerk-Boot von Ihrem TFTP-Server.
2. Wählen Sie nach den ersten Startmeldungen und dem Bildschirm Willkommen bei Citrix Hypervisor die Keymap (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.

3. Der Bildschirm Willkommen bei Citrix Hypervisor Setup wird angezeigt.

   Citrix Hypervisor wird mit einem breiten Treibersatz geliefert, der die meisten modernen Serverhardwarekonfigurationen unterstützt. Wenn Sie jedoch zusätzliche wichtige Gerätetreiber erhalten haben, drücken Sie F9. Das Installationsprogramm führt Sie durch die Installation der erforderlichen Treiber.

   > **Warnhinweis:**
   >
   > Nur Updatepakete, die Treiberdatenträger enthalten, können zu diesem Zeitpunkt im Installationsprozess installiert werden. Sie werden jedoch später im Installationsprozess aufgefordert, alle Updatepakete zu installieren, die zusätzliche Packs enthalten.
   >
   > Nachdem Sie alle erforderlichen Treiber installiert haben, wählen Sie **OK** aus, um fortzufahren.
   >
   > Citrix Hypervisor ermöglicht es Kunden, die Citrix Hypervisor Installation für den Start von FCoE zu konfigurieren. Drücken Sie F10 und folgen Sie den Anweisungen auf dem Bild-

> schirm, um FCoE einzurichten.
>
> **Hinweis:**
>
> Bevor Sie den Citrix Hypervisor or-Server für den Start von FCoE aktivieren, müssen Sie die Konfiguration manuell ausführen, 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 für den öffentlichen World Wide Name (PWWN) Ihres SAN. Nachdem Sie diese Konfiguration abgeschlossen haben, wird die verfügbare LUN als SCSI-Gerät auf dem CNA des Hosts eingehängt. Das SCSI-Gerät kann dann verwendet werden, um auf die LUN zuzugreifen, 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.
>
> Wenn Sie die FCoE-Fabric konfigurieren, verwenden Sie VLAN 0 nicht. Der Citrix Hypervisor or-Server kann keinen Datenverkehr finden, der sich auf VLAN 0 befindet.
>
> **Warnhinweis:**
>
> Gelegentlich kann das Starten eines Citrix Hypervisor or-Servers von FCoE SAN mithilfe des Software-FCoE-Stacks dazu führen, dass der Host nicht mehr reagiert. Dieses Problem wird durch eine vorübergehende Verbindungsstörung in der Hostinitialisierungsphase verursacht. Wenn der Host für eine lange Zeit nicht reagiert, können Sie den Host neu starten, um dieses Problem zu umgehen.

4. Die Citrix Hypervisor EULA wird angezeigt. Verwenden Sie die Bildrauf- und Bildrunten-Tasten, um durch die Vereinbarung zu blättern und zu lesen. Select **EULA akzeptieren** , um fortzufahren.

5. Select die entsprechende Aktion aus. Möglicherweise sehen Sie eine der folgenden Optionen:

   - *Führen Sie eine saubere Installation durch*
   - *Upgrade*: Wenn das Installationsprogramm eine zuvor installierte Version von Citrix Hypervisor oder XenServer erkennt, bietet es die Option zum Upgrade. Informationen zum Aktualisieren des Citrix Hypervisor or-Servers finden Sie unterUpgrade von einer vorhandenen Version.
   - *Wiederherstellen*: Wenn das Installationsprogramm eine zuvor erstellte Sicherungsinstallation erkennt, bietet es die Möglichkeit, Citrix Hypervisor aus der Sicherung wiederherzustellen.

   Treffen Sie Ihre Auswahl und wählen Sie **OK**, um fortzufahren.

6. Wenn Sie mehrere lokale Festplatten haben, wählen Sie einen primären Datenträger für die Installation aus. Wählen Sie **OK**aus.

7. Wählen Sie die Datenträger aus, die Sie für die Speicherung virtueller Maschinen verwen-

den möchten. Informationen zu einer bestimmten Festplatte können durch Drücken von **F5**angezeigt werden.

Wenn Sie Thin Provisioning verwenden möchten, um die Nutzung des verfügbaren Speichers zu optimieren, wählen Sie Thin Provisioning aktivieren aus. Mit dieser Option wird der lokale SR des Hosts ausgewählt, der für das lokale Caching von VM-VDIs verwendet werden soll. Benutzern von Citrix Virtual Desktops wird empfohlen, diese Option auszuwählen, damit das lokale Caching ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Speicher.

Wählen Sie **OK**.

8. Select die Installationsmedienquelle aus.

   Um von einer CD zu installieren, wählen Sie **Lokale Medien**. Um über das Netzwerk zu installieren, wählen Sie **HTTPoder FTP** oder **NFS** . Wählen Sie **OK**, um fortzufahren.

   Wenn Sie **HTTPoder FTP** oder **NFS** auswählen, richten Sie das Netzwerk so ein, dass das Installationsprogramm eine Verbindung mit den Citrix Hypervisor Installationsmediendateien herstellen kann:

   a) Wenn der Computer über mehrere Netzwerkkarten verfügt, wählen Sie eine von ihnen aus, die für den Zugriff auf die Citrix Hypervisor 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 die Option **Statische Konfiguration**wählen, geben Sie die entsprechenden Details ein.

   c) Geben Sie 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 ein.

      Wenn Sie **NFS**auswählen, geben Sie den Server und den Pfad Ihrer NFS-Freigabe an.

      Select **OK**, um fortzufahren.

9. Geben Sie an, ob Sie die Integrität des Installationsmediums überprüfen möchten. Wenn Sie **Installationsquelle überprüfen**auswählen, wird die SHA256-Prüfsumme der Pakete berechnet und anhand des bekannten Werts überprüft. Die Überprüfung kann einige Zeit in Anspruch nehmen. Treffen Sie Ihre Auswahl und wählen Sie **OK** , um fortzufahren.

10. Festlegen und bestätigen Sie ein Stammkennwort, das XenCenter für die Verbindung mit dem Citrix Hypervisor or-Server verwendet. Sie verwenden dieses Kennwort (mit dem Benutzernamen „root“) auch, um sich bei **xsconsole, der Systemkonfigurationskonsole**, anzumelden.

> **Hinweis:**
>
> Citrix Hypervisor Stammkennwörter dürfen keine Nicht-ASCII-Zeichen enthalten.

11. Richten Sie die primäre Verwaltungsschnittstelle ein, die für die Verbindung mit XenCenter verwendet wird.

    Wenn Ihr Computer über mehrere Netzwerkkarten verfügt, wählen Sie die Netzwerkkarte aus, die Sie für die Verwaltung verwenden möchten. Wählen Sie **OK**, um fortzufahren.

12. Konfigurieren Sie die IP-Adresse der Verwaltungs-NIC, indem Sie die Option **Automatische Konfiguration (DHCP)** wählen, um die Netzwerkkarte mit DHCP zu konfigurieren, oder **Statische Konfiguration** , um die Netzwerkkarte manuell zu konfigurieren. Um die Verwaltungsschnittstelle in einem VLAN-Netzwerk zu haben, geben Sie die VLAN-ID an.

    > **Hinweis:**
    >
    > Um Teil eines Pools zu sein, müssen Citrix Hypervisor or-Server über statische IP-Adressen verfügen oder DNS-adressierbar sein. Stellen Sie bei Verwendung von DHCP sicher, dass eine statische DHCP-Reservierungsrichtlinie vorhanden ist.

13. Geben Sie den Hostnamen und die DNS-Konfiguration manuell oder automatisch über DHCP an.

    Wählen Sie im Abschnitt **Hostname-Konfiguration** die Option **Automatisch über DHCP festlegen** aus, damit der DHCP-Server den Hostnamen zusammen mit der IP-Adresse bereitstellt. Wenn Sie **Manuell angeben**auswählen, 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 (Fully Qualified Domain Name, FQDN)*ein. Die Eingabe eines FQDN kann dazu führen, dass die externe Authentifizierung fehlschlägt, oder der Citrix Hypervisor-Server kann AD mit einem anderen Namen hinzugefügt werden.

    Wählen Sie im Abschnitt **DNS-Konfiguration** die Option **Automatisch über DHCP festlegen** , um die Namendienstkonfiguration mit DHCP abrufen zu können. Wenn Sie **Manuell angeben**auswählen, geben Sie die IP-Adressen Ihrer primären (erforderlich), sekundären (optional) und tertiären (optionalen) DNS-Server in die dafür vorgesehenen Felder ein.

    Select **OK**, um fortzufahren.

14. Select 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.

15. Geben Sie an, wie der Server die lokale Zeit bestimmen soll: mit NTP oder manueller Zeiteingabe. Treffen Sie Ihre Auswahl und wählen Sie **OK**, um fortzufahren.
16. Wenn Sie NTP verwenden, wählen Sie **NTP wird von meinem DHCP-Server konfiguriert** , oder geben Sie mindestens einen NTP-Servernamen oder eine IP-Adresse in die Felder unten ein. Wählen Sie **OK**.

    > **Hinweis:**
    >
    > Citrix Hypervisor geht davon aus, dass die Zeiteinstellung im BIOS des Servers die aktuelle Uhrzeit in UTC ist.

17. Select **Citrix Hypervisor installieren aus**.

    Wenn Sie das Datum und die Uhrzeit manuell festlegen möchten, werden Sie während der Installation dazu aufgefordert. Wählen Sie **OK** , um fortzufahren.

18. Wenn Sie von CD installieren, wird im nächsten Bildschirm gefragt, ob Sie zusätzliche Packs von einer CD installieren möchten. Wenn Sie zusätzliche Packs installieren möchten, die von Ihrem Hardwarehersteller bereitgestellt werden, wählen Sie **Ja**.

    Wenn Sie Zusatzpakete installieren möchten, werden Sie aufgefordert, sie einzufügen. Auswerfen der Citrix Hypervisor Installations-CD, und legen Sie die Zusatzpack-CD ein. Wählen Sie **OK**.

    Select **Medien verwenden** , um mit der Installation fortzufahren.

    Wiederholen Sie den Vorgang für jede zu installierende Packung.

19. Aus dem Fenster **Installation abgeschlossen** , werfen Sie die Installations-CD aus (bei Installation von CD) und wählen Sie **OK** , um den Server neu zu starten.

    Nach dem Neustart des Servers zeigt Citrix Hypervisor **xsconsole**an, eine Systemkonfigurationskonsole. Um über **xsconsole**auf eine lokale Shell zuzugreifen, drücken Sie **Alt+F3**; um zu **xsconsole**zurückzukehren, drücken Sie **Alt+F1**.

    > **Hinweis:**
    >
    > Notieren Sie sich die angezeigte IP-Adresse. Verwenden Sie diese IP-Adresse, wenn Sie XenCenter mit dem Citrix Hypervisor or-Server verbinden.

Installieren von XenCenter

XenCenter muss auf einem Windows Computer installiert sein, der über Ihr Netzwerk eine Verbindung mit dem Citrix Hypervisor or-Server herstellen kann. Stellen Sie sicher, dass .NET Framework Version 4.6 oder höher auf diesem System installiert ist.

So installieren Sie XenCenter:

1. Laden Sie das Installationsprogramm für die neueste Version von XenCenter aus herunterCitrix Hypervisor Download-Seite.
2. Starten Sie die `.msi` Installationsdatei.
3. Folgen Sie dem Setup-Assistenten, mit dem Sie den Standardzielordner ändern und anschließend XenCenter installieren können.

Verbinden von XenCenter mit dem Citrix Hypervisor or-Server

So verbinden Sie XenCenter mit dem Citrix Hypervisor or-Server:

1. Starten Sie XenCenter. Das Programm öffnet sich zur Registerkarte **Startseite**.
2. Klicken Sie auf das Symbol **Neuen Server hinzufügen** .
3. Geben Sie die IP-Adresse des Citrix Hypervisor or-Servers in das Feld **Server** ein. Geben Sie den Stammbenutzernamen und das Kennwort ein, die Sie während der Citrix Hypervisor 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 Dialogfeld können Sie Ihre Einstellungen für das Speichern Ihrer Hostverbindungsinformationen und das automatische Wiederherstellen von Hostverbindungen festlegen.

   Wenn Sie Ihre Einstellungen später ändern möchten, können Sie dies mit XenCenter oder dem Windows Registrierungseditor tun.

   Dazu in XenCenter: Wählen Sie im Hauptmenü **Extras** und dann **Optionen** aus. Das Dialogfeld **Optionen** wird geöffnet. Select die Registerkarte **Speichern und Wiederherstellen** und legen Sie Ihre Einstellungen fest. Klicken Sie auf **OK**, um die Änderungen zu speichern.

   Navigieren Sie dazu mit dem Windows Registrierungseditor zu dem Schlüssel`HKEY_LOCAL_MACHINE\Software\Citrix\XenCenter` und fügen Sie einen Schlüssel`AllowCredentialSave` mit dem Zeichenfolgenwert`true` oder hinzu`false` .

Kopiert!
Failed!

Installations- und Bereitstellungsszenarien

October 16, 2019

In diesem Abschnitt werden die folgenden allgemeinen Installations- und Bereitstellungsszenarien beschrieben:

- Ein oder mehrere Citrix Hypervisor or-Server mit lokalem Speicher
- Pools von Citrix Hypervisor or-Servern mit gemeinsam genutztem Speicher:
  - Mehrere Citrix Hypervisor or-Server mit gemeinsam genutztem NFS-Speicher
  - Mehrere Citrix Hypervisor or-Server mit gemeinsam genutztem iSCSI-Speicher

Citrix Hypervisor -Server mit lokalem Speicher

Die einfachste Bereitstellung von Citrix Hypervisor besteht darin, VMs auf einem oder mehreren Citrix Hypervisor or-Servern mit lokalem Speicher auszuführen.

> **Hinweis:**
>
> Die Livemigration von VMs zwischen Citrix Hypervisor or-Servern ist nur verfügbar, wenn sie Speicher gemeinsam nutzen. Die Livemigration von Speicher ist jedoch weiterhin verfügbar.

Grundlegende Hardwareanforderungen

- Ein oder mehrere 64-Bit-x86-Server mit lokalem Speicher
- Ein oder mehrere Windows -Systeme im selben Netzwerk wie die Citrix Hypervisor or-Server

High-Level-Verfahren

1. Installieren Sie die Citrix Hypervisor or-Serversoftware auf den Servern.
2. Installieren Sie XenCenter auf den Systemen.
3. Verbinden Sie XenCenter mit den Citrix Hypervisor or-Servern.

Nachdem Sie XenCenter mit den Citrix Hypervisor or-Servern verbunden haben, wird der Speicher automatisch auf dem lokalen Datenträger der Hosts konfiguriert.

Pools von Citrix Hypervisor or-Servern mit gemeinsam genutztem Speicher

Ein *Pool* besteht aus mehreren Citrix Hypervisor or-Serverinstallationen, die als eine einzelne verwaltete Entität miteinander verbunden sind. In Kombination mit gemeinsam genutztem Speicher können VMs auf *jedem* Citrix Hypervisor or-Server im Pool gestartet werden, der über ausreichend Arbeitsspeicher verfügt. Die VMs können dann während der Ausführung dynamisch zwischen Hosts verschoben werden (Live-Migration) mit minimalen Ausfallzeiten. Wenn ein einzelner Citrix Hypervisor or-Server einen Hardwarefehler erleidet, können Sie die ausgefallenen VMs auf einem anderen Host im selben Pool neu starten.

Wenn das Feature Hochverfügbarkeit (HA) aktiviert ist, werden geschützte VMs *automatisch* verschoben, wenn ein Hostfehler vorliegt.

Um **gemeinsam genutzten Speicher** zwischen Hosts in einem Pool einzurichten, erstellen Sie ein Speicher-Repository. Citrix Hypervisor or-Speicher-Repositories (SR) sind Speichercontainer, in denen virtuelle Festplatten gespeichert werden. SRs, wie virtuelle Laufwerke, sind persistente Objekte auf der Festplatte, die unabhängig von Citrix Hypervisor vorhanden sind. SRs können auf verschiedenen Arten von physischen Speichergeräten vorhanden sein, sowohl intern als auch extern, einschließlich lokaler Datenträgergeräte und freigegebener Netzwerkspeicher. Beim Erstellen einer SR stehen verschiedene Speicherarten zur Verfügung, darunter:

- NFS-VHD-Speicher
- Software-iSCSI-Speicher
- Hardware-HBA-Speicher

In den folgenden Abschnitten werden zwei gemeinsame gemeinsame Speicherlösungen — NFS und iSCSI — für einen Pool von Citrix Hypervisor or-Servern eingerichtet. Bevor Sie eine SR erstellen, konfigurieren Sie Ihren NFS- oder iSCSI-Speicher. Setup unterscheidet sich je nach Art der Speicherlösung, die Sie verwenden. Weitere Informationen finden Sie in der Dokumentation Ihres Herstellers. Um Teil eines Pools zu sein, müssen die Server, die gemeinsam genutzten Speicher bereitstellen, über statische IP-Adressen verfügen oder DNS-adressierbar sein. Weitere Informationen zum Einrichten von freigegebenem Speicher finden Sie unterSpeicher.

Es wird empfohlen, vor dem Hinzufügen von freigegebenem Speicher einen Pool zu erstellen. Informationen zu Pool-Anforderungen und Einrichtungsprozeduren finden Sie in der XenCenter Hilfe oderHosts und Ressourcenpools.

Citrix Hypervisor -Server mit gemeinsam genutztem NFS-Speicher

Grundlegende Hardwareanforderungen

- Zwei oder mehr 64-Bit-x86-Server mit lokalem Speicher
- Ein oder mehrere Windows -Systeme im selben Netzwerk wie die Citrix Hypervisor or-Server
- Ein Server, der ein freigegebenes Verzeichnis über NFS exportiert

High-Level-Verfahren

1. Installieren Sie die Citrix Hypervisor or-Serversoftware auf den Servern.
2. Installieren Sie XenCenter auf den Systemen.
3. Verbinden Sie XenCenter mit den Citrix Hypervisor or-Servern.

4. Erstellen Sie Ihren Pool von Citrix Hypervisor -Servern.
5. Konfigurieren Sie den NFS-Server.
6. Erstellen Sie eine SR auf der NFS-Freigabe auf Poolebene.

Konfigurieren des NFS-Speichers

Bevor Sie eine SR erstellen, konfigurieren Sie den NFS-Speicher. Um Teil eines Pools zu sein, muss die NFS-Freigabe über eine statische IP-Adresse verfügen oder DNS-adressierbar sein. Konfigurieren Sie den NFS-Server für ein oder mehrere Ziele, die von NFS-Clients bereitgestellt werden können (z. B. Citrix Hypervisor or-Server in einem Pool). Setup unterscheidet sich je nach Speicherlösung. Daher sollten Sie sich am besten die Herstellerdokumentation ansehen.

So erstellen Sie eine SR auf der NFS-Freigabe auf Poolebene in XenCenter:

1. Wählen Sie im Bereich **Ressourcen** den Pool aus. Klicken Sie auf der Symbolleiste auf die Schaltfläche **Neuer Speicher**. Der Assistent **Neues Speicher-Repository** wird geöffnet.
2. Wählen Sie unter **Virtueller Festplattenspeicher**NFS-VHD als Speichertyp aus. Wählen Sie **Weiter**, um fortzufahren.
3. Geben Sie einen Namen für die neue SR und den Namen der Freigabe ein, in der sie sich befindet. Klicken Sie auf **Scannen** , damit der Assistent nach vorhandenen NFS-SRs am angegebenen Speicherort sucht.

   > **Hinweis:**
   >
   > Der NFS-Server muss so konfiguriert sein, dass er den angegebenen Pfad in alle Citrix Hypervisor or-Server im Pool exportiert.

4. Klicken Sie auf **Fertig stellen**.

   Der neue SR wird im **Ressourcenbereich** auf Pool-Ebene angezeigt.

Erstellen einer SR auf der NFS-Freigabe auf Poolebene mithilfe der XE-CLI

1. Öffnen Sie eine Konsole auf einem beliebigen Citrix Hypervisor or-Server im Pool.
2. Erstellen Sie das Speicher-Repository auf *server:/path*, indem Sie Folgendes eingeben:

```
xe sr-create content-type=user type=nfs name-label=sr_name= \
    shared=true device-config:server=server \
    device-config:serverpath=path
```

   Das`device-config-server` Argument bezieht sich auf den Namen des NFS-Servers und das`device-config-serverpath` Argument bezieht sich auf den Pfad auf dem Server. Da

auf true festgelegt`shared` ist, wird der gemeinsam genutzte Speicher automatisch mit jedem Host im Pool verbunden. Alle Hosts, die später beitreten, sind ebenfalls mit dem Speicher verbunden. Die UUID des erstellten Speicher-Repositorys wird auf der Konsole gedruckt.

3. Suchen Sie die UUID des Pools mithilfe des`pool-list` Befehls.
4. Legen Sie die neue SR als Pool-weite Standardeinstellung fest, indem Sie Folgendes eingeben:

```
xe pool-param-set uuid=pool_uuid \
    default-SR=storage_repository_uuid
```

Da Shared Storage als Pool-weiter Standard festgelegt wurde, haben alle zukünftigen VMs ihre Festplatten auf dieser SR erstellt.

Citrix Hypervisor or-Server mit gemeinsam genutztem iSCSI-Speicher

Grundlegende Hardwareanforderungen

- Zwei oder mehr 64-Bit-x86-Server mit lokalem Speicher
- Ein oder mehrere Windows -Systeme im selben Netzwerk wie die Citrix Hypervisor or-Server
- Ein Server, der ein freigegebenes Verzeichnis über iSCSI bereitstellt

High-Level-Verfahren

1. Installieren Sie die Citrix Hypervisor or-Serversoftware auf den Servern.
2. Installieren Sie XenCenter auf den Windows -Systemen.
3. Verbinden Sie XenCenter mit den Citrix Hypervisor or-Servern.
4. Erstellen Sie Ihren Pool von Citrix Hypervisor -Servern.
5. Konfigurieren Sie den iSCSI-Speicher.
6. Aktivieren Sie ggf. mehrere Initiatoren auf Ihrem iSCSI-Gerät.
7. Konfigurieren Sie ggf. den iSCSI-IQN für jeden Citrix Hypervisor or-Server.
8. Erstellen Sie eine SR auf der iSCSI-Freigabe auf Pool-Ebene.

Konfigurieren des iSCSI-Speichers

Bevor Sie einen SR erstellen, konfigurieren Sie den iSCSI-Speicher. Um Teil eines Pools zu sein, muss der iSCSI-Speicher über eine statische IP-Adresse verfügen oder DNS-adressierbar sein. Bereitstellen einer iSCSI-Ziel-LUN im SAN für den VM-Speicher. Konfigurieren Sie Citrix Hypervisor or-Server, um die

iSCSI-Ziel-LUN anzeigen und darauf zugreifen zu können. Sowohl das iSCSI-Ziel als auch jeder iSCSI-Initiator auf jedem Citrix Hypervisor or-Server müssen über einen gültigen und **eindeutigen** iSCSI-qualifizierten Namen (IQN) verfügen. Informationen zur Konfiguration finden Sie am besten in Ihrer Herstellerdokumentation.

Konfigurieren eines iSCSI-IQN für jeden Citrix Hypervisor or-Server

Bei der Installation weist Citrix Hypervisor jedem Host automatisch einen eindeutigen IQN zu. Wenn Sie sich an eine lokale administrative Benennungsrichtlinie halten müssen, können Sie den IQN ändern, indem Sie Folgendes auf der Hostkonsole eingeben:

```
xe-set-iscsi-iqn iscsi_iqn
```

Oder Sie können die xe CLI verwenden, indem Sie Folgendes eingeben:

```
xe host-param-set uuid=host_uuid other-config-iscsi_iqn=iscsi_iqn
```

So erstellen Sie eine SR auf der iSCSI-Freigabe auf Poolebene mit XenCenter:

> **Warnhinweis:**
>
> Wenn Sie Citrix Hypervisor SRs auf iSCSI- oder HBA-Speicher erstellen, werden alle vorhandenen Inhalte des Volumes gelöscht.

1. Wählen Sie im Bereich **Ressourcen** den Pool aus. Klicken Sie auf der Symbolleiste auf die Schaltfläche **Neuer Speicher**. Der Assistent **Neues Speicher-Repository** wird geöffnet.
2. Wählen Sie unter **Virtueller Festplattenspeicher**Software-iSCSI als Speichertyp aus. Wählen Sie **Weiter**, um fortzufahren.
3. Geben Sie einen Namen für den neuen SR und dann die IP-Adresse oder den DNS-Namen des iSCSI-Ziels ein.

   > **Hinweis:**
   >
   > Das iSCSI-Speicherziel muss so konfiguriert sein, dass jeder Citrix Hypervisor or-Server im Pool Zugriff auf eine oder mehrere LUNs hat.

4. Wenn Sie das iSCSI-Ziel für die Verwendung der CHAP-Authentifizierung konfiguriert haben, geben Sie den Benutzer und das Kennwort ein.
5. Klicken Sie auf die Schaltfläche **IQNs ermitteln** , und wählen Sie dann den iSCSI-Ziel-IQN aus der Liste Ziel-IQN aus.

   > **Warnhinweis:**

> Das iSCSI-Ziel und alle Server im Pool müssen über *eindeutige* IQNs verfügen.

6. Klicken Sie auf die Schaltfläche **LUNs ermitteln** , und wählen Sie dann in der Liste Ziel-LUNs die LUN aus, für die der SR erstellt werden soll.

   > **Warnhinweis:**
   >
   > Jedes einzelne iSCSI-Speicher-Repository muss sich vollständig auf einer einzelnen LUN befinden und darf nicht mehr als eine LUN umfassen. Alle Daten, die auf der ausgewählten LUN vorhanden sind, werden zerstört.

7. Klicken Sie auf **Fertig stellen**.

   Der neue SR wird im **Ressourcenbereich** auf Pool-Ebene angezeigt.

So erstellen Sie einen SR auf der iSCSI-Freigabe auf Pool-Ebene mithilfe der xe-CLI:

> **Warnhinweis:**
>
> Wenn Sie Citrix Hypervisor SRs auf iSCSI- oder HBA-Speicher erstellen, werden alle vorhandenen Inhalte des Volumes gelöscht.

1. Führen Sie auf der Konsole eines beliebigen Servers im Pool den Befehl aus:

   ```
   xe sr-create name-label=name_for_sr \
       host-uuid=host_uuid device-config:target=
           iscsi_server_ip_address \
       device-config:targetIQN=iscsi_target_iqn device-config:SCSIid=
           scsi_id \
       content-type=user type=lvmoiscsi shared=true
   ```

   Das`device-config:target` Argument bezieht sich auf den Namen oder die IP-Adresse des iSCSI-Servers. Da das`shared` Argument auf festgelegt ist**`true`** , wird der freigegebene Speicher automatisch mit jedem Host im Pool verbunden. Alle Hosts, die später beitreten, sind ebenfalls mit dem Speicher verbunden.

   Der Befehl gibt die UUID des erstellten Speicher-Repositorys zurück.

2. Suchen Sie die UUID des Pools, indem Sie den`pool-list` Befehl ausführen.

3. Legen Sie die neue SR als Pool-weite Standardeinstellung fest, indem Sie Folgendes eingeben:

   ```
   xe pool-param-set uuid=pool_uuid default-SR=iscsi_shared_sr_uuid
   ```

   Da Shared Storage als Pool-weiter Standard festgelegt wurde, haben alle zukünftigen VMs ihre Festplatten auf dieser SR erstellt.

Kopiert!
Failed!

Upgrade von einer vorhandenen Version

October 16, 2019

Wir bieten Upgrade- und Updatefunktionen, mit denen Sie von einigen früheren Versionen von Citrix Hypervisor auf Citrix Hypervisor 8.0 wechseln können. Mithilfe der Upgrade- oder Updatefunktion können Sie Citrix Hypervisor 8.0 anwenden, ohne einen vollständigen Installationsvorgang abzuschließen. Wenn Sie ein Upgrade oder ein Update durchführen, behält Citrix Hypervisor 8.0 Ihre VMs, SRs und Konfiguration bei.

- Sie können ein Upgrade von XenServer 7.6, 7.5, 7.1 Kumulatives Update 2 (LTSR) oder 7.0 auf Citrix Hypervisor 8.0 mithilfe des **Basisinstallations-ISO durchführen**. In diesem Abschnitt wird beschrieben, wie Sie ein Upgrade auf Citrix Hypervisor 8.0 durchführen.

  > **Hinweis:**
  >
  > Ein Upgrade von XenServer 7.1 auf Citrix Hypervisor 8.0 wird nicht unterstützt. Stellen Sie sicher, dass das neueste kumulative Update auf Citrix Hypervisor 7.1 angewendet wird, bevor Sie ein Upgrade durchführen.

- Für alle anderen Versionen von XenServer können Sie kein direktes Upgrade auf Citrix Hypervisor 8.0 durchführen. Sie können entweder zuerst ein Upgrade auf eine neuere Version von Citrix Hypervisor durchführen und diese Version auf 8.0 aktualisieren, oder Sie können eine Neuinstallation mit dem **Basisinstallations-ISO**durchführen. Weitere Informationen finden Sie unter Installieren.

> **Hinweis:**
>
> Wenn Sie VMs aus der vorherigen XenServer Installation beibehalten möchten, exportieren Sie die VMs und importieren Sie sie in die Neuinstallation von Citrix Hypervisor 8.0. VMs, die aus jeder unterstützten XenServer Version exportiert werden, können in Citrix Hypervisor 8.0 importiert werden. Weitere Informationen finden Sie unter Importieren und Exportieren von VMs.

In diesem Abschnitt wird beschrieben, wie Sie XenServer mithilfe von XenCenter oder der xe-CLI aktualisieren. Sie führt Sie durch das automatische Upgrade Ihrer Citrix Hypervisor or-Server - sowohl im Pool als auch im eigenständigen Modus - automatisch (mithilfe des XenCenter Rolling-Pool-Upgrade-Assistenten) und manuell.

> **Wichtig:**
>
> - Das Upgrade von Citrix Hypervisor or-Servern und insbesondere eines Pools von Citrix Hypervisor or-Servern erfordert eine sorgfältige Planung und Aufmerksamkeit. Um den Verlust vorhandener Daten zu vermeiden, gehen Sie entweder:
>   - Ordnen Sie Ihren Upgrade-Pfad sorgfältig zu.

  - Verwenden Sie den XenCenter Rolling Pool-Upgrade-Assistenten, und stellen Sie sicher, dass Sie die Option zum *Upgrade* auswählen, wenn Sie das Installationsprogramm durchlaufen.

- Wenn Sie XenCenter zum Aktualisieren Ihrer Hosts verwenden, laden Sie die neueste Version von XenCenter herunter und installieren Sie sie. Wenn Sie beispielsweise ein Upgrade auf Citrix Hypervisor 8.0 durchführen, verwenden Sie XenCenter, das mit Citrix Hypervisor 8.0 ausgestellt wurde. Die Verwendung früherer XenCenter Versionen für das Upgrade auf eine neuere Version von Citrix Hypervisor wird nicht unterstützt.
- Boot-from-SAN-Einstellungen werden während des manuellen Upgrades *nicht* vererbt. Befolgen Sie beim Upgrade mit dem ISO- oder PXE-Prozess die gleichen Anweisungen wie im folgenden Installationsprozess, um sicherzustellen, dass diese korrekt konfiguriert`multipathd` ist. Weitere Informationen finden Sie unter Starten von SAN.
- Wenn Sie von XenServer 6.5 Service Pack 1 oder früher auf die neueste Version aktualisieren, unterscheiden sich die Reihenfolge und Benennung der Netzwerkkarten. Um diese Änderung zu umgehen, können Sie die Reihenfolge der Netzwerkkarten während der Installation ändern. Weitere Informationen finden Sie unter CTX135809 - Ändern der Reihenfolge von NICs.

Upgrades für rollende Schwimmbecken

Mit Citrix Hypervisor können Sie ein Rolling Pool-Upgrade durchführen. Ein Upgrade für Rolling Pools hält alle vom Pool angebotenen Dienste und Ressourcen zur Verfügung, während alle Hosts in einem Pool aktualisiert werden. Bei dieser Upgrademethode wird jeweils nur ein Citrix Hypervisor or-Server offline geschaltet. Kritische VMs werden während des Upgradeprozesses ausgeführt, indem die VMs live auf andere Hosts im Pool migriert werden.

Hinweis:

Der Pool muss über einen gemeinsam genutzten Speicher verfügen, damit Ihre VMs während eines Upgrades im Rolling Pool ausgeführt werden können. Wenn Ihr Pool über keinen freigegebenen Speicher verfügt, müssen Sie die VMs vor dem Upgrade beenden, da die VMs nicht live migriert werden können.

Storage-Livemigration wird bei Upgrades des Rolling-Pools nicht unterstützt.

Sie können ein Rolling Pool-Upgrade mit XenCenter oder der xe CLI durchführen. Bei Verwendung von XenCenter wird empfohlen, den Rolling Pool-Upgrade-Assistenten zu verwenden. Dieser Assistent organisiert den Upgrade-Pfad automatisch und führt Sie durch das Upgrade-Verfahren. Wenn Sie die xe-CLI verwenden, planen Sie zunächst Ihren Upgradepfad und migrieren dann laufende VMs zwischen Citrix Hypervisor or-Servern live, während Sie das Rolling Pool-Upgrade manuell durchführen.

Der Rolling Pool-Upgrade-Assistent ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

> **Wichtig:**
>
> Verwenden Sie kein Rolling Pool Upgrade with Boot from SAN-Umgebungen. Weitere Informationen zum Upgrade des Boots von SAN-Umgebungen finden Sie unterStarten von SAN.

Aktualisieren von Citrix Hypervisor or-Servern mithilfe des XenCenter Aktualisierungsassistenten für Rolling Pool

Mit dem Rolling Pool-Upgrade-Assistenten können Sie Citrix Hypervisor or-Server, Hosts in einem Pool oder eigenständige Hosts auf die aktuelle Version von Citrix Hypervisor aktualisieren.

Der Rolling Pool-Upgrade-Assistent führt Sie durch das Upgrade-Verfahren und organisiert den Upgrade-Pfad automatisch. Bei Pools wird jeder der Hosts im Pool nacheinander aktualisiert, beginnend mit dem Poolmaster. Vor dem Start eines Upgrades führt der Assistent eine Reihe von Vorüberprüfungen durch. Diese Vorprüfungen stellen sicher, dass bestimmte Pool-weite Funktionen, wie z. B. hohe Verfügbarkeit, vorübergehend deaktiviert sind und dass jeder Host im Pool für ein Upgrade vorbereitet ist. Nur ein Host ist gleichzeitig offline. Alle ausgeführten VMs werden automatisch von jedem Host migriert, bevor das Upgrade auf diesem Host installiert wird.

Mit dem Rolling Pool-Upgrade-Assistenten können Sie auch die verfügbaren Hotfixes beim Upgrade auf eine neuere Version von Citrix Hypervisor automatisch anwenden. Auf diese Weise können Sie Ihre Standalone-Hosts oder Pools mit einer minimalen Anzahl von Neustarts am Ende auf dem neuesten Stand bringen. Sie müssen während des Upgradevorgangs mit dem Internet verbunden sein, damit diese Funktion funktioniert.

Sie können von der automatischen Anwendung von Hotfixes profitieren, wenn Sie XenCenter, das mit Citrix Hypervisor 7.6 ausgestellt wurde, verwenden, um von einer beliebigen unterstützten Version von Citrix Hypervisor auf Citrix Hypervisor 7.0 und höher zu aktualisieren.

> **Hinweis:**
>
> Das Rolling Pool-Upgrade mit XenCenter ist nur für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps- und Desktopberechtigung Zugriff auf Citrix Hypervisor haben.

Der Assistent kann im **manuellen** oder **automatischen** Modus arbeiten:

- Im **manuellen Modus**müssen Sie das Citrix Hypervisor Installationsprogramm manuell auf jedem Host ausführen und die Anweisungen auf dem Bildschirm auf der seriellen Konsole des Hosts befolgen. Wenn das Upgrade beginnt, fordert XenCenter Sie auf, das

XenCenter-Installationsmedium einzufügen oder für jeden Host, den Sie aktualisieren, einen Netzwerkstartserver anzugeben.

- Im **automatischen Modus**verwendet der Assistent Netzwerkinstallationsdateien auf einem HTTP-, NFS- oder FTP-Server, um die einzelnen Hosts nacheinander zu aktualisieren. In diesem Modus müssen Sie kein Installationsmedium einfügen, manuell neu starten oder das Installationsprogramm auf jedem Host 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 das Upgrade starten.

Vor dem Upgrade

Bevor Sie mit dem Upgrade beginnen, sollten Sie folgende Vorbereitungen treffen:

- Laden Sie XenCenter herunter, das mit Citrix Hypervisor 8.0 ausgestellt wurde, und installieren Sie sie von derCitrix Hypervisor Produkt herunterladenSeite. Die Verwendung früherer XenCenter Versionen für das Upgrade auf eine neuere Version von Citrix Hypervisor wird nicht unterstützt.
- Wir empfehlen dringend, eine Sicherung des Status Ihres vorhandenen Pools mit dem Befehl `pool-dump-database` xe CLI zu erstellen. Weitere Informationen finden Sie unter Befehlszeilenschnittstelle. Wenn Sie einen Sicherungsstatus durchführen, stellen Sie sicher, dass Sie ein teilweise vollständiges Upgrade auf den ursprünglichen Zustand zurücksetzen können, ohne VM-Daten zu verlieren.
- Stellen Sie sicher, dass Ihre Hosts nicht zu viel bereitgestellt sind: Überprüfen Sie, ob Hosts über genügend Arbeitsspeicher verfügen, um das Upgrade durchzuführen. Wenn N der Gesamtzahl der Hosts in einem Pool entspricht, muss für N-1-Hosts ausreichend Arbeitsspeicher vorhanden sein, um alle Live-VMs im Pool auszuführen. Es empfiehlt sich, während des Upgradevorgangs nicht kritische VMs zu suspendieren.
- Wenn auf Ihrem Pool VGPU-fähige VMs ausgeführt werden, führen Sie die folgenden Schritte aus, um den Pool zu migrieren, während diese VMs ausgeführt werden:
  - Stellen Sie sicher, dass die von Ihnen verwendete GPU in der Version unterstützt wird, auf die Sie aktualisieren möchten.
  - Identifizieren Sie eine Version der nVidia GRID-Treiber, die sowohl für die aktuelle Version von Citrix Hypervisor als auch für die Version von Citrix Hypervisor verfügbar ist, die Sie aktualisieren möchten. Wählen Sie nach Möglichkeit die neuesten verfügbaren Treiber aus.
  - Installieren Sie die neuen GRID-Treiber auf Ihren Citrix Hypervisor or-Servern und die entsprechenden Gasttreiber auf allen VGPU-fähigen VMs.
  - Stellen Sie sicher, dass Sie auch über die Version des GRID-Treibers verfügen, die der Version von Citrix Hypervisor entspricht, auf die Sie aktualisieren. Sie werden aufgefordert,

diese Treiber als ergänzendes Paket im Rahmen des Rolling Pool Upgrade-Prozesses zu installieren.

Rolling Pool Upgrade-Assistent überprüft, ob die folgenden Aktionen ausgeführt wurden. Führen Sie die folgenden Aktionen aus, bevor Sie mit dem Upgrade beginnen:

- Leeren Sie die CD/DVD-Laufwerke der VMs in den Pools.
- Deaktivieren Sie die hohe Verfügbarkeit.

So aktualisieren Sie Citrix Hypervisor Hosts mithilfe des XenCenter Rolling-Pool-Upgrade-Assistenten:

1. Öffnen Sie den Rolling Pool Upgrade-Assistenten: Wählen Sie im Menü **Extras** die Option **Rolling Pool Upgrade** aus.
2. Lesen **Sie die Informationen vor dem Start** , und klicken Sie dann auf **Weiter** , um fortzufahren.
3. Select die Pools und die einzelnen Hosts aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie einen der folgenden Modi:
   - **Automatischer Modus** für ein automatisches Upgrade von Netzwerkinstallationsdateien auf einem HTTP-, NFS- oder FTP-Server
   - **Manueller Modus** für ein manuelles Upgrade von einer CD/DVD oder über Netzwerkstart (mit vorhandener Infrastruktur)

   > **Hinweis:**
   >
   > Wenn Sie den **manuellen Modus**wählen, müssen Sie das Citrix Hypervisor Installationsprogramm nacheinander auf jedem Host ausführen. Folgen Sie den Anweisungen auf dem Bildschirm auf der seriellen Konsole des Hosts. Wenn das Upgrade beginnt, fordert XenCenter Sie auf, das Citrix Hypervisor Installationsmedium einzufügen oder für jeden Host, den Sie aktualisieren, einen Netzwerkstartserver anzugeben.
5. Wählen Sie aus, ob XenCenter nach dem Upgrade der Server auf eine neuere Version die minimalen Updates (Hotfixes) automatisch herunterladen und installieren soll. Die Option Updates anwenden ist standardmäßig ausgewählt. Sie müssen jedoch über eine Internetverbindung verfügen, um die Updates herunterzuladen und zu installieren.
6. Nachdem Sie den Upgrade-Modus ausgewählt haben, klicken Sie auf **Vorüberprüfungen ausführen**.
7. Befolgen Sie die Empfehlungen, um alle fehlgeschlagenen Upgrade-Vorprüfungen zu beheben. Wenn XenCenter alle fehlgeschlagenen Vorprüfungen automatisch auflösen soll, klicken Sie auf **Alle auflösen**.

   Wenn alle Vorprüfungen gelöst wurden, klicken Sie auf **Weiter** , um fortzufahren.

8. Bereiten Sie das Citrix Hypervisor Installationsmedium vor.

   Wenn Sie den **Automatikmodus**gewählt haben, geben Sie die Installationsmediendetails ein. Wählen Sie **HTTP**, **NFS**oder **FTP**, und geben Sie dann die URL, den Benutzernamen und das Kennwort an.

   > **Hinweise:**
   >
   > - Wenn Sie FTP wählen, stellen Sie sicher, dass Sie alle führenden Schrägstriche, die sich im Dateipfadbereich der URL befinden, umgehen.
   >
   > - Geben Sie den Benutzernamen und das Kennwort ein, die Ihrem HTTP- oder FTP-Server zugeordnet sind, wenn Sie Sicherheitsanmeldeinformationen konfiguriert haben. Geben Sie den Benutzernamen und das Kennwort für Ihren Citrix Hypervisor Pool nicht ein.
   >
   > - Citrix Hypervisor unterstützt FTP nur im passiven Modus.

   Wenn Sie den **manuellen Modus**gewählt haben, beachten Sie den Upgradeplan und die Anweisungen.

   Klicken Sie auf **Upgrade starten**.

9. Wenn das Upgrade beginnt, führt Sie der Rolling Pool-Upgrade-Assistent durch alle Aktionen, die Sie ausführen müssen, um die einzelnen Hosts zu aktualisieren. Folgen Sie den Anweisungen, bis Sie alle Hosts in den Pools aktualisiert und aktualisiert haben.

   Wenn Sie über VGPU-fähige VMs verfügen, laden Sie den GRID-Treiber hoch, der mit dem auf Ihren VGPU-fähigen VMs übereinstimmt, wenn Sie den Schritt erreichen, der Ihnen die Möglichkeit bietet, ein zusätzliches Paket bereitzustellen. Stellen Sie sicher, dass Sie die Version des Treibers für die Citrix Hypervisor Version hochladen, auf die Sie upgraden möchten.

   > **Hinweis:**
   >
   > Wenn das Upgrade oder der Aktualisierungsvorgang aus irgendeinem Grund fehlschlägt, hält der Aktualisierungsassistent für Rolling Pool den Prozess an. Auf diese Weise können Sie das Problem beheben und den Upgrade- oder Updateprozess fortsetzen, indem Sie auf die Schaltfläche **Wiederholen** klicken.

10. Der Rolling Pool-Upgrade-Assistent druckt eine Zusammenfassung, wenn das Upgrade abgeschlossen ist. Klicken Sie auf **Fertig stellen** , um den Assistenten zu schließen.

Upgrade von Citrix Hypervisor or-Servern mithilfe der XE CLI

> **Wichtig:**
>
> Die Durchführung eines Rolling Pool-Upgrades mit der xe CLI erfordert eine sorgfältige Planung. Lesen Sie den folgenden Abschnitt sorgfältig, bevor Sie beginnen.

Planen eines Upgrade-Pfads

Bei der Planung Ihres Upgrades sollten Sie Folgendes beachten:

- Sie können VMs nur von Citrix Hypervisor or-Servern mit einer älteren Version von Citrix Hypervisor auf eine Version mit derselben oder höher migrieren. Beispielsweise von Version 7.0 auf Version 7.1 oder von Version 7.1 bis Version 8.0. VMs können **nicht** von einem aktualisierten Host zu einem Host migriert werden, auf dem eine ältere Version von Citrix Hypervisor ausgeführt wird. Beispielsweise von Version 8.0 bis Version 7.1. Stellen Sie sicher, dass auf Ihren Citrix Hypervisor-Servern Platz eingeräumt wird.
- Wir empfehlen dringend, einen gemischten Pool (mit mehreren Versionen von Citrix Hypervisor) länger als nötig auszuführen, da der Pool während des Upgrades in einem verschlechterten Zustand arbeitet.
- Wichtige Steuerungsvorgänge sind während des Upgrades nicht verfügbar. Versuchen Sie nicht, Kontrollvorgänge durchzuführen. Obwohl VMs weiterhin normal 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 durchzuführen.
- Aktualisieren Sie den Master-Host immer zuerst. Platzieren Sie den Host nicht mit XenCenter in den Wartungsmodus, bevor Sie das Upgrade durchführen. Wenn Sie den Master in den Wartungsmodus versetzen, wird ein neuer Master festgelegt.
- Wenden Sie nach dem Upgrade eines Hosts alle Hotfixes an, die für die aktualisierte Version von Citrix Hypervisor freigegeben wurden, bevor Sie VMs auf den Host migrieren.
- Wir empfehlen dringend, eine Sicherung des Status Ihres vorhandenen Pools mit dem Befehl `pool-dump-database` xe CLI zu erstellen. Weitere Informationen finden Sie unter Befehlszeilenschnittstelle. Auf diese Weise können Sie ein teilweise vollständiges Rolling-Upgrade in den ursprünglichen Zustand zurückversetzen, ohne VM-Daten zu verlieren. Wenn Sie das rollende Upgrade aus irgendeinem Grund wiederherstellen müssen, müssen Sie möglicherweise VMs herunterfahren. Diese Aktion ist erforderlich, da eine VM nicht von einem aktualisierten Citrix Hypervisor or-Server auf einen Host migriert werden kann, auf dem eine ältere Version von Citrix Hypervisor ausgeführt wird.

Bevor Sie mit dem Upgrade des Rollpools beginnen

- Wenn Sie XenCenter verwenden, aktualisieren Sie XenCenter auf die neueste Version. Die neuere Version von XenCenter steuert ältere Versionen von Citrix Hypervisor or-Servern korrekt.
- Leeren Sie die CD/DVD-Laufwerke der VMs im Pool. Weitere Informationen und Anweisungen finden Sie unter *Vor dem Upgrade eines einzelnen Citrix Hypervisor or-Servers*.
- Deaktivieren Sie die hohe Verfügbarkeit.

Durchführen von Rolling-Pool-Upgrades mithilfe der XE-CLI

1. **Beginnen Sie mit dem Poolmaster**. Deaktivieren Sie den Master mithilfe deshost-disable Befehls. Dadurch wird verhindert, dass neue VMs auf dem angegebenen Host gestartet werden.
2. Stellen Sie sicher, dass keine VMs auf dem Master ausgeführt werden. Herunterfahren, Anhalten oder Migrieren von VMs zu anderen Hosts im Pool.

   Verwenden Sie den vm-migrate Befehl, um bestimmte VMs auf bestimmte Hosts zu migrieren. Mithilfe des vm-migrate Befehls haben Sie die volle Kontrolle über die Verteilung migrierter VMs auf andere Hosts im Pool.

   Verwenden Sie denhost-evacuate Befehl, um alle VMs auf andere Hosts im Pool live zu migrieren. Mithilfe des host-evacuate Befehls belassen Sie die Verteilung migrierter VMs in Citrix Hypervisor.
3. Schalten Sie den Poolmaster ab.

   > **Wichtig:**
   >
   > Sie können den Poolmaster erst kontaktieren, wenn das Upgrade des Masters abgeschlossen ist. Durch das Herunterfahren des Poolmasters gelangen die anderen Hosts im Pool in den *Notfallmodus*. Hosts können in den Notfallmodus wechseln, wenn sie sich in einem Pool befinden, dessen Master aus dem Netzwerk verschwunden ist und nach mehreren Versuchen nicht kontaktiert werden kann. VMs werden weiterhin auf Hosts im Notfallmodus ausgeführt, Steuerungsvorgänge sind jedoch nicht verfügbar.
4. Starten Sie den Poolmaster mit dem Citrix Hypervisor Installationsmedium und -Methode Ihrer Wahl (z. B. Installations-CD oder Netzwerk). Folgen Sie dem Citrix Hypervisor Installationsverfahren (sieheInstallieren), bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. **Wählen Sie ein Upgrade aus.**

   > **Warnungen:**
   >
   > ```
   > - Stellen Sie sicher, dass Sie die Upgrade-Option auswählen,
   >   um vorhandene Daten zu vermeiden.
   >
   > - Wenn das Upgrade des Poolmasters durch irgendetwas
   > ```



```
        unterbrochen wird oder wenn das Upgrade aus irgendeinem
        Grund fehlschlägt, versuchen Sie nicht, mit dem Upgrade
        fortzufahren. Starten Sie den Poolmaster neu und stellen
        Sie eine funktionierende Version des Masters wieder her.
```

Wenn der Poolmaster neu gestartet wird, verlassen die anderen Hosts im Pool den Notfallmodus und der normale Dienst wird nach einigen Minuten wiederhergestellt.

5. Wenden Sie alle Hotfixes, die für die neue Version von Citrix Hypervisor auf den Poolmaster veröffentlicht wurden.
6. Starten Sie auf dem Poolmaster alle herunterfahrenden oder angehaltenen VMs oder setzen Sie sie fort. Migrieren Sie alle VMs, die Sie möchten, zurück zum Poolmaster.
7. Select den nächsten Citrix Hypervisor or-Server im Upgrade-Pfad aus. Deaktivieren Sie den Host.
8. Stellen Sie sicher, dass keine VMs auf dem Host ausgeführt werden. Herunterfahren, Anhalten oder Migrieren von VMs zu anderen Hosts im Pool.
9. Schalten Sie den Host ab.
10. Befolgen Sie das Upgradeverfahren für den Host, wie für den Master in Schritt 4 beschrieben.

    Hinweis:

    Wenn das Upgrade eines Hosts, der nicht der Master ist, fehlschlägt oder unterbrochen wird, müssen Sie das Upgrade nicht wiederherstellen. Verwenden Sie den`host-forget` Befehl, um den Host zu vergessen. Installieren Sie Citrix Hypervisor auf dem Host neu, und verbinden Sie ihn dann mit dem`pool-join` Befehl als neuer Host mit dem Pool.

11. Wenden Sie alle für die neue Version von Citrix Hypervisor freigegebenen Hotfixes auf den Host an.
12. Starten Sie auf dem Host alle herunterzufahrenden oder angehaltenen VMs oder setzen Sie sie fort. Migrieren Sie alle VMs, die Sie wieder auf den Host möchten.
13. Wiederholen Sie die Schritte 6 bis 10 für die übrigen Hosts im Pool.

Aktualisieren eines einzelnen Citrix Hypervisor or-Servers mithilfe der XE CLI

Vor dem Upgrade eines einzelnen Citrix Hypervisor -Servers

Fahren Sie vor dem Upgrade eines eigenständigen Citrix Hypervisor or-Servers alle auf diesem Host ausgeführten VMs herunter oder halten Sie sie an. Es ist wichtig, CD/DVD-Laufwerke aller VMs auszuwerfen und zu leeren, die Sie anhalten möchten. Wenn Sie die CD/DVD-Laufwerke nicht leeren, können Sie die angehaltenen VMs nach dem Upgrade möglicherweise nicht fortsetzen.

Ein *leeres* VM-CD/DVD-Laufwerk bedeutet, dass die VM nicht an ein ISO-Image oder eine physische CD/DVD angeschlossen ist, die über den Citrix Hypervisor or-Server bereitgestellt wird. Außerdem müssen Sie sicherstellen, dass die VM überhaupt nicht an ein physisches CD/DVD-Laufwerk auf dem Citrix Hypervisor or-Server angeschlossen ist.

So leeren Sie das CD/DVD-Laufwerk einer VM mithilfe der xe-CLI:

1. Geben Sie Folgendes ein, welche VMs keine leeren CD/DVD-Laufwerke haben:

```
xe vbd-list type=CD empty=false
```

   Dies gibt eine Liste aller VM-CD/DVD-Laufwerke zurück, die nicht leer sind, zum Beispiel:

```
    uuid ( RO) : abae3997-39af-2764-04a1-ffc501d132d9
    vm-uuid ( RO): 340a8b49-866e-b27c-99d1-fb41457344d9
    vm-name-label ( RO): VM02_DemoLinux
    vdi-uuid ( RO): a14b0345-b20a-4027-a233-7cbd1e005ede
    empty ( RO): false
    device ( RO): xvdd

    uuid ( RO) : ec174a21-452f-7fd8-c02b-86370fa0f654
    vm-uuid ( RO): db80f319-016d-0e5f-d8db-3a6565256c71
    vm-name-label ( RO): VM01_DemoLinux
    vdi-uuid ( RO): a14b0345-b20a-4027-a233-7cbd1e005ede
    empty ( RO): false
    device ( RO): xvdd
```

   Beachten Sie die`uuid`, die das erste Element in der Liste ist.

2. Geben Sie Folgendes ein, um die CD/DVD-Laufwerke der aufgelisteten VMs zu leeren:

```
xe vbd-eject uuid=uuid
```

Aktualisieren eines einzelnen Citrix Hypervisor or-Servers mithilfe der XE CLI

So aktualisieren Sie einen einzelnen Citrix Hypervisor or-Server mithilfe der xe-CLI:

1. Deaktivieren Sie den Citrix Hypervisor or-Server, den Sie aktualisieren möchten, indem Sie Folgendes eingeben:

```
xe host-disable host-selector=host_selector_value
```

   Wenn der Citrix Hypervisor or-Server deaktiviert ist, können VMs auf diesem Host nicht erstellt oder gestartet werden. VMs können auch nicht auf einen deaktivierten Host migriert werden.

2. Herunterfahren oder Anhalten von VMs, die auf dem Host ausgeführt werden, für den Sie ein Upgrade durchführen möchten, mithilfe der`xe vm-shutdown` Befehle`xe vm-suspend` oder.
3. Fahren Sie den Host mit dem`xe host-shutdown` Befehl herunter.
4. Führen Sie die Citrix Hypervisor Installationsprozedur aus, bis das Installationsprogramm Ihnen die Option zum Upgrade anbietet. **Wählen Sie ein Upgrade aus.** Weitere Informationen finden Sie unter Installieren.

   > **Warnhinweis:**
   >
   > Stellen Sie sicher, dass Sie die Upgrade-Option auswählen, um zu vermeiden, dass vorhandene Daten verloren gehen.

   Während des Setup-Vorgangs müssen Sie keine Einstellungen erneut konfigurieren. Der Upgrade-Prozess folgt dem Erstinstallationsprozess, aber mehrere Setup-Schritte werden umgangen. Die vorhandenen Einstellungen für Netzwerkkonfiguration, Systemzeit usw. werden beibehalten.

   Wenn Ihr Host neu gestartet wird, wird der normale Dienst nach einigen Minuten wiederhergestellt.
5. Wenden Sie alle Hotfixes an, die für die neue Version von Citrix Hypervisor veröffentlicht wurden.
6. Starten Sie alle herunterfahrenden VMs neu, und setzen Sie alle angehaltenen VMs fort.

Kopiert!
Failed!

Aktualisieren Sie Ihre Hosts

October 16, 2019

Updates können oft mit minimaler Dienstunterbrechung angewendet werden. Es wird empfohlen, dass Kunden XenCenter verwenden, um alle Updates anzuwenden. Wenn Sie einen Citrix Hypervisor Pool aktualisieren, können Sie Ausfallzeiten von virtuellen Rechnern vermeiden, indem Sie den Assistenten zum **Installieren von Updates** in XenCenter verwenden. Der Assistent zum **Installieren** von Updates wendet Updates an, aktualisiert jeweils einen Host und migriert VMs automatisch weg von jedem Host, wenn der Hotfix oder Update angewendet wird.

Sie können XenCenter so konfigurieren, dass sie regelmäßig nach verfügbaren Citrix Hypervisor or- und XenCenter Updates und neuen Versionen sucht. Alle Warnungen werden im Bereich **Benachrichtigungen** angezeigt.

Aktualisierungstypen

Die folgenden Aktualisierungstypen sind für Citrix Hypervisor verfügbar:

- **Aktuelle Releases (CRs)**, bei denen es sich um vollständige Versionen von Citrix Hypervisor aus dem CR-Stream handelt. Einige CRs können als Updates für die unterstützten Versionen von Citrix Hypervisor aus dem CR-Stream angewendet werden.
- **Hotfixes**, die in der Regel Fehlerbehebungen für ein oder mehrere spezifische Probleme bereitstellen. Hotfixes werden für Citrix Hypervisor Versionen in den Streams Long Term Service Release (LTSR) und Current Release (CR) sowie für frühere unterstützte Versionen bereitgestellt, die nicht Teil eines Streams sind.
- **Kumulative Updates**, die zuvor veröffentlichte Hotfixes enthalten und möglicherweise Unterstützung für neue Gäste und Hardware enthalten. Kumulative Updates werden auf Citrix Hypervisor Releases aus dem LTSR-Stream (Long Term Service Release) angewendet.

Ergänzende Packs , die von unseren Partnern bereitgestellt werden, können auch als Updates für Citrix Hypervisor angewendet werden.

Aktuelle Veröffentlichungen

Citrix Hypervisor 8.0 ist eine aktuelle Version von Citrix Hypervisor. Da es sich bei Citrix Hypervisor 8.0 um eine Plattformaktualisierung handelt, kann es jedoch nicht als Update auf frühere Versionen von XenServer angewendet werden.

Verwenden Sie für XenServer Versionen, für die Citrix Hypervisor 8.0 nicht als Update angewendet werden kann, stattdessen die Basisinstallations-ISO, und aktualisieren Sie die vorhandene Installation.

Hotfixes

Möglicherweise veröffentlichen wir Hotfixes für Citrix Hypervisor 8.0, die Fixes für bestimmte Probleme bereitstellen.

Hotfixes für Citrix Hypervisor 8.0 werden über die zur Verfügung gestelltCitrix Wissenszentrum. Wir empfehlen Kunden, regelmäßig das Knowledge Center auf neue Updates zu überprüfen. Alternativ können Sie E-Mail-Benachrichtigungen für Updates für Citrix Hypervisor abonnieren, indem Sie sich für ein Konto unter registrierenhttp://www.citrix.com/support/.

Hotfixes auf dem neuesten CR stehen allen Citrix Hypervisor Kunden zur Verfügung. Hotfixes auf früheren CRs, die noch unterstützt werden, sind jedoch nur für Kunden mit einem aktiven Citrix Customer Success Services Konto (CSS) verfügbar.

Hotfixes im LTSR-Stream stehen Kunden mit aktivem CSS Konto zur Verfügung. Weitere Informationen finden Sie unterLizenzierung.

Kumulative Updates

Kumulative Updates werden für LTSRs von Citrix Hypervisor bereitgestellt. Diese Updates bieten Fehlerbehebungen für Probleme und können Unterstützung für neue Gäste und Hardware enthalten.

Kumulative Updates stehen Kunden mit aktivem CSS Konto zur Verfügung.

Citrix Hypervisor 8.0 ist eine aktuelle Version. Für diese Version werden keine kumulativen Updates bereitgestellt.

Vorbereiten eines Pools für ein Update

Updates für Citrix Hypervisor können als Hotfix, Kumulatives Update oder aktuelle Version bereitgestellt werden. Achten Sie auf die mit jedem Update veröffentlichten Versionshinweise. Jedes Update kann einzigartige Installationsanweisungen enthalten, insbesondere in Bezug auf Vorbereitungs- und Nachaktualisierungsvorgänge. In den folgenden Abschnitten finden Sie allgemeine Anleitungen und Anweisungen zum Anwenden von Updates auf Ihre Citrix Hypervisor or-Systeme.

> **Wichtig:**
>
> Bevor Sie ein Update für den Citrix Hypervisor Pool anwenden, beachten Sie Folgendes:

- (Gilt nur für Citrix Hypervisor 8.0 Hotfixes) Alle Hosts im Pool müssen Citrix Hypervisor 8.0 ausgeführt werden, bevor Sie den Hotfix anwenden.
- Sichern Sie Ihre Daten, bevor Sie ein Update anwenden. Hinweise zu Sicherungsprozeduren finden Sie unterDisaster Recovery und Backup.
- Aktualisieren Sie alle Server in einem Pool innerhalb eines kurzen Zeitraums: Das Ausführen eines gemischten Pools (eines Pools, der aktualisierte und nicht aktualisierte Server enthält) ist keine unterstützte Konfiguration. Planen Sie Ihre Aktualisierungen, um die Zeit zu minimieren, die ein Pool in einem gemischten Zustand ausgeführt wird.
- Aktualisieren Sie alle Server innerhalb eines Pools sequenziell, wobei Sie immer mit dem Poolmaster beginnen. Der **XenCenter-Installationsassistent** verwaltet diesen Prozess automatisch.
- Aktualisieren Sie nach dem Anwenden eines Updates auf alle Hosts in einem Pool alle erforderlichen Treiberdatenträger, bevor Sie Citrix Hypervisor or-Server neu starten.
- Nachdem Sie ein kumulatives Update oder eine aktuelle Version auf einen Hosts angewendet haben, wenden Sie alle Hotfixes an, die für dieses kumulative Update oder die aktuelle Version freigegeben wurden, bevor Sie VMs auf den Host migrieren.

Bevor Sie mit der Aktualisierung beginnen

- Melden Sie sich bei einem Benutzerkonto mit Vollzugriff an (z. B. als Pooladministrator oder mit einem lokalen Stammkonto).
- Leeren Sie die CD/DVD-Laufwerke aller VMs, die Sie anhalten möchten. Einzelheiten und Anweisungen finden Sie unterVor dem Upgrade eines einzelnen Citrix Hypervisor -Servers.
- Deaktivieren Sie ggf. die Hochverfügbarkeit.

Anwenden von Aktualisierungen auf einen Pool

Mit dem Updateinstallationsmechanismus in XenCenter können Sie das ausgewählte Update von der Support-Website herunterladen und extrahieren. Sie können ein Update auf mehrere Hosts und Pools gleichzeitig anwenden, indem **Sie den Assistenten zum Installieren von Updates** verwenden. Während des Vorgangs führt der **Update-Installations-Assistent** die folgenden Schritte für jeden Server aus:

- Migriert VMs vom Server
- Stellt den Server in den Wartungsmodus
- Wendet das Update auf den Server an
- Startet den Host bei Bedarf neu
- Migriert die VMs zurück auf den aktualisierten Host.

Alle Aktionen, die in der Vorprüfungsphase ausgeführt werden, um die Aktualisierungen anzuwenden, z. B. das Deaktivieren von HA, werden rückgängig gemacht.

Der Assistent zum **Installieren von Updates** führt eine Reihe von Prüfungen durch, die als Vorüberprüfungen bezeichnet werden, bevor der Aktualisierungsvorgang gestartet wird. Diese Überprüfungen stellen sicher, dass sich der Pool in einem gültigen Konfigurationsstatus befindet. Anschließend werden der Updatepfad und die VM-Migration automatisch verwaltet. Wenn Sie den Updatepfad und die VM-Migration manuell steuern möchten, können Sie jeden Host einzeln aktualisieren.

Automatisches Anwenden von Updates

Mit XenCenter können Sie automatische Updates anwenden, die erforderlich sind, um Ihre Server auf dem neuesten Stand zu bringen. Sie können diese Updates auf einen oder mehrere Pools anwenden. Wenn Sie automatisierte Updates anwenden, wendet XenCenter den Mindestsatz an Updates an, die erforderlich sind, um den ausgewählten Pool oder den eigenständigen Server auf dem neuesten Stand zu bringen. XenCenter minimiert die Anzahl der Neustarts, die erforderlich sind, um den Pool oder den eigenständigen Serverpool auf dem neuesten Stand zu bringen. Wenn möglich, beschränkt XenCenter es auf einen einzelnen Neustart am Ende. Weitere Informationen finden Sie unter Automatische Updates anwenden.

Verfügbare Updates anzeigen

Im Abschnitt **Updates** der Ansicht **Benachrichtigungen** werden die Updates aufgeführt, die für alle verbundenen Server und Pools verfügbar sind.

Hinweise:

- Standardmäßig sucht XenCenter regelmäßig nach Citrix Hypervisor und XenCenter Updates. Klicken Sie auf **Aktualisieren** , um manuell nach verfügbaren Updates zu suchen.
- Wenn die Registerkarte **Updates** keine Updates finden kann, weil Sie die automatische Suche nach Updates deaktiviert haben, wird auf der Registerkarte **Updates** eine Meldung angezeigt. Klicken Sie auf **Jetzt nach Updates suchen** , um manuell nach Updates zu suchen.

Sie können aus der Liste **Ansicht** auswählen, ob die Liste der Updates **Nach Update oder NachServer angezeigt werden** soll.

Wenn Sie die Liste der Updates Nach Update anzeigen, zeigt XenCenter die Liste der Updates an. Sie können diese Updates nach Server/Pool oder nach Datum bestellen.

- Kumulative Updates und neue Versionen werden oben in dieser Liste angezeigt. Nicht alle neuen Versionen können als Update angewendet werden.
- Um diese Informationen als CSV-Datei zu exportieren, klicken Sie auf **Alle exportieren**. Die CSV-Datei listet die folgenden Informationen auf:
  - Name aktualisieren
  - Beschreibung des Updates
  - Server, auf die dieses Update angewendet werden kann
  - Zeitstempel des Updates
  - Ein Verweis auf die Webseite, von der das Update heruntergeladen wird
- Um ein Update auf einen Server anzuwenden, wählen Sie in der Liste **Aktionen** für dieses Update **Herunterladen und Installieren** aus. Diese Option extrahiert das Update und öffnet den Assistenten zum **Installieren von Updates** auf der Seite **Server Select** , wobei die entsprechenden Server ausgewählt sind. Weitere Informationen finden Sie unter Anwenden eines Updates auf einen Pool.
- Um die Versionshinweise eines Updates in Ihrem Browser zu öffnen, klicken Sie auf die Liste **Aktionen** und wählen Sie **Gehe zu Webseite** aus.

Wenn Sie die Liste der Updates **By Server**anzeigen, zeigt XenCenter die Liste der mit XenCenter verbundenen Server an. Diese Liste zeigt sowohl die Updates, die auf die Server angewendet werden können, als auch die Updates, die auf den Servern installiert sind.

- Um diese Informationen als CSV-Datei zu exportieren, klicken Sie auf Alle exportieren. Die CSV-Datei listet die folgenden Informationen auf:

  - Pool, zu dem der Server gehört
  - Servername
  - Status des installierten Citrix Hypervisor
  - Update-Status des Servers
  - Erforderliche Updates für diesen Server
  - Installierte Updates für diesen Server.
- Klicken Sie auf Updates **installieren, um die Updates**anzuwenden. Mit dieser Auswahl wird der **Update-Assistent** auf der Seite Update Select geöffnet. Weitere Informationen finden Sie unter Anwenden eines Updates auf einen Pool.

Anwenden eines Updates auf einen Pool

So wenden Sie ein Update auf einen Pool mithilfe von XenCenter an:

1. Wählen Sie im XenCenter Menü **Extras** und dann **Update installieren** aus.
2. Lesen Sie die Informationen, die auf der Seite **Vor dem Start** angezeigt werden, und klicken Sie dann auf **Weiter**.
3. Der Assistent zum Installieren von Updates listet die verfügbaren Updates auf der Seite **Update Select** auf. Select das erforderliche Update aus der Liste aus, und klicken Sie dann auf **Weiter**.
4. Select auf der Seite Server auswählen den Pool und die Server aus, die Sie aktualisieren möchten.

   Wenn Sie ein kumulatives Update oder eine aktuelle Version anwenden, können Sie auch auswählen, ob der minimale Satz von Hotfixes für die CU oder CR angewendet werden soll.

   Klicken Sie auf **Weiter**.
5. Der Assistent zum **Installieren von Updates** führt mehrere Update-Vorprüfungen durch, um sicherzustellen, dass sich der Pool in einem gültigen Konfigurationsstatus befindet. Der Assistent prüft auch, ob die Hosts neu gestartet werden müssen, nachdem das Update angewendet wurde, und zeigt das Ergebnis an. Der Assistent zum **Installieren von Updates** prüft auch, ob ein Live-Patch für den Hotfix verfügbar ist und ob der Live-Patch auf die Hosts angewendet werden kann. Hinweise zum Live-Patching finden Sie unterLive-Patching.
6. Befolgen Sie die Empfehlungen auf dem Bildschirm, um alle fehlgeschlagenen Aktualisierungsvorprüfungen zu beheben. Wenn XenCenter alle fehlgeschlagenen Vorprüfungen automatisch auflösen soll, klicken Sie auf **Alle auflösen**. Wenn die Vorprüfungen gelöst wurden, klicken Sie auf **Weiter**.
7. Wenn Sie eine CU oder eine CR installieren, lädt XenCenter die Updates herunter, lädt sie in die Standard-SR des Pools hoch und installiert die Updates. Auf der Seite **Hochladen und Installieren** wird der Fortschritt angezeigt.

> **Hinweise:**
>
> ```
> - Wenn die Standard-SR in einem Pool nicht freigegeben ist
>  oder nicht genügend Speicherplatz hat, versucht XenCenter,
>  das Update in eine andere freigegebene SR hochzuladen. Wenn
>   keiner der freigegebenen SRs über ausreichend
>  Speicherplatz verfügt, wird das Update auf den lokalen
>  Speicher des Poolmasters hochgeladen. -  Wenn der
>  Aktualisierungsvorgang aus irgendeinem Grund nicht
>  abgeschlossen werden kann, stoppt XenCenter den Vorgang.
>  Auf diese Weise können Sie das Problem beheben und den
>  Aktualisierungsvorgang fortsetzen, indem Sie auf die
>  Schaltfläche **Wiederholen** klicken.
> ```

Siehe Schritt 10., um den Installationsvorgang abzuschließen.

8. Wenn Sie einen Hotfix installieren, wählen Sie einen **Update-Modus**. Überprüfen Sie die auf dem Bildschirm angezeigten Informationen und wählen Sie einen geeigneten Modus aus. Wenn der Hotfix einen Live-Patch enthält, der erfolgreich auf die Hosts angewendet werden kann, wird er`No action required` auf dem Bildschirm **Aufgaben ausgeführt werden** angezeigt.

   > **Hinweis:**
   >
   > Wenn Sie zu diesem Zeitpunkt auf **Abbrechen** klicken, werden die Änderungen vom Assistenten zum Installieren von Updates zurückgesetzt und die Update-Datei vom Server entfernt.

9. Klicken Sie auf **Update installieren** , um mit der Installation fortzufahren. Der Assistent zum Installieren von Updates zeigt den Fortschritt des Updates an und zeigt die wichtigsten Vorgänge an, die XenCenter während der Aktualisierung der einzelnen Server im Pool ausführt.
10. Wenn das Update angewendet wird, klicken Sie auf **Fertig stellen** , um den Update-Assistenten zu schließen. Wenn Sie Tasks nach dem Update manuell ausführen möchten, tun Sie dies jetzt.

Aktualisieren eines Pools von Citrix Hypervisor or-Servern mithilfe der XE CLI

So aktualisieren Sie einen Pool von Citrix Hypervisor Hosts mithilfe der xe-CLI:

1. Laden Sie die Update-Datei an einen bekannten Speicherort auf dem Computer herunter, auf dem die xe-CLI ausgeführt wird. Notieren Sie sich den Pfad zur Datei.
2. Laden Sie die Update-Datei in den Pool hoch, den Sie aktualisieren möchten, indem Sie Folgendes ausführen:

   ```
   xe -s server -u username -pw password update-upload file-name=
      filename [sr-uuid=storage_repository_uuid]
   ```


Hier `-s` bezieht sich auf den Namen des Poolmasters. Citrix Hypervisor weist der Aktualisierungsdatei eine UUID zu, die dieser Befehl druckt. Notieren Sie sich die UUID.

> **Tipp:**
>
> Nachdem eine Updatedatei auf den Citrix Hypervisor or-Server hochgeladen wurde, können Sie die`update-list` Befehle`update-param-list` und verwenden, um Informationen zur Datei anzuzeigen.

3. Wenn Citrix Hypervisor Fehler oder Vorbereitungsschritte erkennt, die noch nicht durchgeführt wurden, werden Sie benachrichtigt. Befolgen Sie unbedingt alle Anleitungen, bevor Sie mit dem Update fortfahren.

   Bei Bedarf können Sie VMs auf den Hosts, die Sie aktualisieren möchten, mithilfe der`vm-shutdown` Befehle oder herunterfahren`vm-suspend` oder suspendieren.

   Verwenden Sie den `vm-migrate` Befehl, um bestimmte VMs auf bestimmte Hosts zu migrieren. Mithilfe des `vm-migrate` Befehls haben Sie die volle Kontrolle über die Verteilung migrierter VMs auf andere Hosts im Pool.

   Verwenden Sie den`host-evacuate` Befehl, um alle VMs automatisch auf andere Hosts im Pool zu migrieren. Mithilfe des `host-evacuate` Befehls belassen Sie die Verteilung migrierter VMs in Citrix Hypervisor.

4. Aktualisieren Sie den Pool, indem Sie die UUID der Update-Datei angeben, indem Sie Folgendes ausführen:

   ```
   xe update-pool-apply uuid=UUID_of_file
   ```

   Dieser Befehl wendet das Update oder den Hotfix auf alle Hosts im Pool an, beginnend mit dem Poolmaster.

   Um Hosts im Rolling zu aktualisieren und neu zu starten, können Sie die Update-Datei auf einen einzelnen Host anwenden, indem Sie den folgenden Befehl ausführen:

   ```
   xe update-apply host=host uuid=UUID_of_file
   ```

   Stellen Sie sicher, dass Sie den Poolmaster aktualisieren, bevor Sie ein anderes Poolmitglied aktualisieren.

5. Stellen Sie sicher, dass das Update mithilfe des`update-list` Befehls angewendet wurde. Wenn die Aktualisierung erfolgreich war, enthält das `hosts` Feld die Host-UUID.

6. Führen Sie alle erforderlichen Vorgänge nach der Aktualisierung durch, z. B. den XAPI-Toolstack neu starten oder die Hosts neu starten. Führen Sie diese Operation zuerst auf dem Poolmaster aus.

Aktualisieren einzelner Hosts mithilfe der xe-CLI

So aktualisieren Sie einzelne Hosts mithilfe der xe-CLI:

1. Laden Sie die Update-Datei an einen bekannten Speicherort auf dem Computer herunter, auf dem die xe-CLI ausgeführt wird. Notieren Sie sich den Pfad zur Datei.
2. Herunterfahren oder Anhalten von VMs auf den Hosts, die Sie aktualisieren möchten, mithilfe der`vm-shutdown` Befehle`vm-suspend` oder.
3. Laden Sie die Update-Datei auf den Host hoch, den Sie aktualisieren möchten, indem Sie Folgendes ausführen:

   ```
   xe -s server -u username -pw password update-upload file-name=
       filename [sr-uuid=storage_repository_uuid]
   ```

   Hier`-s` bezieht sich auf den Hostnamen. Citrix Hypervisor weist der Aktualisierungsdatei eine UUID zu, die dieser Befehl druckt. Notieren Sie sich die UUID.

   > **Tipp:**
   >
   > Nachdem eine Updatedatei auf den Citrix Hypervisor or-Server hochgeladen wurde, können Sie die`update-list` Befehle`update-param-list` und verwenden, um Informationen zur Updatedatei anzuzeigen.

4. Wenn Citrix Hypervisor Fehler oder Vorbereitungsschritte erkennt, die noch nicht durchgeführt wurden, werden Sie benachrichtigt. Befolgen Sie unbedingt alle Anleitungen, bevor Sie mit dem Update fortfahren.
5. Aktualisieren Sie den Host, indem Sie die UUIDs des Hosts und der Update-Datei angeben, indem Sie Folgendes ausführen:

   ```
   xe update-apply host-uuid=UUID_of_host uuid=UUID_of_file
   ```

   Wenn der Host Mitglied eines Pools ist, stellen Sie sicher, dass Sie den Poolmaster aktualisieren, bevor Sie ein anderes Poolmitglied aktualisieren.
6. Stellen Sie sicher, dass das Update erfolgreich angewendet wurde, indem Sie den`update-list` Befehl verwenden. Wenn die Aktualisierung erfolgreich war, enthält das `hosts` Feld die Host-UUID.
7. Führen Sie bei Bedarf alle Vorgänge nach der Aktualisierung durch (z. B. Neustart des XAPI-Toolstapels oder Neustart des Hosts).

Automatische Updates anwenden

Automatischer Aktualisierungsmodus wendet alle Hotfixes und kumulativen Updates an, die für einen Host verfügbar sind. Dieser Modus minimiert die Anzahl der Neustarts, die erforderlich sind, um den Pool oder den eigenständigen Serverpool auf dem neuesten Stand zu bringen. Der **automatische Aktualisierungsmodus** beschränkt ihn nach Möglichkeit auf einen einzelnen Neustart am Ende.

Wenn eine neue Version der aktuellen Version als Update verfügbar **ist** , wird dieses Update nicht angewendet. Stattdessen müssen Sie manuell auswählen, um auf die neue aktuelle Version zu aktualisieren.

XenCenter benötigt Internetzugang, um die erforderlichen Updates abzurufen.

So zeigen Sie die Liste der erforderlichen Updates an:

1. Select den Host im Ressourcenbereich in XenCenter aus.
2. Navigieren Sie zur Registerkarte **Allgemein** .
3. Erweitern Sie den Abschnitt **Updates** .

   Sie können sehen:

   - **Angewandt** — listet bereits angewendete Aktualisierungen auf.
   - **Erforderliche Updates** — listet die erforderlichen Aktualisierungen auf, um den Server auf dem neuesten Stand zu bringen.

     > **Hinweis:**
     >
     > Wenn keine Updates erforderlich sind, wird der Abschnitt **Erforderliche Updates** nicht angezeigt.

   - **Installierte Zusatzpakete** — Listet zusätzliche Packs auf, die auf dem Server installiert sind (falls vorhanden).

     > **Hinweis:**
     >
     > Wenn Sie einen Pool anstelle eines Servers auswählen, werden im Abschnitt Updates Updates Updates aufgeführt, die bereits als **Vollständig angewendet gelten**.

Wenn Sie ein bestimmtes Update auswählen und installieren möchten, finden SieAnwenden eines Updates auf einen Poolim Abschnitt.

> **Hinweis:**
>
> Die Funktion Automated Updates ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie im Citrix Website. Weitere Informationen finden Sie unter Lizenzierung.

> Die Funktion Automated Updates ist für Citrix Hypervisor Premium Edition-Kunden verfügbar.

Automatische Updates mithilfe des Assistenten zum Installieren von Updates anwenden

Der folgende Abschnitt enthält Schritt-für-Schritt-Anleitungen zum automatischen Anwenden der erforderlichen Updates, um den Pool oder den eigenständigen Host auf dem neuesten Stand zu bringen.

1. Wählen Sie im XenCenter Menü **Extras** und dann **Update installieren** aus.
2. Lesen Sie die Informationen, die auf der Seite **Vor dem Start** angezeigt werden, und klicken Sie dann auf **Weiter**.
3. Select auf der Seite Update auswählen den Mechanismus aus, mit dem die Updates installiert werden sollen. Sie können die folgenden Optionen sehen:
   - **Automatische Updates** — (Standard) Diese Option ist nur sichtbar, wenn XenCenter mit mindestens einem lizenzierten Pool oder einem lizenzierten Standalone-Server verbunden ist. Select diese Option aus, um alle aktuellen Updates automatisch herunterzuladen und zu installieren, um den Pool oder einen eigenständigen Server auf dem neuesten Stand zu bringen.
   - **Update von Citrix herunterladen** — Der Assistent zum Installieren von Updates listet die verfügbaren Updates auf der Support-Site auf. Informationen zum Anwenden der Updates finden Sie unterAnwenden eines Updates auf einen Pool.
   - **Select Update oder Supplemental Pack von der Festplatte aus** — Informationen zur Installation eines bereits heruntergeladenen Updates finden Sie unterAnwenden eines Updates auf einen Pool . Informationen zum Installieren zusätzlicher Pack-Updates finden Sie im Abschnitt **Installieren von Supplemental Packs** in der XenCenter Hilfe.
4. Um mit der automatischen Anwendung von Hotfixes fortzufahren, wählen Sie **Automatische Updates** aus, und klicken Sie dann auf **Weiter** .
5. Select einen oder mehrere Pools oder eigenständige Server aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**. Jeder Server oder Pool, der nicht aktualisiert werden kann, wird nicht verfügbar.
6. Der Assistent zum **Installieren von Updates** führt mehrere Update-Vorprüfungen durch, um sicherzustellen, dass sich der Pool in einem gültigen Konfigurationsstatus befindet.

   Befolgen Sie die Empfehlungen auf dem Bildschirm, um alle fehlgeschlagenen Aktualisierungsvorprüfungen zu beheben. Wenn XenCenter alle fehlgeschlagenen Vorprüfungen automatisch auflösen soll, klicken Sie auf **Alle auflösen**. Wenn die Vorprüfungen gelöst wurden, klicken Sie auf **Weiter**.

7. Der Update-Assistent lädt die empfohlenen Updates automatisch herunter und installiert sie. Der Assistent zeigt außerdem den Gesamtfortschritt des Updates an und zeigt die wichtigsten Vorgänge an, die XenCenter während der Aktualisierung der einzelnen Server im Pool ausführt.

   Hinweise:

   ```
   - Die Updates werden in die Standard-SR des Pools hochgeladen. Wenn die Standard-SR nicht freigegeben ist oder nicht genügend Speicherplatz hat, versucht XenCenter, das Update auf eine andere freigegebene SR mit ausreichend Speicherplatz hochzuladen. Wenn keine der freigegebenen SRs über ausreichend Speicherplatz verfügt, wird das Update auf den lokalen Speicher auf jedem Host hochgeladen.

   - Der Aktualisierungsvorgang kann aus irgendeinem Grund nicht abgeschlossen werden, XenCenter stoppt den Prozess. Auf diese Weise können Sie das Problem beheben und den Aktualisierungsvorgang fortsetzen, indem Sie auf die Schaltfläche **Wiederholen** klicken.
   ```

8. Wenn alle Updates angewendet wurden, klicken Sie auf **Fertig stellen** , um den Update-Assistenten zu schließen.

Live-Patches in Citrix Hypervisor

Die Live-Patch-Funktion gilt nur für Hotfixes. Aktuelle Versionen und kumulative Updates können nicht als Live-Patches angewendet werden.

Citrix Hypervisor Kunden, die Citrix Hypervisor or-Server bereitstellen, müssen ihre Hosts nach der Anwendung von Hotfixes oft neu starten. Dieser Neustart führt zu unerwünschten Ausfallzeiten für die Hosts, während Kunden warten müssen, bis das System neu gestartet wird. Diese unerwünschten Ausfallzeiten können sich auf das Geschäft auswirken. Mit Live-Patching können Kunden einige Linux-Kernel und Xen Hypervisor-Hotfixes installieren, ohne die Hosts neu starten zu müssen. Solche Hotfixes umfassen sowohl einen Live-Patch, der auf den Speicher des Hosts angewendet wird, als auch einen Hotfix, der die Dateien auf der Festplatte aktualisiert. Die Verwendung von Live-Patching kann Wartungskosten und Ausfallzeiten reduzieren.

Wenn Sie ein Update mithilfe von XenCenter anwenden, prüft der Assistent zum **Installieren von Updates** , ob die Hosts nach der Installation des Updates neu gestartet werden müssen. XenCenter zeigt das Ergebnis auf der Seite „ **Vorüberprüfungen** “ an. Diese Prüfung ermöglicht es Kunden, die Aufgaben nach dem Update im Voraus kennen zu lernen und die Anwendung von Hotfixes entsprechend zu planen.

> **Hinweis:**
>
> Citrix Hypervisor Live Patching ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie im Citrix Website. Ausführliche Informationen zur Lizenzierung finden Sie unterLizenzierung.

Live-Patching-Szenarien

Hotfixes können live über Pools, Hosts oder auf einem eigenständigen Server gepatcht werden. Einige erfordern einen Neustart, einige erfordern einen Neustart des XAPI-Toolstapels und einige Hotfixes haben keine Aufgaben nach dem Update. In den folgenden Szenarien wird das Verhalten beschrieben, wenn ein Live-Patch für ein Update verfügbar ist und nicht verfügbar ist.

- **Updates mit Live-Patch** — Einige Hotfixes, die den Linux-Kernel und den Xen Hypervisor aktualisieren, erfordern normalerweise keinen Neustart nach der Installation des Hotfixes. In einigen seltenen Fällen kann jedoch ein Neustart erforderlich sein, wenn der Live-Patch nicht angewendet werden kann.
- **Updates ohne Live-Patch** — Keine Änderung des Verhaltens hier. Es funktioniert wie gewohnt.

  > **Hinweis:**
  >
  > Wenn ein Host keinen Neustart erfordert oder der Hotfix Live-Patches enthält, wird XenCenter`No action required` auf der Seite Updatemodus angezeigt.

Automatische Updates und Live-Patches anwenden

Mit dem**automatischen Aktualisierungsmodus** in XenCenter können Sie den Mindestsatz an Hotfixes herunterladen und anwenden, die erforderlich sind, um Ihren Pool oder eigenständigen Host automatisch auf den neuesten Stand zu bringen. **Automatischer Aktualisierungsmodus** wendet alle kumulativen Updates an, die für einen Host verfügbar sind. Wenn jedoch eine neue Version der aktuellen Version als Update verfügbar **ist** , wird dieses Update nicht angewendet. Sie müssen manuell auswählen, um auf die neue aktuelle Version zu aktualisieren.

Sie können von der Live-Patch-Funktion profitieren, wenn Sie Hotfixes im Modus „Automatische Updates“ in XenCenter anwenden. Sie können den Neustart von Hosts vermeiden, wenn Live-Patches verfügbar sind und erfolgreich auf die Hosts angewendet werden, die im Modus **Automatische Updates** aktualisiert werden. Weitere Informationen zu den automatisierten Updates finden Sie unterAutomatische Updates anwenden.

Aktivieren des Live-Patches mit XenCenter und der XE-CLI

Die Funktion „Live-Patching“ ist standardmäßig aktiviert. Kunden können Live Patching mit XenCenter oder xe CLI-Befehl aktivieren oder deaktivieren.

Verwenden von XenCenter

1. Select den Pool oder den eigenständigen Host im Ressourcenbereich aus.
2. Wählen Sie im Menü **Pool** (**Server** bei Standalone-Hosts) die Option **Eigenschaften** aus, und klicken Sie dann auf **Live-Patching** .
3. Auf der Seite „Live Patching“:
   - Select **Live-Patching verwenden, wenn möglich** , um Live-Patching zu aktivieren.
   - Select **Live-Patching nicht verwenden** , um Live-Patching zu deaktivieren.

Verwenden der XE CLI

- Führen Sie den folgenden Befehl aus, um Live-Patching zu aktivieren:

```
xe pool-param-set live-patching-disabled=false uuid=”pool_uuid”
```

- Führen Sie den folgenden Befehl aus, um Live-Patching zu deaktivieren:

```
xe pool-param-set live-patching-disabled=true uuid=”pool_uuid”
```

Kopiert!
Failed!

Problembehandlung bei der Installation

October 16, 2019

Citrix bietet zwei Arten von Support: kostenloser Selbsthilfe-Support vonwww.citrix.com/supportund bezahlte Support-Services, die Sie über die Support-Website erwerben können. Mit dem technischen Support von Citrix können Sie einen Support-Fall online öffnen oder sich telefonisch an das Support-Center wenden.

Die Citrix Support-Website,www.citrix.com/support, beherbergt verschiedene Ressourcen. Diese Ressourcen können für Sie hilfreich sein, wenn während der Installation ein seltsames Verhalten, Abstürze oder andere Probleme auftreten. Zu den Ressourcen gehören Foren, Knowledge Base-Artikel, Softwareupdates, Security Bulletins, Tools und Produktdokumentation.

Mit einer Tastatur, die direkt mit dem Hostcomputer verbunden ist (nicht über einen seriellen Anschluss verbunden), können Sie während der Installation auf drei virtuelle Terminals zugreifen:

- Drücken Sie **Alt+F1** , um auf das Citrix Hypervisor Hauptinstallationsprogramm zuzugreifen
- Drücken Sie **Alt+F2** , um auf eine lokale Shell zuzugreifen
- Drücken Sie **Alt+F3** , um auf das Ereignisprotokoll zuzugreifen

Wenn während der Installation ein unbekannter Fehler auftritt, erfassen Sie die Protokolldatei von Ihrem Host und stellen Sie sie dem technischen Support zur Verfügung. Führen Sie das folgende Verfahren aus, um die Protokolldatei zu erfassen.

So erfassen und speichern Sie die Protokolldateien:

1. Drücken Sie **Alt+F2** , um auf die lokale Shell zuzugreifen.
2. Geben Sie Folgendes ein:

   ```
   1 /opt/xensource/installer/report.py
   ```

3. Sie werden aufgefordert, auszuwählen, wo Sie die Protokolldatei speichern möchten: **NFS**, **FTP**oder **Lokales Medium**.

   Select **NFS** oder **FTP** aus, um die Protokolldatei auf einen anderen Computer im Netzwerk zu kopieren. Dazu muss das Netzwerk ordnungsgemäß funktionieren, und Sie müssen Schreibzugriff auf einen Remotecomputer haben.

   Select **Lokales Medium** aus, um die Datei auf einem Wechseldatenträger, z. B. einem USB-Flashlaufwerk, auf dem lokalen Computer zu speichern.

   Sobald Sie Ihre Auswahl getroffen haben, schreibt das Programm die Protokolldatei an den von Ihnen gewählten Speicherort. Der Dateiname lautet`support.tar.bz2`.

Senden Sie die erfasste Protokolldatei an das Support-Team, damit sie sie überprüfen können.

Kopiert!
Failed!

Starten von SAN-Umgebungen

October 16, 2019

Boot-von-SAN-Umgebungen bieten mehrere Vorteile, darunter hohe Leistung, Redundanz und Speicherplatzkonsolidierung. In diesen Umgebungen befindet sich die Startdiskette auf einem Remote-SAN und nicht auf dem lokalen Host. Der Host kommuniziert mit dem SAN über einen Hostbusadapter (HBA). Das BIOS des HBA enthält die Anweisungen, mit denen der Host die Startdiskette finden kann.

Der Start von SAN hängt von SAN-basierten Festplatten-Arrays ab, die entweder Hardware-Fibre-Channel- oder HBA-iSCSI-Adapter auf dem Host unterstützen. Für einen vollständig redundanten Start von SAN-Umgebung müssen Sie mehrere Pfade für den E/A-Zugriff konfigurieren. Stellen Sie dazu sicher, dass für das Root-Gerät die Multipath-Unterstützung aktiviert ist. Informationen darüber, ob Multipath für Ihre SAN-Umgebung verfügbar ist, erhalten Sie von Ihrem Speicheranbieter oder Administrator. Wenn mehrere Pfade verfügbar sind, können Sie Multipathing in der Citrix Hypervisor Bereitstellung nach der Installation aktivieren.

> **Warnhinweis:**
>
> Boot-from-SAN-Einstellungen werden während des Upgrade-Vorgangs *nicht* vererbt. Befolgen Sie beim Upgrade mit ISO oder Netzwerkstart die gleichen Anweisungen wie beim Installationsvorgang unten, um sicherzustellen, dass diese korrekt konfiguriert`multipath` ist.

So installieren Sie Citrix Hypervisor auf einem Remote-Datenträger in einem SAN mit aktiviertem Multipathing:

1. Drücken Sie auf dem Bildschirm Willkommen bei Citrix Hypervisor **F2**.
2. Geben`multipath`Sie an der Startaufforderung

Der Citrix Hypervisor Installationsprozess konfiguriert den Citrix Hypervisor or-Server, der von einem Remote-SAN mit aktiviertem Multipathing gestartet wird.

Um das Multipathing des Dateisystems mithilfe der PXE- oder UEFI-Installation`device_mapper_multipath=yes` zu aktivieren, fügen Sie der Konfigurationsdatei hinzu. Im Folgenden finden Sie eine Beispielkonfiguration:

```
default xenserver
label xenserver
   kernel mboot.c32
   append /tftpboot/xenserver/xen.gz dom0_max_vcpus=1-2 \
   dom0_mem=1024M,max:1024M com1=115200,8n1 \
   console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
   xencons=hvc console=hvc0 console=tty0 \
   device_mapper_multipath=yes \
   install ---  /tftpboot/xenserver/install.img
```

Weitere Informationen zum Massenspeicher-Multipathing in Ihrer Citrix Hypervisor Umgebung finden Sie unterSpeicher.

Software-Boot-von-iSCSI für Cisco UCS

Die Software-Boot-from-iSCSI-Funktion ermöglicht es Kunden, Citrix Hypervisor mithilfe von iSCSI vom SAN zu installieren und zu starten. Mithilfe dieser Funktion kann Citrix Hypervisor in einer von

einem iSCSI-Ziel bereitgestellten LUN installiert, gestartet und von dieser ausgeführt werden. Das iSCSI-Ziel wird in der iSCSI-Boot-Firmware-Tabelle angegeben. Diese Funktion ermöglicht das Anhängen der Stammdatenträger über iSCSI.

Citrix Hypervisor unterstützt die folgenden Funktionen für Software-Boot-from-iSCSI:

- Host-Installation durch PXE-Boot
- Cisco UCS vNIC

  Software-Boot-from-iSCSI wurde im Legacy-BIOS- und UEFI-Boot-Modus unter Verwendung von Cisco UCS vNICs und Power Vault, NetApp und EqualLogic Arrays getestet. Andere Konfigurationen können funktionieren, sie wurden jedoch nicht validiert.
- Jumbo Frames (MTU=9000) konfiguriert mit dem Cisco UCS-Manager
- Cisco UCS Line-Rate Begrenzung
- VLANs ohne Tags
- Netzwerke mit dem vSwitch-Back-End
- LVHDOiSCSI-SRs und NFS-SRs auf demselben oder einem anderen SAN/NAS
- Multipathing des iSCSI-Stammdatenträgers
- Kompatibilität mit gängigen Citrix Hypervisor Vorgängen (Netzwerk, Wartung)

Anforderungen

- Die primäre Verwaltungsschnittstelle (IP-adressierbar) und das Netzwerk für den VM-Datenverkehr müssen separate Schnittstellen verwenden.
- Der Speicher (iSCSI-Ziele) muss sich in einem separaten IP-Netzwerk (Layer 3) mit allen anderen Netzwerkschnittstellen mit IP-Adressen auf dem Host befinden.
- Der Speicher muss sich im selben Subnetz wie die Speicherschnittstelle des Citrix Hypervisor or-Servers befinden.

Installieren von Citrix Hypervisor mithilfe von CD-Medien

Führen Sie die folgenden Schritte aus, um Citrix Hypervisor mithilfe einer CD zu installieren:

1. Öffnen Sie das Boot-Menü, geben Sie an der`boot:` Eingabeaufforderung`menu.c32`
2. Wählen Sie mit den Cursortasten eine Installationsoption aus:
   - Wählen Sie für eine einzelne Pfad-LUN **installieren**
   - Wählen Sie für eine Multipath-LUN **Multipath**

3. Drücken Sie die Tabulatortaste.

   Bearbeiten Sie die Zeile, die wie folgt endet:

   ```
   ---  /install.img
   ```

4. Bearbeiten Sie diese Zeile mit den Cursortasten, um zu lesen:

   ```
   use_ibft ---  /install.img
   ```

5. Drücken Sie die **Eingabetaste**.

   Die Installation des Citrix Hypervisor or-Servers erfolgt wie gewohnt.

Installieren von Citrix Hypervisor mithilfe von PXE

Führen Sie die folgenden Schritte aus, um Citrix Hypervisor mithilfe von PXE zu installieren:

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie das Schlüsselwort **use_ibft** in den Kernel-Parametern hinzufügen. Wenn Multipathing erforderlich ist, müssen Sie **device_mapper_multipath=enabled**hinzufügen.

Das folgende Beispiel zeigt die PXE-Konfiguration für eine einzelne LUN:

```
label xenserver
kernel mboot.c32
append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
com1=115200,8n1 console=com1,vga ---  XS/vmlinuz xencons=hvc
   console=tty0
console=hvc0 use_ibft ---  XS/install.img
```

Das folgende Beispiel zeigt die PXE-Konfiguration für eine Multipath-LUN:

```
label xenserver
kernel mboot.c32
append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
com1=115200,8n1 console=com1,vga ---  XS/vmlinuz xencons=hvc
   console=tty0
console=hvc0 use_ibft device_mapper_multipath=enabled ---  XS/
   install.img
```

Kopiert!
Failed!

Netzwerk-Boot-Installationen

October 16, 2019

Citrix Hypervisor unterstützt das Booten von Hosts im UEFI-Modus. Der UEFI-Modus bietet eine umfangreiche Reihe von standardisierten Einrichtungen für den Bootloader und die Betriebssysteme. Mit dieser Funktion kann Citrix Hypervisor einfacher auf Hosts installiert werden, auf denen UEFI der Standardstartmodus ist.

Der folgende Abschnitt enthält Informationen zum Einrichten der TFTP- und NFS-, FTP- oder HTTP-Server zum Aktivieren des PXE- und UEFI-Boots von Citrix Hypervisor or-Serverinstallationen. Anschließend wird beschrieben, wie Sie eine XML-Antwortdatei erstellen, mit der Sie unbeaufsichtigte Installationen durchführen können.

Konfigurieren der PXE- und UEFI-Umgebung für die Citrix Hypervisor Installation

Bevor Sie das Citrix Hypervisor Installationsmedium einrichten, konfigurieren Sie die TFTP- und DHCP-Server. Die folgenden Abschnitte enthalten Informationen zum Konfigurieren des TFTP-Servers für den PXE- und UEFI-Boot. Allgemeine Einrichtungsverfahren finden Sie in der Herstellerdokumentation.

> **Hinweis:**
>
> Citrix Hypervisor 6.0 wurde von der MBR-Festplattenpartitionierung in die GUID-Partitionstabelle (GPT) verschoben. Einige PXE-Bereitstellungssysteme von Drittanbietern versuchen möglicherweise, die Partitionstabelle auf der Festplatte eines Computers zu lesen, *bevor* das Image auf dem Host bereitgestellt wird.
>
> Wenn das Bereitstellungssystem nicht mit dem GPT-Partitionierungsschema kompatibel ist und die Festplatte zuvor für eine Version von Citrix Hypervisor verwendet wurde, die GPT verwendet, schlägt das PXE-Bereitstellungssystem möglicherweise fehl. Eine Problemumgehung für diesen Fehler besteht darin, die Partitionstabelle auf dem Datenträger zu löschen.

Zusätzlich zu den TFTP- und DHCP-Servern benötigen Sie einen NFS-, FTP- oder HTTP-Server, um die Citrix Hypervisor Installationsdateien zu speichern. Diese Server können auf einem Server nebeneinander existieren oder über verschiedene Server im Netzwerk verteilt werden.

Darüber hinaus muss jeder Citrix Hypervisor or-Server, den Sie PXE starten möchten, über eine PXE-Start-fähige Ethernet-Karte verfügen.

Bei den folgenden Schritten wird davon ausgegangen, dass der Linux-Server, den Sie verwenden, RPM unterstützt.

Konfigurieren des TFTP-Servers für den PXE-Start

1. Erstellen Sie im `/tftpboot` Verzeichnis ein Verzeichnis namens `xenserver`
2. Kopieren Sie die `mboot.c32` Dateien `pxelinux.0` und aus dem `/usr/lib/syslinux` Verzeichnis in das `/tftboot` Verzeichnis.

   > **Hinweis:**
   >
   > Wir empfehlen dringend die Verwendung von `mboot.c32` Dateien `pxelinux.0` und Dateien aus derselben Quelle (z. B. aus demselben Citrix Hypervisor ISO).

3. Kopieren Sie auf dem Citrix Hypervisor Installationsmedium die Dateien `install.img` (aus dem Stammverzeichnis) und `vmlinuz` (aus dem `xen.gz` Verzeichnis) `/boot` in das neue `/tftpboot/xenserver` Verzeichnis auf dem TFTP-Server.
4. Erstellen Sie im `/tftboot` Verzeichnis ein Verzeichnis namens `pxelinux.cfg`.
5. Erstellen Sie im `pxelinux.cfg` Verzeichnis Ihre Konfigurationsdatei mit dem Namen **`default`** .

   Der Inhalt dieser Datei hängt davon ab, wie Sie Ihre PXE-Boot-Umgebung konfigurieren möchten. Im Folgenden sind zwei Beispielkonfigurationen aufgeführt. Die erste Beispielkonfiguration startet eine Installation auf jedem Computer, der vom TFTP-Server gestartet wird. Diese Installation erfordert manuelle Antworten. Die zweite Beispielkonfiguration ist für eine unbeaufsichtigte Installation.

   > **Hinweis:**
   >
   > Die folgenden Beispiele zeigen, wie Sie das Installationsprogramm so konfigurieren, dass es auf der physischen Konsole ausgeführt wird `tty0`. Um einen anderen Standard zu verwenden, stellen Sie sicher, dass die Konsole, die Sie verwenden möchten, die ganz rechts ist.

   ```
   default xenserver
   label xenserver
       kernel mboot.c32
       append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
           dom0_mem=1024M,max:1024M com1=115200,8n1 \
       console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
       xencons=hvc console=hvc0 console=tty0 \
       ---  /tftpboot/xenserver/install.img
   ```

   Eine Beispielkonfiguration, die eine unbeaufsichtigte Installation unter Verwendung der Antwortdatei unter der angegebenen URL durchführt:

> **Hinweis:**
>
> Um anzugeben, welcher Netzwerkadapter zum Abrufen der Antwortdatei verwendet werden soll, geben Sie den`answerfile_device=ethX` Parameter`answerfile_device=MAC` oder ein, und geben Sie entweder die Ethernet-Gerätenummer oder die MAC-Adresse des Geräts an.

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
    append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
        dom0_mem=1024M,max:1024M com1=115200,8n1 \
        console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
        xencons=hvc console=hvc0 console=tty0 \
        answerfile=http://pxehost.example.com/answerfile \
        install ---  /tftpboot/xenserver/install.img
```

Weitere Informationen zum Inhalt der PXE-Konfigurationsdatei finden SieSYSLINUXauf der Website.

Konfigurieren Sie Ihren TFTP-Server für den UEFI-Boot

So konfigurieren Sie Ihren TFTP-Server für den UEFI-Boot:

1. Erstellen Sie im `/tftpboot` Verzeichnis ein Verzeichnis namens `EFI/xenserver`.
2. Konfigurieren Sie Ihren DHCP-Server so, dass`/EFI/xenserver/grubx64.efi` er als Startdatei bereitgestellt wird.
3. grub.cfg“ Datei erstellen. Zum Beispiel:
   - Bei einer Installation, die manuelle Antworten auf Installationsaufforderungen erfordert:

     ```
     menuentry ”Citrix Hypervisor Install (serial)” {

         multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
             watchdog \
         dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
         module2 /EFI/xenserver/vmlinuz console=hvc0
         module2 /EFI/xenserver/install.img
      }
     ```

   - Für eine unbeaufsichtigte Installation, die eine Antwortdatei verwendet:

     ```
     menuentry ”Citrix Hypervisor Install (serial)” {

     ```



```
3       multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
            watchdog \
4       dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
5       module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
            answerfile_device=eth0 answerfile=ftp://ip_address/
            path_to_answerfile install
6       module2 /EFI/xenserver/install.img
7   }
```

Weitere Informationen zum Verwenden einer Antwortdatei finden Sie unter *Erstellen einer Antwortdatei für die unbeaufsichtigte PXE- und UEFI-Installation*.

4. Kopieren Sie die`grub.cfg` Datei in das`/tftpboot/EFI/xenserver` Verzeichnis auf dem TFTP-Server.
5. Kopieren Sie auf dem Citrix Hypervisor Installationsmedium die Dateien `grubx64.efi`, `install.img` (aus dem Stammverzeichnis), `vmlinuz`, und `xen.gz` (aus dem Verzeichnis `/boot`) in das neue Verzeichnis `/tftpboot/EFI/xenserver` auf dem TFTP-Server.

Weitere Informationen zu Ihrem spezifischen Betriebssystem finden Sie in Ihrem Serverbetriebssystemhandbuch. Die Informationen hier sind eine Anleitung, die für Red Hat, Fedora und einige andere RPM-basierte Distributionen verwendet werden kann.

So richten Sie das Citrix Hypervisor Installationsmedium auf einem HTLP-, FTP- oder NFS-Server ein:

1. Erstellen Sie auf dem Server ein Verzeichnis, aus dem das Citrix Hypervisor Installationsmedium über HTTP, FTP oder NFS exportiert werden kann.
2. Kopieren Sie den gesamten Inhalt des Citrix Hypervisor Installationsmediums in das neu erstellte Verzeichnis auf dem HTTP-, FTP- oder NFS-Server. Dieses Verzeichnis ist Ihr Installations-Repository.

   > **Hinweis:**
   >
   > Achten Sie beim Kopieren des Citrix Hypervisor Installationsmediums darauf, dass Sie die Datei in `.treeinfo` das neu erstellte Verzeichnis kopieren.

So bereiten Sie das Zielsystem vor:

1. Starten Sie das System und rufen Sie das Boot-Menü auf (**F12** in den meisten BIOS-Programmen).
2. Select aus, um von Ihrer Ethernet-Karte zu booten.
3. Das System startet dann PXE von der Installationsquelle, die Sie eingerichtet haben, und das Installationsskript wird gestartet. Wenn Sie eine Antwortdatei eingerichtet haben, kann die Installation unbeaufsichtigt fortgesetzt werden.

Installieren von Supplemental Packs während der Citrix Hypervisor Installation

Ergänzende Packs werden verwendet, um die Funktionen von Citrix Hypervisor zu ändern und zu erweitern, indem Software in der Steuerdomäne (Dom0) installiert wird. Beispielsweise möchte ein OEM-Partner Citrix Hypervisor mit einer Reihe von Verwaltungstools ausliefern, für die SNMP-Agenten installiert werden müssen. Benutzer können zusätzliche Packs entweder während der ersten Citrix Hypervisor-Installation oder jederzeit danach hinzufügen.

Entpacken Sie beim Installieren zusätzlicher Packs während der Citrix Hypervisor Installation jedes Zusatzpaket in ein separates Verzeichnis.

Es gibt auch Einrichtungen für OEM-Partner, die ergänzende Packs zu Citrix Hypervisor Installationsrepositories hinzufügen, um automatisierte Werkseinstellungen zu ermöglichen.

Erstellen einer Antwortdatei für die unbeaufsichtigte PXE- und UEFI-Installation

Um Installationen unbeaufsichtigt durchzuführen, erstellen Sie eine XML-Antwortdatei. Hier ist eine Beispiel-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/citrix-hypervisor
            /</source>
        <post-install-script type="url">
          http://pxehost.example.com/myscripts/post-install-script
        </post-install-script>
        <admin-interface name="eth0" proto="dhcp" />
        <timezone>Europe/London</timezone>
    </installation>
```

Enthält alle Knoten innerhalb eines Stammknotens namens *installation*.

> **Hinweis:**
>
> Um die Thin Provisioning zu aktivieren, geben Sie ein`srtype` Attribut als an`ext` . Wenn dieses Attribut nicht angegeben wird, ist der lokale Standardspeichertyp LVM. Die Thin Provisioning setzt den lokalen Speichertyp auf EXT3 und ermöglicht das lokale Caching für Citrix Virtual Desktops ordnungsgemäß. Weitere Informationen finden Sie unter Speicher.

Im Folgenden finden Sie eine Zusammenfassung der Elemente. Alle Knotenwerte sind Text, sofern nicht anders angegeben. Erforderliche Elemente sind angegeben.

<primary-disk>

Erforderlich? Ja

Beschreibung: Der Name des Speichergeräts, auf dem die Steuerdomäne installiert ist. Dieses Element entspricht der Auswahl, die im Schritt *„Primärer Datenträger auswählen“* des manuellen Installationsprozesses getroffen wurde.

Attribute: Sie können ein`guest-storage` Attribut mit möglichen Werten`yes` und angeben`no` . 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 Speicher-Repository erstellt wird. Geben Sie in diesem Fall keine Gastdisk-Schlüssel an.

<guest-disk>

Erforderlich? Nein

Beschreibung: Der Name eines Speichergeräts, das für die Speicherung von Gästen verwendet werden soll. Verwenden Sie eines dieser Elemente für jede zusätzliche Festplatte.

Attribute: Keine

<keymap>

Erforderlich? Ja

Beschreibung: Der Name der Keymap, 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

Sie können auch automatisierte Upgrades durchführen, indem Sie die Antwortdatei entsprechend ändern. Legen Sie das Attribut mode des zu *aktualisierenden*Installationselements fest, und geben Sie den Datenträger an, auf dem die vorhandene Installation mit dem *vorhandenen Installationselement*gespeichert ist. Lassen Sie die *Primärdatenträger-**und Gastdatenträgerelemente* nicht angegeben. Zum Beispiel:

```
<?xml version=”1.0”?>
<installation mode=”upgrade”>
    <existing-installation>sda</existing-installation>
```



```
4     <source type="url">http://pxehost.example.com/citrix-hypervisor/</
          source>
5     <post-install-script type="url">
6         http://pxehost.example.com/myscripts/post-install-script
7     </post-install-script>
8 </installation>
```

Kopiert!
Failed!

Host-Partitionslayout

October 16, 2019

Citrix Hypervisor 7.0 hat ein neues Host-Datenträgerpartitionslayout eingeführt. Durch das Verschieben von Protokolldateien auf eine größere, separate Partition kann Citrix Hypervisor für einen längeren Zeitraum detailliertere Protokolle speichern. Diese Funktion verbessert die Fähigkeit, Probleme zu diagnostizieren. Gleichzeitig entlastet das neue Partitionslayout die Anforderungen an die Root-Festplatte von Dom0 und vermeidet potenzielle Speicherprobleme aufgrund des Speicherplatzes in der Protokolldatei. Das neue Layout enthält die folgenden Partitionen:

- 18 GB Citrix Hypervisor-Serversteuerungsdomo-Partition (dom0)
- 18 GB Sicherungspartition
- 4 GB Log-Partition
- 1 GB Swap-Partition
- 0,5 GB UEFI-Boot-Partition

In Citrix Hypervisor 6.5 und früheren Versionen wurde die dom0 Partition mit 4 GB für alle dom0-Funktionen, einschließlich Swap und Protokollierung, verwendet. Kunden, die kein Remote-Syslog verwenden oder die mit Überwachungstools von Drittanbietern und ergänzenden Packs verwendet haben, haben festgestellt, dass die Größe der Partition begrenzt ist. Citrix Hypervisor beseitigt dieses Problem und stellt dom0 eine dedizierte 18-GB-Partition bereit. Darüber hinaus reduziert eine größere Partition, die dom0 gewidmet ist, den Bedarf an der dom0 Root-Festplatte, was erhebliche Leistungsverbesserungen bieten kann.

Die Einführung der dedizierten 4-GB-Protokollpartition beseitigt Szenarien, in denen übermäßige Protokollierung die dom0-Partition gefüllt und das Verhalten des Hosts beeinflusst. Diese Partition ermöglicht es Kunden auch, eine detaillierte Liste der Protokolle für einen längeren Zeitraum aufzubewahren, was die Diagnose von Problemen verbessert.

Das Partitionslayout enthält auch eine dedizierte 500-MB-Partition, die für den UEFI-Boot erforderlich ist.

> **Hinweis:**
>
> Wenn Sie Citrix Hypervisor mit dem oben beschriebenen neuen Partitionslayout installieren, stellen Sie sicher, dass Sie über einen Datenträger verfügen, der mindestens 46 GB groß ist.

Um Citrix Hypervisor auf kleineren Geräten zu installieren, können Sie Citrix Hypervisor mithilfe des Legacy-DOS-Partitionslayouts neu installieren. Ein kleines Gerät ist ein Gerät mit mehr als 12 GB, aber weniger als 46 GB Speicherplatz. Weitere Informationen finden Sie unter Installation auf kleinen Geräten.

> **Wichtig:**
>
> Es wird empfohlen, mindestens 46 GB Speicherplatz zuzuweisen und Citrix Hypervisor mithilfe des neuen GPT-Partitionslayouts zu installieren.

Upgrade auf das neue Partitionslayout

Beim Upgrade auf Citrix Hypervisor 8.0 von XenServer 6.5 oder einer früheren Version mit XenCenter wird das Hostpartitionslayout auf das neue Layout aktualisiert, vorausgesetzt:

- Es gibt mindestens 46 GB Speicherplatz auf der lokalen SR
- Es gibt keine VDIs auf der lokalen SR
- Sie verwenden XenCenter, das mit Citrix Hypervisor 8.0 ausgestellt wurde, um ein Rolling Pool Upgrade (RPU) auf Citrix Hypervisor 8.0 durchzuführen.

  > **Warnhinweis:**
  >
  > Kunden können kein Upgrade auf das neue Host-Partitionslayout mit xe CLI durchführen.

Während des Upgradevorgangs überprüft der RPU-Assistent auf der lokalen SR nach VDIs. Wenn während des Upgradevorgangs virtuelle Laufwerke (VDIs) vorhanden sind, werden Sie vom Assistenten aufgefordert, den VDI zu verschieben. Verschieben Sie VDIs auf der lokalen SR in eine freigegebene SR, und starten Sie den Upgradevorgang neu, um mit dem neuen Layout fortzufahren. Wenn die VDIs nicht verschoben werden können oder der lokale SR nicht genügend Speicherplatz (weniger als 46 GB) hat, wird das Upgrade mit dem alten Partitionslayout fortgesetzt. 0,5 GB Speicherplatz werden von der dom0-Partition dem UEFI-Boot zugewiesen.

Wiederherstellen des alten Partitionslayouts

Wenn Sie Citrix Hypervisor von Version 8.0 auf Version 6.x wiederherstellen möchten, wird das Layout der Hostpartition auf das Layout 6.x zurückgesetzt.

Legacy-Partitionslayouts

- XenServer 5.6 Service Pack 2 und früher verwendeten DOS-Partitionstabellen, um das Root-Dateisystem und die Backups vom lokalen Speicher zu trennen.
- XenServer 6.0 führte GUID-Partitionstabellen ein, um Root-Dateisystem, Backup und lokalen Speicher zu trennen.
- Bei der Installation von Citrix Hypervisor 8.0 auf Computern mit einer erforderlichen Anfangspartition, die beibehalten werden muss, wird das DOS-Partitionierungsschema weiterhin verwendet.

In der folgenden Tabelle sind die Installations- und Upgrade-Szenarien sowie das Partitionslayout aufgeführt, das nach diesen Vorgängen angewendet wird:

Betrieb	Anzahl der Partitionen vor dem Upgrade	Anzahl der Partitionen nach Installation/Upgrade	Partitionstabellentyp
Saubere Installation mit mindestens 46 GB primären Festplattenspeicher	Nicht zutreffend	6	Neue GPT
Saubere Installation`disable-gpt` mit mindestens 12 GB Speicherplatz auf der primären Festplatte	Nicht zutreffend	3 (oder 4, wenn eine Dienstprogrammpartition vorhanden ist)	DOS
Saubere Installation auf einem Computer mit einer Dienstprogrammpartition	Nicht zutreffend	3 (oder 4, wenn eine Dienstprogrammpartition vorhanden ist)	DOS
Upgrade von Citrix Hypervisor 6.x mit VMs auf lokaler SR oder mit weniger als 46 GB primären Festplattenspeicher	3	4	Alte GPT

Betrieb	Anzahl der Partitionen vor dem Upgrade	Anzahl der Partitionen nach Installation/Upgrade	Partitionstabellentyp
Upgrade von Citrix Hypervisor 6.x ohne VMs auf lokaler SR oder mit mehr als 46 GB primären Festplattenspeicher	3	6	Neue GPT
Upgrade von Citrix Hypervisor 6.x DOS-Partition (und ggf. Dienstprogramm-partition)	3 (oder 4, wenn eine Dienstprogrammpar-tition vorhanden ist)	3 (oder 4, wenn eine Dienstprogrammpar-tition vorhanden ist)	DOS

Kopiert!
Failed!

Installation auf kleinen Geräten

October 16, 2019

Mit Citrix Hypervisor können Kunden mit kleineren Geräten Citrix Hypervisor 8.0 mithilfe des Legacy-DOS-Partitionslayouts installieren. Ein kleines Gerät ist ein Gerät mit mehr als 12 GB, aber weniger als 46 GB Speicherplatz. Das Legacy-DOS-Partitionslayout umfasst:

- 4 GB Boot-Partition
- 4 GB Backup-Partition
- SR-Partition (falls vorhanden auf dem lokalen Datenträger)

Um Citrix Hypervisor auf kleinen Geräten`disable-gpt` zu installieren, müssen Sie die dom0-Parameter hinzufügen. Sie können menu.c32 verwenden, um den Parameter dom0 hinzuzufügen.

> **Hinweis:**
>
> Das Installationsprogramm bewahrt alle Dienstprogrammpartition auf, die vor dem Installationsvorgang auf dem Host vorhanden ist.
>
> **Wichtig:**

> Es wird empfohlen, mindestens 46 GB Speicherplatz zuzuweisen und Citrix Hypervisor mithilfe des neuen GPT-Partitionslayouts zu installieren. Weitere Informationen finden Sie unter Host-Partitionslayout.

Kopiert!
Failed!

Hosts und Ressourcenpools

October 16, 2019

In diesem Abschnitt wird beschrieben, wie Ressourcenpools anhand einer Reihe von Beispielen mit der xe-Befehlszeilenschnittstelle erstellt werden können. Eine einfache NFS-basierte Shared Storage-Konfiguration wird vorgestellt und einige einfache VM-Verwaltungsbeispiele werden diskutiert. Es enthält auch Verfahren für den Umgang mit physischen Knotenfehlern.

Übersicht über Citrix Hypervisor or-Server und Ressourcenpools

Ein *Ressourcenpool* besteht aus mehreren Citrix Hypervisor or-Serverinstallationen, die an eine einzelne verwaltete Entität gebunden sind, die virtuelle Maschinen hosten kann. In Kombination mit gemeinsam genutztem Speicher ermöglicht ein Ressourcenpool das Starten von VMs auf *jedem* Citrix Hypervisor or-Server, der über ausreichend Arbeitsspeicher verfügt. Die VMs können dann dynamisch zwischen den Citrix Hypervisor or-Servern verschoben werden, während sie mit minimalen Ausfallzeiten ausgeführt werden (Live-Migration). Wenn ein einzelner Citrix Hypervisor or-Server einen Hardwarefehler erleidet, kann der Administrator ausgefallene VMs auf einem anderen Citrix Hypervisor or-Server 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 erzwungen wird.

Ein Pool hat immer mindestens einen physischen Knoten, der als *Master*bezeichnet wird. Nur der Master-Knoten stellt eine Verwaltungsschnittstelle bereit (die von XenCenter und der Citrix Hypervisor Befehlszeilenschnittstelle (XE CLI genannt). Der Master leitet Befehle nach Bedarf an einzelne Mitglieder weiter.

> **Hinweis:**
>
> Wenn der Poolmaster fehlschlägt, findet die Master-Wiederwahl nur statt, wenn die hohe Verfügbarkeit aktiviert ist.

Anforderungen für das Erstellen von Ressourcenpools

Ein Ressourcenpool ist ein homogenes (oder heterogenes Aggregat mit Einschränkungen) von einem oder mehreren Citrix Hypervisor or-Servern mit bis zu 64 Jahren. Die Definition von homogen ist:

- CPUs auf dem Server, der dem Pool beitritt, sind (in Bezug auf Hersteller, Modell und Funktionen) dieselben wie die CPUs auf Servern, die sich bereits im Pool befinden.
- Auf dem Server, der dem Pool beitritt, wird dieselbe Version der Citrix Hypervisor or-Software auf derselben Patch-Ebene ausgeführt wie Server, die sich bereits im Pool befinden.

Die Software erzwingt zusätzliche Einschränkungen beim Verbinden eines Servers mit einem Pool. Insbesondere überprüft Citrix Hypervisor, ob die folgenden Bedingungen für den Server zutreffen, der dem Pool beitritt:

- Der Server ist kein Mitglied eines vorhandenen Ressourcenpools.
- Auf dem Server ist kein freigegebener Speicher konfiguriert.
- Der Server hostet keine laufenden oder suspendierten VMs.
- Auf den VMs auf dem Server werden keine aktiven Vorgänge ausgeführt, z. B. beim Herunterfahren einer virtuellen Maschine.
- Die Uhr auf dem Server wird zur gleichen Zeit wie der Poolmaster synchronisiert (z. B. mithilfe von NTP).
- Die Verwaltungsschnittstelle des Servers ist nicht gebunden. Sie können die Verwaltungsschnittstelle konfigurieren, wenn der Server erfolgreich dem Pool beitritt.
- Die Verwaltungs-IP-Adresse ist statisch, entweder auf dem Server selbst oder mithilfe einer entsprechenden Konfiguration auf Ihrem DHCP-Server konfiguriert.

Citrix Hypervisor or-Server in Ressourcenpools können unterschiedliche physische Netzwerkschnittstellen enthalten und lokale Speicher-Repositorys unterschiedlicher Größe aufweisen. In der Praxis ist es oft schwierig, mehrere Server mit genau denselben CPUs zu erhalten, und daher sind kleinere Abweichungen zulässig. Wenn es akzeptabel ist, Hosts mit unterschiedlichen CPUs als Teil desselben Pools zu haben, können Sie den Pool-Joining-Vorgang erzwingen, indem Sie`--force` Parameter übergeben.

Alle Hosts im Pool müssen sich am selben Standort befinden und über ein Netzwerk mit niedriger 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-Repositories enthalten, um auszuwählen, auf welchem Citrix Hypervisor or-Server eine VM ausgeführt werden soll und eine VM dynamisch zwischen Citrix

Hypervisor-Servern verschoben werden soll. Erstellen Sie nach Möglichkeit einen Pool, nachdem der freigegebene Speicher verfügbar ist. Es wird empfohlen, vorhandene VMs mit Datenträgern im lokalen Speicher nach dem Hinzufügen von freigegebenem Speicher in den freigegebenen Speicher zu verschieben. Sie können den`xe vm-copy` Befehl verwenden oder XenCenter zum Verschieben von VMs verwenden.

Erstellen eines Ressourcenpools

Ressourcenpools können mit XenCenter oder der CLI erstellt werden. Wenn ein neuer Host einem Ressourcenpool beitritt, synchronisiert der beitrittende Host seine lokale Datenbank mit der Pool-weiten Datenbank und erbt einige Einstellungen aus dem Pool:

- VM-, lokale und Remotespeicherkonfiguration wird der Pool-weiten Datenbank hinzugefügt. Diese Konfiguration wird auf den beitrittenden Host im Pool angewendet, es sei denn, Sie machen die Ressourcen explizit freigegeben, nachdem der Host dem Pool beitritt.
- Der beitrittsende Host erbt vorhandene freigegebene Speicher-Repositories im Pool. Geeignete PBD-Datensätze werden erstellt, damit der neue Host automatisch auf vorhandenen freigegebenen Speicher zugreifen kann.
- Netzwerkinformationen werden teilweise an den beitrittenden Host vererbt: Die *strukturellen* Details von NICs, VLANs und gebundenen Schnittstellen werden alle vererbt, die *Richtlinieninformationen* jedoch nicht. Diese Richtlinieninformationen, die neu konfiguriert werden müssen, umfassen:
  - Die IP-Adressen von Verwaltungs-NICs, die von der ursprünglichen Konfiguration beibehalten werden.
  - Der Speicherort der Verwaltungsschnittstelle, der mit der ursprünglichen Konfiguration übereinstimmt. Wenn die anderen Pool-Hosts beispielsweise Verwaltungsschnittstellen auf einer gebundenen Schnittstelle haben, muss der beitrittende Host nach dem Beitritt auf die Bindung migriert werden.
  - Dedizierte Speicher-NICs, die dem beitrittenden Host über XenCenter oder die CLI neu zugewiesen werden müssen, und die PBDs werden neu angeschlossen, um den Datenverkehr entsprechend weiterzuleiten. Dies liegt daran, dass IP-Adressen nicht als Teil des Pool-Join-Vorgangs zugewiesen werden und die Speicher-Netzwerkkarte nur funktioniert, wenn diese korrekt konfiguriert ist. Weitere InformationenVerwalten von Netzwerkenzum Deditieren einer Speicher-NIC über die CLI finden Sie unter.

> **Hinweis:**
>
> Sie können einen neuen Host nur dann zu einem Ressourcenpool beitreten, wenn sich die Verwaltungsschnittstelle des Hosts auf demselben getaggten VLAN befindet wie das des

> Ressourcenpools.

So verbinden Sie Citrix Hypervisor or-Server host1 und host2 mithilfe der CLI mit einem Ressourcenpool

1. Öffnen Sie eine Konsole auf dem Citrix Hypervisor *or-Serverhost2*.
2. Befehlen Sie Citrix Hypervisor or-Server *host2* , um dem Pool auf dem Citrix Hypervisor or-Server *host1* beizutreten, indem Sie den folgenden Befehl ausführen:

   ```
   xe pool-join master-address=host1 master-username=
       administrators_username master-password=password
   ```

   Der`master-address` muss auf den vollqualifizierten Domänennamen des Citrix *Hypervisor-Serverhost1* festgelegt sein. Das`password` muss das Administratorkennwort sein, das bei der Installation des Citrix Hypervisor or-Servers *host1* festgelegt wurde.

Citrix Hypervisor or-Server gehören standardmäßig zu einem unbenannten Pool. Benennen Sie den vorhandenen namenlosen Pool um, um Ihren ersten Ressourcenpool zu erstellen. Verwenden Sie tab-complete, um Folgendes zu finden`pool_uuid`:

```
xe pool-param-set name-label=”New Pool” uuid=pool_uuid
```

Erstellen heterogener Ressourcenpools

Citrix Hypervisor vereinfacht die Erweiterung der Bereitstellungen im Laufe der Zeit, da unterschiedliche Hosthardware mit einem Ressourcenpool verbunden werden kann, der als heterogene Ressourcenpools bezeichnet wird. Heterogene Ressourcenpools werden durch die Verwendung von Technologien in Intel (FlexMigration) und AMD (Extended Migration) CPUs ermöglicht, die „Maskierung“ oder „Nivellierung“ der CPU ermöglichen. Die CPU-Maskierungs- und Nivellierfunktionen ermöglichen es, eine CPU so zu konfigurieren , dass sie eine andere Marke, ein Modell oder eine andere Funktionalität bereitstellt, als sie tatsächlich tut. Mit dieser Funktion können Sie Pools von Hosts mit unterschiedlichen CPUs erstellen, die Livemigration jedoch sicher unterstützen.

> **Hinweis:**
>
> Die CPUs von Citrix Hypervisor or-Servern, die heterogene Pools verbinden, müssen vom selben Anbieter (d. h. AMD, Intel) sein wie CPUs auf Hosts im Pool. Der spezifische Typ (Familie, Modell und Schrittnummern) muss jedoch nicht sein.

Citrix Hypervisor vereinfacht die Unterstützung heterogener Pools. Hosts können nun zu vorhandenen Ressourcenpools hinzugefügt werden, unabhängig vom zugrunde liegenden CPU-Typ (solange

die CPU aus derselben Herstellerfamilie stammt). Das Pool-Feature-Set wird jedes Mal dynamisch berechnet:

- Ein neuer Host tritt in den Pool ein
- Ein Poolmitglied verlässt den Pool
- Ein Poolmitglied verbindet sich nach einem Neustart erneut

Jede Änderung des Pool-Feature-Sets wirkt sich nicht auf VMs aus, die derzeit im Pool ausgeführt werden. Eine laufende VM verwendet weiterhin den Featuresatz, der beim Start angewendet wurde. Dieser Funktionsumfang wird beim Booten behoben und bleibt bei Migrations-, Suspende- und Fortsetzungsvorgängen bestehen. Wenn die Poolebene abfällt, wenn ein weniger fähiger Host 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 über Pools hinweg verschieben oder migrieren, vergleicht Citrix Hypervisor den Featuresatz der VM mit dem Feature-Set des Zielhosts. Wenn die Feature-Sets als kompatibel erfunden werden, darf die VM migriert werden. Dadurch kann sich die VM frei innerhalb und über 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 inkompatiblen Funktionsumfang nicht als Zielhost empfohlen.

Hinzufügen von freigegebenenSpeicher

Eine vollständige Liste der unterstützten freigegebenen Speichertypen finden Sie unterSpeicher-Repository-Formate. Dieser Abschnitt zeigt, wie gemeinsam genutzter Speicher (dargestellt als Speicher-Repository) auf einem vorhandenen NFS-Server erstellt werden kann.

So fügen Sie einem Ressourcenpool mithilfe der CLI gemeinsam genutzten NFS-Speicher hinzu

1. Öffnen Sie eine Konsole auf einem beliebigen Citrix Hypervisor or-Server im Pool.
2. Erstellen Sie das Speicher-Repository auf Server: /path, indem Sie den Befehl

```
1 xe sr-create content-type=user type=nfs name-label=”Example SR”
    shared=true \
2     device-config:server=server \
3     device-config:serverpath=path
```

`device-config:server` Ist der Hostname des NFS-Servers und`device-config:serverpath` der Pfad auf dem NFS-Server. Wie`shared` auf true festgelegt, wird gemeinsam genutzter Speicher automatisch mit jedem Citrix Hypervisor or-Server im Pool verbunden. Alle Citrix Hypervisor or-Server, die später beitreten, sind ebenfalls mit dem Speicher verbunden.

Die Universally Unique Identifier (UUID) des Speicher-Repositories wird auf dem Bildschirm gedruckt.

3. Suchen Sie die UUID des Pools, indem Sie den folgenden Befehl ausführen:

```
xe pool-list
```

4. Legen Sie den gemeinsam genutzten Speicher als den Pool-weiten Standard mit dem Befehl

```
xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
```

Da der freigegebene Speicher als Pool-weiter Standard festgelegt wurde, haben alle zukünftigen VMs ihre Festplatten standardmäßig auf freigegebenem Speicher erstellt. Weitere InformationenSpeicher-Repository-Formatezum Erstellen anderer freigegebener Speichertypen finden Sie unter.

Entfernen von Citrix Hypervisor -Servern aus einem Ressourcenpool

> **Hinweis:**
>
> Stellen Sie vor dem Entfernen eines Citrix Hypervisor or-Servers aus einem Pool sicher, dass Sie alle auf diesem Host ausgeführten VMs herunterfahren. Andernfalls wird eine Warnung angezeigt, die besagt, 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 wie bei einer Neuinstallation belassen. Auswerfen von Citrix Hypervisor or-Servern nicht aus einem Pool, wenn wichtige Daten auf den lokalen Datenträgern vorhanden sind.

So entfernen Sie einen Host aus einem Ressourcenpool mithilfe der CLI

1. Öffnen Sie eine Konsole auf einem beliebigen Host im Pool.
2. Suchen Sie die UUID des Hosts, indem Sie den Befehl

```
xe host-list
```

3. Den erforderlichen Host aus dem Pool auswerfen:

```
xe pool-eject host-uuid=host_uuid
```

Der Citrix Hypervisor or-Server wird ausgeworfen und in einem neu installierten Zustand belassen.

> **Warnhinweis:**
>
> Auswerfen eines Hosts *nicht* aus einem Ressourcenpool, 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 `xe vm-copy` CLI-Befehl in den freigegebenen Speicher im Pool.

Wenn Citrix Hypervisor or-Server, die lokal gespeicherte VMs enthalten, aus einem Pool ausgeworfen werden, sind die VMs in der Pooldatenbank vorhanden. Die lokal gespeicherten VMs sind auch für die anderen Citrix Hypervisor or-Server sichtbar. Die VMs werden erst gestartet, wenn die ihnen zugeordneten virtuellen Laufwerke so geändert wurden, dass sie auf freigegebenen Speicher zeigen, die von anderen Citrix Hypervisor or-Servern im Pool angezeigt werden, oder entfernt wurden. Daher wird empfohlen, dass Sie jeden lokalen Speicher in den freigegebenen Speicher verschieben, wenn Sie einem Pool beitreten. Durch die Umstellung auf freigegebenen Speicher können einzelne Citrix Hypervisor or-Server ohne Datenverlust ausgeworfen (oder physisch ausfallen) werden.

> **Hinweis:**
>
> Wenn ein Host aus einem Pool entfernt wird, der über seine Verwaltungsschnittstelle in einem markierten VLAN-Netzwerk verfügt, wird der Computer neu gestartet und seine Verwaltungsschnittstelle ist im selben Netzwerk verfügbar.

Vorbereiten eines Pools von Citrix Hypervisor or-Servern für die Wartung

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 auf ihm gestartet werden. Anschließend müssen Sie die VMs auf einen anderen Citrix Hypervisor or-Server im Pool migrieren. Sie können dies tun, indem Sie den Citrix Hypervisor or-Server mit XenCenter in den Wartungsmodus versetzen. Weitere Informationen finden Sie in der XenCenter Hilfe.

Die Datensicherungssynchronisierung erfolgt alle 24 Stunden. Wenn Sie den Master-Host in den Wartungsmodus versetzen, gehen die letzten 24 Stunden RRD-Updates für Offline-VMs verloren.

> **Warnhinweis:**
>
> Wir empfehlen dringend, alle Citrix Hypervisor or-Server neu zu starten, bevor Sie ein Update installieren und anschließend deren Konfiguration überprüfen. Einige Konfigurationsänderungen werden nur wirksam, wenn Citrix Hypervisor neu gestartet wird. Daher kann der Neustart Konfigurationsprobleme aufdecken, die dazu führen können, dass das Update fehlschlägt.

So bereiten Sie einen Host in einem Pool für Wartungsvorgänge mithilfe der CLI vor

1. Führen Sie den folgenden Befehl aus:

   ```
   xe host-disable uuid=Citrix Hypervisor_host_uuid
   xe host-evacuate uuid=Citrix Hypervisor_host_uuid
   ```

   Mit diesem Befehl wird der Citrix Hypervisor or-Server deaktiviert und anschließend alle ausgeführten VMs auf andere Citrix Hypervisor-Server im Pool migriert.

2. Führen Sie den gewünschten Wartungsvorgang durch.

3. Aktivieren Sie den Citrix Hypervisor or-Server, wenn der Wartungsvorgang abgeschlossen ist:

   ```
   xe host-enable
   ```

4. Starten Sie alle angehaltenen VMs neu und setzen Sie alle angehaltenen VMs fort.

Ressourcen-Pool-Daten exportieren

Mit der Option Ressourcendaten exportieren können Sie einen Ressourcendatenbericht für Ihren Pool generieren und den Bericht in eine XLS- oder CSV-Datei exportieren. Dieser Bericht enthält detaillierte Informationen zu verschiedenen Ressourcen im Pool wie Server, Netzwerke, Speicher, virtuelle Maschinen, VDIs und GPUs. Mit dieser Funktion können Administratoren Ressourcen basierend auf verschiedenen Arbeitslasten wie CPU, Speicher und Netzwerk nachverfolgen, planen und zuweisen.

> **Hinweis:**
>
> Exportieren von Ressourcenpooldaten ist für Citrix Hypervisor Premium Edition-Kunden oder für Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.

Die Liste der Ressourcen und verschiedene Arten von Ressourcendaten, die im Bericht enthalten sind:

Server:

- Name
- Pool Master
- UID
- Adresse
- CPU-Auslastung
- Netzwerk (Durchschn. /max. KBs)
- Verwendeter Speicher
- Speicher
- Betriebszeit

- Beschreibung

Netzwerke:

- Name
- Link Status
- MAC
- MTU
- VLAN
- Typ
- Lage

VDI:

- Name
- Typ
- UID
- Größe
- Speicher
- Beschreibung

Lagerung:

- Name
- Typ
- UID
- Größe
- Lage
- Beschreibung

VMs:

- Name
- Energiezustand
- Laufen auf
- Adresse
- MAC
- NIC
- Betriebssystem
- Speicher
- Verwendeter Speicher
- CPU-Auslastung
- UID
- Betriebszeit
- Vorlage

- Beschreibung

GPU:

- Name
- Server
- PCI-Buspfad
- UID
- Energieverbrauch
- Temperatur
- Verwendeter Speicher
- Computerauslastung

> **Hinweis:**
>
> Informationen zu GPUs sind nur verfügbar, wenn GPUs an den Citrix Hypervisor or-Server angeschlossen sind.

So exportieren Sie Ressourcendaten

1. Wählen Sie im XenCenter Navigationsbereich **Infrastruktur** aus, und wählen Sie dann den Pool aus.
2. Select das Menü **Pool** und dann **Ressourcendaten exportieren** aus.
3. Navigieren Sie zu einem Speicherort, an dem Sie den Bericht speichern möchten, und klicken Sie dann auf **Speichern**.

Host-Einschalten

Remote-Einschalten von Hosts

Mit der Funktion „Power On“ des Citrix Hypervisor or-Servers können Sie einen Server remote ein- und ausschalten, entweder über XenCenter oder mithilfe der CLI.

Um die Hostleistung zu aktivieren, muss der Host über eine der folgenden Stromsteuerungslösungen verfügen:

- **Wake-on-LAN-fähige Netzwerkkarte**.
- **Dell Remote Access Cards (DRAC)**. Um Citrix Hypervisor mit DRAC verwenden zu können, müssen Sie das Dell Zusatzpaket installieren, um DRAC-Unterstützung zu erhalten. DRAC-Unterstützung erfordert die Installation des RACADM-Befehlszeilenprogramms auf dem Server mit dem RAS-Controller und die Aktivierung von DRAC und dessen Schnittstelle. RACADM ist

oft in der DRAC-Management-Software enthalten. Weitere Informationen finden Sie in der DRAC-Dokumentation von Dell.

- **Hewlett-Packard Integrated Lights-Out (iLO)**. Um Citrix Hypervisor mit iLO zu verwenden, müssen Sie iLO auf dem Host aktivieren und die Schnittstelle mit dem Netzwerk verbinden. Weitere Informationen finden Sie in der HP iLO-Dokumentation.
- Ein benutzerdefiniertes Skript, das auf der Verwaltungs-API basiert, mit dem Sie das Ein- und Ausschalten über Citrix Hypervisor ermöglicht. Weitere Informationen finden Sie unter *Konfigurieren eines benutzerdefinierten Skripts für die Host-Einschaltfunktion* im folgenden Abschnitt.

Für die Verwendung der Host-Einschaltfunktion 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, eine DRAC- oder iLO-Karte oder Sie haben ein benutzerdefiniertes Skript erstellt).
2. Aktivieren Sie die Host-Einschaltfunktion mithilfe der CLI oder XenCenter.

Verwenden der CLI zum Verwalten der Stromversorgung des Hosts

Sie können die Host-Einschaltfunktion entweder über die CLI oder XenCenter verwalten. Dieser Abschnitt enthält Informationen zum Verwalten der CLI.

Host Power On ist auf Hostebene (d. h. auf jedem Citrix Hypervisor) aktiviert.

Nachdem Sie Host Power On aktiviert haben, können Sie Hosts entweder mit der CLI oder XenCenter aktivieren.

So aktivieren Sie das Einschalten des Hosts mithilfe der CLI

Führen Sie den Befehl aus:

```
xe host-set-power-on-mode host=<host uuid> \
    power-on-mode=(”” , ”wake-on-lan”,  ”iLO”, ”DRAC”,”custom”) \
    power-on-config=key:value
```

Für iLO und DRAC`power_on_ip` müssen die Schlüssel das Kennwort angeben, wenn Sie die geheime Funktion verwenden. Weitere Informationen finden Sie unter Geheimnisse.

So aktivieren Sie Hosts mithilfe der CLI remote

Führen Sie den Befehl aus:

```
xe host-power-on host=<host uuid>
```


Konfigurieren eines benutzerdefinierten Skripts für die Host-Einschaltfunktion

Wenn die Remote-Power-Lösung Ihres Servers ein Protokoll verwendet, das standardmäßig nicht unterstützt wird (z. B. Wake-On-Ring- oder Intel Active Management-Technologie), können Sie ein benutzerdefiniertes Linux Python-Skript erstellen, um Ihre Citrix Hypervisor Computer remote einschalten zu können. Sie können jedoch auch benutzerdefinierte Skripte für iLO, DRAC und Wake-on-LAN-Fernversorgungslösungen erstellen.

Dieser Abschnitt enthält Informationen zum Konfigurieren eines benutzerdefinierten Skripts für Host Power On mithilfe der Schlüssel/Wert-Paare, die mit dem Citrix Hypervisor API-Aufruf verknüpft sind`host.power_on`.

Wenn Sie ein benutzerdefiniertes Skript erstellen, führen Sie es in der Befehlszeile jedes Mal aus, wenn Sie die Stromversorgung von Citrix Hypervisor remote steuern möchten. Alternativ können Sie es in XenCenter angeben und die XenCenter-UI-Features verwenden, um damit zu interagieren.

Die Citrix Hypervisor API ist in dem Dokument, der Citrix Hypervisor Verwaltungs-API, dokumentiert, dasEntwicklerdokumentationauf der Website verfügbar ist.

> **Warnhinweis:**
>
> Ändern Sie die standardmäßig im`/etc/xapi.d/plugins/` Verzeichnis bereitgestellten Skripte nicht. 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`host.power_on_mode` Schlüssel`host.power_on_config` und. Weitere Informationen zu den Werten finden Sie im folgenden Abschnitt.

Es gibt auch einen API-Aufruf, mit dem Sie diese Felder gleichzeitig festlegen können:

```
1 void host.set_host_power_on_mode(string mode, Dictionary<string,string>
      config)
```

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 Power-Control deaktiviert
  - „iLO“: Ermöglicht die Angabe von HP iLO.

  - „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 (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. Enthält zusätzliche Informationen für iLO und DRAC.
- **Mögliche Werte:**
  - Wenn Sie iLO oder DRAC als Remotestromlösung konfiguriert haben, müssen Sie auch einen der folgenden Schlüssel angeben:
    * „power_on_ip“: Die IP-Adresse, die Sie für die Kommunikation mit der Stromsteuerungskarte angegeben haben. Alternativ können Sie den Domänennamen für die Netzwerkschnittstelle eingeben, auf der iLO oder DRAC konfiguriert ist.
    * „power_on_user“: Der dem Verwaltungsprozessor zugeordnete iLO oder DRAC Benutzername, den Sie möglicherweise von den Werkseinstellungen geändert haben.
    * „power_on_password_secret“: Gibt die Verwendung der Secrets-Funktion zum Sichern Ihres Passworts an.
  - Um die Secrets-Funktion zum Speichern Ihres Passworts zu verwenden, geben Sie den Schlüssel „power_on_password_secret“ an. Weitere Informationen finden Sie unter Geheimnisse.
- **Typ**: Map (string, string)

Beispielskript

Das Beispielskript importiert die Citrix Hypervisor API, definiert sich selbst als benutzerdefiniertes Skript und übergibt dann Parameter, die für den Host spezifisch sind, den Sie remote steuern möchten. Sie müssen die Parameter`session` in allen benutzerdefinierten Skripten definieren.

Das Ergebnis wird angezeigt, wenn das Skript nicht erfolgreich ist.

```
1 import XenAPI
2 def custom(session,remote_host,
3 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
```

> **Hinweis:**
>
> Nachdem Sie das Skript erstellt haben, speichern Sie es in /etc/xapi.d/plugins mit der Erweiterung.py.

Kommunikation mit Citrix Hypervisor -Servern und Ressourcenpools

Citrix Hypervisor verwendet TLS-Protokolle zum Verschlüsseln des Management-API-Datenverkehrs. Jede Kommunikation zwischen Citrix Hypervisor und Verwaltungs-API-Clients (oder -Appliances) verwendet jetzt standardmäßig das TLS 1.2-Protokoll. Wenn der Verwaltungs-API-Client oder die Appliance jedoch nicht mit TLS 1.2 kommuniziert, können frühere Protokolle für die Kommunikation verwendet werden.

Citrix Hypervisor verwendet die folgenden Verschlüsselungssammlungen:

-TLS_RSA_WITH_AES_128_CBC_SHA256

-TLS_RSA_WITH_AES_256_CBC_SHA

-TLS_RSA_WITH_AES_128_CBC_SHA

-TLS_RSA_WITH_RC4_128_SHA

-TLS_RSA_WITH_RC4_128_MD5

-TLS_RSA_WITH_3DES_EDE_CBC_SHA

Mit Citrix Hypervisor können Sie auch Ihren Host oder Ressourcenpool so konfigurieren, dass die Kommunikation **nur über TLS 1.2**möglich ist. Diese Option ermöglicht die Kommunikation zwischen Citrix Hypervisor und Verwaltungs-API-Clients (oder -Appliances) mithilfe des TLS 1.2-Protokolls. Die Option nur TLS 1.2 verwendet Chiffre SuiteTLS_RSA_WITH_AES_128_CBC_SHA256.

> **Warnung:**
>
> Select die Option **Nur TLS 1.2**aus, nachdem Sie sichergestellt haben, dass alle Verwaltungs-API-Clients und -Appliances, die mit dem Citrix Hypervisor Pool kommunizieren, mit TLS 1.2 kompatibel sind.

Aktivieren von IGMP-Snooping auf Ihrem Citrix Hypervisor Pool

Citrix Hypervisor sendet Multicastdatenverkehr an alle Gast-VMs, was zu unnötiger Last auf Hostgeräten führt, indem sie von ihnen verlangt werden, Pakete zu verarbeiten, die sie nicht angefordert haben. Das Aktivieren von IGMP-Snooping verhindert, dass Hosts in einem lokalen Netzwerk Datenverkehr für eine Multicastgruppe empfangen, die sie nicht explizit beigetreten sind, und verbessert die Leistung von Multicast. IGMP-Snooping ist besonders nützlich für bandbreitenintensive IP-Multicastanwendungen wie IPTV.

Sie können IGMP-Snooping in einem Pool mithilfe von XenCenter oder der Befehlszeilenschnittstelle aktivieren. Um IGMP-Snooping mit XenCenter zu aktivieren, navigieren Sie zu **Pooleigenschaften** und wählen Sie **Netzwerkoptionen** aus. Weitere Informationen finden Sie in der XenCenter Hilfe. Hinweise zu xe-Befehlen finden Sie unterpool-igmp-schnüffeln.

> **Hinweise:**
>
> - IGMP-Snooping ist nur verfügbar, wenn das Netzwerk-Backend Open vSwitch verwendet.
> - Wenn Sie diese Funktion in einem Pool aktivieren, ist es möglicherweise auch notwendig, IGMP-Querier auf einem der physischen Switches zu aktivieren. Andernfalls wird Multicast im Unternetzwerk auf Broadcast zurückgreifen und die Leistung von Citrix Hypervisor verringern.
> - Wenn Sie diese Funktion in einem Pool aktivieren, auf dem IGMP v3 ausgeführt wird, führt VM-Migration oder Netzwerkanleihe-Failover dazu, dass IGMP-Version auf v2 umgeschaltet wird.
> - Um diese Funktion mit dem GRE-Netzwerk zu aktivieren, müssen Benutzer einen IGMP-Querier im GRE-Netzwerk einrichten. Alternativ können Sie die IGMP-Abfragenachricht aus dem physischen Netzwerk an das GRE-Netzwerk weiterleiten. Andernfalls kann Multicastdatenverkehr im GRE-Netzwerk blockiert werden.

Kopiert!
Failed!

Cluster-Pools

October 16, 2019

Clustering bietet zusätzliche Funktionen, die für Ressourcenpools erforderlich sind, die GFS2-SRs verwenden. Weitere Informationen zu GFS2 finden Sie unterKonfigurieren des Speichers.

Ein Cluster ist ein Pool von Citrix Hypervisor Hosts, die enger miteinander verbunden und koordiniert sind als nicht gruppierte Pools. Die Hosts im Cluster unterhalten eine konstante Kommunikation un-

tereinander 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 die Inhalte der GFS2 SR zu steuern.

Quorum

Jeder Host in einem Cluster muss immer mit mindestens der Hälfte der Hosts im Cluster kommunizieren (einschließlich selbst). Dieser Zustand wird als Host mit Quorum bezeichnet.

Der Quorumwert für einen Pool mit ungeraden Zahlen ist die Hälfte von eins plus die Gesamtzahl der Hosts im Cluster: (n+1) /2. Der Quorumwert für einen Pool mit geraden Zahlen entspricht der Hälfte der Gesamtzahl der Hosts im Cluster: n/2.

Bei einem Pool mit geraden Zahlen ist es möglich, dass der laufende Cluster genau in zwei Hälften aufgeteilt wird. Der laufende Cluster entscheidet, welche Hälfte der Cluster-Selbstzäune und welche Hälfte des Clusters Quorum hat. Wenn ein geclusterter Pool mit geraden Nummern von einem Kaltstart aktiviert wird, müssen (n/2) +1 Hosts verfügbar sein, bevor die Hosts Quorum haben. Nachdem die Hosts Quorum haben, wird der Cluster aktiv.

Wenn ein Host kein Quorum hat, setzt sich dieser Host selbst ein.

Selbstzäunung

Wenn ein Host erkennt, dass er kein Quorum hat, setzt er sich innerhalb weniger Sekunden selbst ein. Wenn ein Host sich selbst einzäunt, wird er sofort neu gestartet. Alle VMs, die auf dem Host ausgeführt werden, werden beendet, weil der Host ein hartes Herunterfahren durchführt. In einem Clusterpool mit hoher Verfügbarkeit startet Citrix Hypervisor die VMs entsprechend ihrer Neustartkonfiguration auf anderen Pool-Mitgliedern neu. Der Host, der selbst eingegrenzt wurde, wird neu gestartet und versucht, dem Cluster erneut beizutreten.

Wenn die Anzahl der Live-Hosts im Cluster kleiner als der Quorumwert wird, verlieren alle verbleibenden Hosts das Quorum.

In einem idealen Szenario verfügt Ihr Clusterpool immer über mehr Live-Hosts, als für Quorum erforderlich sind, und Citrix Hypervisor setzt sich nie ein. Um dieses Szenario wahrscheinlicher zu machen, sollten Sie beim Einrichten des Clusterpools die folgenden Empfehlungen beachten:

- Stellen Sie sicher, dass Sie über eine gute Hardware-Redundanz verfügen.
- Verwenden Sie ein dediziertes gebundenes Netzwerk für das Clusternetzwerk. Stellen Sie sicher, dass sich die gebundenen NICs auf demselben L2-Segment befinden. Weitere Informationen finden Sie unter Vernetzung.
- Konfigurieren Sie das Speicher-Multipathing zwischen dem Pool und dem GFS2 SR. Weitere Informationen finden Sie unter Massenspeicher-Multipathing.

- Konfigurieren Sie die hohe Verfügbarkeit im Clusterpool. In gruppierten Pools muss der Heartbeat SR ein GFS2 SR sein. Weitere Informationen finden Sie unter Hohe Verfügbarkeit.

Erstellen eines Cluster-Pools

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Alle Citrix Hypervisor or-Server im Clusterpool müssen über mindestens 2 GiB Steuerdomänenspeicher verfügen.
- Alle Hosts im Cluster müssen statische IP-Adressen für das Clusternetzwerk verwenden.
- Es wird empfohlen, Clustering nur in Pools zu verwenden, die mindestens drei Hosts enthalten, da Pools von zwei Hosts empfindlich darauf reagieren, den gesamten Pool selbst zu fechten.
- Wenn Sie über eine Firewall zwischen den Hosts in Ihrem Pool verfügen, stellen Sie sicher, dass Hosts über die folgenden Ports im Clusternetzwerk kommunizieren können:
  - TCP: 8892, 21064
  - UDP: 5404, 5405

  Weitere Informationen finden Sie unter Von Citrix Technologies verwendete Kommunikationsports.
- Wenn Sie einen vorhandenen Pool gruppieren, stellen Sie sicher, dass die hohe Verfügbarkeit deaktiviert ist. Sie können die Hochverfügbarkeit wieder aktivieren, nachdem das Clustering aktiviert ist.

Wenn Sie möchten, können Sie Clustering in Ihrem Pool mithilfe von XenCenter einrichten. Weitere Informationen finden Sie unter XenCenter Produktdokumentation.

So erstellen Sie einen gruppierten Pool mithilfe der xe-CLI:

1. Erstellen Sie ein gebundenes Netzwerk, das als Clusternetzwerk verwendet werden soll. Führen Sie auf dem Citrix Hypervisor or-Server, der der Poolmaster sein soll, die folgenden Schritte aus:
   a) Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.
   b) Benennen Sie Ihren Ressourcenpool mithilfe des folgenden Befehls:

   ```
   xe pool-param-set name-label="New Pool" uuid=<pool_uuid>
   ```

   c) Erstellen Sie mit dem folgenden Befehl ein Netzwerk zur Verwendung mit der gebundenen NIC:

   ```
   xe network-create name-label=bond0
   ```

   Die UUID des neuen Netzwerks wird zurückgegeben.

d) Suchen Sie die UUIDs der PIF, die in der Bindung verwendet werden sollen, indem Sie den folgenden Befehl verwenden:

```
xe pif-list
```

e) Erstellen Sie Ihr gebundene Netzwerk entweder im Aktiv-Aktiv-Modus, im Aktiv-Passiv-Modus oder im LACP-Bond-Modus. Je nach Anleihemodus, den Sie verwenden möchten, führen Sie eine der folgenden Aktionen aus:

- Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den `bond-create` Befehl, um die Bindung zu erstellen. Geben Sie mithilfe von Kommas die neu erstellte Netzwerk-UUID und die UUIDs der zu gebundenen PIFs an:

```
xe bond-create network-uuid=<network_uuid> /
     pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
        pif_uuid_4>
```

  Geben Sie zwei UUIDs ein, wenn Sie zwei Netzwerkkarten und vier UUIDs verkleben, wenn Sie vier Netzwerkkarten miteinander vereinen. Die UUID für die Bindung wird nach dem Ausführen des Befehls zurückgegeben.

- Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie die gleiche Syntax, fügen Sie den optionalen `mode` Parameter hinzu und geben Sie Folgendes `lacp` an `active-backup`:

```
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
```

Nachdem Sie das gebundene Netzwerk auf dem Poolmaster erstellt haben und andere Citrix Hypervisor or-Server mit dem Pool verbinden, werden die Netzwerk- und Bondinformationen automatisch auf den beitrittenden Server repliziert.

Weitere Informationen finden Sie unter Vernetzung.

2. Erstellen Sie einen Ressourcenpool mit mindestens drei Citrix Hypervisor or-Servern.

   Wiederholen Sie die folgenden Schritte auf jedem Citrix Hypervisor or-Server, der ein (nicht Master-) Pool-Mitglied ist:

   a) Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.

   b) Verbinden Sie den Citrix Hypervisor or-Server mit dem Pool auf dem Poolmaster mithilfe des folgenden Befehls:


```
xe pool-join master-address=master_address master-username=
    administrators_username master-password=password
```

Der Wert des`master-address` Parameters muss auf den vollqualifizierten Domänennamen des Citrix Hypervisor or-Servers festgelegt werden, der der Poolmaster ist. Das`password` muss das Administratorkennwort sein, das bei der Installation des Poolmasters festgelegt wurde.

Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

3. Legen Sie für jedes PIF fest, das zu diesem Netzwerk gehört`disallow-unplug=`**`true`**.

   a) Suchen Sie die UUIDs der PIFs, die zum Netzwerk gehören, mithilfe des folgenden Befehls:

   ```
   xe pif-list
   ```

   b) Führen Sie den folgenden Befehl auf einem Citrix Hypervisor or-Server im Ressourcenpool aus:

   ```
   xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
   ```

4. Aktivieren Sie Clustering in Ihrem Pool. Führen Sie den folgenden Befehl auf einem Citrix Hypervisor or-Server im Ressourcenpool aus:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   ```

   Geben Sie die UUID des gebundenen Netzwerks an, das Sie in einem früheren Schritt erstellt haben.

Verwalten Ihres Cluster-Pools

Bei der Verwaltung Ihres Cluster-Pools können die folgenden Praktiken das Risiko verringern, dass der Pool Quorum verliert.

Stellen Sie sicher, dass Hosts sauber heruntergefahren werden

Wenn ein Host sauber heruntergefahren wird, wird er vorübergehend aus dem Cluster entfernt, bis er erneut gestartet wird. Während der Host heruntergefahren wird, zählt er nicht zum Quorumwert des Clusters. Die Abwesenheit des Hosts führt nicht dazu, dass andere Hosts Quorum verlieren.

Wenn ein Host jedoch zwangsweise oder unerwartet heruntergefahren wird, wird er nicht aus dem Cluster entfernt, bevor er offline geschaltet wird. Dieser Host zählt auf den Quorumwert des Clusters. Das Herunterfahren kann dazu führen, dass andere Hosts Quorum verlieren.

Wartungsmodus verwenden

Bevor Sie auf einem Host etwas ausführen, das dazu führen könnte, dass dieser Host Quorum verliert, versetzen Sie den Host in den Wartungsmodus. Wenn sich ein Host im Wartungsmodus befindet, werden ausgeführte VMs auf einen anderen Host im Pool migriert. Wenn dieser Host der Poolmaster war, wird diese Rolle an einen anderen Host im Pool übergeben. Wenn Ihre Aktionen dazu führen, dass sich ein Host im Wartungsmodus selbst einstellt, verlieren Sie keine VMs oder verlieren die XenCenter Verbindung mit dem Pool.

Hosts im Wartungsmodus zählen weiterhin auf den Quorumwert für den Cluster.

Sie können die IP-Adresse eines Hosts, der Teil eines Clusterpools ist, nur ändern, wenn sich dieser Host im Wartungsmodus befindet. Wenn Sie die IP-Adresse eines Hosts ändern, verlässt der Host den Cluster. Wenn die IP-Adresse erfolgreich geändert wurde, tritt der Host erneut in den Cluster ein. Nachdem der Host wieder dem Cluster beitritt, können Sie ihn aus dem Wartungsmodus entfernen.

Wiederherstellen von Hosts, die selbst eingezäunt sind oder offline sind

Es ist wichtig, Hosts wiederherzustellen, die selbst eingezäunt sind. Während diese Clustermitglieder offline sind, zählen sie zur Quorumnummer für den Cluster und verringern die Anzahl der Clustermitglieder, die kontaktiert werden können. Diese Situation erhöht das Risiko eines nachfolgenden Hostfehlers, der dazu führt, dass der Cluster Quorum verliert und vollständig heruntergefahren wird.

Wenn Sie Offline-Hosts in Ihrem Cluster haben, können Sie auch bestimmte Aktionen nicht ausführen. In einem Clusterpool muss jedes Mitglied des Pools jeder Änderung der Poolmitgliedschaft zustimmen, bevor die Änderung erfolgreich sein kann. Wenn ein Clustermitglied nicht kontaktierbar ist, verhindert Citrix Hypervisor Vorgänge, die die Clustermitgliedschaft ändern (z. B.

Hosts als tot markieren

Wenn ein oder mehrere Offline-Hosts nicht wiederhergestellt werden können, können Sie sie als tot im Cluster markieren. Wenn Hosts als tot markiert werden, werden sie dauerhaft aus dem Cluster entfernt. Nachdem Hosts als tot markiert wurden, zählen sie nicht mehr auf den Quorumwert.

Einschränkungen

- Cluster-Pools unterstützen nur bis zu 16 Hosts pro Pool.
- Wenn ein Netzwerk sowohl für die Verwaltung als auch für die Clustererstellung verwendet wurde, können Sie das Verwaltungsnetzwerk nicht trennen, ohne den Cluster neu zu erstellen.
- Wenn Sie die IP-Adresse des Clusternetzwerks mithilfe von XenCenter ändern, müssen Clustering und GFS2 vorübergehend deaktiviert werden.

- Ändern Sie die Bindung Ihres Clusternetzwerks nicht, solange der Cluster live ist und VMs ausgeführt hat. Diese Aktion kann dazu führen, dass der Cluster einen Zaun aufweist.
- Wenn Sie einen IP-Adresskonflikt (mehrere Hosts mit derselben IP-Adresse) in Ihrem Clusternetzwerk haben, an dem mindestens ein Host mit aktiviertem Clustering beteiligt ist, werden die Hosts nicht gegrenzt. Um dieses Problem zu beheben, beheben Sie den IP-Adresskonflikt.

Kopiert!
Failed!

Benutzer verwalten

October 16, 2019

Durch das Definieren von Benutzern, Gruppen, Rollen und Berechtigungen können Sie steuern, wer Zugriff auf Ihre Citrix Hypervisor or-Server und -Pools hat und welche Aktionen sie ausführen können.

Wenn Sie Citrix Hypervisor zum ersten Mal installieren, wird Citrix Hypervisor automatisch ein Benutzerkonto hinzugefügt. Dieses Konto ist der lokale Superbenutzer (LSU) oder root, den Citrix Hypervisor lokal authentifiziert.

Die LSU oder root ist ein spezielles Benutzerkonto für die Systemverwaltung und verfügt über alle Berechtigungen. In Citrix Hypervisor ist die LSU das Standardkonto bei der Installation. Citrix Hypervisor authentifiziert das LSU-Konto. LSU erfordert keinen externen Authentifizierungsdienst. Wenn ein externer Authentifizierungsdienst fehlschlägt, kann sich die LSU weiterhin anmelden und das System verwalten. Die LSU kann jederzeit über SSH auf den physischen Server von Citrix Hypervisor zugreifen.

Sie können mehr Benutzer erstellen, indem Sie die Active Directory Konten entweder über die XenCenter-Registerkarte Benutzer oder die xe-CLI hinzufügen. Wenn Ihre Umgebung Active Directory nicht verwendet, sind Sie auf das LSU-Konto beschränkt.

> **Hinweis:**
>
> Wenn Sie Benutzer erstellen, weist Citrix Hypervisor neu erstellte Benutzerkonten RBAC-Rollen nicht automatisch zu. Daher haben diese Konten keinen Zugriff auf den Citrix Hypervisor Pool, bis Sie ihnen eine Rolle zuweisen.

Diese Berechtigungen werden über Rollen erteilt, wie im Abschnitt *Authentifizieren von Benutzern mit Active Directory (AD)* beschrieben.

Authentifizieren von Benutzern mit Active Directory (AD)

Wenn Sie mehrere Benutzerkonten auf einem Server oder Pool haben möchten, müssen Sie Active Directory Benutzerkonten für die Authentifizierung verwenden. AD-Konten ermöglichen es Citrix

Hypervisor Benutzern, sich mit ihren Windows Domänenanmeldeinformationen an einem Pool anzumelden.

Sie können unterschiedliche 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`-u` Argumente`-pw` und Argumente übergeben) und über XenCenter auch eine Verbindung mit dem Host herstellen. Die Authentifizierung erfolgt auf Ressourcenpoolbasis.

Subjekte steuern den Zugriff auf Benutzerkonten. Ein Betreff in Citrix Hypervisor wird einer Entität auf dem Verzeichnisserver (entweder einem Benutzer oder einer Gruppe) zugeordnet. Wenn Sie die externe Authentifizierung aktivieren, überprüft Citrix Hypervisor die zum Erstellen einer Sitzung verwendeten Anmeldeinformationen mit den lokalen Stammanmeldeinformationen (falls der Verzeichnisserver nicht verfügbar ist) und dann mit der Betreffliste. Um den Zugriff zu erlauben, erstellen Sie einen Betreffeintrag für die Person oder Gruppe, auf 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 Citrix Hypervisor CLI etwas andere Terminologie verwendet, um auf Active Directory - und Benutzerkontofunktionen zu verweisen: XenCenter Term Citrix Hypervisor CLI-Term-Benutzer Subjekte hinzufügen

Obwohl Citrix Hypervisor Linux-basiert, können Sie mit Citrix Hypervisor Active Directory Konten für Citrix Hypervisor-Benutzerkonten verwenden. Dazu werden Active Directory tory-Anmeldeinformationen an den Active Directory-Domänencontroller übergeben.

Wenn Sie Active Directory zu Citrix Hypervisor hinzufügen, werden Active Directory Benutzer und -Gruppen zu Citrix Hypervisor Themen. Die Themen werden in XenCenter als Benutzer bezeichnet. Benutzer/Gruppen werden bei der Anmeldung mithilfe von Active Directory authentifiziert, wenn Sie einen Betreff bei Citrix Hypervisor registrieren. Benutzer und Gruppen müssen ihren Benutzernamen nicht mithilfe eines Domänennamens qualifizieren.

Um einen Benutzernamen zu qualifizieren, müssen Sie den Benutzernamen im Format Anmeldename unten eingeben,`mydomain\myuser`z. B.

> **Hinweis:**
>
> Wenn Sie den Benutzernamen nicht qualifiziert haben, versucht XenCenter standardmäßig, Benutzer bei AD-Authentifizierungsservern mit der Domäne anzumelden, der er angehört. Die Ausnahme hiervon ist das LSU-Konto, das XenCenter immer lokal authentifiziert (d. h. auf dem Citrix Hypervisor).

Der externe Authentifizierungsprozess funktioniert wie folgt:

1. Die beim Herstellen einer Verbindung mit einem Server angegebenen Anmeldeinformationen werden zur Authentifizierung an den Active Directory Domänencontroller übergeben.

2. Der Domänencontroller überprüft 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 Betreffkennung und die Gruppenmitgliedschaft zu erhalten, die den Anmeldeinformationen zugeordnet sind.
4. Wenn die Antragsteller-ID mit der im Citrix Hypervisor gespeicherten ID 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, mit der er Vertrauensstellungen aufweist) eine Verbindung mit dem 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.

Konfigurieren der Active Directory Authentifizierung

Citrix Hypervisor unterstützt die Verwendung von Active Directory -Servern unter Windows 2008 oder höher.

Um Active Directory für Citrix Hypervisor or-Server zu authentifizieren, müssen Sie denselben DNS-Server sowohl für den Active Directory -Server (für die Interoperabilität konfiguriert) als auch für den Citrix Hypervisor or-Server verwenden.
In einigen Konfigurationen kann der Active Directory Server das DNS selbst bereitstellen. Dies kann entweder mit DHCP zur Bereitstellung der IP-Adresse und einer Liste der DNS-Server für den Citrix Hypervisor or-Server erreicht werden. Alternativ können Sie die Werte in den PIF-Objekten festlegen oder das Installationsprogramm verwenden, wenn eine manuelle statische Konfiguration verwendet wird.

Es wird empfohlen, DHCP zum Zuweisen von Hostnamen zu aktivieren. Weisen Sie die Hostnamen`localhost` oder Hosts nicht`linux` zu.

> **Warnhinweis:**
>
> Citrix Hypervisor or-Servernamen müssen in der Citrix Hypervisor Bereitstellung eindeutig sein.

Beachten Sie Folgendes:

- Citrix Hypervisor beschriftet seinen AD-Eintrag in der AD-Datenbank unter Verwendung seines Hostnamens. Wenn zwei Citrix Hypervisor-Server mit demselben Hostnamen derselben AD-Domäne verbunden sind, überschreibt der zweite Citrix Hypervisor den AD-Eintrag des ersten

Citrix Hypervisors. 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 Citrix Hypervisor nicht mehr funktioniert.

Sie können denselben Hostnamen in zwei Citrix Hypervisor or-Servern verwenden, solange sie verschiedenen AD-Domänen beitreten.

- Die Citrix Hypervisor or-Server können sich in verschiedenen Zeitzonen befinden, da es sich um die UTC-Zeit handelt, die verglichen wird. Um sicherzustellen, dass die Synchronisierung korrekt ist, können Sie dieselben NTP-Server für Ihren Citrix Hypervisor Pool und den Active Directory -Server verwenden.
- Mischauthentifizierungspools werden nicht unterstützt. Sie können keinen Pool haben, in dem einige Server im Pool für die Verwendung von Active Directory konfiguriert sind und andere nicht).
- Die Citrix Hypervisor Active Directory Integration verwendet das Kerberos-Protokoll, um mit den Active Directory -Servern zu kommunizieren. Daher unterstützt Citrix Hypervisor nicht die Kommunikation mit Active Directory -Servern, die Kerberos nicht verwenden.
- Damit die externe Authentifizierung mit Active Directory erfolgreich ist, müssen die Uhren auf den Citrix Hypervisor or-Servern mit den Uhren auf dem Active Directory -Server synchronisiert werden. Wenn Citrix Hypervisor der Active Directory Domäne beitritt, wird die Synchronisierung überprüft, und die Authentifizierung schlägt fehl, wenn zwischen den Servern zu stark verzerrt ist.

> **Warnhinweis:**
>
> Hostnamen dürfen ausschließlich aus nicht mehr als 63 alphanumerischen Zeichen bestehen und dürfen nicht rein numerisch sein.

Wenn Sie einen Server zu einem Pool hinzufügen, nachdem Sie die Active Directory Authentifizierung aktiviert haben, werden Sie aufgefordert, Active Directory auf dem Server zu konfigurieren, der dem Pool beitritt. Wenn Sie auf dem beitrittenden Server zur Eingabe von Anmeldeinformationen aufgefordert werden, geben Sie Active Directory Anmeldeinformationen mit ausreichenden Berechtigungen ein, um dieser Domäne Server hinzuzufügen.

Integration von Active Directory

Stellen Sie sicher, dass die folgenden Firewallports für ausgehenden Datenverkehr geöffnet sind, damit Citrix Hypervisor auf die Domänencontroller zugreifen kann.

Hafen	Protokoll	Verwenden
53	UDP/TCP	DNS

Hafen	Protokoll	Verwenden
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	Änderungen des Maschinenkennworts
3268	TCP	Globale Katalogsuche

> **Hinweise:**
>
> - Führen Sie den folgenden Befehl aus, um die Firewallregeln auf einem Linux-Computer mithilfe von *iptables*anzuzeigen:`iptables -nL`.
> - Citrix Hypervisor verwendet PowerBroker Identity Services (PBIS), um den AD-Benutzer auf dem AD-Server zu authentifizieren und die Kommunikation mit dem AD-Server zu verschlüsseln.

Wie verwaltet Citrix Hypervisor das Computerkontokennwort für die AD-Integration?

Ähnlich wie bei Windows Clientcomputern aktualisiert PBIS das Kennwort des Computerkontos automatisch. PBIS erneuert das Kennwort alle 30 Tage oder gemäß der Kennworterneuerungsrichtlinie des Computerkontos auf dem AD-Server.

Aktivieren der externen Authentifizierung für einen Pool

Die externe Authentifizierung mit Active Directory kann 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
```

Der angegebene Benutzer muss über`Add/remove computer objects or workstations` Berechtigungen verfügen. Dies ist der Standardwert für Domänenadministratoren.

Wenn Sie DHCP nicht in dem Netzwerk verwenden, das von Active Directory und Ihren Citrix Hypervisor or-Servern verwendet wird, verwenden Sie die folgenden Ansätze, um Ihren DNS einzurichten:

1. Richten Sie Ihre DNS-Suffix-Suchreihenfolge für das Auflösen von Nicht-FQDN-Einträgen ein:

```
xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \
   "other-config:domain=suffix1.com suffix2.com suffix3.com"
```

2. Konfigurieren Sie den DNS-Server für die Verwendung auf Ihren Citrix Hypervisor or-Servern:

```
xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \
  gateway=gateway netmask=netmask uuid=uuid
```

3. Legen Sie die Verwaltungsschnittstelle manuell so fest, dass eine PIF im selben Netzwerk wie Ihr DNS-Server verwendet wird:

```
xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
```

> **Hinweis:**
>
> Die externe Authentifizierung ist eine Eigenschaft pro Host. Es wird jedoch empfohlen, die externe Authentifizierung pro Pool zu aktivieren und zu deaktivieren. Mit einer Pool-Einstellung kann Citrix Hypervisor Fehler beheben, die beim Aktivieren der Authentifizierung auf einem bestimmten Host auftreten. Citrix Hypervisor rollt auch alle erforderlichen Änderungen zurück, um eine konsistente Konfiguration im gesamten Pool sicherzustellen. Verwenden Sie den`host-param-list` Befehl, um Eigenschaften eines Hosts zu überprüfen und den Status der externen Authentifizierung zu bestimmen, indem Sie die Werte der relevanten Felder überprüfen.

Verwenden Sie XenCenter, um die Active Directory Authentifizierung zu deaktivieren, oder den folgenden xe-Befehl:

```
xe pool-disable-external-auth
```

Benutzerauthentifizierung

Um einem Benutzer den Zugriff auf den Citrix Hypervisor or-Server zu ermöglichen, müssen Sie einen Betreff für diesen Benutzer oder eine Gruppe hinzufügen, in der er sich befindet. (Transitive Gruppenmitgliedschaften werden ebenfalls normal geprüft. `Beispiel: Hinzufügen eines Betreffs für GruppeA, wobei Gruppe Gruppe GruppeAenthältBund Mitglied der Gruppeuser 1ist Bwürde den Zugang zu ermöglichenuser 1.)` Wenn Sie Benutzerberechtigungen in Active Directory verwalten möchten, können Sie eine einzelne Gruppe erstellen, die Sie dann Benutzer zu/aus hinzufügen und löschen. Alternativ können Sie einzelne Benutzer aus

Citrix Hypervisor oder eine Kombination von Benutzern und Gruppen entsprechend Ihren Authentifizierungsanforderungen 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 zuerst mit dem lokalen Stammkonto überprüft, sodass Sie ein System wiederherstellen können, dessen AD-Server ausfallen. Wenn die Anmeldeinformationen (Benutzername und Kennwort) nicht übereinstimmen, wird eine Authentifizierungsanforderung an den AD-Server gestellt. Wenn die Authentifizierung erfolgreich ist, werden die Informationen des Benutzers abgerufen und anhand der lokalen Betreffliste validiert. Der Zugriff wird verweigert, wenn die Authentifizierung fehlschlägt. Die Überprüfung gegen die Betreffliste ist erfolgreich, wenn sich der Benutzer oder eine Gruppe in der transitiven Gruppenmitgliedschaft des Benutzers in der Betreffliste befindet.

> **Hinweis:**
>
> Wenn Sie Active Directory Gruppen verwenden, um den Zugriff für Pooladministratorbenutzer zu gewähren, die Host-SSH-Zugriff benötigen, darf die Anzahl der Benutzer in der Active Directory-Gruppe 500 nicht überschreiten.

So fügen Sie Citrix Hypervisor einen AD-Betreff hinzu:

```
xe subject-add subject-name=entity_name
```

Der entity_name ist der Name des Benutzers oder der Gruppe, dem Sie Zugriff gewähren möchten. Sie können die Domäne der Entität einschließen (z. B. ‘xendtuser1’ im Gegensatz zu ‘user1’), obwohl das Verhalten dasselbe ist, es sei denn, eine Begriffsklärung ist erforderlich.

Suchen Sie die Betreffkennung des Benutzers. Der Bezeichner ist der Benutzer oder die Gruppe, die den Benutzer enthält. Wenn Sie eine Gruppe entfernen, wird der Zugriff auf alle Benutzer in dieser Gruppe entfernt, sofern sie nicht auch in der Betreffliste angegeben sind. Verwenden Sie den`subject list` Befehl, um die Betreffkennung des Benutzers zu finden. :

```
xe subject-list
```

Dieser Befehl gibt eine Liste aller Benutzer zurück.

Verwenden Sie den folgenden Befehl, um einen Filter auf die Liste anzuwenden, z. B. um den Betreff-Bezeichner für einen Benutzer`user1` in der`testad` Domäne zu finden:

```
xe subject-list other-config:subject-name='testad\user1'
```

Entfernen Sie den Benutzer mit dem`subject-remove` Befehl und übergeben Sie die Betreff-ID, die Sie im vorherigen Schritt gelernt haben:

```
xe subject-remove subject-uuid=subject_uuid
```


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 Sitzungen nicht beenden, können Benutzer mit widerrufen Berechtigungen weiterhin auf das System zugreifen, bis sie sich abmelden.

Führen Sie den folgenden Befehl aus, um die Liste der Benutzer und Gruppen mit der Berechtigung für den Zugriff auf den Citrix Hypervisor-Server oder -Pool zu identifizieren:

```
1 xe subject-list
```

Zugriff für einen Benutzer entfernen

Wenn ein Benutzer authentifiziert wird, kann er auf den Server zugreifen, bis er seine Sitzung beendet oder ein anderer Benutzer seine Sitzung beendet. Wenn Sie einen Benutzer aus der Betreffliste entfernen oder aus einer Gruppe entfernen, die sich in der Betreffliste befindet, werden bereits authentifizierte Sitzungen des Benutzers nicht automatisch widerrufen. Benutzer können weiterhin mit XenCenter oder anderen API-Sitzungen, die sie bereits erstellt haben, auf den Pool zugreifen. XenCenter und die Befehlszeilenschnittstelle bieten Möglichkeiten, einzelne Sitzungen oder alle aktiven Sitzungen zwangsweise zu beenden. In der XenCenter Hilfe finden Sie Informationen zu Prozeduren, die XenCenter verwenden, oder im folgenden Abschnitt finden Sie Informationen zu Prozeduren, die die CLI verwenden.

Beenden Sie alle authentifizierten Sitzungen mit xe

Führen Sie den folgenden CLI-Befehl aus, um alle authentifizierten Sitzungen mit xe zu beenden:

```
1 xe session-subject-identifier-logout-all
```

Beenden einzelner Benutzersitzungen mit xe

1. Bestimmen Sie die Betreffkennung, deren Sitzung Sie abmelden möchten. Verwenden Sie entweder die Befehle`session-subject-identifier-list` oder`subject-list` xe, um den Betreff-Bezeichner 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`. Möglicherweise benötigen Sie einen doppelten umgekehrten Schrägstrich, wie in Abhängigkeit von Ihrer Shell gezeigt).
2. Verwenden Sie den`session-subject-logout` Befehl, indem Sie die im vorherigen Schritt ermittelte Betreff-ID als Parameter übergeben, zum Beispiel:


```
xe session-subject-identifier-logout subject-identifier=subject_id
```

Hinterlassen einer AD-Domäne

> **Warnhinweis:**
>
> Wenn Sie die Domäne verlassen (d. h. die Active Directory Authentifizierung deaktivieren und einen Pool oder einen Server von seiner Domäne trennen), werden alle Benutzer, die sich am Pool oder Server mit Active Directory-Anmeldeinformationen authentifiziert haben, getrennt.

Verwenden Sie XenCenter, um eine AD-Domäne zu verlassen. Weitere Informationen finden Sie in der XenCenter Hilfe. Führen Sie den`pool-disable-external-auth` Befehl alternativ aus und geben Sie ggf. den Pool uuid an.

> **Hinweis:**
>
> Wenn Sie die Domäne verlassen, werden die Hostobjekte nicht aus der AD-Datenbank gelöscht. Informationen zum Löschen von deaktivierten Hosteinträgen finden Sie unterMicrosoft Support-Artikel.

Kopiert!
Failed!

Rollenbasierte Zugriffssteuerung

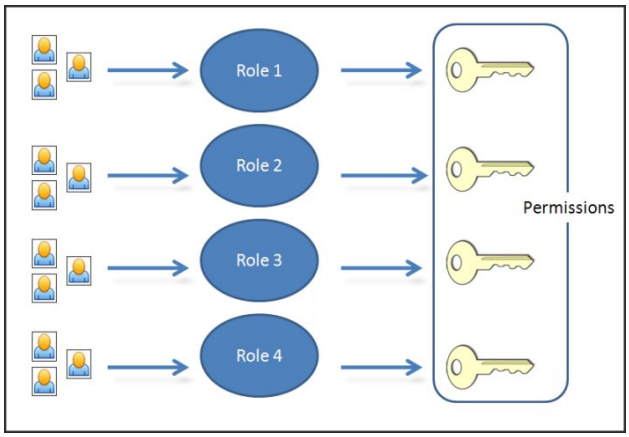
October 16, 2019

Mit der Funktion Role Based Access Control (RBAC) in Citrix Hypervisor können Sie Benutzern, Rollen und Berechtigungen zuweisen, um zu steuern, wer Zugriff auf Ihren Citrix Hypervisor hat und welche Aktionen sie ausführen können. Das Citrix Hypervisor RBAC-System ordnet einen Benutzer (oder eine Gruppe von Benutzern) definierten Rollen (einem benannten Satz von Berechtigungen) zu. Die Rollen verfügen über Citrix Hypervisor Berechtigungen zum Ausführen bestimmter Vorgänge.

Berechtigungen werden Benutzern nicht direkt zugewiesen. Benutzer erwerben Berechtigungen über ihnen zugewiesene Rollen. Daher wird das Verwalten einzelner Benutzerberechtigungen eine Frage der Zuweisung des Benutzers zu der entsprechenden Rolle, was allgemeine Vorgänge vereinfacht. Citrix Hypervisor verwaltet eine Liste der autorisierten Benutzer und deren Rollen.

Mit RBAC können Sie einschränken, welche Operationen verschiedene Benutzergruppen ausführen können, wodurch die Wahrscheinlichkeit eines Unfalls durch einen unerfahrenen Benutzer reduziert wird.

RBAC bietet auch eine Überwachungsprotokollfunktion für Compliance und Auditing.



RBAC hängt von Active Directory für Authentifizierungsdienste ab. Insbesondere enthält Citrix Hypervisor eine Liste der autorisierten Benutzer, die auf Active Directory Benutzer- und Gruppenkonten basieren. Daher müssen Sie dem Pool der Domäne beitreten und Active Directory Konten hinzufügen, bevor Sie Rollen zuweisen können.

Der lokale Superbenutzer (LSU) oder root ist ein spezielles Benutzerkonto, das für die Systemverwaltung verwendet wird und über alle Rechte oder Berechtigungen verfügt. Der lokale Superbenutzer ist das Standardkonto bei der Installation in Citrix Hypervisor. Die LSU wird über Citrix Hypervisor und nicht über einen externen Authentifizierungsdienst authentifiziert. Wenn der externe Authentifizierungsdienst fehlschlägt, kann sich die LSU weiterhin anmelden und das System verwalten. Die LSU kann jederzeit über SSH auf den physischen Citrix Hypervisor Host zugreifen.

RBAC-Prozess

Im folgenden Abschnitt wird der Standardprozess für die Implementierung von RBAC und das Zuweisen eines Benutzers oder einer Gruppe einer Rolle beschrieben:

1. Treten Sie der Domäne bei. Weitere Informationen finden Sie unter Aktivieren der externen Authentifizierung in einem Pool.
2. Fügen Sie dem Pool einen Active Directory Benutzer oder eine Active Directory-Gruppe hinzu. Dies wird zu einem Subjekt. Weitere Informationen finden Sie unter So fügen Sie einen Betreff zu RBAC hinzu.
3. Weisen Sie die RBAC-Rolle des Betreffs zu (oder ändern). Weitere Informationen finden Sie unter So weisen Sie einem Betreff eine RBAC-Rolle zu.

Kopiert!
Failed!

RBAC-Rollen und Berechtigungen

October 16, 2019

Rollen

Citrix Hypervisor wird mit den folgenden sechs vordefinierten Rollen ausgeliefert:

- *Pool-Administrator* (Pool-Admin) — identisch mit dem lokalen Stammverzeichnis. Kann alle Operationen ausführen.

  > **Hinweis:**
  >
  > Der lokale Superbenutzer (root) hat die Rolle „Pool Admin“. Die Pool-Admin-Rolle hat dieselben Berechtigungen wie der lokale Stamm.

- *Pool Operator* (Pool Operator) — kann alles außer dem Hinzufügen/Entfernen von Benutzern und Ändern ihrer Rollen ausführen. Diese Rolle konzentriert sich hauptsächlich auf das Host- und Pool-Management (d. h. das Erstellen von Speicher, Erstellen von Pools, 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 für die Verwendung durch einen VM-Betreiber.
- *Virtual Machine Administrator* (VM Admin) — ähnlich wie ein VM Power Admin, kann jedoch keine VMs migrieren oder Snapshots ausführen.
- *Virtual Machine Operator* (VM-Operator) — ähnlich wie VM-Admin, aber keine VMs erstellen/zerstören — kann jedoch Start-/Stopp-Lebenszyklusvorgänge durchführen.
- *Schreibgeschützt (schreibgeschützt*) — kann Ressourcenpool und Performance-Daten anzeigen.

> **Warnung:**
>
> Wenn Sie Active Directory Gruppen verwenden, um den Zugriff für Pooladministratorbenutzer zu gewähren, die Host-SSH-Zugriff benötigen, darf die Anzahl der Benutzer in der Active Directory-Gruppe 500 nicht überschreiten.

Eine Zusammenfassung der für die einzelnen Rollen verfügbaren Berechtigungen sowie Informationen zu den für die einzelnen Berechtigungen verfügbaren Vorgängen finden Sie unter *Definitionen von RBAC-Rollen und -Berechtigungen* im folgenden Abschnitt.

Wenn Sie einen Benutzer in Citrix Hypervisor erstellen, müssen Sie zunächst dem neu erstellten Benutzer eine Rolle zuweisen, bevor er das Konto verwenden kann. Citrix Hypervisor **weist dem neu**

erstellten Benutzer nicht automatisch eine Rolle zu. Daher haben diese Konten keinen Zugriff auf den Citrix Hypervisor Pool, bis Sie ihnen eine Rolle zuweisen.

1. Ändern Sie den Betreff der Rollenzuordnung. Dies erfordert die Berechtigung zum Zuweisen/Ändern der Rolle, die nur für einen Pooladministrator verfügbar ist.
2. Ändern Sie die Gruppenmitgliedschaft des Benutzers in Active Directory.

Definitionen von RBAC-Rollen und Berechtigungen

Die folgende Tabelle fasst zusammen, welche Berechtigungen für die einzelnen Rollen verfügbar sind. Weitere Informationen zu den für die einzelnen Berechtigungen verfügbaren Vorgängen finden Sie unter *Definitionen von Berechtigungen*.

Rollenberechtigung	Pool Admin	Poolbetreiber	VM Power Admin	VM-Administrator	VM-Betreiber	Schreibgeschützt
Rollen zuweisen/ändern	X					
Anmelden bei (physischen) Serverkonsolen (über SSH und XenCenter)	X					
Serversicheru wiederherste	X					
Import/Export von PARTIALURLPLACEHOLDER Paketen und Disk-Images	X					
Kerne pro Sockel einstellen	X	X	X	X		

Rollenberechtigung	Pool-Admin	Poolbetreiber	VM Power Admin	VM-Administrator	VM-Betreiber	Schreibgeschützt
Konvertieren virtueller Maschinen mit Citrix Hypervisor Conversion Manager	X					
Switch-Port-Verriegelung	X	X				
Multipathing	X	X				
Aktive Benutzerverbindungen abmelden	X	X				
Erstellen und Beenden von Warnungen	X	X				
Aufgabe eines Benutzers abbrechen	X	X				
Poolmanagement	X	X				
Live-Migration	X	X	X			
Live-Migration von Massenspeicher	X	X	X			
Erweiterte VM-Vorgänge	X	X	X			

Rollenberechtigung	Pool Admin	Poolbetreiber	VM Power Admin	VM-Administrator	VM-Betreiber	Schreibgeschützt
VM Erstellen/Löschen von Vorgängen	X	X	X	X		
VM ändern CD-Medien	X	X	X	X	X	
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
Audit-Protokolle lesen	X	X	X	X	X	X
Verbindung mit Pool herstellen und alle Pool-Metadaten lesen	X	X	X	X	X	X
Konfigurieren der virtuellen GPU	X	X				

Rollenberechtigungen	Pool-Admin	Poolbetreiber	VM Power Admin	VM-Administrator	VM-Betreiber	Schreibgeschützt
Virtuelle GPU-Konfiguration anzeigen	X	X	X	X	X	X
Zugriff auf das Konfigurationslaufwerk (nur CoreOS-VMs)	X					
Containerma	X					
Geplante Snapshots (VMs zu vorhandenen Snapshot-Zeitplänen hinzufügen/entfernen)	X	X	X			
Geplante Snapshots (Snapshot-Zeitpläne hinzufügen/ändern/löschen	X	X				
Integritätsprüfung konfigurieren	X	X				

Rollenberechtigung	Pool Admin	Poolbetreiber	VM Power Admin	VM-Administrator	VM-Betreiber	Schreibgeschützt
Ergebnisse und Einstellungen für die Integritätsprüfung anzeigen	X	X	X	X	X	X
Ändern der Blockverfolgung konfigurieren	X	X	X	X		
Geänderte Blöcke auflisten	X	X	X	X	X	
PVS-Beschleuniger konfigurieren	X	X				
PVS-Beschleunige anzeigen	X	X	X	X	X	X

Definitionen von Berechtigungen

Rollen zuweisen/ändern:

- Benutzer hinzufügen/entfernen
- Rollen von Benutzern hinzufügen/entfernen
- Aktivieren und Deaktivieren der Active Directory Integration (Mitglied der Domäne)

Diese Berechtigung ermöglicht es dem Benutzer, sich selbst eine Berechtigung zu erteilen oder eine Aufgabe auszuführen.

Warnung: Mit dieser Rolle kann der Benutzer die Active Directory Integration und alle Themen deaktivieren, die aus Active Directory hinzugefügt wurden.

Melden Sie sich bei Serverkonsolen an:

- Zugriff auf die Serverkonsole über ssh
- Zugriff auf die Serverkonsole über XenCenter

Warnung: Mit Zugriff auf eine Root-Shell kann der Beauftragte das gesamte System, einschließlich RBAC, beliebig neu konfigurieren.

Serversicherung/-wiederherstellung von virtuellen Rechnern erstellen/zerstören Vorgänge:

- Sichern und Wiederherstellen von Servern
- Sichern und Wiederherstellen von Pool-Metadaten

Die Möglichkeit, eine Sicherung wiederherzustellen, ermöglicht es dem Beauftragten, RBAC-Konfigurationsänderungen wiederherzustellen.

Importieren/Exportieren von OVF/OVA-Paketen und Disk-Images:

- Importieren von OVF- und OVA-Paketen
- Importieren von Disk-Images
- Exportieren von VMs als OVF/OVA-Pakete

Kerne pro Sockel einstellen:

- Festlegen der Anzahl der Kerne pro Socket für die virtuellen CPUs der VM

Diese Berechtigung ermöglicht es dem Benutzer, die Topologie für die virtuellen CPUs der virtuellen Maschine anzugeben.

Konvertieren von VMs mit Citrix Hypervisor Conversion Manager:

- Konvertieren von VMware VMs in Citrix Hypervisor VMs

Diese Berechtigung ermöglicht es dem Benutzer, Arbeitslasten von VMware in Citrix Hypervisor zu konvertieren, indem Stapel von VMware VMs in die Citrix Hypervisor-Umgebung kopiert werden.

Switch-Port-Verriegelung:

- Steuern des Datenverkehrs 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
- Multipathing deaktivieren

Aktive Benutzerverbindungen abmelden:

- Möglichkeit, angemeldete Benutzer zu trennen

Warnungen erstellen/verwerfen:

- Konfigurieren von XenCenter zum Generieren von Warnungen, wenn die Ressourcennutzung bestimmte Schwellenwerte überschreitet
- Entfernen von Warnungen aus der Warnungsansicht

Warnung: Ein Benutzer mit dieser Berechtigung kann Warnungen für den gesamten Pool schließen.

Hinweis: Die Möglichkeit zum Anzeigen von Warnungen ist Teil der Berechtigung zum Verbinden mit Pool und zum Lesen aller Pool-Metadaten.

Aufgabe eines beliebigen Benutzers abbrechen:

- Abbrechen der ausgeführten Aufgabe eines Benutzers

Mit dieser Berechtigung kann der Benutzer anfordern, dass Citrix Hypervisor eine laufende Aufgabe abbricht, die von einem Benutzer initiiert wurde.

Poolmanagement:

- Pool-Eigenschaften festlegen (Benennung, Standard-SRs)
- Erstellen eines Cluster-Pools
- Aktivieren, Deaktivieren und Konfigurieren von Hochverfügbarkeit
- Festlegen von Hochverfügbarkeits-Neustartprioritäten pro VM
- Konfigurieren der DR und Ausführen von DR-Failover-, Failback- und Test-Failovervorgängen
- Aktivieren, Deaktivieren und Konfigurieren von Workload Balancing (WLB)
- Hinzufügen und Entfernen des Servers aus dem Pool
- Notübergang zum Master
- Notfall-Hauptadresse
- Notfallwiederherstellung Slaves
- Neuen Master festlegen
- Verwalten von Pool- und Serverzertifikaten
- Patchen
- Servereigenschaften festlegen
- Konfigurieren der Serverprotokollierung
- Aktivieren und Deaktivieren von Servern
- Herunterfahren, Neustart und Einschalten von Servern
- Toolstack neu starten
- Systemstatusberichte
- Lizenz anwenden
- Live-Migration aller anderen VMs auf einem Server auf einen anderen Server aufgrund des Wartungsmodus oder hoher Verfügbarkeit
- Konfigurieren der Serververwaltungsschnittstelle und sekundären Schnittstellen
- Deaktivieren der Serververwaltung
- Crashdumps löschen
- Hinzufügen, Bearbeiten und Entfernen von Netzwerken

- Hinzufügen, Bearbeiten und Entfernen von PBDs/PIFs/VLANs/Bonds/SRs
- Hinzufügen, Entfernen und Abrufen von Geheimnissen

Diese Berechtigung enthält alle Aktionen, die zum Verwalten eines Pools erforderlich sind.

Hinweis: Wenn die Management-Schnittstelle nicht funktioniert, können sich keine Anmeldungen mit Ausnahme lokaler Root-Logins authentifizieren.

Live-Migration:

- Migrieren von VMs von einem Host auf einen anderen Host, wenn sich die VMs auf einem von beiden Hosts gemeinsam genutzten Speicher befinden

Massenspeicher-Live-Migration:

- Migrieren von einem Host auf einen anderen Host, wenn sich die VMs nicht im Speicher befinden, der zwischen den beiden Hosts gemeinsam genutzt wird
- Verschieben von Virtual Disk (VDIs) von einem SR in einen anderen SR

Erweiterte VM-Vorgänge:

- Anpassen des VM-Speichers (über Dynamic Memory Control)
- Erstellen eines VM-Snapshots mit Arbeitsspeicher, Erstellen von VM-Snapshots und Rollback von VMs
- Migrieren von VMs
- Starten von VMs, einschließlich Angabe des physischen Servers
- VMs fortsetzen

Diese Berechtigung bietet dem Beauftragten genügend Berechtigungen zum Starten einer virtuellen Maschine auf einem anderen Server, wenn er mit dem ausgewählten Citrix Hypervisor nicht zufrieden ist.

VM Erstellen/Löschen von Vorgängen:

- Installieren oder Löschen
- Klonieren/Kopieren von VMs
- Hinzufügen, Entfernen und Konfigurieren von virtuellen Laufplatten/CD-Geräten
- Hinzufügen, Entfernen und Konfigurieren virtueller Netzwerkgeräte
- XVA-Dateien importieren/exportieren
- Änderung der VM-Konfiguration
- Serversicherung/-wiederherstellung

> **Hinweis:**
>
> Die Rolle „VM Admin“ kann XVA-Dateien nur in einen Pool mit einem freigegebenen SR importieren. Die Rolle „VM-Administrator“ verfügt nicht über ausreichende Berechtigungen zum Importieren einer XVA-Datei in einen Host oder in einen Pool ohne gemeinsam genutzten

> Speicher.

VM ändern CD-Medien:

- Aktuelle CD auswerfen
- Neue CD einlegen

Importieren/Exportieren von Paketen; Importieren von Disk-Images

VM-Energiezustand ändern:

- VMs starten (automatische Platzierung)
- Herunterfahren von VMs
- VMs neu starten
- Anhalten von VMs
- VMs fortsetzen (automatische Platzierung)

Diese Berechtigung enthält nicht start_on, resume_on und migrate, die Teil der erweiterten VM-Betriebsberechtigung sind.

VM-Konsolen anzeigen:

- Anzeigen und Interaktion mit VM-Konsolen

Diese Berechtigung lässt den Benutzer keine Serverkonsolen anzeigen.

XenCenter Ansichtsverwaltungsvorgänge:

- Erstellen und Ändern globaler XenCenter Ordner
- Erstellen und Ändern von benutzerdefinierten globalen XenCenter Feldern
- Erstellen und Ändern globaler XenCenter Suchen

Ordner, benutzerdefinierte Felder und Suchen werden von allen Benutzern gemeinsam genutzt, die auf den Pool zugreifen

Eigene Aufgaben abbrechen:

- Ermöglicht es einem Benutzer, seine eigenen Aufgaben abzubrechen

Audit-Protokoll lesen:

- Citrix Hypervisor Überwachungsprotokoll herunterladen

Verbinden Sie sich mit Pool und lesen Sie alle Pool-Metadaten:

- In Pool einloggen
- Pool-Metadaten anzeigen
- Anzeigen historischer Performance-Daten
- Angemeldete Benutzer anzeigen
- Anzeigen von Benutzern und Rollen
- Nachrichten anzeigen

- Melden Sie sich für Veranstaltungen an und erhalten Sie

Virtuelle GPU konfigurieren:

- Angeben einer Pool-weiten Platzierungsrichtlinie
- Zuweisen einer virtuellen GPU zu einer VM
- Entfernen einer virtuellen GPU von einer VM
- Zulässige virtuelle GPU-Typen ändern
- Erstellen, Löschen oder Zuweisen einer GPU-Gruppe

Virtuelle GPU-Konfiguration anzeigen:

- Anzeigen von GPUs, GPU-Platzierungsrichtlinien und virtuellen GPU-Zuweisungen

Zugriff auf das Konfigurationslaufwerk (nur CoreOS-VMs):

- Zugriff auf den Konfigurationstreiber der VM
- Ändern der Parameter für die Cloud-Konfiguration

Containermanagement:

- Starten
- Stoppen
- Pausieren
- Wiederaufnehmen
- Zugriff auf Informationen über den Container

Geplante Snapshots:

- Hinzufügen von VMs zu vorhandenen Snapshot-Zeitplänen
- Entfernen von VMs aus vorhandenen Snapshot-Zeitplänen
- Snapshot-Zeitpläne hinzufügen
- Ändern von Snapshot-Zeitplänen
- Snapshot-Zeitpläne löschen

Integritätsprüfung konfigurieren:

- Integritätsprüfung aktivieren
- Integritätsprüfung deaktivieren
- Einstellungen für die Integritätsprüfung aktualisieren
- Manuelles Hochladen eines Serverstatusberichts

Ergebnisse und Einstellungen der Integritätsprüfung anzeigen:

- Anzeigen der Ergebnisse eines Uploads von Health Check
- Einstellungen für die Integritätsprüfung anzeigen

Ändern der Blockverfolgung konfigurieren:

- Ändern der Blockverfolgung aktivieren

- Änderte Blockverfolgung deaktivieren
- Löschen der mit einem Snapshot verknüpften Daten und Beibehaltung der Metadaten
- Abrufen der NBD-Verbindungsinformationen für einen VDI

Die geänderte Blockverfolgung kann nur für lizenzierte Instanzen von Citrix Hypervisor Premium Edition aktiviert werden.

Geänderte Blöcke auflisten:

- Vergleichen Sie zwei VDI-Snapshots und listen Sie die Blöcke auf, die zwischen ihnen geändert wurden

PVS-Beschleuniger konfigurieren:

- PVS-Beschleuniger aktivieren
- PVS-Beschleuniger deaktivieren
- Update-Cache-Konfiguration (PVS-Accelerator)
- Cache-Konfiguration (PVS-Accelerator) hinzufügen/entfernen

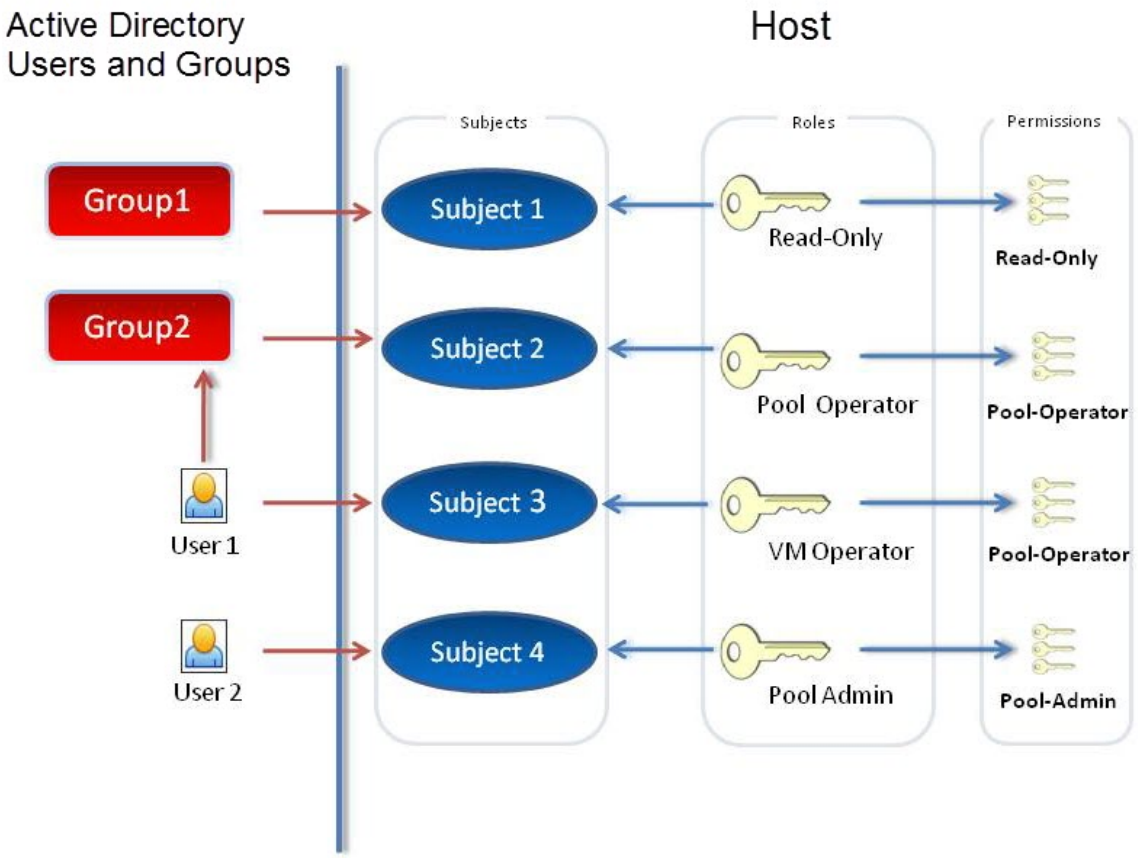
PVS-Beschleunigerkonfiguration anzeigen:

- Anzeigen des Status des PVS-Beschleunigers

> **Hinweis:**
>
> Manchmal kann ein schreibgeschützter Benutzer eine Ressource nicht in einen Ordner in XenCenter verschieben, selbst nachdem er eine Eingabeaufforderung für Erhöhungen erhalten und die Anmeldeinformationen eines Benutzers mit mehr Berechtigungen angegeben hat. Melden Sie sich in diesem Fall bei XenCenter als privilegierter Benutzer an, und wiederholen Sie die Aktion.

Wie berechnet Citrix Hypervisor die Rollen für die Sitzung?

1. Der Betreff wird über den Active Directory -Server authentifiziert, um zu überprüfen, zu welchen Gruppen der Betreff auch gehört.
2. Citrix Hypervisor überprüft dann, welche Rollen sowohl dem Betreff als auch den darin enthaltenen Gruppen zugewiesen wurden.
3. Da Subjekte Mitglieder mehrerer Active Directory Gruppen sein können, erben sie alle Berechtigungen der zugeordneten Rollen.



Kopiert!
Failed!

Verwenden von RBAC mit der CLI

October 16, 2019

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 aus:`xe role-list`

Dieser Befehl gibt eine Liste der aktuell definierten Rollen zurück, zum Beispiel:


```
    uuid( RO): 0165f154-ba3e-034e-6b27-5d271af109ba
    name ( RO): pool-admin
    description ( RO): The Pool Administrator role has full access to
       all
    features and settings, including accessing Dom0 and managing
       subjects,
    roles and external authentication

    uuid ( RO): b9ce9791-0604-50cd-0649-09b3284c7dfd
    name ( RO): pool-operator
    description ( RO): The Pool Operator role manages host-  and pool-
       wide resources,
    including setting up storage, creating resource pools and managing
       patches, and
    high availability (HA).

    uuid( RO): 7955168d-7bec-10ed-105f-c6a7e6e63249
    name ( RO): vm-power-admin
    description ( RO): The VM Power Administrator role has full access
       to VM and
    template management and can choose where to start VMs and use the
       dynamic memory
    control and VM snapshot features

    uuid ( RO): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
    name ( RO): vm-admin
    description ( RO):  The VM Administrator role can manage VMs and
       templates

    uuid ( RO): fb8d4ff9-310c-a959-0613-54101535d3d5
    name ( RO): vm-operator
    description ( RO):  The VM Operator role can use VMs and interact
       with VM consoles

    uuid ( RO): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
    name ( RO): read-only
    description ( RO): The Read-Only role can log in with basic read-
       only access
```

> **Hinweis:**
>
> Diese Liste der Rollen ist statisch. Rollen können nicht hinzugefügt, entfernt oder geändert werden.

So zeigen Sie eine Liste der aktuellen Themen an

Führen Sie den folgenden Befehl aus:

```
xe subject-list
```

Dieser Befehl gibt eine Liste der Citrix Hypervisor Benutzer, deren uuid und die Rollen zurück, denen sie zugeordnet sind:

```
    uuid ( RO): bb6dd239-1fa9-a06b-a497-3be28b8dca44
    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:
```



```
27        S-1-5-21-1539997073-1618981536-2562117463-2242; \
28        subject-gecos: user_pool_op; subject-displayname: user_pool_op; \
29        subject-is-group: false; subject-account-disabled: false; \
30        subject-account-expired: false; subject-account-locked: \
31        false; subject-password-expired: false
32        roles (SRO): pool-operator
```

So fügen Sie einen Betreff zu RBAC hinzu

Um vorhandenen AD-Benutzern die Verwendung von RBAC zu ermöglichen, erstellen Sie eine Betreffinstanz in Citrix Hypervisor, entweder direkt für den AD-Benutzer oder für die enthaltenen Gruppen:

Führen Sie den folgenden Befehl aus, um eine neue Betreffinstanz hinzuzufügen:

```
1 xe subject-add subject-name=AD user/group
```

So weisen Sie einem Betreff eine RBAC-Rolle zu

Nachdem Sie einen Betreff hinzugefügt haben, können Sie ihn einer RBAC-Rolle zuweisen. Sie können auf die Rolle entweder durch ihre uuid oder den Namen verweisen:

Führen Sie den Befehl aus:

```
1 xe subject-role-add uuid=subject uuid role-uuid=role_uuid
```

Oder

```
1 xe subject-role-add uuid=subject uuid role-name=role_name
```

Mit dem folgenden Befehl wird der Pooladministratorrolle beispielsweise ein Betreff mit der uuid`b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4` hinzugefügt:

```
1 xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name
     =pool-admin
```

So ändern Sie die RBAC-Rolle eines Betreffs

Um die Rolle eines Benutzers zu ändern, müssen Sie diese aus der vorhandenen Rolle entfernen und 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
```

Der Benutzer muss sich abmelden und wieder anmelden, um sicherzustellen, dass die neue Rolle wirksam wird. Dies erfordert die Berechtigung „Aktive Benutzerverbindungen abmelden“, die einem Pooladministrator oder Pooloperator zur Verfügung steht.)

> **Warnung:**
>
> Wenn Sie ein Pool-Admin-Betreff hinzufügen oder entfernen, kann es einige Sekunden dauern, bis alle Hosts im Pool SSH-Sitzungen akzeptieren, die diesem Betreff zugeordnet sind.

Auditing

Das RBAC-Überwachungsprotokoll zeichnet alle Vorgänge auf, die von einem angemeldeten Benutzer ausgeführt werden.

- Die Nachricht zeichnet die Betreff-ID und den Benutzernamen auf, die der Sitzung zugeordnet sind, die den Vorgang aufgerufen hat.
- Wenn ein Betreff einen Vorgang aufruft, der nicht autorisiert ist, wird der Vorgang protokolliert.
- Jede erfolgreiche Operation 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 ‘since’ vorhanden ist, lädt er nur die Datensätze von diesem bestimmten Zeitpunkt herunter.

```
xe audit-log-get [since=timestamp] filename=output filename
```

So erhalten Sie alle Überwachungsdatensätze aus dem Pool

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get filename=/tmp/auditlog-pool-actions.out
```


So erhalten Sie Überwachungsdatensätze des Pools seit einem genauen Millisekundenzeitstempel

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z \
    filename=/tmp/auditlog-pool-actions.out
```

So erhalten Sie Audit-Datensätze des Pools seit einem genauen Minutenzeitstempel

Führen Sie den folgenden Befehl aus:

```
xe audit-log-get since=2009-09-24T17:56Z \
    filename=/tmp/auditlog-pool-actions.out
```

Kopiert!
Failed!

Vernetzung

October 16, 2019

Dieser Abschnitt bietet einen Überblick über das Citrix Hypervisor Netzwerk, einschließlich Netzwerke, VLANs und NIC-Anleihen. Außerdem wird erläutert, wie Sie Ihre Netzwerkkonfiguration verwalten und Probleme beheben können.

> **Wichtig:**
>
> vSwitch ist der Standard-Netzwerkstapel von Citrix Hypervisor. Folgen Sie den Anweisungen untervSwitch-Netzwerke, um den Linux-Netzwerkstapel zu konfigurieren.

Wenn Sie bereits mit den Netzwerkkonzepten von Citrix Hypervisor vertraut sind, können Sie weitereVerwalten von NetzwerkenInformationen zu den folgenden Abschnitten erhalten:

- Erstellen von Netzwerken für eigenständige Citrix Hypervisor -Server
- Erstellen privater Netzwerke über Citrix Hypervisor -Server hinweg
- Erstellen von Netzwerken für Citrix Hypervisor or-Server, die in einem Ressourcenpool konfiguriert sind
- Erstellen von VLANs für Citrix Hypervisor or-Server, entweder eigenständig oder Teil eines Ressourcenpools

- Anleihen für eigenständige Citrix Hypervisor -Server erstellen
- Erstellen von Anleihen für Citrix Hypervisor or-Server, die in einem Ressourcenpool konfiguriert sind

> **Hinweis:**
>
> Der Begriff „Verwaltungsschnittstelle“ wird verwendet, um die IP-fähige Netzwerkkarte anzugeben, die den Verwaltungsdatenverkehr trägt. Der Begriff „sekundäre Schnittstelle“ wird verwendet, um eine IP-fähige Netzwerkkarte anzuzeigen, die für den Speicherdatenverkehr konfiguriert ist.

Netzwerkunterstützung

Citrix Hypervisor unterstützt bis zu 16 physische Netzwerkschnittstellen (oder bis zu 4 gebundene Netzwerkschnittstellen) pro Host und bis zu 7 virtuelle Netzwerkschnittstellen pro VM.

> **Hinweis:**
>
> Citrix Hypervisor ermöglicht die automatisierte Konfiguration und Verwaltung von Netzwerkkarten mithilfe der xe-Befehlszeilenschnittstelle. Bearbeiten Sie die Hostnetzkonfigurationsdateien nicht direkt.

vSwitch-Netzwerke

Bei Verwendung mit einer Controller-Appliance unterstützen vSwitch-Netzwerke Open Flow und bieten zusätzliche Funktionen wie Access Control Lists (ACL). Die Controller-Appliance für den Citrix Hypervisor vSwitch wird als vSwitch Controller bezeichnet. Mit dem vSwitch Controller können Sie Ihre Netzwerke über eine GUI überwachen. Der vSwitch Controller:

- Unterstützt feinkörnige Sicherheitsrichtlinien zur Steuerung des Datenverkehrs, der an und von einer VM gesendet wird.
- Bietet detaillierte Einblicke in das Verhalten und die Leistung des gesamten in der virtuellen Netzwerkumgebung gesendeten Datenverkehrs.

Ein vSwitch vereinfacht die IT-Administration in virtualisierten Netzwerkumgebungen erheblich. Alle VM-Konfiguration und Statistiken bleiben an die VM gebunden, selbst wenn die VM von einem physischen Host im Ressourcenpool auf einen anderen migriert. Weitere Informationen finden Sie unter vSwitch und Controller.

Führen Sie den folgenden Befehl aus, um zu bestimmen, welcher Netzwerkstapel konfiguriert ist:

```
1 xe host-list params=software-version
```


Suchen Sie in der Befehlsausgabe nach`network_backend`. Wenn der vSwitch als Netzwerkstapel konfiguriert ist, wird die Ausgabe wie folgt angezeigt:

```
network_backend: openvswitch
```

Wenn die Linux-Brücke als Netzwerkstapel konfiguriert ist, wird die Ausgabe wie folgt angezeigt:

```
network_backend: bridge
```

Um den Linux-Netzwerkstapel wiederherzustellen, führen Sie den folgenden Befehl aus:

```
xe-switch-network-backend bridge
```

Starten Sie Ihren Host neu, nachdem Sie diesen Befehl ausgeführt haben.

> **Warnung:**
>
> Der Linux-Netzwerkstapel ist nicht Open Flow aktiviert, unterstützt Cross-Server-Private Networks nicht. Der Citrix Hypervisor vSwitch Controller verwaltet den Linux-Netzwerkstapel nicht.

Übersicht über das Citrix Hypervisor Netzwerk

In diesem Abschnitt werden die allgemeinen Netzwerkkonzepte in der Citrix Hypervisor Umgebung beschrieben.

Citrix Hypervisor erstellt während der Installation ein Netzwerk für jede physische Netzwerkkarte. Wenn Sie einem Pool einen Server hinzufügen, werden die Standardnetzwerke zusammengeführt. Damit soll sichergestellt werden, dass alle physischen Netzwerkkarten mit demselben Gerätenamen mit demselben Netzwerk verbunden 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 Netzwerkkarte zu erstellen.

Sie können vier verschiedene Netzwerktypen in Citrix Hypervisor konfigurieren:

- **Externe Netzwerke** sind mit einer physischen Netzwerkschnittstelle verbunden. Externe Netzwerke stellen eine Brücke zwischen einer virtuellen Maschine und der mit dem Netzwerk verbundenen physischen Netzwerkschnittstelle bereit. Externe Netzwerke ermöglichen es einer virtuellen Maschine, eine Verbindung zu Ressourcen herzustellen, die über die physische Netzwerkkarte des Servers verfügbar sind.
- **Gebundene Netzwerke** bilden eine Verbindung zwischen zwei oder mehr Netzwerkkarten, um einen einzigen, leistungsstarken Kanal zwischen der virtuellen Maschine und dem Netzwerk zu erstellen.

- **Private Einzelserver Netzwerke** haben keine Zuordnung zu einer physischen Netzwerkschnittstelle. Private Netzwerke mit einem Server können verwendet werden, um Verbindungen zwischen den virtuellen Maschinen auf einem bestimmten Host ohne Verbindung zur Außenwelt bereitzustellen.
- **Serverübergreifende private Netzwerke** erweitern das private Netzwerkkonzept für einen einzelnen Server, um VMs auf verschiedenen Hosts die Kommunikation mit dem vSwitch zu ermöglichen.

> **Hinweis:**
>
> Einige Netzwerkoptionen weisen unterschiedliche Verhaltensweisen bei Verwendung mit eigenständigen Citrix Hypervisor or-Servern im Vergleich zu Ressourcenpools auf. 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 einzelnen.

Netzwerkobjekte

In diesem Abschnitt werden drei Typen serverseitiger Softwareobjekte verwendet, um Netzwerkentitäten darzustellen. Diese Objekte sind:

- Eine *PIF*, die eine physische Netzwerkkarte auf einem Host darstellt. PIF-Objekte haben einen Namen und eine Beschreibung, eine UUID, die Parameter der Netzwerkkarte, die sie darstellen, sowie das Netzwerk und den Server, 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 verfügen über 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 die Konfiguration von Netzwerkoptionen. Sie können die für Verwaltungsvorgänge verwendete Netzwerkkarte steuern und erweiterte Netzwerkfunktionen wie VLANs und NIC-Anleihen erstellen.

Netzwerke

Jeder Citrix Hypervisor-Server verfügt über ein oder mehrere Netzwerke, bei denen es sich um virtuelle Ethernet-Switches handelt. Netzwerke, die nicht mit einem PIF verknüpft sind, gelten als *intern*. Interne Netzwerke können nur für die Konnektivität zwischen VMs auf einem bestimmten Citrix Hypervisor or-Server ohne Verbindung zur Außenwelt verwendet werden. Netzwerke, die mit

einem PIF verknüpft sind, gelten als *extern*. Externe Netzwerke bieten eine Brücke zwischen VIFs und PIF, die mit dem Netzwerk verbunden sind, und ermöglichen so die Konnektivität zu Ressourcen, die über die PIF-Netzwerkkarte verfügbar sind.

VLANs

VLANs, wie im IEEE 802.1Q-Standard definiert, ermöglichen ein einzelnes physisches Netzwerk, mehrere logische Netzwerke zu unterstützen. Citrix Hypervisor -Server unterstützen VLANs auf verschiedene Arten.

> **Hinweis:**
>
> Alle unterstützten VLAN-Konfigurationen sind gleichermaßen für Pools und eigenständige Hosts sowie gebundene und nicht gebundene Konfigurationen anwendbar.

Verwenden von VLANs mit virtuellen Maschinen

Switch-Ports, die als 802.1Q-VLAN-Trunk-Ports konfiguriert sind, können mit den Citrix Hypervisor VLAN-Funktionen verwendet werden, um virtuelle Gastnetzwerkschnittstellen (VIFs) mit bestimmten VLANs zu verbinden. In diesem Fall führt der Citrix Hypervisor or-Server die VLAN-Tagging/Enttagging-Funktionen für den Gast aus, die keine VLAN-Konfiguration kennen.

Citrix Hypervisor VLANs werden durch zusätzliche PIF-Objekte dargestellt, die VLAN-Schnittstellen darstellen, die einem angegebenen VLAN-Tag entsprechen. Sie können Citrix Hypervisor Netzwerke mit der PIF verbinden, die die physische Netzwerkkarte darstellt, um den gesamten Datenverkehr auf der Netzwerkkarte anzuzeigen. Alternativ können Sie Netzwerke mit einem PIF verbinden, das ein VLAN darstellt, um nur den Datenverkehr mit dem angegebenen VLAN-Tag anzuzeigen. Sie können ein Netzwerk auch so verbinden, dass es nur den nativen VLAN-Datenverkehr sieht, indem Sie es an VLAN 0 anhängen.

Weitere Informationen zum Erstellen von VLANs für Citrix Hypervisor or-Server, entweder eigenständig oder Teil eines Ressourcenpools, finden Sie unterErstellen von VLANs.

Verwenden von VLANs mit Verwaltungsschnittstellen

Die Verwaltungsschnittstelle kann in einem VLAN über einen Switch-Port konfiguriert werden, der als Trunk-Port oder Access Mode Port konfiguriert ist. Verwenden Sie XenCenter oder xe CLI, um ein VLAN einzurichten und es zur Verwaltungsschnittstelle zu machen. Weitere Informationen finden Sie unter Verwaltungsoberfläche.

Verwenden von VLANs mit Verwaltungsschnittstellen

Die Verwaltungsschnittstelle kann in einem VLAN über einen Switch-Port konfiguriert werden, der als Trunk-Port oder Access Mode Port konfiguriert ist. Verwenden Sie XenCenter oder xe CLI, um ein VLAN einzurichten und es zur Verwaltungsschnittstelle zu machen. Weitere Informationen finden Sie unter Verwaltungsoberfläche.

Verwenden von VLANs mit dedizierten Speicher-NICs

Dedizierte Speicher-NICs können so konfiguriert werden, dass native VLAN- oder Zugriffsmode-Ports verwendet werden, wie im vorherigen Abschnitt für Verwaltungsschnittstellen beschrieben. Dedizierte Speicher-Netzwerkkarten werden auch als IP-fähige Netzwerkkarten oder sekundäre Schnittstellen bezeichnet. Sie können dedizierte Speicher-Netzwerkkarten für die Verwendung von Trunk-Ports und Citrix Hypervisor VLANs konfigurieren, wie im vorherigen Abschnitt für virtuelle Maschinen beschrieben. Weitere Informationen finden Sie unter Konfigurieren einer dedizierten Speicher-NIC.

Kombination von Verwaltungsschnittstellen und Gast-VLANs auf einer einzigen Host-NIC

Ein einzelner Switch-Port kann sowohl mit Stamm- als auch nativen VLANs konfiguriert werden, sodass eine Host-NIC für eine Verwaltungsschnittstelle (im nativen VLAN) und für die Verbindung von Gast-VIFs mit bestimmten VLAN-IDs verwendet werden kann.

Jumbo-Rahmen

Jumbo-Frames können verwendet werden, um die Performance des Speicherdatenverkehrs zu optimieren. Jumbo-Frames sind Ethernet-Frames mit mehr als 1.500 Bytes 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:**
>
> Citrix Hypervisor unterstützt Jumbo-Frames nur, wenn vSwitch als Netzwerkstapel auf allen Hosts im Pool verwendet wird.

Anforderungen für die Verwendung von Jumbo-Frames

Kunden müssen Folgendes beachten, wenn sie Jumbo-Frames verwenden:

- Jumbo-Frames werden auf Poolebene konfiguriert
- vSwitch muss als Netzwerk-Back-End auf allen Hosts im Pool konfiguriert werden
- Jedes Gerät im Subnetz muss so konfiguriert sein, dass Jumbo-Frames verwendet werden
- Aktivieren von Jumbo-Frames in einem dedizierten Speichernetzwerk (empfohlen)

- Das Aktivieren von Jumbo-Frames im Verwaltungsnetzwerk ist keine unterstützte Konfiguration.
- Jumbo-Frames werden für die Verwendung auf VMs 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-Anleihen

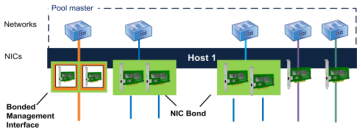
NIC-Anleihen, manchmal auch als NIC-Teaming bezeichnet, verbessern die Ausfallsicherheit und Bandbreite des Citrix Hypervisor or-Servers, indem Administratoren zwei oder mehr Netzwerkkarten gemeinsam konfigurieren können. NIC-Anleihen funktionieren logisch als eine Netzwerkkarte und alle gebundenen NICs teilen sich die MAC-Adresse.

Wenn eine Netzwerkkarte in der Bindung fehlschlägt, wird der Netzwerkverkehr des Hosts automatisch über die zweite Netzwerkkarte umgeleitet. Citrix Hypervisor unterstützt bis zu acht gebundene Netzwerke.

Citrix Hypervisor unterstützt Aktiv-Aktiv-, Aktiv-Passiv- und LACP-Bonding-Modi. Die Anzahl der unterstützten Netzwerkkarten und der unterstützte Bonding-Modus variiert je nach Netzwerkstapel:

- Die LACP-Bindung ist nur für den vSwitch verfügbar, während aktiv-aktiv und aktiv-passiv sowohl für die vSwitch- als auch für die Linux-Brücke verfügbar sind.
- Wenn der vSwitch der Netzwerkstapel ist, können Sie zwei, drei oder vier Netzwerkkarten verbinden.
- Wenn die Linux-Brücke der Netzwerk-Stack ist, können Sie nur zwei Netzwerkkarten verbinden.

In der folgenden Abbildung befindet sich die Verwaltungsschnittstelle auf einem gebundenen Paar von NICs. Citrix Hypervisor verwendet diese Bindung für den Verwaltungsdatenverkehr.



Alle Bonding-Modi unterstützen Failover. Nicht alle Modi erlauben jedoch, dass alle Links für alle Verkehrstypen aktiv sind. Citrix Hypervisor unterstützt das Verbinden der folgenden Netzwerkkarten:

- **NICs (Nicht-Management)**. Sie können Netzwerkkarten binden, die Citrix Hypervisor ausschließlich für den VM-Datenverkehr verwendet. Durch die Bindung dieser Netzwerkkarten wird nicht nur die Ausfallsicherheit gewährleistet, sondern auch der Datenverkehr mehrerer VMs zwischen den Netzwerkkarten ausgeglichen.

- **Management-Schnittstellen**. Sie können eine Verwaltungsschnittstelle mit einer anderen Netzwerkkarte verbinden, sodass die zweite Netzwerkkarte ein Failover für den Verwaltungsdatenverkehr bereitstellt. Obwohl die Konfiguration einer LACP-Link-Aggregationsanleihe einen Lastausgleich für den Verwaltungsdatenverkehr bietet, ist die aktiv-aktive NIC-Bindung jedoch nicht möglich. Sie können ein VLAN auf gebundenen NICs erstellen und diesem VLAN kann eine Host-Management-Schnittstelle zugewiesen werden.
- **Sekundäre Schnittstellen**. Sie können Netzwerkkarten binden, die Sie als sekundäre Schnittstellen konfiguriert haben (z. B. für Speicher). Für die meisten iSCSI-Softwareinitiator-Speicher empfehlen wir jedoch, Multipathing anstelle der NIC-Bindung zu konfigurieren, wie in den Citrix Hypervisor Netzwerkkonfigurationen entwerfen 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 soll: Der VM-Datenverkehr wird automatisch auf die neue gebundene Schnittstelle migriert.

In Citrix Hypervisor stellt eine zusätzliche PIF eine NIC-Bindung dar. Citrix Hypervisor NIC-Anleihen subsumieren die zugrunde liegenden physischen Geräte (PIF) vollständig.

> **Hinweise:**
>
> - Das Erstellen einer Bindung, die nur eine Netzwerkkarte enthält, wird nicht unterstützt.
> - NIC-Anleihen werden auf Netzwerkkarten, die FCoE-Datenverkehr tragen, nicht unterstützt.

Wichtige Punkte zur IP-Adressierung

Bonded NICs haben entweder eine IP-Adresse oder keine IP-Adressen, wie folgt:

- **Management- und Speichernetzwerke**.
  - Wenn Sie eine Verwaltungsschnittstelle oder eine sekundäre Schnittstelle verbinden, wird der Bindung eine einzige IP-Adresse zugewiesen. Das heißt, jede NIC hat keine eigene IP-Adresse. Citrix Hypervisor behandelt die beiden Netzwerkkarten als eine logische Verbindung.
  - Wenn Anleihen für Nicht-VM-Datenverkehr verwendet werden, z. B. um eine Verbindung mit gemeinsam genutztem Netzwerkspeicher oder XenCenter für die Verwaltung herzustellen, konfigurieren Sie eine IP-Adresse für die Anleihe. 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 mit einer NIC ohne IP-Adresse verbinden, übernimmt die Bindung die IP-Adresse der jeweiligen Schnittstelle.
  - Wenn Sie eine getaggte VLAN-Verwaltungsschnittstelle und eine sekundäre Schnittstelle verbinden, wird das Management-VLAN auf dieser gebundenen Netzwerkkarte erstellt.

- **VM-Netzwerke**. Wenn gebundene Netzwerkkarten für den VM-Datenverkehr verwendet werden, müssen Sie keine IP-Adresse für die Bindung konfigurieren. Dies liegt daran, dass die Bindung auf Layer 2 des OSI-Modells, der Datenverknüpfungsschicht, funktioniert und auf diesem Layer keine IP-Adressierung verwendet wird. IP-Adressen für virtuelle Maschinen sind VIFs zugeordnet.

Klebungstypen

Citrix Hypervisor bietet drei verschiedene Arten von Anleihen, die alle mit der CLI oder XenCenter konfiguriert werden können:

- Aktiv-Aktiv-Modus, wobei der VM-Datenverkehr zwischen den gebundenen Netzwerkkarten ausgeglichen wird. Siehe Aktiv-aktive Verklebung.
- Aktiv-passiver Modus, in dem nur eine Netzwerkkarte den Datenverkehr aktiv trägt. Siehe Aktiv-Passiv-Verklebung.
- LACP Link Aggregation, bei der aktive Netzwerkkarten und Standby-Netzwerkkarten zwischen dem Switch und dem Server ausgehandelt werden. Siehe LACP Link Aggregation Control Protocol Bonding.

> **Hinweis:**
>
> Die Bonding wird mit einer Up-Delay von 31.000 ms und einer Down-Delay von 200 ms eingerichtet. Die scheinbar lange Up-Delay ist bewusst wegen der Zeit, die einige Switches benötigen, um den Port zu aktivieren. Wenn eine Verbindung nach einem Ausfall zurückkommt, kann die Bindung ohne Verzögerung den Datenverkehr auf sie neu ausgleichen, bevor der Switch bereit ist, den Datenverkehr zu übergeben. Um beide Verbindungen auf einen anderen Schalter zu verschieben, bewegen Sie einen und warten Sie 31 Sekunden, bis er wieder verwendet wird, bevor Sie den anderen verschieben. Hinweise zum Ändern der Verzögerung finden Sie unterÄnderung der Up-Verzögerung für Anleihen.

Status der Anleihe

Citrix Hypervisor stellt den Status für Anleihen in den Ereignisprotokollen für jeden Host bereit. Wenn ein oder mehrere Links in einer Anleihe fehlschlagen oder wiederhergestellt werden, wird dies im

Ereignisprotokoll vermerkt. Ebenso können Sie den Status der Verknüpfungen einer Anleihe abfragen, indem Sie den`links-up` Parameter verwenden, wie im folgenden Beispiel gezeigt:

```
1 xe bond-param-get uuid=bond_uuid param-name=links-up
```

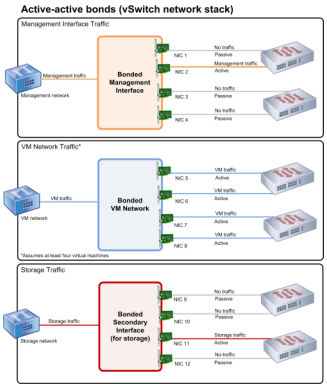
Citrix Hypervisor überprüft den Status von Links in Anleihen etwa alle fünf Sekunden. Wenn daher mehr Links in der Anleihe im Fünf-Sekunden-Fenster fehlschlagen, wird der Fehler erst bei der nächsten Statusprüfung protokolliert.

Bonding-Ereignisprotokolle werden auf der Registerkarte XenCenter Protokolle angezeigt. Für Benutzer, die nicht XenCenter ausführen, werden auch Ereignisprotokolle`/var/log/xensource.log` auf jedem Host angezeigt.

Aktiv-aktive Verklebung

Active-Active ist eine aktive/aktive Konfiguration für Gastdatenverkehr: Beide Netzwerkkarten können VM-Datenverkehr gleichzeitig weiterleiten. Wenn Anleihen für den Verwaltungsdatenverkehr verwendet werden, kann nur eine Netzwerkkarte in der Anleihe den Datenverkehr leiten: Die andere Netzwerkkarte bleibt ungenutzt und bietet Failover-Unterstützung. Active-Active-Modus ist der Standard-Bonding-Modus, wenn entweder die Linux-Brücke oder der vSwitch-Netzwerkstapel aktiviert ist.

Wenn aktives Bonding mit der Linux-Bridge verwendet wird, können Sie nur zwei Netzwerkkarten verbinden. Wenn Sie den vSwitch als Netzwerkstapel verwenden, können Sie entweder zwei, drei oder vier Netzwerkkarten im aktiv-aktiven Modus verbinden. Im aktiv-aktiven Modus ist das Verbinden von drei oder vier Netzwerkkarten jedoch nur für den VM-Datenverkehr von Vorteil, wie in der folgenden Abbildung dargestellt.



Citrix Hypervisor kann Datenverkehr nur über zwei oder mehr Netzwerkkarten senden, wenn mehr als eine MAC-Adresse mit der Bindung verknüpft ist. Citrix Hypervisor kann die virtuellen MAC-Adressen im VIF verwenden, um Datenverkehr über mehrere Links zu senden. Speziell:

- **VM-Datenverkehr**. Sofern Sie die Bindung auf Netzwerkkarten aktivieren, die nur VM-Datenverkehr (Gast) tragen, sind alle Verbindungen aktiv, und die NIC-Bindung kann den

verteilten VM-Datenverkehr über NICs hinweg ausgleichen. Der Datenverkehr eines einzelnen VIF wird niemals zwischen Netzwerkkarten aufgeteilt.

- **Verwaltungs- oder Speicherdatenverkehr**. Nur einer der Links (NICs) in der Anleihe ist aktiv, und die anderen Netzwerkkarten bleiben ungenutzt, es sei denn, der Datenverkehr wird auf diese übertragen. Die Konfiguration einer Verwaltungsschnittstelle oder einer sekundären Schnittstelle in einem gebundenen Netzwerk bietet Ausfallsicherheit.
- **Mischverkehr**. Wenn die gebundene Netzwerkkarte eine Mischung aus IP-basiertem Speicherdatenverkehr und Gastdatenverkehr trägt, wird nur der Gast- und Steuerdomänenverkehr Lastausgleich ausgeglichen. Die Steuerdomäne ist im Wesentlichen eine virtuelle Maschine, so dass sie wie die anderen Gäste eine Netzwerkkarte verwendet. Citrix Hypervisor gleicht den Datenverkehr der Steuerdomäne so aus, wie er den VM-Datenverkehr ausgleicht.

Verkehrsausgleich

Citrix Hypervisor gleicht den Datenverkehr zwischen Netzwerkkarten mithilfe der Quell-MAC-Adresse des Pakets aus. Da für den Verwaltungsdatenverkehr nur eine Quell-MAC-Adresse vorhanden ist, kann der Aktiv-Aktiv-Modus nur eine Netzwerkkarte verwenden und der Datenverkehr wird nicht ausgeglichen. Der Verkehrsausgleich basiert auf zwei Faktoren:

- Die virtuelle Maschine und die zugehörige VIF senden oder empfangen den Datenverkehr
- Die Menge der Daten (in Kilobyte), die gesendet werden.

Citrix Hypervisor wertet die Datenmenge (in Kilobyte), die jede Netzwerkkarte sendet und empfängt. Wenn die Datenmenge, die über eine Netzwerkkarte gesendet wird, die Datenmenge überschreitet, die über die andere Netzwerkkarte gesendet wird, gleicht Citrix Hypervisor neu aus, welche VIFs welche Netzwerkkarten verwenden. Die gesamte Ladung des VIF wird übertragen. Eine VIF-Last wird niemals auf zwei Netzwerkkarten aufgeteilt.

Obwohl die aktiv-aktive NIC-Bonding einen Lastausgleich für den Datenverkehr von mehreren VMs bieten kann, kann sie keine einzelne VM mit dem Durchsatz von zwei Netzwerkkarten bereitstellen. Jedes angegebene VIF verwendet jeweils nur einen der Links in einer Bindung. Da Citrix Hypervisor den Datenverkehr regelmäßig neu ausgleicht, werden VIFs nicht dauerhaft einer bestimmten Netzwerkkarte in der Bindung zugewiesen.

Active-Active-Modus wird manchmal als SLB-Bonding (Source Load Balancing) beschrieben, da Citrix Hypervisor SLB verwendet, um die Last über gebundene Netzwerkschnittstellen zu teilen. SLB wird vom Open-Source-Modus (Adaptive Load Balancing, ALB) abgeleitet und verwendet die ALB-Funktionalität, um die Last dynamisch über Netzwerkkarten hinweg neu auszugleichen.

Beim Rebalancing wird die Anzahl der Bytes, die über jeden Slave (Schnittstelle) gehen, über einen bestimmten Zeitraum verfolgt. Wenn ein zu sendendes Paket eine neue Quell-MAC-Adresse enthält, wird

es der Slave-Schnittstelle mit der geringsten Auslastung zugewiesen. Der Verkehr wird in regelmäßigen Abständen neu ausgeglichen.

Jede MAC-Adresse verfügt über eine entsprechende Last, und Citrix Hypervisor kann ganze Lasten zwischen Netzwerkkarten verschieben, abhängig von der Datenmenge, die eine VM sendet und empfängt. Bei aktivem Datenverkehr kann der gesamte Datenverkehr von einer VM auf nur einer Netzwerkkarte gesendet werden.

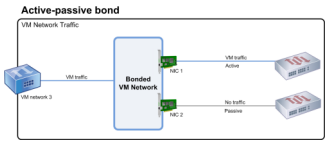
> **Hinweis:**
>
> Active-Active Bonding erfordert keine Switch-Unterstützung für EtherChannel oder 802.3ad (LACP).

Aktiv-Passiv-Verklebung

Eine aktive und passive Bindung leitet den Verkehr nur über eine der NICs. Wenn die aktive Netzwerkschnittstelle die Netzwerkkonnektivität verliert, wird der Datenverkehr an die andere Netzwerkkarte in der Bindung weitergeleitet. Aktiv-Passive Anleihen leiten den Datenverkehr über die aktive NIC. Der Datenverkehr wird auf die passive Netzwerkkarte verschoben, wenn die aktive Netzwerkkarte ausfällt.

Aktiv-Passiv-Bonding ist in der Linux-Brücke und im vSwitch-Netzwerkstapel verfügbar. Bei Verwendung mit der Linux-Brücke können Sie zwei Netzwerkkarten miteinander verbinden. Wenn Sie mit dem vSwitch verwendet werden, können Sie nur zwei, drei oder vier Netzwerkkarten miteinander verbinden. Unabhängig vom Traffic-Typ ist jedoch beim Anbinden von Netzwerkkarten im aktiv-passiven Modus nur eine Verbindung aktiv und es gibt keinen Lastausgleich zwischen Verbindungen.

Die folgende Abbildung zeigt zwei gebundene Netzwerkkarten, die im aktiv-passiven Modus konfiguriert sind.



Active-Active-Modus ist die standardmäßige Bonding-Konfiguration in Citrix Hypervisor. Wenn Sie Anleihen mit der CLI konfigurieren, müssen Sie einen Parameter für den Aktiv-Passiv-Modus angeben. Andernfalls wird eine aktiv-aktive Bindung erstellt. Sie müssen den Aktiv-Passiv-Modus nicht konfigurieren, da ein Netzwerk Verwaltungsdatenverkehr oder Speicherdatenverkehr trägt.

Aktiv-Passiv kann eine gute Wahl für die Widerstandsfähigkeit sein, da es mehrere Vorteile bietet. Bei aktiv-passiven Anleihen bewegt sich der Verkehr zwischen NICs nicht. In ähnlicher Weise können Sie mit aktiv-passiver Bindung zwei Switches für Redundanz konfigurieren, jedoch kein Stapeln erforderlich. Wenn der Management-Switch abstirbt, können gestapelte Switches ein Single Point of Failure

sein.

Der Aktiv-Passiv-Modus erfordert keine Switch-Unterstützung für EtherChannel oder 802.3ad (LACP).

Erwägen Sie, den Aktiv-Passiv-Modus in Situationen zu konfigurieren, in denen Sie keinen Lastausgleich benötigen oder wenn Sie nur Datenverkehr auf einer Netzwerkkarte senden möchten.

> **Wichtig:**
>
> Nachdem Sie VIFs erstellt haben oder Ihr Pool in Produktion ist, achten Sie darauf, Anleihen zu ändern oder Anleihen zu erstellen.

LACP Link Aggregation Control Protocol Bonding

Das LACP Link Aggregation Control Protocol ist eine Art von Bindung, die eine Gruppe von Ports zusammen bündelt und wie ein einziger logischer 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 Switch-Konfiguration für LACP-Anleihen. Sie müssen den vSwitch als Netzwerkstapel konfigurieren, um LACP-Bonding zu verwenden. Außerdem müssen Ihre Switches den IEEE 802.3ad-Standard unterstützen.

Ein Vergleich von aktiv-aktivem SLB-Bonding und LACP-Bonding:

Aktiv-aktive SLB-Verklebung

Vorteile:

- Kann mit jedem Schalter in der Hardwarekompatibilitätsliste verwendet werden.
- Erfordert keine Switches, die das Stapeln unterstützen.
- Unterstützt vier NICs.

Überlegungen:

- Der optimale Lastausgleich erfordert mindestens eine NIC pro VIF.
- Speicher- oder Verwaltungsdatenverkehr kann nicht auf mehreren Netzwerkkarten aufgeteilt werden.
- Der Lastenausgleich erfolgt nur, wenn mehrere MAC-Adressen vorhanden sind.

LACP-Verklebung

Vorteile:

- Alle Links können unabhängig vom Verkehrstyp aktiv sein.

- Der Verkehrsausgleich hängt nicht von den MAC-Quelladressen ab, sodass alle Datenverkehrstypen ausgeglichen werden können.

Überlegungen:

- Switches müssen den IEEE 802.3ad-Standard unterstützen.
- Erfordert eine Switch-Side-Konfiguration.
- Wird nur für den vSwitch unterstützt.
- Benötigt einen einzelnen Schalter oder einen gestapelten Schalter.

Verkehrsausgleich

Citrix Hypervisor unterstützt zwei LACP-Bonding-Hashing-Typen. Der Begriff Hashing beschreibt, wie die Netzwerkkarten und der Switch den Datenverkehr verteilen — (1) Load Balancing basierend auf IP und Port von Quell- und Zieladressen und (2) Load Balancing basierend auf Quell-MAC-Adresse.

Je nach Hashing-Typ und Datenverkehrsmuster kann die LACP-Bindung den Datenverkehr möglicherweise gleichmäßiger verteilen als die aktiv-aktive NIC-Bindung.

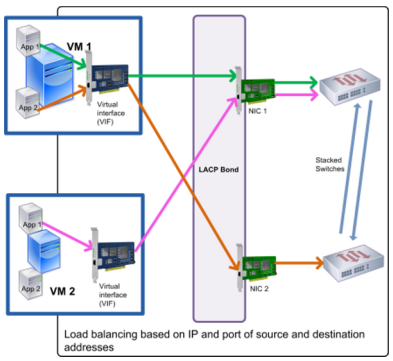
> **Hinweis:**
>
> Sie konfigurieren Einstellungen für ausgehenden und eingehenden Datenverkehr separat auf dem Host und dem Switch: Die Konfiguration muss nicht auf beiden Seiten übereinstimmen.

Lastenausgleich basierend auf IP und Port von Quell- und Zieladressen.

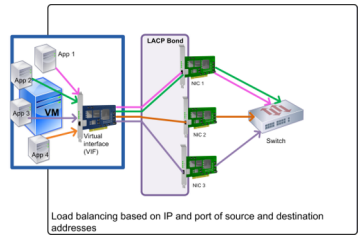
Dieser Hashing-Typ ist der Standard-LACP-Bonding-Hashing-Algorithmus. Wenn die Quell- oder Ziel-IP- oder Portnummern variiert, kann der Datenverkehr von einem Gast über zwei Links verteilt werden.

Wenn auf einer virtuellen Maschine mehrere Anwendungen ausgeführt werden, die unterschiedliche IP- oder Portnummern verwenden, verteilt dieser Hashing-Typ den Datenverkehr über mehrere Links. Die Verteilung des Datenverkehrs gibt dem Gast die Möglichkeit, den Gesamtdurchsatz zu nutzen. Mit diesem Hashing-Typ kann ein Gast den gesamten Durchsatz mehrerer Netzwerkkarten verwenden.

Wie in der folgenden Abbildung gezeigt, kann dieser Hashing-Typ den Datenverkehr von zwei verschiedenen Anwendungen auf einer virtuellen Maschine auf zwei verschiedene Netzwerkkarten verteilen.



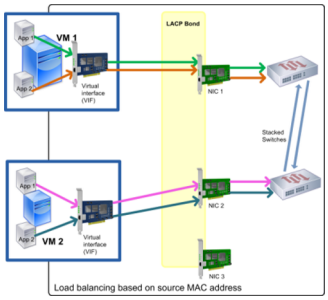
Die Konfiguration der LACP-Bindung basierend auf IP und Port der Quell- und Zieladresse ist von Vorteil, wenn Sie den Datenverkehr zweier verschiedener Anwendungen auf derselben VM ausgleichen möchten. Wenn beispielsweise nur eine virtuelle Maschine für die Verwendung einer Bindung von drei Netzwerkkarten konfiguriert ist.



Der Ausgleichsalgorithmus für diesen Hashing-Typ verwendet fünf Faktoren, um den Datenverkehr über die Netzwerkkarten zu verteilen: die Quell-IP-Adresse, die Quellportnummer, die Ziel-IP-Adresse, die Zielportnummer und die MAC-Quelladresse.

Lastenausgleich basierend auf Quell-MAC-Adresse.

Dieser Lastenausgleich 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. Citrix Hypervisor sendet ausgehenden Datenverkehr mit demselben Algorithmus wie beim aktiven Binden. Der Datenverkehr, der von demselben Gast stammt, wird nicht über 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.



Switch-Konfiguration

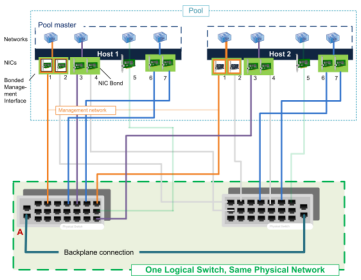
Abhängig von Ihren Redundanzanforderungen können Sie die Netzwerkkarten in der Verbindung entweder mit denselben oder separaten gestapelten Switches verbinden. Wenn Sie eine der Netzwerkkarten mit einem zweiten, redundanten Switch verbinden und eine Netzwerkkarte oder Switch ausfällt, wird der Datenverkehr mit der anderen Netzwerkkarte weitergeleitet. Durch das Hinzufügen eines zweiten Switches wird ein einzelner Fehlerpunkt in Ihrer Konfiguration auf folgende Weise verhindert:

- Wenn Sie einen 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 einen beliebigen Datenverkehrstyp) mit einem zweiten Switch verbinden und die Netzwerkkarte oder der Switch ausfällt, verbleiben die virtuellen Maschinen im Netzwerk, während ihr Datenverkehr mit dem anderen NIC/Switch ausfällt.

Verwenden Sie gestapelte Switches, wenn Sie gebundene Netzwerkkarten mit mehreren Switches verbinden und den LACP-Bonding-Modus konfiguriert haben. Der Begriff „gestapelte Switches“ wird verwendet, um die Konfiguration mehrerer physischer Switches als einziger logischer Switch zu beschreiben. Sie müssen die Schalter physisch und über die Switch-Management-Software miteinander verbinden, damit die Switches als eine einzige logische Schalteinheit funktionieren, gemäß den Richtlinien des Schalterherstellers. Typischerweise ist Switch-Stacking nur über proprietäre Erweiterungen verfügbar, und Switch-Anbieter können diese Funktionalität unter unterschiedlichen Bedingungen vermarkten.

> **Hinweis:**
>
> Wenn Sie Probleme mit aktiv-aktiven Bindungen haben, ist möglicherweise die Verwendung von gestapelten Switches erforderlich. Aktiv-passive Bindungen erfordern keine gestapelten Schalter.

Die folgende Abbildung zeigt, wie die Kabel und die Netzwerkkonfiguration für die gebundenen NICs übereinstimmen müssen.



Switch-Konfiguration für LACP-Anleihen

Da die spezifischen Details der Switch-Konfiguration je nach Hersteller unterschiedlich sind, 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 für jede LACP-Bindung auf dem Host eine LAG-Gruppe erstellen. Wenn Sie beispielsweise über einen Fünf-Host-Pool verfügen und eine LACP-Bindung auf NICs 4 und 5 auf jedem Host erstellt haben, müssen Sie fünf LAG-Gruppen auf dem Switch erstellen. Eine Gruppe für jeden Satz von Ports, der den Netzwerkkarten auf dem Host entspricht.

  Möglicherweise müssen Sie Ihre VLAN-ID auch Ihrer LAG-Gruppe hinzufügen.
- Citrix Hypervisor LACP-Anleihen erfordern das Festlegen der Einstellung Statischer Modus in der LAG-Gruppe auf Deaktiviert.

Wie bereits in der *Switch-Konfiguration*erwähnt, sind Stapelschalter erforderlich, um LACP-Verbindungen mit mehreren Switches zu verbinden.

Erste Netzwerkkonfiguration nach dem Setup

Die Netzwerkkonfiguration des Citrix Hypervisor or-Servers wird bei der Erstinstallation des Hosts angegeben. Optionen wie IP-Adresskonfiguration (DHCP/statisch), die als Verwaltungsschnittstelle verwendete Netzwerkkarte und Hostname werden basierend auf den bei der Installation angegebenen Werten 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:

- PIF werden für jede NIC im Host erstellt
- Die PIF der Netzwerkkarte, die für die Verwendung als Verwaltungsschnittstelle ausgewählt wurde, wird mit den IP-Adressierungsoptionen konfiguriert, die während der Installation angegeben wurden.
- Für jede PIF wird ein Netzwerk erstellt („network 0”, „network 1” usw.)
- Jedes Netzwerk ist mit einem PIF verbunden
- Die IP-Adressierungsoptionen werden für alle PIF außer der PIF, die als Verwaltungsschnittstelle verwendet wird, nicht konfiguriert.

Wenn ein Host über eine einzelne Netzwerkkarte verfügt, ist die folgende Konfiguration nach der Installation vorhanden:

- Eine einzelne PIF wird erstellt, die der einzelnen Netzwerkkarte des Hosts entspricht.

- Die PIF wird mit den IP-Adressierungsoptionen konfiguriert, die während der Installation angegeben wurden und um die Verwaltung des Hosts zu ermöglichen
- Die PIF ist für die Verwendung in Hostverwaltungsvorgängen festgelegt
- Ein einzelnes Netzwerk, Netzwerk 0, wird erstellt
- Netzwerk 0 ist mit der PIF verbunden, um externe Konnektivität mit VMs zu ermöglichen

Wenn eine Installation von Citrix Hypervisor in einem markierten VLAN-Netzwerk durchgeführt wird, ist nach der Installation die folgende Konfiguration vorhanden:

- PIF werden für jede NIC im Host erstellt
- Die PIF für das getaggte VLAN auf der Netzwerkkarte, die für die Verwendung als Verwaltungsschnittstelle ausgewählt wurde, wird mit der während der Installation angegebenen IP-Adresskonfiguration konfiguriert.
- Für jedes PIF wird ein Netzwerk erstellt (z. B. Netzwerk 1, Netzwerk 2 usw.). Zusätzliches VLAN-Netzwerk wird erstellt (z. B. für Pool-weites Netzwerk, das eth0 auf VLAN zugeordnet ist <TAG>)
- Jedes Netzwerk ist mit einem PIF verbunden. Die VLAN-PIF ist für die Verwendung in Hostverwaltungsvorgängen festgelegt

In beiden Fällen ermöglicht die resultierende Netzwerkkonfiguration die Verbindung mit dem Citrix Hypervisor or-Server über XenCenter, die xe CLI und jede andere Verwaltungssoftware, die auf separaten Computern über die IP-Adresse der Verwaltungsschnittstelle ausgeführt wird. Die Konfiguration stellt auch externe Netzwerke für VMs bereit, die auf dem Host erstellt wurden.

Die PIF, die für Verwaltungsvorgänge verwendet wird, ist die einzige PIF, die jemals mit einer IP-Adresse während der Citrix Hypervisor Installation konfiguriert wurde. Eine externe Vernetzung für VMs wird durch die Überbrückung von PIF zu VIFs mithilfe des Netzwerkobjekts erreicht, das als virtueller Ethernet-Switch fungiert.

Die Schritte, die für Netzwerkfunktionen wie VLANs, NIC-Anleihen und das Einrichten einer Netzwerkkarte für Speicherdatenverkehr erforderlich sind, werden in den folgenden Abschnitten erläutert.

Netzwerkkonfiguration ändern

Sie können die Netzwerkkonfiguration ändern, indem Sie das Netzwerkobjekt ändern. Dazu führen Sie einen Befehl aus, der sich auf das Netzwerkobjekt oder das VIF auswirkt.

Ändern des Netzwerkobjekts

Sie können Aspekte eines Netzwerks ändern, z. B. die Frame-Größe (MTU), Name-Label, Name-Description, Zweck und andere Werte. Verwenden Sie den`network-param-set` Befehl xe und die zugehörigen Parameter, um die Werte zu ändern.

Wenn Sie dennetwork-param-set Befehl xe ausführen, ist der einzige erforderliche Parameteruuid .

Optionale Parameter sind:

- default_locking_mode. Siehe Vereinfachung der Konfiguration des VIF-Sperrmodus in der Cloud.
- name-**label**
- name-description
- MTU
- purpose. Siehe Hinzufügen eines Zwecks zu einem Netzwerk.
- other-config

Wenn kein Wert für einen Parameter angegeben wird, wird der Parameter auf einen Nullwert gesetzt. Verwenden Sie die Syntax, um ein (Schlüssel, Wert) Paar in einem Kartenparameter festzulegenmap-param:key=value.

Änderung der Up-Verzögerung für Anleihen

Die Bindung ist standardmäßig mit einer Up-Verzögerung von 31.000 ms eingerichtet, um zu verhindern, dass der Datenverkehr nach einem Ausfall auf eine Netzwerkkarte neu ausgeglichen wird. Während scheinbar lang, ist die Up-Delay für alle Bonding-Modi wichtig und nicht nur aktiv-aktiv.

Wenn Sie jedoch die geeigneten Einstellungen für die Auswahl Ihrer Umgebung kennen, können Sie die Up-Verzögerung für Anleihen ändern, indem Sie das folgende Verfahren verwenden.

Legen Sie die Up-Verzögerung in Millisekunden fest:

```
1 xe pif-param-set uuid=<uuid of bond master PIF> other-config:bond-
    updelay=<delay in ms>
```

Damit die Änderung wirksam wird, müssen Sie die physische Schnittstelle trennen und dann erneut anschließen:

```
1 xe pif-unplug uuid=<uuid of bond master PIF>
```

```
1 xe pif-plug uuid=<uuid of bond master PIF>
```

Kopiert!
Failed!

Verwalten von Netzwerken

October 16, 2019

Die Netzwerkkonfigurationsprozeduren in diesem Abschnitt unterscheiden sich je nachdem, ob Sie einen eigenständigen Server oder einen Server konfigurieren, der Teil eines Ressourcenpools ist.

Serverübergreifende private Netzwerke

In früheren Versionen von Citrix Hypervisor konnten Sie private Einzelserver-Netzwerke erstellen, mit denen VMs, die auf demselben Host ausgeführt werden, miteinander kommunizieren konnten. Die *serverübergreifende private Netzwerkfunktion* , die das private Einzelservernetzwerkkonzept erweitert, sodass VMs auf verschiedenen Hosts miteinander kommunizieren können. Serverübergreifende private Netzwerke kombinieren die gleichen Isolationseigenschaften eines privaten Netzwerks mit einem Server, jedoch mit der zusätzlichen Möglichkeit, Hosts über einen Ressourcenpool zu erstrecken. Diese Kombination ermöglicht die Verwendung von VM-Agilitätsfunktionen wie Live-Migration für VMs mit Verbindungen zu serverübergreifenden privaten Netzwerken.

Serverübergreifende private Netzwerke sind isoliert. VMs, die nicht mit dem privaten Netzwerk verbunden sind, können keinen Datenverkehr im Netzwerk ausschnüffeln oder injizieren. Dies geschieht auch dann, wenn sie sich auf demselben physischen Host befinden und VIFs mit einem Netzwerk auf demselben zugrunde liegenden physischen Netzwerkgerät (PIF) verbunden sind. VLANs bieten eine ähnliche Funktionalität. Im Gegensatz zu VLANs bieten serverübergreifende private Netzwerke jedoch Isolation, ohne dass eine Konfiguration einer physischen Switch-Fabric erforderlich ist, indem das GRE IP-Tunneling-Protokoll (Generic Routing Encapsulation) verwendet wird.

Private Netzwerke bieten die folgenden Vorteile, ohne dass ein physischer Switch erforderlich ist:

- Die Isolationseigenschaften privater Einzelserver-Netzwerke
- Die Möglichkeit, sich über einen Ressourcenpool zu erstrecken, sodass VMs, die mit einem privaten Netzwerk verbunden sind, auf mehreren Hosts innerhalb desselben Pools leben können
- Kompatibilität mit Funktionen wie Live-Migration

Erstellen Sie serverübergreifende private Netzwerke auf einer Verwaltungsschnittstelle oder einer sekundären Schnittstelle, da für diese eine IP-adressierbare Netzwerkkarte erforderlich ist. Sie können jede IP-fähige Netzwerkkarte als zugrunde liegende Netzwerk-Transport verwenden. Wenn Sie den serverübergreifenden privaten Netzwerkverkehr auf eine sekundäre Schnittstelle übertragen möchten, **muss** sich diese sekundäre Schnittstelle in einem separaten Subnetz befinden.

Wenn sich Verwaltungs- oder sekundäre Schnittstellen im selben Subnetz befinden, wird der Datenverkehr falsch weitergeleitet.

> **Hinweise:**
>
> Um ein serverübergreifendes privates Netzwerk zu erstellen, müssen die folgenden Bedingungen erfüllt sein:
>
> - Alle Hosts im Pool müssen Citrix Hypervisor 6.0 oder höher verwenden.
> - Alle Hosts im Pool müssen den vSwitch für den Netzwerkstapel verwenden.
> - Der vSwitch Controller muss ausgeführt werden, und Sie müssen den Pool hinzugefügt haben. (Für den Pool muss ein vSwitch Controller konfiguriert sein, der die Initialisierungs- und Konfigurationsaufgaben übernimmt, die für die vSwitch-Verbindung erforderlich sind.)
> - Sie müssen das serverübergreifende private Netzwerk auf einer Netzwerkkarte erstellen, die als Verwaltungsschnittstelle konfiguriert ist. Dies kann die Verwaltungsschnittstelle oder eine sekundäre Schnittstelle (IP-fähige PIF) sein, die Sie speziell für diesen Zweck konfigurieren, sofern sie sich in einem separaten Subnetz befindet.
>
> Weitere Informationen zum Konfigurieren des vSwitches finden Sie unter vSwitch und Controller. UI-basierte Verfahren zum Konfigurieren privater Netzwerke finden Sie in der XenCenter Hilfe.

Erstellen von Netzwerken auf einem eigenständigen Server

Da während der Hostinstallation externe Netzwerke für jede PIF erstellt werden, ist das Erstellen zusätzlicher Netzwerke in der Regel nur erforderlich, um:

- Verwenden eines privaten Netzwerks
- Unterstützung erweiterter Vorgänge wie VLANs oder NIC-Bonding

Informationen zum Hinzufügen oder Löschen von Netzwerken mit XenCenter finden Sie in der XenCenter-Hilfe.

Öffnen Sie die Textkonsole des Citrix Hypervisor or-Servers.

Erstellen Sie das Netzwerk mit dem Befehl network-create, der die UUID des neu erstellten Netzwerks zurückgibt:

```
1 xe network-create name-label=mynetwork
```

An diesem Punkt ist das Netzwerk nicht mit einem PIF verbunden und ist daher intern.

Erstellen von Netzwerken in Ressourcenpools

Alle Citrix Hypervisor or-Server in einem Ressourcenpool müssen dieselbe Anzahl physischer Netzwerkkarten (NICs) aufweisen. Diese Anforderung wird nicht strikt durchgesetzt, wenn ein Host mit einem Pool verbunden wird.

Da alle Hosts in einem Pool ein gemeinsames Netzwerk verwenden. Es ist wichtig, die gleiche physische Netzwerkkonfiguration für Citrix Hypervisor or-Server in einem Pool zu haben. PIF auf den einzelnen Hosts werden basierend auf dem Gerätenamen mit Pool-weiten Netzwerken verbunden. Beispielsweise verfügen alle Citrix Hypervisor or-Server in einem Pool mit eth0 NIC über eine entsprechende PIF an das Pool-weite`Network 0` Netzwerk angeschlossen. Dasselbe gilt für Hosts mit eth1-Netzwerkkarten und anderen Netzwerkkarten`Network 1`, die in mindestens einem Citrix Hypervisor or-Server im Pool vorhanden sind.

Wenn ein Citrix Hypervisor or-Server über eine andere Anzahl von Netzwerkkarten verfügt 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 Hosts *host1* und *host2* im selben Pool befinden und *host1* über vier Netzwerkkarten verfügt und *host2* nur zwei hat, sind nur die mit PIF verbundenen Netzwerke, die eth0 und eth1 entsprechen, auf *host2* gültig. VMs auf *host1* mit VIFs, die mit Netzwerken verbunden sind, die eth2 und eth3 entsprechen, können nicht zu Host *host2* migrieren.

Erstellen von VLANs

Für Server in einem Ressourcenpool können Sie den`pool-vlan-create` Befehl verwenden. Dieser Befehl erstellt das VLAN und erstellt automatisch die erforderlichen PIFs auf den Hosts im Pool und fügt sie ein. Weitere Informationen finden Sie unter pool-vlan-erstellen.

Öffnen Sie die Citrix Hypervisor -Serverkonsole.

Erstellen Sie ein Netzwerk für die Verwendung mit dem VLAN. Die UUID des neuen Netzwerks wird zurückgegeben:

```
1 xe network-create name-label=network5
```

Verwenden Sie den`pif-list` Befehl, um die UUID der PIF zu finden, die der physischen NIC entspricht, die das gewünschte VLAN-Tag unterstützt. Die UUIDs und Gerätenamen aller PIFs werden zurückgegeben, einschließlich vorhandener VLANs:

```
1 xe pif-list
```

Erstellen Sie ein VLAN-Objekt, das das gewünschte physische PIF- und VLAN-Tag auf allen VMs angibt, die mit dem neuen VLAN verbunden werden sollen. Eine neue PIF wird erstellt und an das angegebene Netzwerk angeschlossen. Die UUID des neuen PIF-Objekts wird zurückgegeben.

```
1 xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
```

Fügen Sie VM-VIFs an das neue Netzwerk an. Weitere Informationen Erstellen von Netzwerken auf einem eigenständigen Server finden Sie unter.

Erstellen von NIC-Anleihen auf einem eigenständigen Host

Wir empfehlen die Verwendung von XenCenter zum Erstellen von NIC-Anleihen. Anweisungen finden Sie in der XenCenter Hilfe.

In diesem Abschnitt wird beschrieben, wie Sie mithilfe der xe-CLI NIC-Schnittstellen auf Citrix Hypervisor or-Servern verbinden, die sich nicht in einem Pool befinden. Informationen zur Verwendung der xe-CLI zum Erstellen von NIC-Anleihen auf Citrix Hypervisor or-Servern, die einen Ressourcenpool bilden, finden Sie unter *Erstellen von NIC-Anleihen in Ressourcenpools*.

Erstellen einer NIC-Verbindung

Wenn Sie eine NIC verbinden, absorbiert die Bindung die PIF/NIC, die als Verwaltungsschnittstelle verwendet wird. Ab Citrix Hypervisor 6.0 wird die Verwaltungsschnittstelle automatisch auf die Anleihe-PIF verschoben.

1. Verwenden Sie den`network-create` Befehl, 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
   ```

2. Verwenden Sie den`pif-list` Befehl, um die UUIDs der PIF zu bestimmen, die in der Bindung verwendet werden sollen:

   ```
   xe pif-list
   ```

3. Führen Sie einen der folgenden Schritte aus:

   - Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den `bond-create` Befehl, um die Bindung zu erstellen. Geben Sie mithilfe von Kommas die neu erstellte Netzwerk-UUID und die UUIDs der zu gebundenen PIFs an:

     ```
     xe bond-create network-uuid=network_uuid /
          pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
     ```

     Geben Sie zwei UUIDs ein, wenn Sie zwei Netzwerkkarten und vier UUIDs verkleben, wenn Sie vier Netzwerkkarten miteinander vereinen. Die UUID für die Bindung wird nach dem Ausführen des Befehls zurückgegeben.

   - Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie die gleiche Syntax, fügen Sie den optionalen `mode` Parameter hinzu und geben Sie Folgendes `lacp` an `active-backup`:

     ```
     xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1
        , /
     ```



```
2       pif_uuid_2,pif_uuid_3,pif_uuid_4 /
3       mode=balance-slb | active-backup | lacp
```

Steuern Sie die MAC-Adresse der Anleihe

Wenn Sie die Verwaltungsschnittstelle verbinden, wird die PIF/NIC, die als Verwaltungsschnittstelle verwendet wird, subsumiert. Wenn der Host DHCP verwendet, entspricht die MAC-Adresse der Anleihe der verwendeten PIF/NIC. Die IP-Adresse der Verwaltungsschnittstelle kann unverändert bleiben.

Sie können die MAC-Adresse der Anleihe so ändern, dass sie sich von der MAC-Adresse für die (aktuelle) Verwaltungsschnittstellen-NIC unterscheidet. Da jedoch die Bindung aktiviert ist und sich die verwendete MAC/IP-Adresse ändert, werden vorhandene Netzwerksitzungen zum Host gelöscht.

Sie können die MAC-Adresse für eine Bindung auf zwei Arten steuern:

- Ein optionaler`mac` Parameter kann im`bond-create` Befehl angegeben werden. Sie können diesen Parameter verwenden, um die BindungsMAC-Adresse auf eine beliebige Adresse zu setzen.
- Wenn der`mac` Parameter nicht angegeben ist, verwendet Citrix Hypervisor die MAC-Adresse der Verwaltungsschnittstelle, wenn es sich um eine der Schnittstellen in der Bindung handelt. Wenn die Management-Schnittstelle nicht Teil der Anleihe ist, sondern eine andere Management-Schnittstelle ist, verwendet die Bindung die MAC-Adresse (und auch die IP-Adresse) dieser Management-Schnittstelle. Wenn keine der Netzwerkkarten in der Anleihe eine Verwaltungsschnittstelle ist, verwendet die Anleihe den MAC der ersten benannten NIC.

NIC-Anleihen zurücksetzen

Wenn Sie den Citrix Hypervisor or-Server auf eine nicht gebundene Konfiguration zurücksetzen, konfiguriert der`bond-destroy` Befehl automatisch den Primär-Slave als Schnittstelle für die Verwaltungsschnittstelle. Daher werden alle VIFs auf die Management-Schnittstelle verschoben. Wenn sich die Verwaltungsschnittstelle eines Hosts auf der getaggten VLAN-gebundenen Schnittstelle befindet, wird das Management-VLAN bei der Ausführung`bond-destroy`in den primären Slave verschoben.

Der Begriff Primär-Slave bezieht sich auf die PIF, aus der die MAC- und IP-Konfiguration beim Erstellen der Bindung kopiert wurde. Beim Verbinden von zwei Netzwerkkarten lautet der primäre Slave:

1. Die NIC 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, welches es ist, indem Sie Folgendes ausführen:

```
xe bond-list params=all
```

Erstellen von NIC-Anleihen in Ressourcenpools

Erstellen Sie nach Möglichkeit NIC-Anleihen im Rahmen der anfänglichen Erstellung eines Ressourcenpools, bevor Sie weitere Hosts mit dem Pool verbinden oder VMs erstellen. Dadurch kann die Bondkonfiguration automatisch auf Hosts repliziert werden, wenn sie mit dem Pool verbunden sind, und die Anzahl der erforderlichen Schritte wird reduziert.

Das Hinzufügen einer NIC-Bindung zu einem vorhandenen Pool erfordert einen der folgenden Schritte:

- Verwenden der CLI, um die Anleihen auf dem Master und dann jedes Mitglied des Pools zu konfigurieren.
- Verwenden der CLI, um Anleihen auf dem Master zu konfigurieren und dann jedes Pool-Mitglied neu zu starten, so dass es seine Einstellungen vom Master erbt.
- Konfigurieren der Bindungen auf dem Master mithilfe von XenCenter. XenCenter synchronisiert die Netzwerkeinstellungen auf den Mitgliedsservern automatisch mit dem Master, sodass Sie die Mitgliedsserver nicht neu starten müssen.

Zur Vereinfachung und zur Vermeidung von Fehlkonfiguration empfehlen wir die Verwendung von XenCenter zum Erstellen von NIC-Anleihen. Weitere Informationen finden Sie in der XenCenter Hilfe.

In diesem Abschnitt wird die Verwendung der xe-CLI zum Erstellen von gebundenen NIC-Schnittstellen auf Citrix Hypervisor or-Servern beschrieben, die einen Ressourcenpool umfassen. Informationen zur Verwendung der xe-CLI zum Erstellen von NIC-Anleihen auf einem eigenständigen Host finden Sie unter *Erstellen von NIC-Anleihen auf einem eigenständigen Host*.

> **Warnhinweis:**
>
> Versuchen Sie nicht, Netzwerkanleihen zu erstellen, wenn die hohe Verfügbarkeit aktiviert ist. Der Prozess der Bindungserstellung stört den laufenden Hochverfügbarkeits-Heartbeat und bewirkt, dass Hosts sich selbst zünden (sich selbst abschalten). Die Hosts können nicht ordnungsgemäß neu gestartet werden und benötigen möglicherweise den`host-emergency-ha-disable` Befehl zum Wiederherstellen.

Select den Host aus, der der Master sein soll. Der Master-Host 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
```

Erstellen Sie die NIC-Bindung wie unter beschriebenErstellen einer NIC-Verbindung.

Öffnen Sie eine Konsole auf einem Host, dem Sie dem Pool beitreten möchten, und führen Sie den folgenden Befehl aus:

```
xe pool-join master-address=host1 master-username=root master-password=
    password
```

Die Netzwerk- und Anleihinformationen werden automatisch auf den neuen Host repliziert. Die Verwaltungsschnittstelle wird automatisch von der Host-NIC, in der sie ursprünglich konfiguriert wurde, auf die gebundene PIF verschoben. Das heißt, die Management-Schnittstelle wird nun in die Anleihe aufgenommen, so dass die gesamte Anleihe als Management-Schnittstelle fungiert.

Verwenden Sie den`host-list` Befehl, um die UUID des zu konfigurierenden Hosts zu finden:

```
xe host-list
```

> **Warnung:**Versuchen
>
> Sie nicht, Netzwerkanleihen zu erstellen, wenn die hohe Verfügbarkeit aktiviert ist. Der Prozess der Bindungserstellung stört den laufenden Hochverfügbarkeits-Heartbeat und bewirkt, dass Hosts sich selbst zünden (sich selbst abschalten). Die Hosts können nicht ordnungsgemäß neu gestartet werden, und Sie müssen den`host-emergency-ha-disable` Befehl 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, z. B. dem Speicherdatenverkehr, zuzuweisen. Wenn Sie eine Netzwerkkarte mit einer IP-Adresse konfigurieren, erstellen Sie eine sekundäre Schnittstelle. (Die IP-fähige Netzwerkkarte Citrix Hypervisor, die 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. Damit soll sichergestellt werden, dass die Netzwerkkarte nur für den gewünschten Datenverkehr verwendet wird. Um eine Netzwerkkarte dem Speicherdatenverkehr zu widmen, konfigurieren Sie die Netzwerkkarte, das Speicherziel, den Switch und das VLAN so, dass das Ziel nur über die zugewiesene Netzwerkkarte zugänglich ist. Wenn Ihre physische und IP-Konfiguration den Datenverkehr, der über die Speicher-NIC gesendet wird, nicht einschränkt, können Sie Datenverkehr, z. B. Verwaltungsdatenverkehr über die sekundäre Schnittstelle senden.

Wenn Sie eine neue sekundäre Schnittstelle für Speicherdatenverkehr erstellen, müssen Sie ihr eine IP-Adresse zuweisen, die lautet:

- Im selben Subnetz wie der Speichercontroller, falls zutreffend, und
- Nicht im selben Subnetz wie andere sekundäre 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 die sekundäre Schnittstelle 1 und ein Subnetz für die sekundäre Schnittstelle 2.

Wenn Sie Bonding für die Ausfallsicherheit Ihres Speicherdatenverkehrs verwenden, sollten Sie möglicherweise LACP anstelle der Linux-Bridge-Bonding verwenden. Um LACP-Bonding zu verwenden, müssen Sie den vSwitch als Netzwerkstapel konfigurieren. Weitere Informationen finden Sie unter vSwitch-Netzwerke.

> **Hinweis:**
>
> Wenn Sie eine Netzwerkkarte auswählen, die als sekundäre Schnittstelle für die Verwendung mit iSCSI- oder NFS-SRs konfiguriert werden soll, stellen Sie sicher, dass die dedizierte Netzwerkkarte ein separates IP-Subnetz verwendet, das von der Verwaltungsschnittstelle nicht routingfähig ist. Wenn dies nicht erzwungen wird, kann der Speicherdatenverkehr nach einem Host-Neustart über die Hauptverwaltungsschnittstelle geleitet werden, da Netzwerkschnittstellen initialisiert werden.

Stellen Sie sicher, dass sich die PIF in einem separaten Subnetz befindet oder das Routing entsprechend Ihrer Netzwerktopologie konfiguriert ist, um den gewünschten Datenverkehr über die ausgewählte PIF zu erzwingen.

Richten Sie eine IP-Konfiguration für die PIF ein und fügen Sie entsprechende Werte für den Parameter mode hinzu. Wenn Sie die statische IP-Adressierung verwenden, fügen Sie die IP-, Netzmask-, Gateway- und DNS-Parameter hinzu:

```
1 xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
```

Setzen Sie den disallow-unplug-Parameter des PIF auf true:

```
1 xe pif-param-set disallow-unplug=true uuid=pif-uuid
```

```
1 xe pif-param-set other-config:management_purpose="Storage" uuid=pif-
    uuid
```


Wenn Sie eine sekundäre Schnittstelle für den Speicher verwenden möchten, die auch über die Management-Schnittstelle weitergeleitet werden kann (in Anbetracht der Tatsache, dass diese Konfiguration nicht die bewährte Vorgehensweise ist), haben Sie zwei Möglichkeiten:

- Stellen Sie nach einem Host-Neustart sicher, dass die sekundäre Schnittstelle korrekt konfiguriert ist. Verwenden Sie die`xe pbd-unplug` Befehle`xe pbd-plug` und, 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 Citrix Hypervisor Datenbank löschen und sie manuell in der Steuerdomäne konfigurieren. `xe pif-forget` ist eine erweiterte Option und erfordert, dass Sie sich mit der manuellen Konfiguration von Linux-Netzwerken vertraut machen.

Verwenden von SR-IOV-fähigen Netzwerkkarten

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 wird als Physical Function (PF) bezeichnet, während die anderen als Virtual Functions (VF) bezeichnet werden. Der Hypervisor kann einer virtuellen Maschine (VM) einen oder mehrere VFs zuweisen: Der Gast kann das Gerät dann so verwenden, als wäre es direkt zugewiesen.

Durch die Zuweisung einer oder mehrerer NIC-VFs zu einer VM kann der Netzwerkverkehr den virtuellen Switch umgehen. Bei der Konfiguration verhält sich jede VM so, als ob sie die Netzwerkkarte direkt verwendet, was den Verarbeitungsaufwand verringert und die Leistung verbessert.

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 NIC sicherstellen (unter Umgehung des Citrix Hypervisor Netzwerkstapels).

Mit dieser Funktion können Sie:

- Aktivieren Sie SR-IOV auf Netzwerkkarten, die SR-IOV unterstützen.
- Deaktivieren Sie SR-IOV auf Netzwerkkarten, die SR-IOV unterstützen.
- Verwalten von SR-IOV-VFs als VF-Ressourcenpool.
- Weisen Sie SR-IOV-VFs zu einer VM zu.
- Konfigurieren Sie SR-IOV-VFs (Zum Beispiel MAC-Adresse, VLAN, Rate).
- Führen Sie Tests durch, um zu bestätigen, ob SR-IOV als Teil des Automated Certification Kit unterstützt wird.

Systemkonfiguration

Konfigurieren Sie die Hardwareplattform ordnungsgemäß, um SR-IOV zu unterstützen. Folgende 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 des BIOS zur Aktivierung der genannten Technologien finden Sie in der Dokumentation Ihres Systems.

Aktivieren eines SR-IOV-Netzwerks auf einer Netzwerkkarte

Verwenden Sie in XenCenter den Assistenten „ **Neues Netzwerk** “ auf der Registerkarte „ **Netzwerk** “, um ein SR-IOV-Netzwerk auf einer Netzwerkkarte zu erstellen und zu aktivieren.

Zuweisen eines SR-IOV-Netzwerks zur virtuellen Schnittstelle (VM-Ebene)

Verwenden Sie in XenCenter auf VM-Ebene den Assistenten zum **Hinzufügen virtueller Schnittstelle** auf der Registerkarte **Netzwerk** , um ein SR-IOV-aktiviertes Netzwerk als virtuelle Schnittstelle für diese VM hinzuzufügen. Weitere Informationen finden Sie in der XenCenter Hilfe.

Unterstützte NICs und Gäste

Eine Liste der unterstützten Hardwareplattformen und Netzwerkkarten finden Sie unterHardwarekompatibilitätsli
Sehen Sie in der Dokumentation des Herstellers für einen bestimmten Gast, ob SR-IOV unterstützt wird.

Einschränkungen

- Bei bestimmten Netzwerkkarten, die Legacy-Treiber verwenden (z. B. Intel I350), muss der Host neu gestartet werden, um SR-IOV auf diesen Geräten zu aktivieren oder zu deaktivieren.
- Nur HVM-Gäste werden mit SR-IOV unterstützt.
- Ein SR-IOV-Netzwerk auf Poolebene mit unterschiedlichen NIC-Typen wird nicht unterstützt.

- Ein SR-IOV-VF und ein normaler VIF von derselben NIC können aufgrund der Einschränkungen der NIC-Hardware möglicherweise nicht miteinander kommunizieren. Damit diese Hosts kommunizieren können, stellen Sie sicher, dass die Kommunikation das Muster VF zu VF oder VIF zu VIF und nicht VF zu VIF verwendet.
- Die 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 VMs mit einem SR-IOV-VF nicht unterstützt.
- SR-IOV-VFs unterstützen kein Hot-Plug-ging.
- Bei einigen NICs mit Legacy-NIC-Treibern ist möglicherweise ein Neustart des Servers erforderlich, was darauf hinweist, dass die Netzwerkkarte SR-IOV nicht aktivieren kann.
- VMs, die in früheren Versionen erstellt wurden, können diese Funktion von XenCenter nicht verwenden.
- Wenn Ihre VM über eine SR-IOV-VF verfügt, sind Funktionen, die eine Live-Migration erfordern, nicht möglich. Dies liegt daran, dass die VM direkt an die physische SR-IOV-fähige NIC-VF gebunden ist. Jeder VM-Netzwerkverkehr, der über einen SR-IOV VF gesendet wird, umgeht den vSwitch. Daher ist es nicht möglich, ACLs zu erstellen oder Quality of Service (QoS) anzuzeigen.
- Hardwareeinschränkung: Die SR-IOV-Funktion setzt darauf, dass der Controller Gerätefunktionen auf einen makellosen Zustand innerhalb von 100 ms zurücksetzt, wenn er vom Hypervisor mit Funktion Level Reset (FLR) angefordert wird.
- SR-IOV kann in einer Umgebung verwendet werden, die hohe Verfügbarkeit nutzt. SR-IOV wird jedoch bei der Kapazitätsplanung nicht berücksichtigt. VMs, denen SR-IOV-VFs zugewiesen sind, werden nach bestem Aufwand neu gestartet, wenn sich im Pool ein Host befindet, der über entsprechende Ressourcen verfügt. Zu diesen Ressourcen gehören SR-IOV, die im richtigen Netzwerk aktiviert sind, und ein freier VF.

Konfigurieren von SR-IOV-VFs für Legacy-Treiber

Normalerweise kann die maximale Anzahl von VFs, die eine NIC unterstützen kann, automatisch ermittelt werden. Bei NICs, die Legacy-Treiber verwenden (z. B. Intel I350-Produktreibern), wird der Grenzwert in der Konfigurationsdatei des Treibermoduls festgelegt. 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 beginnend:

```
## VFs-maxvfs-by-user:
```

Um beispielsweise die maximale VFs auf 4 zu setzen, damit der igb-Treiber bearbeitet/`etc/modprobe.d/igb.conf` wird:


```
## VFs-param: max_vfs
## VFs-maxvfs-by-default: 7
## VFs-maxvfs-by-user: 4
options igb max_vfs=0
```

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 der Aktivierung von SR-IOV vor.

CLI

CLI-AnweisungenSR-IOV-Befehlezum Erstellen, Löschen, Anzeigen von SR-IOV-Netzwerken und Zuweisen eines SR-IOV-VF zu einer VM finden Sie unter.

Steuern der Rate ausgehender Daten (QoS)

Um die Menge der *ausgehenden* Daten zu begrenzen, die eine VM pro Sekunde senden kann, legen Sie einen optionalen QoS-Wert (Quality of Service) für virtuelle VM-Schnittstellen (VIFs) fest. Mit dieser Einstellung können Sie eine maximale Übertragungsrate für ausgehende Pakete in *Kilobyte* pro Sekunde festlegen.

Der Wert Quality of Service begrenzt die Übertragungsrate *von* der VM. Die Einstellung Quality of Service beschränkt nicht die Datenmenge, die die VM empfangen kann. Wenn ein solches Limit gewünscht wird, empfehlen wir, die Rate der eingehenden Pakete im Netzwerk höher zu begrenzen (z. B. auf Switch-Ebene).

Je nach Netzwerkstapel, der im Pool konfiguriert ist, können Sie den Wert Quality of Service auf virtuellen VM-Schnittstellen (VIFs) an zwei Stellen festlegen. Entweder auf dem vSwitch Controller oder in Citrix Hypervisor (mit CLI oder XenCenter).

vSwitch

Konfigurationsmethoden:

- **vSwitch Controller** Dies ist die bevorzugte Methode zum Einstellen der maximalen Übertragungsrate eines VIF, wenn der vSwitch der Netzwerkstapel ist. Bei Verwendung des vSwitch-Stacks ist die Option XenCenter Quality of Service nicht verfügbar.

- **xe Befehle** Es ist möglich, die Übertragungsrate von Quality of Service mithilfe der Befehle im folgenden Beispiel festzulegen. Die bevorzugte Methode ist jedoch die vSwitch Controller Benutzeroberfläche, die eine feinere Steuerung bietet.

Linux-Brücke

Verfügbare Konfigurationsmethoden:

- **XenCenter** Sie können den Grenzwert für die Qualitätsübermittlung für die Übertragungsrate im Eigenschaftendialog für die virtuelle Schnittstelle festlegen.
- **xe-Befehle** Sie können die Übertragungsrate von Quality of Service mithilfe der Befehlszeilenschnittstelle mithilfe der Befehle im folgenden Abschnitt festlegen.

> **Wichtig:**
>
> Wenn vSwitch als Netzwerkstapel konfiguriert ist, ist es möglich, einen QoS-Wert versehentlich auf dem vSwitch Controller *und* innerhalb des Citrix Hypervisor or-Servers zu konfigurieren. In diesem Fall beschränkt Citrix Hypervisor den ausgehenden Datenverkehr mit der niedrigsten Rate, die Sie festgelegt haben.

Beispiel für den CLI-Befehl für QoS:

Um eine VIF auf eine maximale Übertragungsrate von 100 Kilobyte pro Sekunde mit der Befehlszeilenschnittstelle zu beschränken, verwenden Sie den`vif-param-set` folgenden Befehl:

```
1 xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
2 xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
```

> **Hinweis:**
>
> Wenn Sie den vSwitch Controller verwenden, empfehlen wir, anstelle dieses CLI-Befehls die Übertragungsrate im vSwitch Controller festzulegen. Hinweise zum Einstellen des QoS-Grenzwerts im vSwitch Controller finden Sie untervSwitch und Controller.

Ändern der Netzwerkkonfigurationsoptionen

In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkkonfiguration Ihres Citrix Hypervisor or-Servers ändern. Es beinhaltet:

- Ändern des Hostnamens (d. h. des DNS-Namenssystems)
- Hinzufügen oder Löschen von DNS-Servern
- Ändern von IP-Adressen
- Ändern der Netzwerkkarte, die als Verwaltungsschnittstelle verwendet wird

- Hinzufügen einer neuen physischen Netzwerkkarte zum Server
- Hinzufügen eines Zwecks zu einem Netzwerk
- Aktivieren der ARP-Filterung (Switch-Port-Verriegelung)

Hostname

Der Systemhostname, auch als Domänen- oder DNS-Name bezeichnet, wird in der Pool-weiten Datenbank definiert und mit dem`xe host-set-hostname-live` CLI-Befehl wie folgt geändert:

```
xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
```

Der zugrunde liegende Steuerdomänenhostname 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 Citrix Hypervisor-Servers hinzuzufügen oder zu löschen. Zum Beispiel für einen PIF mit einer statischen IP:

```
pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip
```

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`pif-reconfigure-ip` CLI-Befehl. pif-reconfigure-ipWeitere Informationen zu den Parametern des`pif-reconfigure-ip`Befehls finden Sie unter. Weitere Informationen zum Ändern von Host-IP-Adressen in Ressourcenpools finden Sie im folgenden Abschnitt.

Ändern der IP-Adresskonfiguration in Ressourcenpools

Citrix Hypervisor or-Server in Ressourcenpools verfügen über eine einzige Verwaltungs-IP-Adresse, die für die Verwaltung und Kommunikation zu und von anderen Hosts im Pool verwendet wird. Die zum Ändern der IP-Adresse der Verwaltungsschnittstelle eines Hosts erforderlichen Schritte sind für Master- und andere Hosts unterschiedlich.

> **Hinweis:**
>
> Sie müssen vorsichtig sein, wenn Sie die IP-Adresse eines Servers und andere Netzwerkparameter ändern. Abhängig von der Netzwerktopologie und der vorgenommenen Änderung können Verbindungen zum Netzwerkspeicher verloren gehen. In diesem Fall muss der Speicher mithilfe der Funktion „ **Speicher reparieren** “ in XenCenter oder mithilfe des`pbd-plug` CLI-Befehls neu angeschlossen werden. Aus diesem Grund empfehlen wir, VMs vom Server weg zu migrieren, bevor die IP-Konfiguration geändert wird.

Verwenden Sie den`pif-reconfigure-ip` CLI-Befehl, um die IP-Adresse wie gewünscht festzulegen. pif-reconfigure-ipWeitere Informationen zu den Parametern des`pif-reconfigure-ip`Befehls finden Sie unter. :

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

Verwenden Sie den`host-list` CLI-Befehl, um zu bestätigen, dass der Mitgliedshost erfolgreich wieder eine Verbindung zum Master-Host hergestellt hat, indem Sie überprüfen, ob alle anderen Citrix Hypervisor or-Server im Pool sichtbar sind:

```
xe host-list
```

Das Ändern der IP-Adresse des Citrix Hypervisor ormasterservers erfordert zusätzliche Schritte. Dies liegt daran, dass jedes Poolmitglied die angekündigte IP-Adresse des Poolmasters für die Kommunikation verwendet. Die Poolmitglieder wissen nicht, wie sie den Master kontaktieren, wenn sich seine IP-Adresse ändert.

Verwenden Sie nach Möglichkeit eine dedizierte IP-Adresse, die sich wahrscheinlich nicht für die Lebensdauer des Pools für Poolmaster ändert.

Verwenden Sie den`pif-reconfigure-ip` CLI-Befehl, um die IP-Adresse wie gewünscht festzulegen:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

Wenn sich die IP-Adresse des Poolmasters ändert, wechseln alle Mitgliedshosts in einen Notfallmodus, wenn sie den Master-Host nicht kontaktieren können.

Verwenden Sie den`pool-recover-slaves` Befehl auf dem Poolmaster, um den Master zu erzwingen, sich mit jedem Pool-Mitglied in Verbindung zu setzen und ihn über die neue Master-IP-Adresse zu informieren:

```
xe pool-recover-slaves
```


Verwaltungsoberfläche

Wenn Citrix Hypervisor auf einem Host mit mehreren Netzwerkkarten installiert ist, wird eine Netzwerkkarte für die Verwendung als Verwaltungsschnittstelle ausgewählt. Die Verwaltungsschnittstelle wird für XenCenter Verbindungen mit dem Host und für die Host-zu-Host-Kommunikation verwendet.

Verwenden Sie den`pif-list` Befehl, um zu bestimmen, welche PIF der NIC entspricht, die als Verwaltungsschnittstelle verwendet werden soll. Die UUID jedes PIF wird zurückgegeben.

```
1 xe pif-list
```

Verwenden Sie den`pif-param-list` Befehl, um die IP-Adressierungskonfiguration für die PIF zu überprüfen, die für die Verwaltungsschnittstelle verwendet wird. Verwenden Sie ggf. den `pif-reconfigure-ip` Befehl, um die IP-Adressierung für die zu verwendende PIF zu konfigurieren.

```
1 xe pif-param-list uuid=pif_uuid
```

Verwenden Sie den`host-management-reconfigure` CLI-Befehl, um die PIF zu ändern, die für die Verwaltungsschnittstelle verwendet wird. Wenn dieser Host Teil eines Ressourcenpools ist, *muss dieser Befehl auf der Mitgliedshostkonsole ausgegeben werden*:

```
1 xe host-management-reconfigure pif-uuid=pif_uuid
```

Verwenden Sie den`network-list` Befehl, um zu bestimmen, welche PIF der NIC entspricht, die als Verwaltungsschnittstelle für alle Hosts im Pool verwendet werden soll. Die UUID des poolweiten Netzwerks wird zurückgegeben.

```
1 xe network-list
```

Verwenden Sie den`network-param-list` Befehl, um die PIF-UUIDs aller Hosts im Pool abzurufen. Verwenden Sie den`pif-param-list` Befehl, um die IP-Adressierungskonfiguration für die PIF für die Verwaltungsschnittstelle zu überprüfen. Verwenden Sie ggf. den `pif-reconfigure-ip` Befehl, um die IP-Adressierung für die zu verwendende PIF zu konfigurieren.

```
1 xe pif-param-list uuid=pif_uuid
```

Verwenden Sie den Befehl`pool-management-reconfigure` CLI, um die PIF zu ändern, die für die in der Liste Netzwerke aufgelistete Verwaltungsschnittstelle verwendet wird.

```
1 xe pool-management-reconfigure network-uuid=network_uuid
```


Deaktivieren des Verwaltungszugriffs

Verwenden Sie den`host-management-disable` CLI-Befehl, um den Remotezugriff auf die Verwaltungskonsole vollständig zu deaktivieren.

> **Warnhinweis:**
>
> Wenn die Verwaltungsschnittstelle deaktiviert ist, müssen Sie sich bei der physischen Hostkonsole anmelden, um Verwaltungsaufgaben auszuführen. Externe Schnittstellen wie XenCenter funktionieren nicht, wenn die Verwaltungsschnittstelle deaktiviert ist.

Hinzufügen einer neuen physischen Netzwerkkarte

Installieren Sie eine neue physische Netzwerkkarte auf dem Citrix Hypervisor or-Server auf die übliche Weise. Führen Sie dann nach dem Neustart des Servers den Befehl xe CLI-Befehl aus,`pif-scan` um ein neues PIF-Objekt für die neue Netzwerkkarte zu erstellen.

Hinzufügen eines Zwecks zu einem Netzwerk

Der Netzwerkzweck kann verwendet werden, um zusätzliche Funktionalitäten zu einem Netzwerk hinzuzufügen. Zum Beispiel die Möglichkeit, das Netzwerk zu verwenden, um NBD-Verbindungen herzustellen.

Um einen Netzwerkzweck hinzuzufügen, verwenden Sie den`xe network-param-add` folgenden Befehl:

```
1 xe network-param-add param-name=purpose param-key=purpose uuid=network-
    uuid
```

Um einen Netzwerkzweck zu löschen, verwenden Sie den`xe network-param-remove` folgenden Befehl:

```
1 xe network-param-remove param-name=purpose param-key=purpose uuid=
    network-uuid
```

Derzeit sind die verfügbaren Werte für den Netzwerkzweck`nbd` und`insecure_nbd` . Weitere Informationen finden Sie unter Citrix Hypervisor Changed Block Tracking Guide.

Switch-Port-Verriegelung verwenden

Mit der Citrix Hypervisor or-Switch-Port-Sperrfunktion können Sie den Datenverkehr steuern, der von unbekannten, nicht vertrauenswürdigen oder potenziell feindlichen VMs gesendet wird, indem

Sie ihre Fähigkeit einschränken, so zu tun, als hätten sie eine MAC- oder IP-Adresse, die ihnen nicht zugewiesen wurde. Mit den Port-Locking-Befehlen können Sie standardmäßig den gesamten Datenverkehr in einem Netzwerk blockieren oder bestimmte IP-Adressen definieren, von denen eine einzelne VM Datenverkehr senden darf.

Switch-Port-Sperrung ist eine Funktion, die für öffentliche Cloud-Service-Provider in Umgebungen entwickelt wurde, die sich um interne Bedrohungen kümmern. Diese Funktionalität unterstützt öffentliche Cloud-Service-Provider, die über eine Netzwerkarchitektur verfügen, in der jede VM über eine öffentliche, mit dem Internet verbundene IP-Adresse verfügt. Da Cloudmandanten nicht vertrauenswürdig sind, können Sie Sicherheitsmaßnahmen wie Spoofing-Schutz verwenden, um sicherzustellen, dass Mandanten andere virtuelle Maschinen in der Cloud nicht angreifen können.

Mit der Switch-Port-Sperrung können Sie Ihre Netzwerkkonfiguration vereinfachen, indem Sie allen Mandanten oder Gästen die Nutzung des gleichen Layer-2-Netzwerks ermöglichen.

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, vorzutäuschen, dass er eine MAC- oder IP-Adresse hat, die er nicht besitzt. Insbesondere können Sie diese Befehle verwenden, um zu verhindern, dass ein Gast:

- Inanspruchnahme einer anderen IP-Adresse oder MAC-Adresse als der vom Citrix Hypervisor Administrator angegebenen IP-Adresse
- Abfangen, Spoofing oder Unterbrechen des Datenverkehrs anderer VMs

Anforderungen

- Die Citrix Hypervisor or-Switch-Port-Sperrfunktion wird auf den Linux-Bridge- und vSwitch-Netzwerkstacks unterstützt.
- Wenn Sie Role Based Access Control (Role Based Access Control, RBAC) in Ihrer Umgebung aktivieren, muss der Benutzer, der die Switch-Port-Sperre konfiguriert, mit einem Konto angemeldet sein, das mindestens eine Pool-Operator- oder Pool-Admin-Rolle besitzt. Wenn RBAC in Ihrer Umgebung nicht aktiviert ist, muss der Benutzer mit dem Stammkonto für den Poolmaster angemeldet sein.
- Wenn Sie die Switch-Port-Sperrbefehle ausführen, können Netzwerke online oder offline sein.
- In Windows Gästen wird das Symbol „Netzwerk getrennt“ nur angezeigt, wenn Citrix VM Tools im Gast installiert sind.

Notizen

Ohne Switch-Port-Sperrkonfigurationen werden VIFs auf „network_default“ und Netzwerke auf „entsperrt“ gesetzt. „

Die Konfiguration der Switch-Port-Sperrung wird nicht unterstützt, wenn der vSwitch-Controller und andere Controller von Drittanbietern in der Umgebung verwendet werden.

Die Switch-Port-Sperrung verhindert nicht, dass Cloud-Mandanten:

- Durchführen eines IP-Level-Angriffs auf einen anderen Mandanten/Benutzer. Die Switch-Port-Sperrung verhindert jedoch, dass sie den Angriff auf IP-Ebene ausführen, wenn sie versuchen, dies zu tun, und die Switch-Port-Sperre konfiguriert ist: a) die Identität eines anderen Mandanten in der Cloud oder des Benutzers oder b) das Einleiten eines für einen anderen Benutzer bestimmten Datenverkehrs.
- Ausschöpfende Netzwerkressourcen.
- Empfangen von Datenverkehr, der für andere virtuelle Maschinen bestimmt ist, durch normales Switch-Überflutungsverhalten (für Broadcast-MAC-Adressen oder unbekannte Ziel-MAC-Adressen).

Ebenso beschränkt die Switch-Port-Sperre nicht, an die eine VM Datenverkehr senden kann.

Implementierungshinweise

Sie können die Switch-Port-Sperrfunktion entweder mithilfe der Befehlszeile oder der Citrix Hypervisor API implementieren. In großen Umgebungen, in denen die Automatisierung ein Hauptanliegen ist, kann die typischste Implementierungsmethode jedoch die Verwendung der API sein.

Beispiele

Dieser Abschnitt enthält Beispiele dafür, wie Switch-Port-Sperren bestimmte Arten von Angriffen verhindern kann. In diesen Beispielen ist VM-C eine virtuelle Maschine, die ein feindseliger Mandant (Tenant C) leacht und für Angriffe verwendet. VM-a und VM-b sind virtuelle Maschinen, die von nicht angreifenden Mandanten geleast werden.

Beispiel 1: Wie die Switch-Port-Sperre ARP-Spoofing verhindern kann:

ARP-Spoofing wird verwendet, um anzuzeigen, dass ein Angreifer versucht, seine MAC-Adresse mit der IP-Adresse eines anderen Knotens zu verknüpfen. ARP-Spoofing kann möglicherweise dazu führen, dass der Datenverkehr des Knotens an den Angreifer gesendet wird. Um dieses Ziel zu erreichen, sendet der Angreifer gefälschte (gefälschte) ARP-Nachrichten an ein Ethernet-LAN.

Szenario:

Virtual Machine A (VM-a) möchte IP-Datenverkehr von VM-a an Virtual Machine B (VM-b) senden, indem sie an die IP-Adresse von VM-b adressieren. Der Besitzer von Virtual Machine C möchte ARP-Spoofing verwenden, um so zu tun, als wäre ihre VM, VM-c, tatsächlich VM-b.

1. VM-c sendet einen spekulativen Stream von ARP-Antworten an VM-a. Die ARP-Antworten behaupten, dass die MAC-Adresse in der Antwort (C_Mac) mit der IP-Adresse b_IP verknüpft ist

Ergebnis: Da der Administrator die Switch-Port-Sperre aktiviert hat, werden diese Pakete alle gelöscht, da die Aktivierung der Switch-Port-Sperre den Identitätswechsel verhindert.

2. VM-b sendet eine ARP-Antwort an VM-a, die behauptet, dass die MAC-Adresse in der Antwort (B_Mac) der IP-Adresse b_IP zugeordnet ist.

   Ergebnis: VM-a erhält die ARP-Antwort von VM-b.

Beispiel 2: Schutz vor IP-Spoofing:

IP-Adressen-Spoofing ist ein Prozess, der die Identität von Paketen verdeckt, indem IP-Pakete (Internet Protocol) mit einer gefälschten Quell-IP-Adresse erstellt werden.

Szenario:

Mandant C versucht, einen Denial-of-Service-Angriff mit seinem Host, Host-C, auf einem Remote-System durchzuführen, um ihre Identität zu verschleiern.

Versuch 1:

Mandant C setzt die IP-Adresse und die 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-Datenverkehr an ein Remote-System zu senden.

Ergebnis: Die Host-C-Pakete werden gelöscht. Dies liegt daran, dass der Administrator die Switch-Port-Sperre aktiviert hat. Die Host-C-Pakete werden gelöscht, da die Aktivierung der Switch-Port-Sperrung die Identitätswechsel verhindert.

Versuch 2:

Mandant C setzt die IP-Adresse von Host-C auf die IP-Adresse von VM-a (a_IP) und behält ihre ursprüngliche C_Mac bei.

Mandant C weist Host-C an, IP-Datenverkehr an ein Remote-System zu senden.

Ergebnis: Die Host-C-Pakete werden gelöscht. Dies liegt daran, dass der Administrator die Switch-Port-Sperre aktiviert hat, wodurch Identitätswechsel verhindert werden.

Beispiel 3: Webhosting:

Szenario:

Alice ist Infrastrukturadministrator.

Einer ihrer Mieter, Mieter B, hostet mehrere Websites von ihrer VM, VM-b. Jede Website benötigt eine eigene IP-Adresse, die auf derselben virtuellen Netzwerkschnittstelle (VIF) gehostet wird.

Alice konfiguriert Host-B VIF so neu, dass sie auf einem einzigen MAC, aber viele IP-Adressen gesperrt werden.

Funktionsweise der 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, bestimmen, wie Pakete gefiltert werden. Sie können die VIF so einstellen, dass die VM keinen Datenverkehr sendet, die VIF so beschränken, dass sie nur Datenverkehr mit der zugewiesenen IP-Adresse senden kann, oder es der VM erlauben, Datenverkehr an eine beliebige IP-Adresse im Netzwerk zu senden, die mit dem VIF verbunden ist.
- **Netzwerkebene**. Das Citrix Hypervisor 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 das Feature auf die gleiche Weise. Wie jedoch in den folgenden Abschnitten ausführlicher beschrieben, unterstützt die Linux-Bridge die Switch-Port Sperren in IPv6 nicht vollständig.

VIF-Sperrmoduszustände

Die Citrix Hypervisor or-Switch-Port-Sperrfunktion bietet einen Sperrmodus, mit dem Sie VIFs in vier verschiedenen Zuständen konfigurieren können. Diese Zustände gelten nur, wenn das VIF an eine ausgeführte virtuelle Maschine angeschlossen ist.

! [Diese Abbildung zeigt, wie sich drei verschiedene VIF-Sperrmoduszustände verhalten, wenn der Netzwerksperrmodus auf Entsperrt eingestellt ist und der VIF-Status konfiguriert ist. Im ersten Bild ist der VIF-Status standardmäßig festgelegt, sodass kein Datenverkehr von der VM gefiltert wird. Das VIF sendet oder empfängt keine Pakete, da der Sperrmodus`disabled` im zweiten Bild auf eingestellt ist. Im dritten Bild ist der VIF-Status auf gesperrt festgelegt. Das bedeutet, dass das VIF Pakete nur dann senden kann, wenn diese Pakete die richtige MAC und IP-Adresse enthalten.] (/en-us/citrix-hypervisor/media/vif-switch-port-locking-modes.png)

- **Network_default**. Wenn der VIF-Status auf festgelegt ist`network_default`, verwendet Citrix Hypervisor den**`default-locking-mode`**Netzwerkparameter, um zu ermitteln, ob und wie Pakete gefiltert werden, die durch das VIF übertragen werden. Das Verhalten variiert je nachdem, ob für das zugeordnete Netzwerk der Standardsparameter für den Netzwerksperrmodus auf deaktiviert oder entsperrt festgelegt ist:

  -**`default-locking-mode=disabled`**, wendet Citrix Hypervisor eine Filterregel an, damit die VIF den gesamten Datenverkehr löscht.

  -**`default-locking-mode`**=entsperrt, entfernt Citrix Hypervisor alle Filterregeln, die mit der VIF verknüpft sind. Standardmäßig ist der Standardparameter für den Sperrmodus auf eingestellt`unlocked`.

  Hinweise zum**`default-locking-mode`** Parameter finden Sie unterNetzwerkbefehle .

Der Standardsperrmodus des Netzwerks hat keine Auswirkungen auf angeschlossene VIFs, deren Sperrstatus etwas anderes ist als`network_default`.

> **Hinweis:**
>
> Ein Netzwerk, das**`default-locking-mode`** aktive VIFs besitzt, kann nicht geändert werden.

- **Verriegelt**. Citrix Hypervisor wendet Filterregeln an, sodass nur Datenverkehr, der an die angegebene MAC- und IP-Adressen gesendet wird, über das VIF gesendet werden darf. Wenn in diesem Modus keine IP-Adressen angegeben sind, kann die VM keinen Datenverkehr über diese VIF in diesem Netzwerk senden.

  Um die IP-Adressen anzugeben, von denen das VIF Datenverkehr akzeptiert, verwenden Sie die IPv4- oder IPv6-IP-Adressen mithilfe der`ipv4_allowed` Parameter`ipv6_allowed` oder. Wenn Sie jedoch die Linux-Brücke konfiguriert haben, geben Sie keine IPv6-Adressen ein.

  Mit Citrix Hypervisor können Sie IPv6-Adressen eingeben, wenn die Linux-Brücke aktiv ist. Citrix Hypervisor kann jedoch nicht anhand der eingegebenen IPv6-Adressen filtern. Der Grund dafür ist, dass die Linux-Brücke keine Module zum Filtern von Neighbor Discovery Protocol (NDP) -Paketen hat. Daher kann kein vollständiger Schutz implementiert werden, und Gäste könnten sich durch Fälschen von NDP-Paketen einen anderen Gast ausgeben. Wenn Sie also nur eine IPv6-Adresse angeben, lässt Citrix Hypervisor den gesamten IPv6-Datenverkehr durch das VIF leiten. Wenn Sie keine IPv6-Adressen angeben, lässt Citrix Hypervisor keinen IPv6-Datenverkehr an die VIF passieren.

- **Entsperrt**. Der gesamte Netzwerkverkehr kann durch das VIF geleitet werden. Das heißt, keine Filter werden auf einen Datenverkehr angewendet, der zum VIF oder aus dem VIF geht.
- **Deaktiviert**. Es ist kein Verkehr durch die VIF erlaubt. (Das heißt, Citrix Hypervisor wendet eine Filterregel an, damit die VIF den gesamten Datenverkehr löscht.)

Konfigurieren der Switch-Port-Sperre

Dieser Abschnitt enthält drei verschiedene Verfahren:

- Einschränken von VIFs auf die Verwendung einer bestimmten IP-Adresse
- Fügen Sie eine IP-Adresse zu einer vorhandenen eingeschränkten Liste hinzu. Zum Beispiel, um einer VIF eine IP-Adresse hinzuzufügen, wenn die VM ausgeführt wird und mit dem Netzwerk verbunden ist (z. B. wenn Sie ein Netzwerk vorübergehend offline schalten).
- Entfernen einer IP-Adresse aus einer vorhandenen eingeschränkten Liste

Wenn der Sperrmodus eines VIF auf eingestellt ist`locked`, können nur die Adressen verwendet werden, die in den`ipv4-allowed`Parametern`ipv6-allowed`oder angegeben sind.

Da VIFs in einigen relativ seltenen Fällen mehr als eine IP-Adresse haben können, können mehrere IP-Adressen für ein VIF angegeben werden.

Sie können diese Prozeduren vor oder nach dem Einstecken des VIF durchführen (oder die VM gestartet wird).

Ändern Sie den Standardsperrmodus in „Gesperrt“, wenn dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

```
1 xe vif-param-set uuid=vif-uuid locking-mode=locked
```

Die`vif-uuid` stellt die UUID der VIF dar, die zum Senden von Datenverkehr zugelassen werden soll. Um die UUID zu erhalten, führen Sie den`vif-list` Befehl xe auf dem Host aus. `vm-uuid` Gibt die virtuelle Maschine an, für die die Informationen angezeigt werden. Die Geräte-ID gibt die Gerätenummer des VIF an.

Führen Sie den`vif-param-set` Befehl 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 mindestens ein IPv4-IP-Adressenziel an. Zum Beispiel:

```
1 xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list
    of ipv4-addresses
```

- Geben Sie mindestens ein IPv6-IP-Adressenziel an. Zum Beispiel:

```
1 xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list
    of ipv6-addresses
```

Sie können mehrere IP-Adressen angeben, indem Sie sie durch ein Komma trennen, wie im vorherigen Beispiel gezeigt.

Nachdem Sie das Verfahren zum Beschränken einer 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`vif-param-add` Befehl aus, um die IP-Adressen der vorhandenen Liste hinzuzufügen. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Geben Sie die IPv4-IP-Adresse an. Zum Beispiel:

```
1 xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list
    of ipv4-addresses
```

- Geben Sie die IPv6-IP-Adresse an. Zum Beispiel:

```
1 xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list
    of ipv6-addresses
```


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`vif-param-remove` Befehl 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. Zum Beispiel:

```
xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated
   list of ipv4-addresses
```

- Geben Sie die zu löschende IPv6-IP-Adresse an. Zum Beispiel:

```
xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated
   list of ipv6-addresses
```

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 ein VIF eine Verbindung zu einem bestimmten Citrix Hypervisor Netzwerk herstellt, können Sie dieses Verfahren verwenden, um zu verhindern, dass eine virtuelle Maschine Datenverkehr von einem bestimmten Netzwerk sendet oder empfängt. Dies bietet eine detailliertere Steuerungsebene als das Deaktivieren 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 noch vorhanden zu sein, die VIF löscht jedoch alle Pakete, die die VM zu senden versucht.

> **Tipp:**
>
> Um die UUID eines VIF zu finden, führen Sie den`vif-list` Befehl xe auf dem Host aus. Die Geräte-ID gibt die Gerätenummer des VIF an.

Um zu verhindern, dass ein VIF Datenverkehr empfängt, deaktivieren Sie die VIF, die mit dem Netzwerk verbunden ist, von dem aus die VM den Datenverkehr nicht empfängt:

```
xe vif-param-set uuid=vif-uuid locking-mode=disabled
```

Sie können die VIF auch in XenCenter deaktivieren, indem Sie die virtuelle Netzwerkschnittstelle auf der Registerkarte „Netzwerk“ der VM auswählen und auf „Deaktivieren“ klicken.

Entfernen der Einschränkung eines VIF auf eine IP-Adresse

Gehen Sie folgendermaßen vor, um den Standardstatus (Original-) Sperrmodus wiederherzustellen. Wenn Sie eine VIF erstellen, konfiguriert Citrix Hypervisor diese 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 VIF-Standardsperrmodus in „Entsperrt“. Wenn dieser Modus nicht bereits verwendet wird, führen Sie den folgenden Befehl aus:

```
1 xe vif-param-set uuid=vif_uuid locking-mode=unlocked
```

Vereinfachte Konfiguration des VIF-Sperrmodus in der Cloud

Anstatt die Befehle für den VIF-Sperrmodus für jede VIF auszuführen, können Sie sicherstellen, dass alle VIFs standardmäßig deaktiviert sind. Dazu müssen Sie die Paketfilterung auf Netzwerkebene ändern. Das Ändern der Paketfilterung bewirkt, dass das Citrix Hypervisor Netzwerk bestimmt, wie Pakete gefiltert werden, wie im vorherigen Abschnitt *Funktionsweise der Switch-Port-Sperrung*beschrieben.

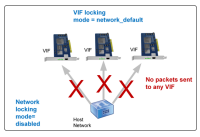
Insbesondere legt die`default-locking-mode` Einstellung eines Netzwerks fest, wie sich neue VIFs mit Standardeinstellungen verhalten. Wenn ein VIF auf eingestellt`locking-mode` ist`default` , bezieht sich der VIF auf den Netzwerksperrmodus (`default-locking-mode`), um zu bestimmen, ob und wie Pakete gefiltert werden, die durch das VIF geleitet werden:

- **Entsperrt**. Wenn der`default-locking-mode` Netzwerkparameter auf festgelegt ist`unlocked` , lässt Citrix Hypervisor die VM Datenverkehr an eine beliebige IP-Adresse im Netzwerk senden, mit der das VIF eine Verbindung herstellt.
- **Deaktiviert**. Wenn der`default-locking-mode` Parameter auf festgelegt ist`disabled` , wendet Citrix Hypervisor eine Filterregel an, sodass die VIF den gesamten Datenverkehr löscht.

Standardmäßig sind die`default-locking-mode` für alle in XenCenter erstellten und mit der CLI erstellten Netzwerke auf eingestellt`unlocked` .

Wenn Sie den Sperrmodus des VIF auf den Standardmodus (`network_default`) festlegen, 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 das VIF, wenn ein VIF auf seine Standardeinstellung (`locking-mode`) gesetzt`network_default` ist, das Netzwerk verwendet,`default-locking-mode` um sein Verhalten zu bestimmen.



Beispielsweise werden VIFs standardmäßig mit ihrer`locking-mode` Einstellung auf erstellt`network_default` . Wenn Sie das`default-locking-mode`= eines Netzwerks festlegen`disabled`, werden alle neuen

VIFs deaktiviert, für die Sie den Sperrmodus nicht konfiguriert haben. Die VIFs bleiben deaktiviert, bis Sie entweder (a) den`locking-mode` Parameter des einzelnen VIF ändern oder (b) die VIFs explizit`locking-mode` auf 'entlocked setzen. Dies ist hilfreich, wenn Sie einer bestimmten VM genug vertrauen, damit Sie den 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:

```
xe network-param-set uuid=network-uuid default-locking-mode=[unlocked|
    disabled]
```

> **Hinweis:**
>
> Führen Sie den`network-list` Befehl xe aus, um die UUID für ein Netzwerk abzurufen. 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
```

ODER

```
xe network-list uuid=network-uuid params=default-locking-mode
```

Netzwerkeinstellungen für die VIF-Datenverkehrsfilterung verwenden

Im folgenden Verfahren wird ein VIF auf einer virtuellen Maschine angewiesen, mithilfe der Citrix Hypervisor`default-locking-mode` Netzwerkeinstellungen im Netzwerk selbst zu bestimmen, wie der Datenverkehr gefiltert wird.

1. Ändern Sie den VIF-Sperrstatus in`network_default`, wenn dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

   ```
   xe vif-param-set uuid=vif_uuid locking-mode=network_default
   ```

2. Ändern Sie den Standardsperrmodus in`unlocked`, wenn dieser Modus nicht bereits verwendet wird, indem Sie den folgenden Befehl ausführen:

   ```
   xe network-param-set uuid=network-uuid default-locking-mode=
       unlocked
   ```


Kopiert!
Failed!

Problembehandlung bei Netzwerken

October 16, 2019

Wenn Sie Probleme mit der Netzwerkkonfiguration haben, stellen Sie zunächst sicher, dass Sie keine der`ifcfg-*` Steuerdomänendateien direkt geändert haben. Der Host-Agent der Steuerdomäne verwaltet die`ifcfg` Dateien direkt und alle Änderungen werden überschrieben.

Diagnose von Netzwerkbeschädigung

Einige Netzwerkkartenmodelle erfordern Firmware-Upgrades vom Hersteller, um zuverlässig unter Last zu arbeiten, oder wenn bestimmte Optimierungen aktiviert sind. Wenn der Datenverkehr zu VMs beschädigt wird, versuchen Sie, die neueste Firmware vom Hersteller zu erhalten, und wenden Sie dann ein BIOS-Update an.

Wenn das Problem weiterhin besteht, können Sie die CLI verwenden, um Empfangen oder Übertragen von Offload-Optimierungen auf der physischen Schnittstelle zu deaktivieren.

> **Warnhinweis:**
>
> Die Deaktivierung von Empfangen oder Senden Offload-Optimierungen kann zu Performance-Verlusten und einer erhöhten CPU-Auslastung führen.

Bestimmen Sie zunächst die UUID der physikalischen Schnittstelle. Sie können das`device` Feld wie folgt filtern:

```
1 xe pif-list device=eth0
```

Legen Sie als Nächstes den folgenden Parameter auf der PIF fest, um die TX-Offload zu deaktivieren:

```
1 xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
```

Schließen Sie schließlich die PIF erneut an, oder starten Sie den Host neu, damit die Änderung wirksam wird.

Notfallnetzwerk-Reset

Falsche Netzwerkeinstellungen können zu einem Verlust der Netzwerkkonnektivität führen. Wenn keine Netzwerkkonnektivität vorhanden ist, kann der Citrix Hypervisor or-Server über XenCenter oder

Remote-SSH-Zugriff nicht mehr möglich sein. Der Notfallnetzwerk-Reset bietet einen einfachen Mechanismus zum Wiederherstellen und Zurücksetzen des Netzwerkes eines Hosts.

Die Funktion zum Zurücksetzen des Notfallnetzwerks ist über die Befehlszeilenschnittstelle mit dem`xe-reset-networking` Befehl und im Abschnitt Netzwerk- und Verwaltungsschnittstelle von xsconsole verfügbar.

Falsche Einstellungen, die zu einem Verlust der Netzwerkkonnektivität führen, umfassen das Umbenennen von Netzwerkschnittstellen, das Erstellen von Anleihen oder VLANs oder Fehler beim Ändern der Verwaltungsschnittstelle. Geben Sie beispielsweise die falsche IP-Adresse ein. Sie können dieses Dienstprogramm auch in den folgenden Szenarien ausführen:

- Wenn ein Rolling Pool-Upgrade, manuelles Upgrade, Hotfixinstallation oder Treiberinstallation zu einem Mangel an Netzwerkkonnektivität führt, oder
- Wenn ein Poolmaster oder -Host in einem Ressourcenpool keine Verbindung mit anderen Hosts herstellen kann.

Verwenden Sie das`xe-reset-networking` Dienstprogramm nur im Notfall, da es die Konfiguration für alle PIF, Anleihen, VLANs und Tunnel löscht, die mit dem Host verknüpft sind. Gastnetzwerke und VIFs bleiben erhalten. Als Teil dieses Dienstprogramms werden VMs 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 Statisch verwendet werden kann.

Wenn für den Poolmaster ein Zurücksetzen des Netzwerks erforderlich ist, setzen Sie zuerst das Netzwerk auf dem Poolmaster zurück, bevor Sie einen Netzwerkreset auf Poolmitglieder anwenden. Wenden Sie das Zurücksetzen des Netzwerks auf alle verbleibenden Hosts im Pool an, um sicherzustellen, dass die Netzwerkkonfiguration des Pools homogen ist. Netzwerkhomogenität ist ein wichtiger Faktor für die Live-Migration.

> **Hinweis:**
>
> Wenn sich die IP-Adresse des Poolmasters (die Verwaltungsschnittstelle) infolge eines Netzwerkrücksetzens ändert`xe host-management-reconfigure`, oder wenden Sie den Befehl zum Zurücksetzen des Netzwerks auf andere Hosts im Pool an. Damit soll sichergestellt werden, dass die Poolmitglieder eine erneute Verbindung mit dem Poolmaster auf seiner neuen IP-Adresse herstellen können. In diesem Fall muss die IP-Adresse des Poolmasters angegeben werden.
>
> Das Zurücksetzen des Netzwerks wird NICHT unterstützt, wenn Hochverfügbarkeit aktiviert ist. Um die Netzwerkkonfiguration in diesem Szenario zurückzusetzen, müssen Sie zuerst die hohe Verfügbarkeit manuell deaktivieren und dann den Befehl Netzwerkreset ausführen.

Überprüfen des Zurücksetzens des Netzwerks

Nachdem Sie den Konfigurationsmodus angegeben haben, der nach dem Zurücksetzen des Netzwerks verwendet werden soll, werden xsconsole und die CLI-Anzeigeeinstellungen angezeigt, die nach dem Neustart des Hosts angewendet werden. Es ist eine letzte Chance, sich zu ändern, bevor Sie den Notfall-Netzwerk-Reset-Befehl anwenden. Nach dem Neustart kann die neue Netzwerkkonfiguration in XenCenter und xsconsole überprüft werden. Wählen Sie in XenCenter bei ausgewähltem Host die Registerkarte **Netzwerk** aus, um die neue Netzwerkkonfiguration anzuzeigen. Im Abschnitt Netzwerk- und Verwaltungsschnittstelle in **xsconsole** werden diese Informationen angezeigt.

> **Hinweis:**
>
> Führen Sie einen Notfallnetzwerk-Reset für andere Pool-Mitglieder aus, um Anleihen, VLANs oder Tunnel aus der neuen Konfiguration des Poolmasters zu replizieren.

Verwenden der CLI für das Zurücksetzen des Netzwerks

Die folgende Tabelle zeigt die verfügbaren optionalen Parameter, die durch Ausführen des`xe-reset-networking` Befehls verwendet werden können.

> **Warnhinweis:**
>
> Die Benutzer sind dafür verantwortlich, die Gültigkeit der Parameter für den`xe-reset-networking` Befehl zu gewährleisten und die Parameter sorgfältig zu überprüfen. Wenn Sie ungültige Parameter angeben, können Netzwerkkonnektivität und -konfiguration verloren gehen. In diesem Fall empfehlen wir, den Befehl erneut auszuführen,`xe-reset-networking` ohne Parameter zu verwenden.
>
> Das Zurücksetzen der Netzwerkkonfiguration eines ganzen Pools **muss** auf dem Poolmaster beginnen, gefolgt von dem Zurücksetzen des Netzwerks auf allen verbleibenden Hosts im Pool.

Parameter	Erforderlich/optional	Beschreibung
-m, —master	Optional	IP-Adresse der Verwaltungsschnittstelle des Pool Masters. Standardmäßig wird die IP-Adresse des letzten bekannten Pool Masters verwendet.

Parameter	Erforderlich/optional	Beschreibung
—Gerät	Optional	Gerätename der Verwaltungsoberfläche. Standardmäßig wird der bei der Installation angegebene Gerätename verwendet.
—mode=statisch	Optional	Aktiviert die folgenden vier Netzwerkparameter für die statische IP-Konfiguration für die Verwaltungsschnittstelle. Wenn nicht angegeben, wird das Netzwerk mithilfe von DHCP konfiguriert.
—IP	Erforderlich, wenn Modus=statisch	IP-Adresse für die Verwaltungsschnittstelle des Hosts. Nur gültig, wenn mode=statisch.
—netmask	Erforderlich, wenn Modus=statisch	Netzmaske für die Management-Schnittstelle. Nur gültig, wenn mode=statisch.
—Gateway	Optional	Gateway für die Verwaltungsschnittstelle. Nur gültig, wenn mode=statisch.
—dns	Optional	DNS-Server für die Verwaltungsschnittstelle. Nur gültig, wenn mode=statisch.
—vlan	Optional	VLAN-Tag für die Management-Schnittstelle. Standardmäßig wird das bei der Installation angegebene VLAN-Tag verwendet.

Poolmaster-Befehlszeilenbeispiele

Beispiele für Befehle, die auf einen Poolmaster angewendet werden können:

So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück:


```
xe-reset-networking
```

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
```

So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück, wenn nach der erstmaligen Einrichtung eine andere Schnittstelle zur Verwaltungsschnittstelle wurde:

```
xe-reset-networking --device=device-name
```

So setzen Sie das Netzwerk für die statische IP-Konfiguration zurück, wenn nach der ersten Einrichtung eine andere Schnittstelle zur Verwaltungsschnittstelle wurde:

```
xe-reset-networking --device=device-name --mode=static \
    --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
```

So setzen Sie das Netzwerk für die Verwaltungsschnittstelle auf VLAN zurück:

```
xe-reset-networking --vlan=VLAN TAG
```

> **Hinweis:**
>
> Der`reset-network` Befehl kann auch zusammen mit den IP-Konfigurationseinstellungen verwendet werden.

Befehlszeilenbeispiele für Poolmitglieder

Alle vorherigen Beispiele gelten auch für Pool-Mitglieder. Zusätzlich kann die IP-Adresse des Pool Masters angegeben werden (was notwendig ist, wenn sie geändert wurde).

So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück:

```
xe-reset-networking
```

So setzen Sie das Netzwerk für DHCP zurück, wenn die IP-Adresse des Poolmasters geändert wurde:

```
xe-reset-networking --master=master-ip-address
```

Um das Netzwerk für die statische IP-Konfiguration zurückzusetzen, vorausgesetzt, dass sich die IP-Adresse des Poolmasters nicht geändert hat:


```
xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
```

So setzen Sie das Netzwerk für die DHCP-Konfiguration zurück, wenn die Verwaltungsschnittstelle und die IP-Adresse des Poolmasters nach der erstmaligen Einrichtung geändert wurden:

```
xe-reset-networking --device=device-name --master=master-ip-address
```

Kopiert!
Failed!

Speicher

October 16, 2019

In diesem Abschnitt wird beschrieben, wie physische Speicherhardware virtuellen Maschinen (VMs) zugeordnet wird, sowie die von der Management-API zum Ausführen speicherbezogener Aufgaben verwendete Softwareobjekte. Detaillierte Abschnitte zu den unterstützten Speichertypen enthalten die folgenden Informationen:

- Verfahren zum Erstellen von Speicher für VMs mithilfe der CLI mit typspezifischen Gerätekonfigurationsoptionen
- Erstellen von Snapshots für Sicherungszwecke
- Best Practices für die Speicherverwaltung
- QoS-Einstellungen (Quality of Service) für virtuelle Laufwerke

Speicher-Repositories (SRs)

Ein Speicher-Repository (SR) ist ein bestimmtes Speicherziel, in dem Virtual Machine (VM) Virtual Disk Images (VDIs) gespeichert sind. Ein VDI ist eine Speicherabstraktion, die eine virtuelle Festplatte (HDD) darstellt.

SRs sind flexibel, mit integrierter Unterstützung für die folgenden Laufwerke:

Lokal verbunden:

- IDE
- SATA
- SCSI
- SAS

Fernzugriff:

- iSCSI
- NFS
- SAS
- Fibre-Channel

Die SR- und VDI-Abstraktionen ermöglichen es, erweiterte Speicherfunktionen auf Speicherzielen verfügbar zu machen, 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.

SR-Befehle bieten Operationen zum Erstellen, Löschen, Ändern, Ändern, Klonen, Verbinden und Erkennen der einzelnen VDIs, die sie enthalten.

Ein Speicher-Repository ist eine persistente Datenstruktur auf der Festplatte. Bei SR-Typen, die ein zugrunde liegendes Blockgerät verwenden, beinhaltet das Erstellen einer SR das Löschen aller vorhandenen Daten auf dem angegebenen Speicherziel. B. NFS, erstellen einen Container auf dem Speicher-Array parallel zu vorhandenen SRs.

Jeder Citrix Hypervisor or-Server kann mehrere SRs und verschiedene SR-Typen gleichzeitig verwenden. Diese SRs können zwischen Hosts geteilt oder für bestimmte Hosts dediziert werden. Gemeinsamer Speicher wird zwischen mehreren Hosts innerhalb eines definierten Ressourcenpools gepoolt. Ein gemeinsam genutzter SR muss für jeden Host im Pool auf das Netzwerk zugegriffen werden. Alle Server in einem einzelnen Ressourcenpool müssen mindestens eine gemeinsam genutzte SR haben. Gemeinsamer Speicher kann nicht zwischen mehreren Pools freigegeben werden.

CLI-Vorgänge zur Verwaltung von Speicher-Repositories werden unter beschriebenSR-Befehle.

Virtual Disk Image (VDI)

Ein Virtual Disk Image (VDI) ist eine Speicherabstraktion, die eine virtuelle Festplatte (HDD) darstellt. VDIs sind die grundlegende Einheit des virtualisierten Speichers in Citrix Hypervisor. VDIs sind persistente Objekte auf der Festplatte, die unabhängig von Citrix Hypervisor or-Servern vorhanden sind. CLI-Vorgänge zur Verwaltung von VDIs werden unter beschriebenVDI-Befehle. Die Darstellung der Daten auf der Festplatte unterscheidet sich je nach SR-Typ. Eine separate Speicher-Plug-in-Schnittstelle für jede SR, die sogenannte SM-API, verwaltet die Daten.

Physische Blockgeräte (PBDs)

Physische Blockgeräte stellen die Schnittstelle zwischen einem physischen Server und einer angeschlossenen SR dar. PBDs sind Connectorobjekte, mit denen eine bestimmte SR einem Host

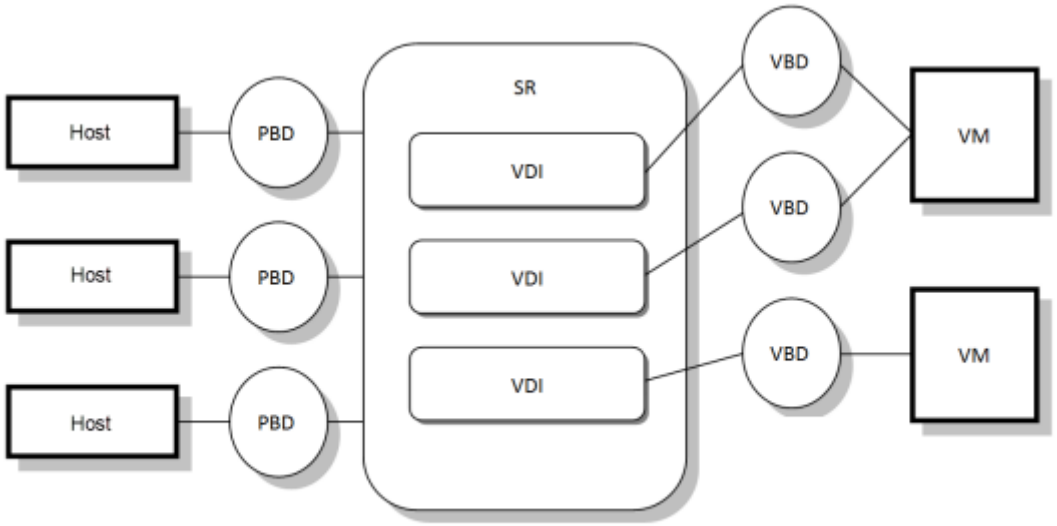
zugeordnet werden kann. In PBDs werden die Gerätekonfigurationsfelder gespeichert, die für die Verbindung zu einem bestimmten Speicherziel und für die Interaktion mit diesen verwendet werden. Beispielsweise umfasst die NFS-Gerätekonfiguration die IP-Adresse des NFS-Servers und den zugeordneten Pfad, den der Citrix Hypervisor or-Server bereitstellt. PBD-Objekte verwalten die Laufzeitanhänge eines bestimmten SR an einen bestimmten Citrix Hypervisor or-Server. CLI-Vorgänge im Zusammenhang mit PBDs werden unter beschriebenPBD-Befehle.

Virtuelle Blockgeräte (VBDs)

Virtuelle Blockgeräte sind Connectorobjekte (ähnlich der oben beschriebenen PBD), die Zuordnungen zwischen VDIs und VMs ermöglichen. Neben der Bereitstellung eines Mechanismus für die Anbringung eines VDI an eine VM ermöglichen VBDs die Feinabstimmung von Parametern bezüglich QoS (Quality of Service) und Statistiken eines bestimmten VDI, und ob dieser VDI gestartet werden kann. CLI-Vorgänge im Zusammenhang mit VBDs werden unter beschriebenVBD-Befehle.

Zusammenfassung der Speicherobjekte

Das folgende Bild zeigt, wie die bisher präsentierten Speicherobjekte zusammenhängen:



Datenformate für virtuelle Laufwerke

Im Allgemeinen gibt es die folgenden Arten der Zuordnung von physischem Speicher zu einem VDI:

1. *Logische Volume-basierte virtuelle Festplatte auf einer LUN:* Der blockbasierte Standardspeicher von Citrix Hypervisor fügt einen logischen Volume-Manager auf einen Datenträger ein. Bei

diesem Datenträger handelt es sich entweder um ein lokal angeschlossenes Gerät (LVM) oder eine mit SAN verbundene LUN über Fibre Channel, iSCSI oder SAS. VDIs werden als Volumes innerhalb des Volume-Managers dargestellt und im VHD-Format gespeichert, um die Thin Provisioning von Referenzknoten auf Snapshot und Clone zu ermöglichen.

2. *Dateibasiertes QCOW2 auf einer LUN:* VM-Images werden als Thin-Provisioned-QCOW2-Formatdateien auf einem GFS2-Dateisystem mit freigegebenen Datenträgern auf einer LUN gespeichert, die entweder über iSCSI-Software-Initiator oder Hardware-HBA verbunden ist.
3. *Dateibasierte virtuelle Festplatte auf einem Dateisystem:* VM-Images werden als Thin-Provisioned-VHD-Formatdateien auf einem lokalen, nicht gemeinsam genutzten Dateisystem (EXT Typ SR) oder einem gemeinsam genutzten NFS-Ziel (NFS-Typ SR) gespeichert.

VDI-Typen

Für die meisten SR-Typen werden VHD-Format-VDIs erstellt. Bei der Erstellung des VDI können Sie sich entscheiden, roh zu verwenden. Diese Option kann nur mit der XE CLI angegeben werden. Für GFS2 SRs werden QCOW2 VDIs erstellt.

Überprüfen Sie die`type=raw`Karte, um zu überprüfen`sm-config`, ob ein VDI mit erstellt wurde. Dazu können die`sr-param-list` Befehle bzw.`vdi-param-list` xe verwendet werden.

Erstellen eines virtuellen Rohdatenträgers mithilfe der XE CLI

1. Führen Sie den folgenden Befehl aus, um einen VDI mit der UUID des SR zu erstellen, in dem Sie das virtuelle Laufwerk ablegen möchten:

```
xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size
    \
        name-label=VDI name sm-config:type=raw
```

2. Schließen Sie das neue virtuelle Laufwerk an eine VM an. Verwenden Sie die Datenträgerwerkzeuge innerhalb der VM zum Partitionieren und Formatieren oder verwenden Sie den neuen Datenträger anderweitig. Sie können den`vbd-create` Befehl verwenden, um eine VBD zu erstellen, um das virtuelle Laufwerk Ihrer VM zuzuordnen.

Konvertieren zwischen VDI-Formaten

Eine direkte Konvertierung zwischen den Roh- und VHD-Formaten ist nicht möglich. Stattdessen können Sie einen VDI (entweder roh, wie oben beschrieben, oder VHD) erstellen und dann Daten von einem vorhandenen Volume in ihn kopieren. Verwenden Sie die xe-CLI, um sicherzustellen, dass der

neue VDI eine virtuelle Größe hat, die mindestens so groß ist wie der VDI, aus dem Sie kopieren. Sie können dies tun, indem Sie das`virtual-size` Feld überprüfen, z. B. mit dem`vdi-param-list` Befehl. 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`dd` Befehl in Linux. Wenn es sich bei dem neuen Volume um ein VHD-Volume handelt, verwenden Sie ein Tool, mit dem Sie vermeiden können, leere Sektoren auf den Datenträger zu schreiben. Diese Aktion kann sicherstellen, dass Speicherplatz im zugrunde liegenden Speicher-Repository optimal genutzt wird. Ein dateibasierter Kopieransatz ist möglicherweise besser geeignet.

VHD-basierte und QCOW2-basierte VDIs

VHD- und QCOW2-Images können *verkettet*werden, wodurch zwei VDIs gemeinsame Daten gemeinsam nutzen können. In Fällen, in denen eine VHD-gestützte oder QCOW2-gestützte VM geklont wird, verwenden die resultierenden VMs die gemeinsamen Daten auf der Festplatte zum Zeitpunkt des Klonens. 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 dadurch Bäume von verketteten VDIs erstellt. Wenn eine der VDIs in einer Kette gelöscht wird, rationalisiert Citrix Hypervisor die anderen VDIs in der Kette, um unnötige VDIs zu entfernen. Dieser *Koaleszierungsprozess* wird asynchron ausgeführt. Die Menge des zurückgeforderten Festplattenspeichers und die Zeit, die für die Ausführung des Prozesses benötigt wird, hängt von der Größe des VDI und der Menge der freigegebenen Daten ab.

Sowohl das VHD- als auch das QCOW2-Format unterstützen *Thin Provisioning*. Die Image-Datei wird automatisch in fein granularen Blöcken erweitert, wenn die VM Daten auf den Datenträger schreibt. Für dateibasierte VHD und GFS2-basierte QCOW2 hat dieser Ansatz den erheblichen Vorteil, dass VM-Imagedateien nur so viel Speicherplatz auf dem physischen Speicher belegen wie erforderlich. Bei LVM-basierter VHD muss der zugrunde liegende logische Volume-Container auf die virtuelle Größe des VDI angepasst werden. Ungenutzter Speicherplatz auf dem zugrunde liegenden Kopier-on-Write-Instanzdatenträger wird jedoch wiederhergestellt, wenn ein Snapshot oder ein Klon auftritt. Der Unterschied zwischen den beiden Verhaltensweisen kann folgendermaßen beschrieben werden:

- Bei *LVM-basierten VHD-Images*verbrauchen die Differenzfestplattenknoten innerhalb der Kette nur so viele Daten, wie sie auf die Festplatte geschrieben wurden. Die Blattknoten (VDI-Klone) bleiben jedoch vollständig auf die virtuelle Größe der Festplatte aufgeblasen. Snapshot-Blattknoten (VDI-Snapshots) bleiben deflationiert, wenn sie nicht verwendet werden, und können schreibgeschützt angehängt werden, um die deflationierte Zuweisung beizubehalten. Snapshot-Knoten, die mit Read-Write verbunden sind, werden beim Anhängen vollständig

aufgeblasen und beim Trennen deflationiert.

- Bei *dateibasierten VHDs* und *GFS2-basierten QCOW2-Images* verbrauchen alle Knoten nur so viele Daten wie geschrieben. Die Blattknotendateien wachsen, um Daten aufzunehmen, während sie aktiv geschrieben werden. Wenn ein VDI mit 100 GB für eine VM zugewiesen wird und ein Betriebssystem installiert ist, entspricht die VDI-Datei physisch nur der Größe der Betriebssystemdaten auf dem Datenträger und einigen geringfügigen Metadaten-Overhead.

Beim Klonen von VMs basierend auf einer einzelnen VHD- oder QCOW2-Vorlage bildet jede untergeordnete VM eine Kette, in der neue Änderungen auf die neue VM geschrieben werden. Alte Blöcke werden direkt aus der übergeordneten Vorlage gelesen. Wenn die neue VM in eine weitere Vorlage konvertiert wurde und mehr VMs geklont wurden, führt die resultierende Kette zu einer Leistungsverschlechterung. Citrix Hypervisor unterstützt eine maximale Kettenlänge von 30. Nähern Sie sich diesem Limit nicht ohne guten Grund. Wenn Sie Zweifel haben, „kopieren“ Sie die VM mit XenCenter oder verwenden Sie den`vm-copy` Befehl, der die Kettenlänge auf 0 zurücksetzt.

VHD-spezifische Hinweise zur Koalesz

Für eine SR ist je nur ein Koaleszenzprozess aktiv. Dieser Prozess-Thread wird auf dem SR-Master-Host ausgeführt.

Wenn kritische VMs auf dem Masterserver des Pools ausgeführt werden, können Sie die folgenden Schritte ausführen, um gelegentlich langsame E/A-Vorgänge zu minimieren:

- Migrieren der VM auf einen anderen Host als den SR-Master
- Legen Sie die E/A-Priorität auf eine höhere Ebene fest, und passen Sie den Scheduler an. Weitere Informationen finden Sie unter QoS-Einstellungen für virtuelle Laufwerke.

Kopiert!
Failed!

Speicher-Repository-Formate

October 16, 2019

Mit dem Assistenten „ **Neues Speicher-Repository** “ in XenCenter können Sie Speicher-Repositories erstellen. Der Assistent führt Sie durch die Konfigurationsschritte. Alternativ können Sie die Befehlszeilenschnittstelle und den`sr-create` Befehl verwenden. sr-create“ Mit dem Befehl wird ein SR auf dem Speichersubstrat erstellt (möglicherweise vorhandene Daten zerstört). Außerdem werden das SR-API-Objekt und ein entsprechender PBD-Datensatz erstellt, wodurch VMs den Speicher verwenden können. Bei erfolgreicher Erstellung der SR wird die PBD automatisch gesteckt.

Wenn das`shared=true` SR-Flag gesetzt ist, wird für jeden Citrix Hypervisor im Ressourcenpool ein PBD-Datensatz erstellt und angeschlossen.

Wenn Sie eine 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 Speicherdatenverkehr. Informationen zum Zuweisen einer IP-Adresse zu einer Netzwerkkarte finden Sie unterKonfigurieren einer dedizierten Speicher-NIC.

Alle Citrix Hypervisor SR-Typen unterstützen die 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, NFS, GFS2) unterstützen die vollständige Thin Provisioning, auch für aktive virtuelle Laufwerke.

> **Warnhinweis:**
>
> Wenn VHD-VDIs nicht an eine VM angeschlossen sind, z. B. für einen VDI-Snapshot, werden sie standardmäßig als Thinly Provisioning gespeichert. Wenn Sie versuchen, den VDI erneut anzuhängen, stellen Sie sicher, dass genügend Speicherplatz zur Verfügung steht, damit der VDI stark bereitgestellt wird. VDI-Klone werden stark bereitgestellt.

Die maximal unterstützten VDI-Größen sind:

Speicher-Repository-Format	Maximale VDI-Größe
EXT3	2 TiB
LVM	2 TiB
NFS	2 TiB
LVMofCoe	2 TiB
LVMoiSCSI	2 TiB
- lvmohba	2 TiB
GFS2 (mit iSCSI oder HBA)	16 TiB

Lokale LVM

Der Typ Local LVMs stellt Datenträger innerhalb einer lokal angeschlossenen Volumegruppe dar.

Standardmäßig verwendet Citrix Hypervisor den lokalen Datenträger auf dem physischen Host, auf dem er 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.

Überlegungen zur LVM-Leistung

Die Snapshot- und schnelle Clone-Funktionalität für LVM-basierte SRs verfügt über einen inhärenten Performance-Overhead. Wenn eine optimale Leistung erforderlich ist, unterstützt Citrix Hypervisor die Erstellung von VDIs im *Rohformat* zusätzlich zum Standard-VHD-Format. Die Snapshot-Funktionalität von Citrix Hypervisor wird auf Raw-VDIs nicht unterstützt.

Nicht transportierbare Snapshots, die den standardmäßigen Windows VSS-Provider verwenden, funktionieren auf jedem VDI-Typ.

> **Warnung:**Versuchen
>
> Sie nicht, einen Snapshot einer virtuellen Maschine mit angeschlossenentype=raw“Festplatten zu erstellen. Diese Aktion kann dazu führen, dass ein Teilsnapshot erstellt wird. In diesem Fall können Sie die verwaiste Snapshot-VDIs identifizieren, indem Sie dassnapshot-of Feld überprüfen und dann löschen.

Erstellen eines lokalen LVM SR

Bei der Hostinstallation wird standardmäßig ein LVM-SR erstellt.

Device-Config-Parameter für LVM-SRs sind:

Parametername	Beschreibung	Erforderlich?
Gerätetyp	Gerätename auf dem lokalen Host, der für die SR verwendet werden soll	Ja

Verwenden Sie den folgenden Befehl/dev/sdb, um eine lokale LVM SR auf zu erstellen.

```
1     xe sr-create host-uuid=valid_uuid content-type=user \
2     name-label=”Example Local LVM SR” shared=false \
3     device-config:device=/dev/sdb type=lvm
```

Lokales EXT3

Die Verwendung von EXT3 ermöglicht die Thin Provisioning auf lokalem Speicher. Der Standardspeicher-Repository-Typ ist jedoch LVM, da er eine konsistente Schreibleistung bietet und Speicherüber-Commit verhindert. Wenn Sie EXT3 verwenden, wird in den folgenden Fällen möglicherweise eine reduzierte Leistung angezeigt:

- Beim Ausführen von VM-Lebenszyklusvorgängen wie Erstellen von virtuellen Rechnern und Anhalten/Fortsetzen
- Beim Erstellen großer Dateien innerhalb der VM

Die lokalen Datenträger EXT SRs müssen mit der Citrix Hypervisor CLI konfiguriert werden.

Erstellen eines lokalen EXT3 SR (ext)

Gerätekonfigurationsparameter für externe SRs:

Parametername	Beschreibung	Erforderlich?
Gerätetyp	Gerätename auf dem lokalen Host, der für die SR verwendet werden soll	Ja

Verwenden Sie den folgenden Befehl/dev/sdb, um einen lokalen ext SR auf zu erstellen:

```
1     xe sr-create host-uuid=valid_uuid content-type=user \
2        name-label=”Example Local EXT3 SR” shared=false \
3        device-config:device=/dev/sdb type=ext
```

udev

Derudev Typ stellt Geräte dar, die mit demudev Geräte-Manager als VDIs verbunden sind.

Citrix Hypervisor verfügt über zwei SRs vom Typudev , die Wechselmedien darstellen. Eine ist für die CD- oder DVD-Festplatte im physischen CD- oder DVD-ROM-Laufwerk des Citrix Hypervisor or-Servers. Der andere ist für ein USB-Gerät, das an einen USB-Anschluss des Citrix Hypervisor or-Servers angeschlossen ist. VDIs, die die Medien darstellen, kommen und gehen, wenn Festplatten oder USB-Sticks eingelegt und entfernt werden.

ISO

Der ISO-Typ verarbeitet CD-Images, die als Dateien im ISO-Format gespeichert sind. Dieser SR-Typ ist nützlich, um gemeinsam genutzte ISO-Bibliotheken zu erstellen. Für Speicher-Repositories, die eine Bibliothek von ISOs speichern, muss dercontent-type Parameter auf gesetzt werdeniso .

Zum Beispiel:

```
1     xe sr-create host-uuid=valid_uuid content-type=iso \
```



```
2       type=iso name-label="Example ISO SR" \
3       device-config:location=nfs server:path
```

Es wird empfohlen, dass Sie SMB Version 3.0 verwenden, um ISO SR auf Windows Dateiserver mounten. Version 3.0 ist standardmäßig ausgewählt, da sie sicherer und robuster ist als SMB-Version 1.0. Sie können jedoch ISO SR mit SMB Version 1.0 mit dem folgenden Befehl mounten:

```
1       xe sr-create content-type=iso type=iso shared=true device-config:
           location=valid location
2       device-config:username=username device-config:cifspassword=
           password
3       device-config:type=cifs device-config:vers=Choose either 1.0 or
           3.0 name-label="Example ISO SR"
```

> **Hinweis:**
>
> Wenn Sie den `sr-create` Befehl ausführen, können Sie das `device-config:cifspassword_secret` Argument verwenden, anstatt das Kennwort in der Befehlszeile anzugeben. Weitere Informationen finden Sie unter Geheimnisse.

Software-iSCSI-Unterstützung

Citrix Hypervisor unterstützt gemeinsam genutzte SRs auf iSCSI-LUNs. iSCSI wird mit dem iSCSI-Software-iSCSI-Initiator oder mithilfe eines unterstützten iSCSI-Host-Bus-Adapters (HBA) unterstützt. Die Schritte zur Verwendung von iSCSI-HBAs sind identisch mit den Schritten für Fibre-Channel-HBAs. Beide Schritte werden unter beschriebenErstellen eines gemeinsam genutzten LVM über Fibre-Channel/Fibre-Channel-over-Ethernet/iSCSI-HBA oder SAS SR.

Die gemeinsam genutzte iSCSI-Unterstützung mit dem Software-iSCSI-Initiator wird basierend auf dem Linux Volume Manager (LVM) implementiert. Diese Funktion bietet die gleichen Leistungsvorteile, die LVM-VDIs im lokalen Festplattengehäuse bieten. Gemeinsame iSCSI-SRs, die den softwarebasierten Hostinitiator verwenden, können VM-Agilität durch Live-Migration unterstützen: VMs können auf jedem Citrix Hypervisor or-Server in einem Ressourcenpool gestartet und ohne spürbare Ausfallzeiten zwischen ihnen migriert werden.

iSCSI-SRs verwenden die gesamte zum Zeitpunkt der Erstellung angegebene LUN und erstrecken sich möglicherweise nicht über mehr als eine LUN. CHAP-Unterstützung wird für die Clientauthentifizierung sowohl während der Datenpfadinitialisierung als auch in der LUN-Erkennungsphase bereitgestellt.

> **Hinweis:**
>
> Die Blockgröße einer iSCSI-LUN muss 512 Byte betragen.

iSCSI-Konfiguration des Citrix Hypervisor or-Servers

Alle iSCSI-Initiatoren und -Ziele müssen über einen eindeutigen Namen verfügen, damit sie im Netzwerk eindeutig identifiziert werden können. Ein Initiator hat eine iSCSI-Initiatoradresse und ein Ziel hat eine iSCSI-Zieladresse. Gemeinsam werden diese Namen als iSCSI-qualifizierte Namen oder IQNs bezeichnet.

Citrix Hypervisor or-Server 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 bieten in der Regel Zugriffssteuerung mithilfe von iSCSI-Initiator-IQN-Listen. Alle iSCSI-Targets/LUNs, auf die der Citrix Hypervisor or-Server zugreift, müssen so konfiguriert sein, dass der Zugriff durch den Initiator-IQN des Hosts gewährt wird. Ebenso müssen Ziele/LUNs, die als gemeinsam genutzte iSCSI-SRs verwendet werden sollen, so konfiguriert sein, dass alle Host-IQNs im Ressourcenpool Zugriff haben.

> **Hinweis:**
>
> iSCSI-Ziele, die keine Zugriffssteuerung bieten, beschränken normalerweise den LUN-Zugriff auf einen einzelnen Initiator, um die Datenintegrität zu gewährleisten. Wenn eine iSCSI-LUN als gemeinsam genutzte SR über mehrere Server in einem Pool hinweg verwendet wird, stellen Sie sicher, dass der Multiinitiator-Zugriff für die angegebene LUN aktiviert ist.

Der IQN-Wert des Citrix Hypervisor or-Servers kann mithilfe von XenCenter oder mithilfe der Befehlszeilenschnittstelle mit dem folgenden Befehl bei Verwendung des iSCSI-Softwareinitiators angepasst werden:

```
1     xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=
         new_initiator_iqn
```

> **Warnhinweis:**
>
> - Jedes iSCSI-Ziel und jeder Initiator muss über einen eindeutigen IQN verfügen. Wenn ein nicht eindeutiger IQN-Bezeichner verwendet wird, kann Datenbeschädigung oder Verweigerung des LUN-Zugriffs auftreten.
> - Ändern Sie den Citrix Hypervisor or-Server-IQN mit angeschlossenen iSCSI-SRs nicht. Dies kann zu Fehlern bei der Verbindung mit neuen Zielen oder vorhandenen SRs führen.

Software FCoE-Speicher

Software-FCoE bietet ein Standard-Framework, in das Hardwarehersteller ihre FCOE-fähige NIC anschließen können und die gleichen Vorteile wie eine hardwarebasierte FCoE nutzen können. Diese Funktion macht die Verwendung teurer HBAs überflüssig.

Bevor Sie einen Software-FCoE-Speicher erstellen, führen Sie die Konfiguration manuell aus, 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 für den öffentlichen World Wide Name (PWWN) Ihres SAN. Nachdem Sie diese Konfiguration abgeschlossen haben, wird die verfügbare LUN als SCSI-Gerät auf dem CNA des Hosts gemountet. Das SCSI-Gerät kann dann verwendet werden, um auf die LUN zuzugreifen, 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 einer Software FCoE SR

Bevor Sie eine Software FCoE SR erstellen, müssen Kunden sicherstellen, dass FCOE-fähige Netzwerkkarten an den Host angeschlossen sind.

Device-Config-Parameter für FCoE SRs sind:

Parametername	Beschreibung	Erforderlich?
`SCSIid`	Die SCSI-Bus-ID der Ziel-LUN	Ja

Führen Sie den folgenden Befehl aus, um eine gemeinsam genutzte FCoE SR zu erstellen:

```
1     xe sr-create type=lvmofcoe \
2     name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
```

Hardware-Hostbusadapter (HBAs)

Dieser Abschnitt behandelt verschiedene Vorgänge, die für die Verwaltung von SAS-, Fibre Channel- und iSCSI-HBAs erforderlich sind.

Beispiel für QLogic iSCSI-HBA-Setup

Weitere Informationen zur Konfiguration von QLogic Fibre Channel- und iSCSI-HBAs finden SieKaviumauf der Website.

Nachdem der HBA physisch auf dem Citrix Hypervisor or-Server installiert wurde, gehen Sie folgendermaßen vor, um den HBA zu konfigurieren:

1. Legen Sie die IP-Netzwerkkonfiguration für den HBA fest. In diesem Beispiel wird DHCP und HBA-Port 0 vorausgesetzt. Geben Sie die entsprechenden Werte an, wenn Sie die statische IP-Adressierung oder einen HBA mit mehreren Ports verwenden.

```
/opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
```

2. Fügen Sie ein persistentes iSCSI-Ziel zu Port 0 des HBA hinzu.

```
/opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0
   iscsi_target_ip_address
```

3. Verwenden Sie den`sr-probe` Befehl xe, um eine erneute Suche des HBA-Controllers zu erzwingen und verfügbare LUNs anzuzeigen. Weitere Informationen finden Sie unter Sonde einer SR und Erstellen eines gemeinsam genutzten LVM über Fibre-Channel/Fibre-Channel-over-Ethernet/iSCSI-HBA oder SAS SR.

Entfernen von HBA-basierten SAS-, FC- oder iSCSI-Geräteeinträgen

> **Hinweis:**
>
> Dieser Schritt ist nicht erforderlich. Wir empfehlen, dass nur Power-User diesen Prozess durchführen, wenn dies erforderlich ist.

Jede HBA-basierte LUN verfügt über 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`sr-destroy` entfernen Sie den SR aus der Citrix Hypervisor or-Serverdatenbank. Weitere Informationen SRs entfernen finden Sie unter.
2. Entfernen Sie die Zoning-Konfiguration im SAN für die gewünschte LUN auf den gewünschten Host.
3. Verwenden Sie den`sr-probe` Befehl, um die ADAPT-, BUS-, TARGET- und LUN-Werte zu ermitteln, die der zu entfernenden LUN entsprechen. Für weitere Informationen,Sonde einer SR.
4. Entfernen Sie die Geräteeinträge mit dem folgenden Befehl:

```
echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/
   delete
```

> **Warnhinweis:**
>
> Stellen Sie sicher, dass Sie sicher sind, welche LUN Sie entfernen. Das versehentliche Entfernen einer LUN, die für den Hostbetrieb erforderlich ist, wie z. B. das Start- oder Root-Gerät, macht

> den Host unbrauchbar.

Gemeinsamer LVM-Speicher

Der Typ Shared LVMs stellt Datenträger als logische Volumes innerhalb einer Volumegruppe dar, die auf einer iSCSI-LUN (FC oder SAS) erstellt wurde.

> **Hinweis:**
>
> Die Blockgröße einer iSCSI-LUN muss 512 Byte betragen.

Erstellen einer 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 die SR hostet	Ja
`targetIQN`	Die IQN-Zieladresse des iSCSI-Filers, der die SR hostet	Ja
`SCSIid`	Die SCSI-Bus-ID der Ziel-LUN	Ja
`chapuser`	Der Benutzername, der für die CHAP-Authentifizierung verwendet werden soll	Nein
`chappassword`	Das Kennwort, das für die CHAP-Authentifizierung verwendet werden soll	Nein
`port`	Die Netzwerkportnummer, auf der das Ziel abgefragt werden soll	Nein
`usediscoverynumber`	Der spezifische iSCSI-Datensatzindex, der verwendet werden soll	Nein
`incoming_chapuser`	Der Benutzername, den der iSCSI-Filter zur Authentifizierung gegen den Host verwendet	Nein

Parametername	Beschreibung	Erforderlich?
incoming_chappassword	Das Kennwort, das der iSCSI-Filter zur Authentifizierung gegen den Host verwendet	Nein

Verwenden Sie den folgenden Befehl, um eine gemeinsam genutzte 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
```

Erstellen eines gemeinsam genutzten LVM über Fibre-Channel/Fibre-Channel-over-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

Führen Sie die folgenden Schritte auf jedem Host im Pool aus, um eine gemeinsam genutzte LVMohba SR zu erstellen:

1. Zonen Sie in einer oder mehreren LUNs zu jedem Citrix Hypervisor or-Server im Pool. Dieser Prozess ist sehr spezifisch für die verwendeten SAN-Geräte. Weitere Informationen finden Sie in der SAN-Dokumentation.
2. Verwenden Sie ggf. die im Citrix Hypervisor or-Server 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-Bus-Adapter (HBAs)* im vorherigen Abschnitt. Weitere Informationen zu Fibre Channel- und iSCSI-HBAs finden Sie auf denBroadcomundKaviumWebsites.

3. Verwenden Sie densr-probe Befehl, um den globalen Gerätepfad der HBA-LUN zu ermitteln. Dersr-probe Befehl erzwingt einen erneuten Scannen der im System installierten HBAs, um neue LUNs zu erkennen, die auf den Host in Zonen aufgeteilt wurden. Der Befehl gibt eine Liste der Eigenschaften für jede gefundene LUN zurück. Geben Sie denhost-uuid Parameter an, um sicherzustellen, dass der Prüfpunkt auf dem gewünschten Host auftritt.

   Der globale Gerätepfad, der als<path> Eigenschaft zurückgegeben wird, ist auf allen Hosts im Pool gemeinsam. Daher muss dieser Pfad als Wert für dendevice-config:device Parameter beim Erstellen der SR verwendet werden.

   Wenn mehrere LUNs vorhanden sind, verwenden Sie den Hersteller, die LUN-Größe, die LUN-Seriennummer oder die SCSI-ID aus 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>
```

4. Erstellen Sie auf dem Master-Host des Pools die SR. Geben Sie den globalen Gerätepfad an, der in der`<path>` Eigenschaft von zurückgegeben wird`sr-probe` . PBDs werden automatisch für jeden Host im Pool 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
```

> **Hinweis:**
>
> Sie können die XenCenter Repair Storage Repository verwenden, um die PBD-Erstellung und das Anschließen von Teilen des`sr-create` Vorgangs zu wiederholen. Diese Funktion kann nützlich sein, wenn die LUN-Zoning für einen oder mehrere Hosts in einem Pool falsch war, als die SR erstellt wurde. Korrigieren Sie die Zoneneinteilung für die betroffenen Hosts und verwenden Sie die Funktion Speicher-Repository reparieren, anstatt die SR zu entfernen und neu zu erstellen.

Thin bereitgestellter gemeinsam genutzter GFS2-Blockspeicher

Thin Provisioning nutzt den verfügbaren Speicher besser, indem VDIs Speicherplatz zugewiesen wird, wenn Daten auf das virtuelle Laufwerk geschrieben werden, anstatt die volle virtuelle Größe des VDIs im Voraus zuzuweisen. Mit der Thin Provisioning können Sie den benötigten Speicherplatz für ein gemeinsam genutztes Speicher-Array und damit Ihre Total Cost of Ownership (TCO) erheblich reduzieren.

Die Thin Provisioning für Shared Block Storage ist in folgenden Fällen von besonderem Interesse:

- Sie wollen mehr Platzeffizienz. Bilder sind dünn und nicht dick zugeordnet.
- Sie möchten die Anzahl der E/A-Vorgänge pro Sekunde auf Ihrem Speicher-Array reduzieren. Der GFS2 SR ist der erste SR-Typ, der Speicherlesecaching auf Shared Block Storage unterstützt.
- Sie verwenden ein gemeinsames Basisabbild für mehrere virtuelle Maschinen. Die Images einzelner VMs verbrauchen dann in der Regel noch weniger Speicherplatz.
- Sie verwenden Schnappschüsse. Jeder Snapshot ist ein Bild, und jedes Bild ist jetzt dünn.
- Ihr Speicher unterstützt NFS nicht und unterstützt nur Blockspeicher. Wenn Ihr Speicher NFS unterstützt, empfehlen wir, 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.

Der freigegebene GFS2-Typ stellt Datenträger als Dateisystem dar, das auf einer iSCSI- oder HBA-LUN erstellt wurde. VDIs, die auf einem GFS2 SR gespeichert sind, werden im QCOW2-Bildformat gespeichert.

Um gemeinsam genutzten GFS2-Speicher zu verwenden, muss der Citrix Hypervisor Ressourcenpool ein Clusterpool sein. Aktivieren Sie Clustering in Ihrem Pool, bevor Sie eine GFS2 SR erstellen. Weitere Informationen finden Sie unter Cluster-Pools.

Stellen Sie sicher, dass Speicher-Multipathing zwischen Ihrem Cluster-Pool und Ihrem GFS2 SR eingerichtet ist. Weitere Informationen finden Sie unter Massenspeicher-Multipathing.

SRs vom Typ GFS2 können mit der xe CLI oder XenCenter erstellt und verwaltet werden.

Einschränkungen

Shared GFS2-Speicher weist derzeit folgende Einschränkungen auf:

- Die VM-Migration mit Speicher-Livemigration wird für VMs, deren VDIs sich auf einem GFS2 SR befinden, nicht unterstützt.
- Das FCoE-Protokoll wird von GFS2 SRs nicht unterstützt.
- Trim/Unmap wird auf GFS2 SRs nicht unterstützt.
- Leistungsmetriken sind für GFS2 SRs und Festplatten auf diesen SRs nicht verfügbar.

- Die geänderte Blockverfolgung wird für VDIs, die auf GFS2 SRs gespeichert sind, nicht unterstützt.
- VDIs, die größer als 2 TiB sind, können nicht als VHD oder OVA/OVF exportiert werden. Sie können jedoch VMs mit VDIs größer als 2 TiB im XVA-Format exportieren.

> **Hinweis:**
>
> Vorgänge auf GFS2 SRs können hängen bleiben, wenn Sie einen IP-Adresskonflikt (mehrere Hosts mit derselben IP-Adresse) in Ihrem Clusternetzwerk haben, auf dem mindestens ein Host mit aktiviertem Clustering beteiligt ist. In diesem Fall werden die Hosts nicht umzäunt. Um dieses Problem zu beheben, beheben Sie den IP-Adresskonflikt.

Erstellen eines gemeinsam genutzten GFS2 über iSCSI SR mithilfe des Software-iSCSI-Initiators

Sie können GFS2 über iSCSI-SRs mit XenCenter erstellen. Weitere Informationen finden Sie Software-iSCSI-Speicher in der XenCenter Produktdokumentation.

Alternativ können Sie die xe CLI verwenden, um eine 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 die SR hostet	Ja
`SCSIid`	SCSI-ID des Geräts	Ja

Sie können die Werte finden, die für diese Parameter verwendet werden sollen, indem Sie den`xe sr-probe-ext` Befehl verwenden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Starten Sie mit dem folgenden Befehl:

```
xe sr-probe-ext type=gfs2 device-config:provider=iscsi
```


Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben und gibt bei jedem Schritt eine Liste möglicher Werte an.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.
3. Wenn die Befehlsausgabe mit beginnt `The following SRs were found:`, können Sie die `device-config` Parameter verwenden, die Sie angegeben haben, um die SR beim Ausführen des `xe sr-create` Befehls zu suchen.

Führen Sie den folgenden Befehl auf einem Server in Ihrem Clusterpool aus, um eine freigegebene GFS2-SR auf einer bestimmten LUN eines iSCSI-Ziels zu erstellen:

```
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, können einige Hosts im Clusterpool einen Zaun aufweisen.

Weitere Hinweise zum Arbeiten mit iSCSI-SRs finden Sie unterSoftware-iSCSI-Unterstützung.

Erstellen eines gemeinsam genutzten GFS2 über HBA SR

Sie können GFS2 über HBA-SRs mit XenCenter erstellen. Weitere Informationen finden Sie Hardware-HBA-Speicher in der XenCenter Produktdokumentation.

Alternativ können Sie die xe CLI verwenden, um eine 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 Werte finden, die für den Parameter SCSIID verwendet werden sollen, indem Sie den`xe sr-probe-ext` Befehl verwenden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Starten Sie mit dem folgenden Befehl:


```
xe sr-probe-ext type=gfs2 device-config:provider=hba
```

Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben und gibt bei jedem Schritt eine Liste möglicher Werte an.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.
3. Wenn die Befehlsausgabe mit beginnt `The following SRs were found:`, können Sie die `device-config` Parameter verwenden, die Sie angegeben haben, um die SR beim Ausführen des `xe sr-create` Befehls zu suchen.

Um eine freigegebene 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
```

Weitere Hinweise zum Arbeiten mit HBA-SRs finden Sie unterHardware-Hostbusadapter.

NFS und SMB

Freigaben auf NFS-Servern (die NFSv4 oder NFSv3 unterstützen) oder auf SMB-Servern (die SMB 3.0 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, Folgendes:

- VMs, die auf allen Citrix Hypervisor or-Servern in einem Ressourcenpool gestartet werden sollen
- VM-Migration zwischen Citrix Hypervisor or-Servern in einem Ressourcenpool mittels Live-Migration (ohne spürbare Ausfallzeiten)

> **Wichtig:**
>
> - Die Unterstützung für SMB 3.0 beschränkt sich auf die Möglichkeit, eine Verbindung mit einer Freigabe mithilfe des 3.0-Protokolls herzustellen. Zusätzliche Funktionen wie Transparent Failover hängen von der Feature-Verfügbarkeit im Upstream-Linux-Kernel ab und werden in Citrix Hypervisor 8.0 nicht unterstützt.
> - Für NFSv4`AUTH_SYS` wird nur der Authentifizierungstyp unterstützt.
> - SMB-Speicher ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.

VDIs, die auf dateibasierten SRs gespeichert sind, werden *dünn bereitgestellt*. Die Image-Datei wird zugewiesen, wenn 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 belegen, wie es erforderlich ist. Wenn beispielsweise ein VDI mit 100 GB für eine VM zugewiesen wird und ein Betriebssystem installiert ist, spiegelt die VDI-Datei nur die Größe der auf den Datenträger geschriebenen Betriebssystemdaten statt der gesamten 100 GB wider.

VHD-Dateien können auch verkettet werden, sodass zwei VDIs gemeinsame Daten gemeinsam nutzen können. In Fällen, in denen eine dateibasierte VM geklont wird, verwenden die resultierenden VMs die gemeinsamen Daten auf der Festplatte zum Zeitpunkt des Klonens. 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 Citrix Hypervisor 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 die Inhalte von VDIs beschädigt werden können.

Citrix Hypervisor wurde für Massenspeicher der Enterprise-Klasse optimiert, der nicht-flüchtigen RAM verwendet, um schnelle Bestätigungen von Schreibanforderungen bereitzustellen und gleichzeitig ein hohes Maß an Datenschutz vor Ausfällen zu gewährleisten. Citrix Hypervisor wurde mit Data onTap 7.3 und 8.1 umfassend gegen Network Appliance FAS2020- und FAS3210-Speicher getestet.

> **Warnhinweis:**
>
> Da VDIs auf dateibasierten SRs als Thin Provisioning erstellt werden, müssen Administratoren sicherstellen, dass die dateibasierten SRs über genügend Speicherplatz für alle erforderlichen VDIs verfügen. Citrix Hypervisor or-Server erzwingen nicht, dass der für VDIs auf dateibasierten SRs erforderliche Speicherplatz vorhanden ist.

Erstellen eines freigegebenen NFS-SR (NFS)

Um eine NFS-SR zu erstellen, müssen Sie den Hostnamen oder die IP-Adresse des NFS-Servers angeben. Sie können die SR auf jedem gültigen Zielpfad erstellen. Verwenden Sie den`sr-probe` Befehl, um eine Liste gültiger Zielpfade anzuzeigen, die vom Server exportiert werden.

In Szenarien, in denen Citrix Hypervisor mit Lower-End-Speicher verwendet wird, wird vorsichtig darauf gewartet, dass alle Schreibvorgänge bestätigt werden, bevor Bestätigungen an VMs übergeben werden. Dieser Ansatz verursacht spürbare Performance-Kosten und kann gelöst werden, indem der Speicher so eingestellt wird, dass der SR-Bereitstellungspunkt als asynchronen Modus exportiert wird.

Asynchrone Exporte bestätigen Schreibvorgänge, die sich nicht auf der Festplatte befinden. Berücksichtigen Sie die Risiken des Scheiterns in diesen Situationen sorgfältig.

> **Hinweis:**
>
> Der NFS-Server muss so konfiguriert sein, dass er den angegebenen Pfad auf alle Server im Pool exportiert. Wenn diese Konfiguration nicht erfolgt, schlägt die Erstellung des SR und das Einstecken des PBD-Datensatzes fehl.

Die Citrix Hypervisor NFS-Implementierung verwendet standardmäßig TCP. Wenn Ihre Situation dies zulässt, können Sie die Implementierung so konfigurieren, dass UDP in Szenarien verwendet wird, in denen ein Leistungsvorteil besteht. Geben Sie für diese Konfiguration beim Erstellen einer SR den`device-config` Parameter an`useUDP=true` .

Gerätekonfigurationsparameter für NFS-SRs:

Parametername	Beschreibung	Erforderlich?
`server`	IP-Adresse oder Hostname des NFS-Servers	Ja
`serverpath`	Pfad, einschließlich des NFS-Bereitstellungspunkts, zum NFS-Server, der die SR hostet	Ja

Verwenden Sie beispielsweise den folgenden Befehl, um einen freigegebenen NFS-SR auf`192.168.1.10:/export1`zu erstellen:

```
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 \
nfsversion="3", "4"
```

Führen Sie den folgenden Befehl aus, um einen nicht freigegebenen NFS-SR 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 \
nfsversion="3", "4"
```


Erstellen eines gemeinsam genutzten SMB-SR (SMB)

Geben Sie zum Erstellen einer SMB-SR den Hostnamen oder die IP-Adresse des SMB-Servers, den vollständigen Pfad der exportierten Freigabe und die entsprechenden Anmeldeinformationen ein.

> **Hinweis:**
>
> SMB SR wurde gegen Network Appliance-Speicher getestet, auf denen OnTap 8.3 und Windows Server 2012 R2 ausgeführt wird.

Gerätekonfigurationsparameter für SMB-SRs:

Parametername	Beschreibung	Erforderlich?
`server`	Vollständiger Pfad zur Freigabe auf dem Server	Ja
`username`	Benutzerkonto mit RW-Zugriff auf Freigabe	Optional
`password`	Passwort für das Benutzerkonto	Optional

Verwenden Sie beispielsweise den folgenden Befehl, um eine gemeinsam genutzte SMB-SR auf`192.168.1.10:/share1`zu erstellen:

```
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=
         valid_password type=smb
```

Führen Sie den folgenden Befehl aus, um eine nicht gemeinsam genutzte 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=
         valid_password type=smb
```

> **Hinweis:**
>
> Wenn Sie den `sr-create` Befehl ausführen, können Sie das `device-config:password_secret` Argument verwenden, anstatt das Kennwort in der Befehlszeile anzugeben. Weitere Informationen finden Sie unter Geheimnisse.

LVM über Hardware-HBA

Der HBA-Typ „LVM over Hardware“ stellt Festplatten als VHDs auf logischen Volumes innerhalb einer Volumegruppe dar, die auf einer HBA-LUN erstellt wurde, die beispielsweise hardwarebasierte iSCSI- oder FC-Unterstützung bietet.

Citrix Hypervisor or-Server 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 machen, muss manuell abgeschlossen werden. Diese Konfiguration umfasst Speichergeräte, Netzwerkgeräte und den HBA innerhalb des Citrix Hypervisor or-Servers. Nachdem die gesamte FC-Konfiguration abgeschlossen ist, stellt der HBA ein von der FC-LUN gesichertes SCSI-Gerät für den Host bereit. 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`sr-probe` Befehl, 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 freigegebene SRs erstellt werden, auf die alle Hosts in einem Ressourcenpool zugreifen können.

Die gleichen Funktionen gelten für QLogic iSCSI-HBAs.

Weitere InformationenErstellen von Speicher-Repositorieszum Erstellen freigegebener HBA-basierter FC- und iSCSI-SRs finden Sie unter.

> **Hinweis:**
>
> Die Citrix Hypervisor 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 einer SR angegeben werden. VDIs innerhalb der SR werden VMs als Standardblockgeräte verfügbar gemacht.

Kopiert!
Failed!

Thin bereitgestellter gemeinsam genutzter GFS2-Blockspeicher

October 16, 2019

Thin Provisioning nutzt den verfügbaren Speicher besser, indem VDIs Speicherplatz zugewiesen wird, wenn Daten auf das virtuelle Laufwerk geschrieben werden, anstatt die volle virtuelle Größe des VDIs im Voraus zuzuweisen. Mit der Thin Provisioning können Sie den benötigten Speicherplatz

für ein gemeinsam genutztes Speicher-Array und damit Ihre Total Cost of Ownership (TCO) erheblich reduzieren.

Die Thin Provisioning für Shared Block Storage ist in folgenden Fällen von besonderem Interesse:

- Sie wollen mehr Platzeffizienz. Bilder sind dünn und nicht dick zugeordnet.
- Sie möchten die Anzahl der E/A-Vorgänge pro Sekunde auf Ihrem Speicher-Array reduzieren. Der GFS2 SR ist der erste SR-Typ, der Speicherlesecaching auf Shared Block Storage unterstützt.
- Sie verwenden ein gemeinsames Basisabbild für mehrere virtuelle Maschinen. Die Images einzelner VMs verbrauchen dann in der Regel noch weniger Speicherplatz.
- Sie verwenden Schnappschüsse. Jeder Snapshot ist ein Bild, und jedes Bild ist jetzt dünn.
- Ihr Speicher unterstützt NFS nicht und unterstützt nur Blockspeicher. Wenn Ihr Speicher NFS unterstützt, empfehlen wir, 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.

Der freigegebene GFS2-Typ stellt Datenträger als Dateisystem dar, das auf einer iSCSI- oder HBA-LUN erstellt wurde. VDIs, die auf einem GFS2 SR gespeichert sind, werden im QCOW2-Bildformat gespeichert.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Alle Citrix Hypervisor or-Server im Clusterpool müssen über mindestens 2 GiB Steuerdomänenspeicher verfügen.
- Alle Hosts im Cluster müssen statische IP-Adressen für das Clusternetzwerk verwenden.
- Es wird empfohlen, Clustering nur in Pools zu verwenden, die mindestens drei Hosts enthalten, da Pools von zwei Hosts empfindlich darauf reagieren, den gesamten Pool selbst zu fechten.
- Wenn Sie über eine Firewall zwischen den Hosts in Ihrem Pool verfügen, stellen Sie sicher, dass Hosts über die folgenden Ports im Clusternetzwerk kommunizieren können:
  - TCP: 8892, 21064
  - UDP: 5404, 5405

  Weitere Informationen finden Sie unter Von Citrix Technologies verwendete Kommunikationsports.
- Wenn Sie einen vorhandenen Pool gruppieren, stellen Sie sicher, dass die hohe Verfügbarkeit deaktiviert ist. Sie können die Hochverfügbarkeit wieder aktivieren, nachdem das Clustering aktiviert ist.
- Sie verfügen über ein blockbasiertes Speichergerät, das für alle Citrix Hypervisor or-Server im Ressourcenpool sichtbar ist.

Einrichten eines Clusterpools für die Verwendung eines gemeinsam genutzten GFS2 SR

Um gemeinsam genutzten GFS2-Speicher zu verwenden, muss der Citrix Hypervisor Ressourcenpool ein Clusterpool sein. Aktivieren Sie Clustering in Ihrem Pool, bevor Sie eine GFS2 SR erstellen.

> **Hinweis:**
>
> Cluster-Pools verhalten sich anders als nicht gruppierte Pools. Weitere Hinweise zum Clusterverhalten finden Sie unterCluster-Pools.

Wenn Sie möchten, können Sie Clustering in Ihrem Pool mithilfe von XenCenter einrichten. Weitere Informationen finden Sie unter XenCenter Produktdokumentation.

So erstellen Sie einen gruppierten Pool mithilfe der xe-CLI:

1. Erstellen Sie ein gebundenes Netzwerk, das als Clusternetzwerk verwendet werden soll. Führen Sie auf dem Citrix Hypervisor or-Server, der der Poolmaster sein soll, die folgenden Schritte aus:

   a) Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.

   b) Benennen Sie Ihren Ressourcenpool mithilfe des folgenden Befehls:

   ```
   xe pool-param-set name-label=”New Pool” uuid=<pool_uuid>
   ```

   c) Erstellen Sie mit dem folgenden Befehl ein Netzwerk zur Verwendung mit der gebundenen NIC:

   ```
   xe network-create name-label=bond0
   ```

   Die UUID des neuen Netzwerks wird zurückgegeben.

   d) Suchen Sie die UUIDs der PIF, die in der Bindung verwendet werden sollen, indem Sie den folgenden Befehl verwenden:

   ```
   xe pif-list
   ```

   e) Erstellen Sie Ihr gebundene Netzwerk entweder im Aktiv-Aktiv-Modus, im Aktiv-Passiv-Modus oder im LACP-Bond-Modus. Je nach Anleihemodus, den Sie verwenden möchten, führen Sie eine der folgenden Aktionen aus:

   - Um die Bindung im Aktiv-Aktiv-Modus (Standard) zu konfigurieren, verwenden Sie den `bond-create` Befehl, um die Bindung zu erstellen. Geben Sie mithilfe von Kommas die neu erstellte Netzwerk-UUID und die UUIDs der zu gebundenen PIFs an:

   ```
   xe bond-create network-uuid=<network_uuid> /
        pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
           pif_uuid_4>
   ```


Geben Sie zwei UUIDs ein, wenn Sie zwei Netzwerkkarten und vier UUIDs verkleben, wenn Sie vier Netzwerkkarten miteinander vereinen. Die UUID für die Bindung wird nach dem Ausführen des Befehls zurückgegeben.

- Um die Bindung im Aktiv-Passiv- oder LACP-Bond-Modus zu konfigurieren, verwenden Sie die gleiche Syntax, fügen Sie den optionalen `mode` Parameter hinzu und geben Sie Folgendes `lacp` an `active-backup`:

```
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
```

Nachdem Sie das gebundene Netzwerk auf dem Poolmaster erstellt haben und andere Citrix Hypervisor or-Server mit dem Pool verbinden, werden die Netzwerk- und Bondinformationen automatisch auf den beitrittenden Server repliziert.

Weitere Informationen finden Sie unter Vernetzung.

2. Erstellen Sie einen Ressourcenpool mit mindestens drei Citrix Hypervisor or-Servern.

   Wiederholen Sie die folgenden Schritte auf jedem Citrix Hypervisor or-Server, der ein (nicht Master-) Pool-Mitglied ist:

   a) Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.

   b) Verbinden Sie den Citrix Hypervisor or-Server mit dem Pool auf dem Poolmaster mithilfe des folgenden Befehls:

```
xe pool-join master-address=master_address master-username=
    administrators_username master-password=password
```

   Der Wert des`master-address` Parameters muss auf den vollqualifizierten Domänennamen des Citrix Hypervisor or-Servers festgelegt werden, der der Poolmaster ist. Das`password` muss das Administratorkennwort sein, das bei der Installation des Poolmasters festgelegt wurde.

   Weitere Informationen finden Sie unter Hosts und Ressourcenpools.

3. Legen Sie für jedes PIF fest, das zu diesem Netzwerk gehört`disallow-unplug=`**`true`**.

   a) Suchen Sie die UUIDs der PIFs, die zum Netzwerk gehören, mithilfe des folgenden Befehls:

```
xe pif-list
```

   b) Führen Sie den folgenden Befehl auf einem Citrix Hypervisor or-Server im Ressourcenpool aus:


```
xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

4. Aktivieren Sie Clustering in Ihrem Pool. Führen Sie den folgenden Befehl auf einem Citrix Hypervisor or-Server im Ressourcenpool aus:

   ```
   xe cluster-pool-create network-uuid=<network_uuid>
   ```

   Geben Sie die UUID des gebundenen Netzwerks an, das Sie in einem früheren Schritt erstellt haben.

Einrichten von Speicher-Multipathing für Ihre gemeinsam genutzte GFS2 SR

> **Wichtig:**
>
> Bevor Sie versuchen, Multipathing zu aktivieren, stellen Sie sicher, dass die folgenden Anweisungen zutreffen:
>
> - Mehrere Ziele sind auf Ihrem Speicherserver verfügbar.
>
>   Beispielsweise gibt ein iSCSI-Speicher-Back-End, das auf einem bestimmten Portal nach `sendtargets` 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.Erdbeer:litchie
>   192.168.0. 204:3260 ,2 iqn.Erdbeer:litchie
>   ```
>
> - Nur für iSCSI verfügt dom0 über eine IP-Adresse in jedem Subnetz, das vom Multipath-Speicher verwendet wird.
>
>   Stellen Sie sicher, dass für jeden Pfad, den Sie zum Speicher benötigen, eine Netzwerkkarte vorhanden ist und dass auf jeder Netzwerkkarte eine IP-Adresse konfiguriert ist. Wenn Sie beispielsweise vier Pfade zu Ihrem Speicher benötigen, müssen Sie über vier Netzwerkkarten verfügen, für die jeweils eine IP-Adresse konfiguriert ist.
>
> - Nur für HBA sind mehrere HBA mit der Switch-Fabric verbunden.

Sie können XenCenter verwenden, um Speicher-Multipathing einzurichten. Weitere Informationen finden Sie Massenspeicher-Multipathing in der XenCenter Produktdokumentation.

Wenn Sie alternativ die xe-CLI zum Einrichten von Speichermultipathing verwenden möchten, führen Sie die folgenden Schritte auf allen Citrix Hypervisor or-Servern im Clusterpool aus:

1. Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.
2. Trennen Sie alle PBDs auf dem Server mithilfe des folgenden Befehls:


```
xe pbd-unplug uuid=<pbd_uuid>
```

3. Setzen Sie den Wert des `other-config:multipathing` Parameters auf, **`true`** indem Sie den folgenden Befehl verwenden:

```
xe host-param-set other-config:multipathing=true uuid=<server_uuid
    >
```

4. Setzen Sie den Wert des `other-config:multipathhandle` Parameters auf, `dmp` indem Sie den folgenden Befehl verwenden:

```
<server_uuid>xe host-param-set other-config:multipathhandle=dmp
    uuid=
```

5. Wenn auf dem Server bereits SRs vorhanden sind, die im Einzelpfadmodus ausgeführt werden, aber mehrere Pfade aufweisen:
   - Migrieren oder suspendieren von laufenden Gästen mit virtuellen Laufwerken in den betroffenen SRs
   - Trennen Sie die PBD aller betroffenen SRs, und schließen Sie sie erneut an, um sie mithilfe von Multipathing wiederherzustellen:

```
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
```

Weitere Informationen finden Sie unter Massenspeicher-Multipathing.

Erstellen einer gemeinsam genutzten GFS2 SR

Sie können Ihre freigegebene GFS2 SR auf einem iSCSI oder einer HBA-LUN erstellen.

Erstellen eines gemeinsam genutzten GFS2 über iSCSI SR

Sie können GFS2 über iSCSI-SRs mit XenCenter erstellen. Weitere Informationen finden Sie Software-iSCSI-Speicher in der XenCenter Produktdokumentation.

Alternativ können Sie die xe CLI verwenden, um eine 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 die SR hostet	Ja
`SCSIid`	SCSI-ID des Geräts	Ja

Sie können die Werte finden, die für diese Parameter verwendet werden sollen, indem Sie den`xe sr-probe-ext` Befehl verwenden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Starten Sie mit dem folgenden Befehl:

   ```
   xe sr-probe-ext type=gfs2 device-config:provider=iscsi
   ```

   Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben und gibt bei jedem Schritt eine Liste möglicher Werte an.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.

3. Wenn die Befehlsausgabe mit beginnt `The following SRs were found:`, können Sie die `device-config` Parameter verwenden, die Sie angegeben haben, um die SR beim Ausführen des `xe sr-create` Befehls zu suchen.

Führen Sie den folgenden Befehl auf einem Server in Ihrem Clusterpool aus, um eine freigegebene GFS2-SR auf einer bestimmten LUN eines iSCSI-Ziels zu erstellen:

```
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, können einige Hosts im Clusterpool einen Zaun aufweisen.

Weitere Hinweise zum Arbeiten mit iSCSI-SRs finden Sie unterSoftware-iSCSI-Unterstützung.

Erstellen eines gemeinsam genutzten GFS2 über HBA SR

Sie können GFS2 über HBA-SRs mit XenCenter erstellen. Weitere Informationen finden Sie Hardware-HBA-Speicher in der XenCenter Produktdokumentation.

Alternativ können Sie die xe CLI verwenden, um eine 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 Werte finden, die für den Parameter SCSIID verwendet werden sollen, indem Sie den `xe sr-probe-ext` Befehl verwenden.

```
xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
    config> sm-config:=<sm_config>
```

1. Starten Sie mit dem folgenden Befehl:

   ```
   xe sr-probe-ext type=gfs2 device-config:provider=hba
   ```

   Die Ausgabe des Befehls fordert Sie auf, zusätzliche Parameter anzugeben und gibt bei jedem Schritt eine Liste möglicher Werte an.

2. Wiederholen Sie den Befehl und fügen Sie jedes Mal neue Parameter hinzu.

3. Wenn die Befehlsausgabe mit beginnt `The following SRs were found:`, können Sie die `device-config` Parameter verwenden, die Sie angegeben haben, um die SR beim Ausführen des `xe sr-create` Befehls zu suchen.

Um eine freigegebene 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
```

Weitere Hinweise zum Arbeiten mit HBA-SRs finden Sie unterHardware-Hostbusadapter.

Einschränkungen

Shared GFS2-Speicher weist derzeit folgende Einschränkungen auf:

- Die VM-Migration mit Speicher-Livemigration wird für VMs, deren VDIs sich auf einem GFS2 SR befinden, nicht unterstützt.
- Das FCoE-Protokoll wird von GFS2 SRs nicht unterstützt.
- Trim/Unmap wird auf GFS2 SRs nicht unterstützt.
- Leistungsmetriken sind für GFS2 SRs und Festplatten auf diesen SRs nicht verfügbar.
- Die geänderte Blockverfolgung wird für VDIs, die auf GFS2 SRs gespeichert sind, nicht unterstützt.
- VDIs, die größer als 2 TiB sind, können nicht als VHD oder OVA/OVF exportiert werden. Sie können jedoch VMs mit VDIs größer als 2 TiB im XVA-Format exportieren.
- Cluster-Pools unterstützen nur bis zu 16 Hosts pro Pool.
- Wenn ein Netzwerk sowohl für die Verwaltung als auch für die Clustererstellung verwendet wurde, können Sie das Verwaltungsnetzwerk nicht trennen, ohne den Cluster neu zu erstellen.
- Wenn Sie die IP-Adresse des Clusternetzwerks mithilfe von XenCenter ändern, müssen Clustering und GFS2 vorübergehend deaktiviert werden.
- Ändern Sie die Bindung Ihres Clusternetzwerks nicht, solange der Cluster live ist und VMs ausgeführt hat. Diese Aktion kann dazu führen, dass der Cluster einen Zaun aufweist.
- Wenn Sie einen IP-Adresskonflikt (mehrere Hosts mit derselben IP-Adresse) in Ihrem Clusternetzwerk haben, an dem mindestens ein Host mit aktiviertem Clustering beteiligt ist, werden die Hosts nicht gegrenzt. Um dieses Problem zu beheben, beheben Sie den IP-Adresskonflikt.

Kopiert!
Failed!

Verwalten von Speicher-Repositories

October 16, 2019

Dieser Abschnitt behandelt das Erstellen von Speicher-Repositor-Typen und deren Bereitstellung für Ihren Citrix Hypervisor or-Server. Es deckt auch verschiedene Vorgänge ab, die für die laufende Verwaltung von Speicher-Repositories (SRs) erforderlich sind, einschließlich Live-VDI-Migration.

Erstellen von Speicher-Repositories

In diesem Abschnitt wird erläutert, wie Sie Storage Repositories (SRs) verschiedener Typen erstellen und für Ihren Citrix Hypervisor or-Server verfügbar machen. Die Beispiele umfassen die Erstellung

von SRs mit der XE CLI. Weitere Informationen zur Verwendung des Assistenten „Neues Speicher-Repository“ zum Hinzufügen von SRs mit XenCenter finden Sie in der XenCenter-Hilfe.

> **Hinweis:**
>
> Lokale SRs vom Typ `lvm` und `ext3` können nur mit der XE CLI erstellt werden. Nach der Erstellung können Sie alle SR-Typen entweder über XenCenter oder die xe CLI verwalten.

Es gibt zwei grundlegende Schritte, um ein Speicher-Repository für die Verwendung auf einem Host mithilfe der CLI zu erstellen:

1. Prüfen Sie den SR-Typ, um Werte für alle erforderlichen Parameter zu ermitteln.
2. Erstellen Sie den SR, um das SR-Objekt und die zugehörigen PBD-Objekte zu initialisieren, die PBDs zu schließen und den SR zu aktivieren.

Diese Schritte unterscheiden sich je nach Typ der SR, die erstellt wird. In allen Beispielen gibt der `sr-create` Befehl die UUID des erstellten SR zurück, falls erfolgreich.

SRs können *zerstört* werden, wenn sie nicht mehr verwendet werden, um das physische Gerät freizumachen. SRs können auch *vergessen* werden, den SR von einem Citrix Hypervisor or-Server zu trennen und ihn an einen anderen anzuschließen. Weitere Informationen finden Sie unter *Entfernen von SRs* im folgenden Abschnitt.

Sonde einer SR

Der `sr-probe` Befehl kann auf folgende Arten verwendet werden:

- So identifizieren Sie unbekannte Parameter für die Verwendung beim Erstellen einer SR
- So geben Sie eine Liste vorhandener SRs zurück

In beiden `sr-probe` Fällen können Sie einen SR-Typ und einen oder mehrere `device-config` Parameter für diesen SR-Typ angeben. Wenn ein unvollständiger Satz von Parametern angegeben wird, gibt der `sr-probe` Befehl eine Fehlermeldung zurück, in der angegeben wird, dass Parameter fehlen und die möglichen Optionen für die fehlenden Parameter angegeben werden. Wenn ein kompletter Satz von Parametern angegeben wird, wird eine Liste der vorhandenen SRs zurückgegeben. Alle `sr-probe` Ausgaben werden als XML zurückgegeben.

Beispielsweise kann ein bekanntes iSCSI-Ziel 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" ?>
```



```
    <iscsi-target-iqns>
        <TGT>
            <Index>
                0
            </Index>
            <IPAddress>
                192.168.1.10
            </IPAddress>
            <TargetIQN>
                iqn.192.168.1.10:filer1
            </TargetIQN>
        </TGT>
    </iscsi-target-iqns>
```

Wenn Sie dasselbe Ziel erneut ermitteln und sowohl den Namen/die IP-Adresse als auch den gewünschten IQN angeben, wird der Satz von`SCSIids` (LUNs) zurückgegeben, der auf dem Target/IQN verfügbar ist.

```
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>
```

Das Sondieren des gleichen Ziels und das Bereitstellen aller drei Parameter gibt eine Liste der SRs zurück, die auf der LUN vorhanden sind.

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
```



```
2     device-config:targetIQN=192.168.1.10:filer1 \
3     device-config:SCSIid=149455400000000000000000002000000
         b70200000f000000
4
5     <?xml version="1.0" ?>
6     <SRlist>
7         <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>
```

Für jeden SR-Typ können folgende Parameter untersucht werden:

SR-Typ	Die`device-config` Parameter, 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
`NetApp`	`target`	Nein	Ja
	`username`	Nein	Ja
	`password`	Nein	Ja
	`chapuser`	Nein	Nein
	`chappassword`	Nein	Nein
	`aggregate`	Nein (siehe Anmerkung 1)	Ja
	`FlexVols`	Nein	Nein

SR-Typ	Die`device-config` Parameter, in der Reihenfolge der Abhängigkeit	Kann untersucht werden?	Erforderlich für`sr-create`?
	`allocation`	Nein	Nein
	`asis`	Nein	Nein
`nfs`	`server`	Nein	Ja
	`serverpath`	Ja	Ja
`lvm`	`device`	Nein	Ja
`ext`	`device`	Nein	Ja
`EqualLogic`	`target`	Nein	Ja
	`username`	Nein	Ja
	`password`	Nein	Ja
	`chapuser`	Nein	Nein
	`chappassword`	Nein	Nein
	`storagepool`	Nein (siehe Anmerkung 2)	Ja

Hinweise:

- Aggregatsondierung ist nur`sr-create` zeitweilig möglich.
- Das Sondieren des Speicherpools ist nur`sr-create` zeitweilig möglich.

SRs entfernen

Ein Speicher-Repository (SR) kann entweder vorübergehend oder dauerhaft entfernt werden.

Trennen: Unterbricht die Verknüpfung zwischen dem Speichergerät und dem Pool oder dem Host (PBD Unplug). Der SR (und seine VDIs) wird nicht mehr zugänglich. Der Inhalt der VDIs und die Meta-Informationen, die von VMs für den Zugriff auf die VDIs verwendet werden, bleiben erhalten. Trennen kann verwendet werden, wenn Sie einen SR vorübergehend offline schalten, z. B. für Wartungsarbeiten. Ein freistehendes SR kann später wieder angebracht werden.

Vergessen: Behält den Inhalt des SR auf der physischen Festplatte bei, aber die Informationen, die eine VM mit ihren VDIs verbindet, werden dauerhaft gelöscht. So können Sie beispielsweise die SR erneut an einen anderen Citrix Hypervisor or-Server anschließen, ohne den SR-Inhalt zu entfernen.

Destroy: Löscht den Inhalt der SR von der physischen Festplatte.

Bei Destroy or Forget muss die mit dem SR verbundene PBD vom Host getrennt werden.

1. Trennen Sie die PBD, um die SR vom entsprechenden Citrix Hypervisor or-Server zu trennen:

```
xe pbd-unplug uuid=pbd_uuid
```

2. Verwenden Sie den`sr-destroy` Befehl, um eine SR zu entfernen. Der Befehl zerstört den SR, löscht den SR und die entsprechende PBD aus der Citrix Hypervisor or-Serverdatenbank und löscht den SR-Inhalt von der physischen Festplatte:

```
xe sr-destroy uuid=sr_uuid
```

3. Verwenden Sie den`sr-forget` Befehl, um eine SR zu vergessen. Der Befehl entfernt die SR und die entsprechende PBD aus der Citrix Hypervisor or-Serverdatenbank, belässt jedoch den tatsächlichen SR-Inhalt auf dem physischen Medium intakt:

```
xe sr-forget uuid=sr_uuid
```

> **Hinweis:**
>
> Es kann einige Zeit dauern, bis das Software-Objekt, das der SR entspricht, Müll gesammelt wird.

Einführung einer SR

Um eine zuvor *vergessene* SR wieder einzuführen, erstellen Sie eine PBD. Schließen Sie die PBD manuell an die entsprechenden Citrix Hypervisor or-Server an, um die SR zu aktivieren.

Im folgenden Beispiel wird ein SR vom Typ eingeführt`lvmoiscsi`.

1. Prüfen Sie den vorhandenen SR, um seine UUID zu bestimmen:

```
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
```

2. Führen Sie die vorhandene SR-UUID ein, die vom`sr-probe` Befehl zurückgegeben wurde. Die UUID des neuen SR wird zurückgegeben:

```
xe sr-introduce content-type=user name-label="Example Shared LVM
   over iSCSI SR" \
    shared=true uuid=valid_sr_uuid type=lvmoiscsi
```

3. Erstellen Sie eine PBD zur Begleitung des 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
```

4. Schließen Sie die PBD an, um die SR zu befestigen:

```
xe pbd-plug uuid=pbd_uuid
```

5. Überprüfen Sie den Status des PBD-Steckers. Wenn dies erfolgreich ist, ist die`currently-attached` Eigenschaft wahr:

```
xe pbd-list sr-uuid=sr_uuid
```

> **Hinweis:**
>
> Führen Sie die Schritte 3 bis 5 für jeden Server im Ressourcenpool aus. Diese Schritte können auch mit der Funktion „Speicher-Repository 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 Citrix Hypervisor or-Server bereitgestellten LUN zu erhöhen. Mit der Live-LUN-Erweiterung können Sie die Größe der LUN ohne Ausfallzeiten der VM erhöhen.

Nachdem Sie Ihrem Storage-Array mehr Kapazität hinzugefügt haben, geben Sie

```
xe sr-scan sr-uuid=sr_uuid
```

Mit diesem Befehl wird die SR erneut eingebläst, und jede zusätzliche Kapazität wird hinzugefügt und zur Verfügung gestellt.

Dieser Vorgang ist auch in XenCenter verfügbar. Select die zu verkleinernde SR aus, und klicken Sie dann auf **Erneut scannen**. Weitere Informationen erhalten Sie, wenn Sie **F1** drücken, um die XenCenter Hilfe anzuzeigen.

> **Warnungen:**
>
> - Es ist nicht möglich, LUNs zu verkleinern oder zu kürzen. Die Verringerung der LUN-Größe im Speicher-Array kann zu Datenverlust führen.

Live-VDI-Migration

Mit der Live-VDI-Migration kann der Administrator das virtuelle Laufwerk (Virtual Disk Image, VDI) verschieben, 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.
- Verschieben zwischen Speicherstufen, wenn eine VM durch die Speicherkapazität begrenzt ist.
- Durchführung von Speicher-Array-Upgrades.

Einschränkungen und Vorbehalte

Live-VDI-Migration unterliegt den folgenden Einschränkungen und Vorbehalte

- Im Ziel-Repository muss genügend Speicherplatz zur Verfügung stehen.

So verschieben Sie virtuelle Laufwerke mithilfe von XenCenter

1. Wählen Sie im Bereich **Ressourcen** die SR aus, in der das virtuelle Laufwerk 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 **Virtuelles Laufwerk verschieben** die Ziel-SR aus, in die Sie den VDI verschieben möchten.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass der SR genügend Speicherplatz für ein anderes virtuelles Laufwerk hat: Der verfügbare Speicherplatz wird in der Liste der verfügbaren SRs angezeigt.

4. Klicken Sie auf **Verschieben**, um das virtuelle Laufwerk zu verschieben.

Informationen zu xe CLI finden Sie unter [`vdi-pool-migrate`] (/de-de/citrix-hypervisor/command-line-interface.html #vdi -pool-migrate).

Cold VDI-Migration zwischen SRs (Offline-Migration)

VDIs, die einer VM zugeordnet sind, können von einem SR in eine andere kopiert werden, um Wartungsanforderungen oder Tiered Storage-Konfigurationen zu erfüllen. Mit XenCenter können Sie eine VM und alle VDIs in dieselbe oder eine andere SR kopieren. Eine Kombination aus XenCenter und der xe CLI kann zum Kopieren einzelner VDIs verwendet werden.

Informationen zu xe CLI finden Sie unter [vm-migrate] (/de-de/citrix-hypervisor/command-line-interface.html #vm -migrate).

Kopieren aller VDIs einer VM in eine andere SR

Die XenCenter Copy VM-Funktion erstellt Kopien aller VDIs für eine ausgewählte VM auf derselben oder einer anderen SR. Die Quell-VM und die VDIs sind standardmäßig nicht betroffen. Um die VM in die 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 Option **VM** > **kopieren**aus.
3. Select die gewünschte Ziel-SR.

Einzelne VDIs in eine andere SR kopieren

Eine Kombination aus 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,`vdi-uuid` wird sie als aufgeführt`not in database` und kann ignoriert werden.

   ```
   1 xe vbd-list vm-uuid=valid_vm_uuid
   ```

   > **Hinweis:**
   >
   > Der`vbd-list` Befehl zeigt sowohl die VBD- als auch die VDI-UUIDs an. Achten Sie darauf, die VDI-UUIDs anstelle der VBD-UUIDs aufzuzeichnen.

3. Wählen Sie in XenCenter die Registerkarte **VM-Speicher** aus. Wählen Sie für jeden VDI, der verschoben werden soll, den VDI aus und klicken Sie auf die Schaltfläche **Trennen** . Dieser Schritt kann auch mit dem`vbd-destroy` Befehl ausgeführt werden.

   > **Hinweis:**
   >
   > Wenn Sie den`vbd-destroy` Befehl zum Trennen der VDI-UUIDs verwenden, prüfen Sie zunächst, ob der Parameter auf der VBD`other-config:owner` eingestellt ist**`true`** . Setzen Sie diesen Parameter auf**`false`**. Durch die Ausgabe des`vbd-destroy` Befehls mit wird`other-config:owner=true` auch der zugehörige VDI zerstört.

4. Verwenden Sie den`vdi-copy` Befehl, um alle VM-VDIs zu kopieren, die in die gewünschte SR verschoben werden sollen.


```
xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
```

5. Wählen Sie in XenCenter die Registerkarte **VM-Speicher** aus. Klicken Sie auf die Schaltfläche **Anfügen** , und wählen Sie die VDIs aus der neuen SR aus. Dieser Schritt kann auch mit dem`vbd -create` Befehl ausgeführt werden.
6. Um die ursprünglichen VDIs zu löschen, wählen Sie die Registerkarte **Speicher** des ursprünglichen SR in XenCenter. Die ursprünglichen VDIs werden mit einem leeren Wert für das VM-Feld aufgeführt. Verwenden Sie die Schaltfläche **Löschen** , um den VDI zu löschen.

Konvertieren lokaler Fibre-Channel-SRs in freigegebene SRs

Verwenden Sie die xe-CLI und das XenCenter **Reparaturspeicher-Repository-Feature** , um einen lokalen FC-SR in einen gemeinsam genutzten FC-SR zu konvertieren:

1. Aktualisieren Sie alle Hosts im Ressourcenpool auf Citrix Hypervisor 8.0.
2. Stellen Sie sicher, dass alle Hosts im Pool die LUN der SR entsprechend in Zonen eingeteilt sind. Weitere InformationenSonde einer SRzur Verwendung des`sr-probe`Befehls zur Überprüfung, ob die LUN auf jedem Host vorhanden ist, finden Sie unter.
3. Konvertieren Sie die SR in gemeinsam genutzte:

```
xe sr-param-set shared=true uuid=local_fc_sr
```

4. Der SR wird von der Hostebene auf die Pool-Ebene in XenCenter verschoben, was darauf hinweist, dass er jetzt freigegeben ist. Der SR ist mit einem roten Ausrufezeichen markiert, um anzuzeigen, dass er derzeit nicht auf allen Hosts im Pool angeschlossen ist.
5. Select die SR und dann die Option Storage**Repair **Storage**Repository** > aus.
6. Klicken Sie auf **Reparieren** , um eine PBD für jeden Host im Pool zu erstellen und zu verbinden.

Rückgewinnung von Speicherplatz für blockbasierte Speicherung im Backing-Array mithilfe von discard

Sie können die Speicherplatzgewinnung verwenden, um nicht verwendete Blöcke auf einer dünn bereitgestellten LUN freizugeben. Nachdem der Speicherplatz freigegeben wurde, kann das Speicher-Array diesen zurückgegebenen Speicherplatz wieder verwenden.

> **Hinweis:**
>
> Speicherplatzgewinnung ist nur bei einigen Arten von Speicher-Arrays verfügbar. Informationen dazu, ob Ihr Array diese Funktion unterstützt und ob es eine bestimmte Konfiguration benötigt,

> finden Sie in der DokumentationHardwarekompatibilitätslisteund Ihrem Speicheranbieter.

So rufen Sie den Speicherplatz mithilfe von XenCenter zurück:

1. Select die **Infrastrukturansicht** aus, und wählen Sie dann den mit der SR verbundenen Server oder Pool aus.
2. Klicken Sie auf die Registerkarte **Speicher**.
3. Select die SR aus der Liste aus, und klicken Sie auf **Freier Speicherplatz zurückfordern**.
4. Klicken Sie auf **Ja** , um den Vorgang zu bestätigen.
5. Klicken Sie auf **Benachrichtigungen** und dann auf **Ereignisse** , um den Status des Vorgangs anzuzeigen.

Weitere Informationen erhalten Sie, wenn SieF1in XenCenter drücken, um auf die Online-Hilfe zuzugreifen.

> **Hinweise:**
>
> - Dieser Vorgang ist nur in XenCenter verfügbar.
> - Der Vorgang ist nur für LVM-basierte SRs verfügbar, die auf dünn bereitgestellten LUNs auf dem Array basieren. Lokale SSDs können auch von der Speicherplatzgewinnung profitieren.
> - Speicherplatzgewinnung ist für dateibasierte SRs wie NFS und Ext3 nicht erforderlich. Die Schaltfläche **Freier Speicherplatz** freigeben ist in XenCenter für diese SR-Typen nicht verfügbar.
> - Space Reclamation ist ein intensiver Vorgang und kann zu einer Verschlechterung der Speicher-Array-Performance führen. Starten Sie diesen Vorgang daher nur, wenn die Speicherplatzgewinnung auf dem Array erforderlich ist. Es wird empfohlen, diese Arbeit außerhalb der maximalen Array-Bedarfsstunden zu planen.

Automatisches Zurückholen von Speicherplatz beim Löschen von Snapshots

Beim Löschen von Snapshots mit Citrix Hypervisor wird der auf LVM-basierten SRs zugewiesene Speicherplatz automatisch wiederhergestellt, und ein Neustart der virtuellen Maschine ist nicht erforderlich. Dieser Vorgang wird als „Online Coalescing“ bezeichnet.

Online Coalescing gilt nur für LVM-basierte SRs (LVM, LVMoiSCSI und LVMOHBA). Es gilt nicht für EXT oder NFS SRs, deren Verhalten unverändert bleibt. In bestimmten Fällen kann die automatische Raumgewinnung möglicherweise nicht fortgesetzt werden. Es wird empfohlen, das Off-Line Coalesce Tool in folgenden Szenarien zu verwenden:

- Unter Bedingungen, in denen ein VM-E/A-Durchsatz beträchtlich ist
- Unter Bedingungen, in denen der Raum nach einer Periode nicht zurückerobert wird

> **Hinweise:**
>
> - Das Ausführen des Off Line Coalesce Tools verursacht aufgrund der ausgeführten Suspending/Fortsetzungsvorgänge einige Ausfallzeiten für die VM.
> - Löschen Sie vor dem Ausführen des Tools alle Snapshots und Klone, die Sie nicht mehr wünschen. Das Werkzeug nimmt bei den verbleibenden Snap-Klonen so viel Platz wie möglich zurück. Wenn Sie den gesamten Speicherplatz zurückfordern möchten, löschen Sie alle Snapshots und Klone.
> - VM-Festplatten müssen sich entweder auf freigegebenem oder lokalem Speicher für einen einzelnen Host befinden. VMs mit Festplatten in beiden Speichertypen können nicht zusammengeführt werden.

Speicherplatz mithilfe des Offline-Koaleszen-Werkzeugs zurückgewinnen

> **Hinweis:**
>
> Online Coalescing gilt nur für LVM-basierte SRs (LVM, LVMoiSCSI und LVMOHBA), sie gilt nicht für EXT oder NFS SRs, deren Verhalten unverändert bleibt.

Aktivieren Sie die ausgeblendeten Objekte mit XenCenter. Klicken Sie auf**Ausgeblendete** > Objekte **anzeigen**. Wählen Sie im Ressourcenbereich die VM aus, für die Sie die UUID abrufen möchten. Die UUID wird auf der Registerkarte **Allgemein** angezeigt.

Wählen Sie im Ressourcenbereich den Ressourcenpoolmaster aus (den ersten Host in der Liste. 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
```

   Wenn beispielsweise die VM-UUID ist9bad4022-2c2d-dee6-abf5-1b6195b1dad5 und die Host-UUID lautetb8722062-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
```

2. Mit diesem Befehl wird die VM angehalten (es sei denn, sie ist bereits ausgeschaltet), der Speicherplatzrückgewinnungsprozess initiiert und die VM dann fortgesetzt.

> **Hinweise:**
>
> Es wird empfohlen, dass Sie die VM manuell herunterfahren oder anhalten, bevor Sie das Offline-Coalesce-Tool ausführen. Sie können die VM entweder mit XenCenter oder der Citrix Hypervisor-CLI herunterfahren oder anhalten. Wenn Sie das Coalesce-Tool auf einer laufenden VM ausführen, wird die VM automatisch angehalten, die erforderlichen VDI-Koaleszen-Vorgänge ausgeführt und die VM fortgesetzt.
>
> Wenn sich die zu koaleszierenden Virtual Disk Images (VDIs) im gemeinsam genutzten Speicher befinden, müssen Sie das Offline-Koaleszierungstool auf dem Poolmaster ausführen.
>
> Wenn sich die zu koaleszierenden VDIs auf dem lokalen Speicher befinden, führen Sie das Offline-Koaleszierungstool auf dem Server aus, an den der lokale Speicher angeschlossen ist.

Anpassen des Datenträger-E/A-Schedulers

Zur allgemeinen Leistung wird der`noop` Standarddatenträgerplaner auf alle neuen SR-Typen angewendet. Der`noop` Scheduler bietet die beste Leistung für konkurrierende VMs, die auf dasselbe Gerät zugreifen. Um Datenträger-QoS anzuwenden, ist es notwendig, die Standardeinstellung außer Kraft zu setzen und den`cfq` Datenträgerplaner dem SR zuzuweisen. Die entsprechende PBD muss getrennt und neu angeschlossen werden, damit der Scheduler-Parameter wirksam wird. Der Disk Scheduler kann mit dem folgenden Befehl angepasst werden:

```
xe sr-param-set other-config:scheduler=noop|cfq|anticipatory|deadline \
    uuid=valid_sr_uuid
```

> **Hinweis:**
>
> Dieser Befehl hat keinen Einfluss auf EqualLogic, NetApp oder NFS-Speicher.

QoS-Einstellungen für virtuelle Laufwerke

Virtuelle Festplatten verfügen über eine optionale E/A-Prioritätseinstellung Quality of Service (QoS). Diese Einstellung kann auf vorhandene virtuelle Laufwerke mithilfe der xe-CLI angewendet werden, wie in diesem Abschnitt beschrieben.

Bei gemeinsam genutzten SR, bei denen mehrere Hosts auf dieselbe LUN zugreifen, wird die QoS-Einstellung auf VBDs angewendet, die von demselben Host auf die LUN zugreifen. QoS wird nicht auf Hosts im Pool angewendet.

Bevor Sie QoS-Parameter für eine VBD konfigurieren, stellen Sie sicher, dass der Festplattenplaner für die SR entsprechend festgelegt wurde. Weitere Informationen *zum Anpassen des Planers finden*

Sie unter Festplatten-E/A-Scheduler im vorherigen Abschnitt anpassen. Der Scheduler-Parameter muss`cfq` auf der SR gesetzt werden, für die die QoS gewünscht ist.

> **Hinweis:**
>
> Denken Sie daran, den Scheduler`cfq` auf der SR zu setzen und sicherzustellen, dass die PBD neu angeschlossen wurde, damit die Scheduler-Änderung wirksam wird.

Der erste Parameter ist`qos_algorithm_type`. Dieser Parameter muss auf den Wert festgelegt werden. Dies ist der einzige Typ von QoS-Algorithmus`ionice`, der für virtuelle Laufwerke in dieser Version unterstützt wird.

Die QoS-Parameter selbst werden mit Schlüssel/Wert-Paaren gesetzt, die dem`qos_algorithm_param` Parameter zugewiesen sind. Für virtuelle Laufwerke,`qos_algorithm_param` nimmt einen`sched` Schlüssel, und abhängig vom Wert, erfordert auch einen**`class`** Schlüssel.

Mögliche Werte von`qos_algorithm_param:sched` sind:

-`sched=rt` oder`sched=real-time` setzt den QoS-Planungsparameter auf Echtzeitpriorität, was einen Klassenparameter benötigt, um einen Wert zu setzen

-`sched=idle` setzt den QoS-Scheduling-Parameter auf Leerlaufpriorität, was keinen Klassenparameter benötigt, um einen beliebigen Wert zu setzen

-`sched=anything` setzt den QoS-Scheduling-Parameter auf die höchste Anstrengung Priorität, was einen Klassenparameter benötigt, um einen Wert zu setzen

Die möglichen Werte für**`class`** sind:

- Eines der folgenden Schlüsselwörter: höchste, hohe, normale, niedrige, niedrigste
- Eine Ganzzahl zwischen 0 und 7, wobei 7 die höchste Priorität und 0 die niedrigste ist. Beispielsweise erhalten E/A-Anforderungen mit einer Priorität von 5 Priorität gegenüber E/A-Anforderungen mit der Priorität 2.

Um die QoS-Einstellungen des Datenträgers`other-config:scheduler` zu aktivieren, müssen Sie auch die PBDs für den betreffenden Speicher festlegen`cfq` und erneut anschließen.

Mit den folgenden CLI-Befehlen wird beispielsweise die VBD des virtuellen Laufwerks so festgelegt, dass die Echtzeitpriorität verwendet wird5:

```
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-plug uuid=pbd_uuid
```

Kopiert!
Failed!

Massenspeicher-Multipathing

October 16, 2019

Dynamische Multipathing-Unterstützung ist für Fibre Channel- und iSCSI-Speicher-Back-Ends verfügbar. Sie können Multipathing in XenCenter oder auf der XE CLI aktivieren.

> **Wichtig:**
>
> Bevor Sie versuchen, Multipathing zu aktivieren, stellen Sie sicher, dass die folgenden Anweisungen zutreffen:
>
> - Mehrere Ziele sind auf Ihrem Speicherserver verfügbar.
>
>   Beispielsweise gibt ein iSCSI-Speicher-Back-End, das auf einem bestimmten Portal nach `sendtargets` 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.Erdbeer:litchie
>   192.168.0. 204:3260 ,2 iqn.Erdbeer:litchie
>   ```
>
> - Nur für iSCSI verfügt dom0 über eine IP-Adresse in jedem Subnetz, das vom Multipath-Speicher verwendet wird.
>
>   Stellen Sie sicher, dass für jeden Pfad, den Sie zum Speicher benötigen, eine Netzwerkkarte vorhanden ist und dass auf jeder Netzwerkkarte eine IP-Adresse konfiguriert ist. Wenn Sie beispielsweise vier Pfade zu Ihrem Speicher benötigen, müssen Sie über vier Netzwerkkarten verfügen, für die jeweils eine IP-Adresse konfiguriert ist.
>
> - Nur für HBA sind mehrere HBA mit der Switch-Fabric verbunden.

1. Öffnen Sie eine Konsole auf dem Citrix Hypervisor or-Server.
2. Trennen Sie alle PBDs auf dem Server mithilfe des folgenden Befehls:

   ```
   xe pbd-unplug uuid=<pbd_uuid>
   ```

3. Setzen Sie den Wert des `other-config:multipathing` Parameters auf, **`true`** indem Sie den folgenden Befehl verwenden:

   ```
   xe host-param-set other-config:multipathing=true uuid=<server_uuid
       >
   ```

4. Setzen Sie den Wert des `other-config:multipathhandle` Parameters auf, `dmp` indem Sie den folgenden Befehl verwenden:


```
<server_uuid>xe host-param-set other-config:multipathhandle=dmp
   uuid=
```

5. Wenn auf dem Server bereits SRs vorhanden sind, die im Einzelpfadmodus ausgeführt werden, aber mehrere Pfade aufweisen:

   - Migrieren oder suspendieren von laufenden Gästen mit virtuellen Laufwerken in den betroffenen SRs
   - Trennen Sie die PBD aller betroffenen SRs, und schließen Sie sie erneut an, um sie mithilfe von Multipathing wiederherzustellen:

     ```
     xe pbd-unplug uuid=<pbd_uuid>
     xe pbd-plug uuid=<pbd_uuid>
     ```

Um das Multipathing zu deaktivieren, trennen Sie zuerst die VBDs, setzen Sie den`other-config:multipathing` Host-Parameter auf**`false`** und schließen Sie dann die PBDs wie oben beschrieben erneut an. Ändern Sie den`other-config:multipathhandle` Parameter nicht, da diese Aktion automatisch ausgeführt wird.

Die Multipath-Unterstützung in Citrix Hypervisor basiert auf dem Device-Mapper`multipathd components`. Die Storage Manager-API übernimmt das automatische Aktivieren und Deaktivieren von Multipath-Knoten. Im Gegensatz zu den`dm-multipath` Standardwerkzeugen in Linux werden Device Mapper-Knoten nicht automatisch für alle LUNs auf dem System erstellt. Device Mapper-Knoten werden nur bereitgestellt, wenn LUNs von der Speicherverwaltungsschicht aktiv verwendet werden. Daher ist es nicht erforderlich, eines der`dm-multipath` CLI-Tools zum Abfragen oder Aktualisieren von DM-Tabellenknoten in Citrix Hypervisor zu verwenden. Wenn es notwendig ist, den Status von Device-Mapper-Tabellen manuell abzufragen oder aktive Device Mapper-Multipath-Knoten auf dem System aufzulisten, verwenden Sie das`mpathutil` Dienstprogramm:

```
mpathutil list
```

```
mpathutil status
```

> **Hinweise:**
>
> - Aufgrund von Inkompatibilitäten mit der integrierten Multipath-Verwaltungsarchitektur wird empfohlen, das`dm-multipath` Standard-CLI-Dienstprogramm nicht mit Citrix Hypervisor zu verwenden. Verwenden Sie das`mpathutil` CLI-Tool, um den Status von Knoten auf dem Host abzufragen.
> - Multipath-Unterstützung in EqualLogic-Arrays umfasst nicht Speicher-E/A-Multipathing im traditionellen Sinne des Begriffs. Multipathing muss auf Netzwerk-/NIC-Anleihenebene

> abgewickelt werden. Informationen zum Konfigurieren von Netzwerk-Failover für EqualLogic SRS/LVMoiSCSI SRs finden Sie in der EqualLogic-Dokumentation.

Kopiert!
Failed!

IntelliCache

October 16, 2019

> **Hinweis:**
>
> Dieses Feature wird nur unterstützt, wenn Citrix Hypervisor mit Citrix Virtual Desktops verwendet wird.
>
> Intellicache wird für VMs, die eine GFS2 SR verwenden, nicht unterstützt.

Die Verwendung von Citrix Hypervisor mit *IntelliCache* macht 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 Betriebssystemabbild gemeinsam nutzen. Die Auslastung des Speicher-Arrays wird reduziert und die Leistung wird erhöht. Darüber hinaus wird der Netzwerkverkehr von und zu gemeinsam genutztem Speicher reduziert, da der lokale Speicher das Masterimage aus dem freigegebenen Speicher zwischenspeichert.

IntelliCache arbeitet, indem Daten von einem übergeordneten VDI VMs im lokalen Speicher auf dem VM-Host zwischengespeichert werden. Dieser lokale Cache wird dann aufgefüllt, wenn Daten aus dem übergeordneten VDI gelesen werden. Wenn viele VMs eine gemeinsame übergeordnete VDI verwenden, kann eine VM die Daten verwenden, die von einer anderen VM in den Cache gelesen werden. Ein weiterer Zugriff auf das Masterimage auf freigegebenen Speicher ist nicht erforderlich.

Ein Thin-Provisioning, lokaler SR ist für IntelliCache erforderlich. Thin Provisioning ist eine Möglichkeit, die Nutzung des verfügbaren Speichers zu optimieren. Mit diesem Ansatz können Sie mehr lokalen Speicher anstelle von gemeinsam genutztem Speicher verwenden. Es basiert auf der On-Demand-Zuweisung von Datenblöcken. In anderen Ansätzen werden alle Blöcke vorne zugeordnet.

> **Wichtig:**
>
> Thin Provisioning ändert den lokalen Standardspeichertyp des Hosts von LVM in EXT3. Die Thin Provisioning **muss aktiviert sein** , damit das lokale Caching von Citrix Virtual Desktops ordnungsgemäß funktioniert.

Thin Provisioning ermöglicht es dem Administrator, den VMs, die eine Verbindung mit dem Storage Repository (SR) herstellen, mehr Speicherplatz als auf der SR verfügbar. Es gibt keine Platzgarantien, und die Zuweisung einer LUN beansprucht keine Datenblöcke, bis die VM Daten schreibt.

> **Warnhinweis:**
>
> Thin Provisioned SRs kann nicht genügend physischer Speicherplatz vorhanden sein, da die VMs innerhalb wachsen können, um die Festplattenkapazität bei Bedarf zu belegen. IntelliCache VMs behandeln diese Bedingung, indem sie automatisch auf den gemeinsam genutzten Speicher zurückkehren, wenn der lokale SR-Cache voll ist. Mischen Sie keine traditionellen virtuellen Maschinen und IntelliCache VMs auf derselben SR, da IntelliCache-VMs schnell wachsen können.

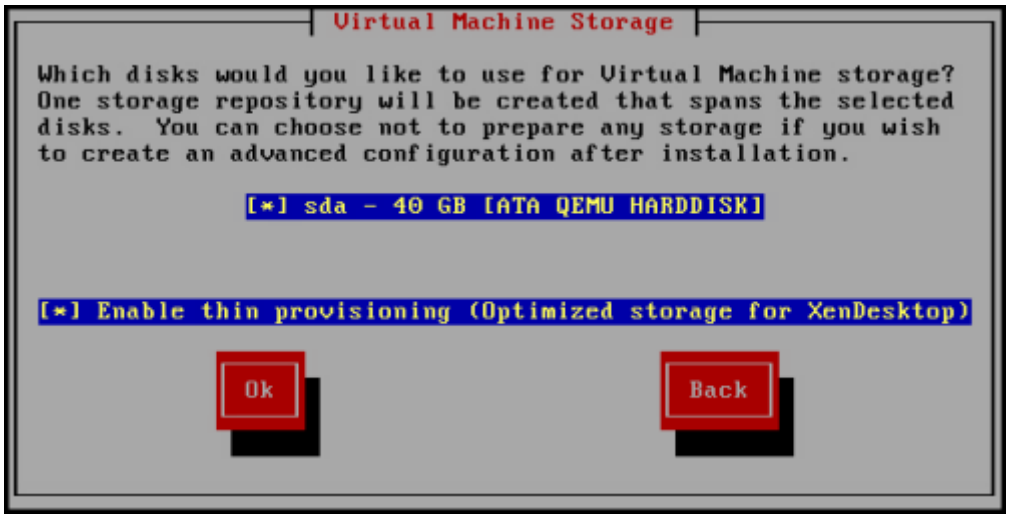
IntelliCache Bereitstellung

IntelliCache muss entweder während der Hostinstallation aktiviert sein oder manuell auf einem laufenden Host mithilfe der CLI aktiviert werden.

Es wird empfohlen, ein leistungsfähiges lokales Speichergerät zu verwenden, um die schnellstmögliche Datenübertragung sicherzustellen. Verwenden Sie beispielsweise eine Solid-State-Festplatte oder ein Hochleistungs-RAID-Array. Berücksichtigen Sie sowohl den Datendurchsatz als auch die Speicherkapazität bei der Dimensionierung lokaler Festplatten. Der freigegebene Speichertyp, der zum Hosten des virtuellen Quelldatenträgerabbilds (VDI) verwendet wird, muss NFS- oder EXT-basiert sein.

Auf Host-Installation aktivieren

Um IntelliCache während der Hostinstallation zu aktivieren, wählen Sie auf dem Bildschirm **Speicher für virtuelle Maschinen** die Option **Thin-Provisioning aktivieren** aus. Mit dieser Option wird die lokale SR des Hosts ausgewählt, die für das lokale Caching von VM-VDIs verwendet werden soll.



Konvertieren eines vorhandenen Hosts zur Verwendung von Thin Provisioning

Um eine vorhandene LVM-basierte lokale SR zu löschen und sie durch eine Thin Provisioned EXT3-basierte SR zu ersetzen, geben Sie die folgenden Befehle ein.

> **Warnhinweis:**
>
> Diese Befehle entfernen Ihre vorhandene lokale SR, und VMs auf der SR werden endgültig 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 /etc/firstboot.d/state/10-prepare-storage
    rm -f /etc/firstboot.d/state/15-set-default-storage
    service firstboot start
    xe sr-list type=ext
```

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
```

VM-Startverhalten

Es gibt zwei Optionen für das Verhalten eines VM-VDI beim Starten der VM:

1. Freigegebener Desktopmodus

   Beim Starten der virtuellen Maschine wird der VDI in den Zustand zurückgesetzt, in dem er sich beim vorherigen Start befand. Alle Änderungen, während die VM ausgeführt wird, gehen verloren, wenn die VM das nächste Mal gestartet wird.

   Select diese Option, wenn Sie standardisierte Desktops bereitstellen möchten, an denen Benutzer keine permanenten Änderungen vornehmen können.

2. Privater Desktop-Modus

   Beim Starten der VM befindet sich der VDI in dem Zustand, in dem er beim letzten Herunterfahren belassen wurde.

   Select diese Option aus, wenn Sie Benutzern erlauben möchten, dauerhafte Änderungen an ihren Desktops vorzunehmen.

Einstellungen für das Caching von VM

Das`allow-caching` VDI-Flag bestimmt das Caching-Verhalten:

Freigegebener Desktopmodus

Bei freigegebenen Desktops ist die`on-boot` Option`reset` und das`allow-caching` Flag lautet**`true`** . Neue VM-Daten werden nur in den lokalen Speicher geschrieben. Es gibt keine Schreibvorgänge in den freigegebenen Speicher. Dieser Ansatz bedeutet, dass die Auslastung des gemeinsam genutzten Speichers reduziert wird. Die VM kann jedoch nicht zwischen Hosts migriert werden.

Privater Desktop-Modus

Bei privaten Desktops ist die On-Boot-Option auf`persist` und das Allow-Caching-Flag auf gesetzt**`true`** . Neue VM-Daten werden sowohl auf lokalen als auch auf freigegebenen Speicher geschrieben. Für das Lesen zwischengespeicherter Daten ist kein E/A-Datenverkehr zum freigegebenen Speicher erforderlich, sodass die Auslastung des gemeinsam genutzten Speichers reduziert wird. Die Migration von virtuellen Rechnern auf einen anderen Host ist zulässig, und der lokale Cache auf dem neuen Host wird beim Lesen der Daten aufgefüllt.

Implementierungsdetails und Fehlerbehebung

F: Ist IntelliCache mit Live-Migration und hoher Verfügbarkeit kompatibel?

A: Sie können Livemigration und High Availability mit IntelliCache verwenden, wenn sich virtuelle Desktops im Privatmodus befinden, d. h. wenn`on-boot=persist`

> **Warnhinweis:**
>
> Eine VM kann nicht migriert werden, wenn auf einer ihrer VDIs Caching-Verhaltens-Flags auf`on-boot=reset` und festgelegt ist`allow-caching=`**`true`** . Migrationsversuche für VMs mit diesen Eigenschaften schlagen fehl.

F: Wo befindet sich der lokale Cache auf der lokalen Festplatte?

A: Der Cache befindet sich in einem Speicher-Repository (SR). Jeder Host verfügt über einen Konfigurationsparameter (Local-cache-sr genannt), der angibt, welcher (lokale) SR für die Cache-Dateien verwendet werden soll. Normalerweise ist dieser SR ein EXT Typ SR. Wenn Sie VMs mit IntelliCache ausführen, werden Dateien innerhalb der SR mit Namen angezeigt`uuid.vhdcache`. Diese Datei ist die Cache-Datei für den VDI mit der angegebenen UUID. Diese Dateien werden in XenCenter nicht angezeigt. Die einzige Möglichkeit, sie zu sehen, besteht darin, sich bei dom0 anzumelden und den Inhalt von`/var/run/sr-mount/sr-uuid`

F: Wie gebe ich eine bestimmte SR für die Verwendung als Cache an?

A: Das Hostobjektfeld`local-cache-sr` verweist auf eine lokale SR. Sie können den Wert anzeigen, indem Sie den folgenden Befehl ausführen:

```
1 xe sr-list params=local-cache-sr,uuid,name-label
```

Dieses Feld ist entweder gesetzt:

- Wenn Sie nach der Hostinstallation die Option „Thin Provisioning aktivieren“ im Host-Installationsprogramm ausgewählt haben, oder
- Durch die Ausführung`xe host-enable-local-storage-caching host=host sr-uuid=sr`. Für den Befehl muss der angegebene Host deaktiviert sein. Fahren Sie die VMs herunter, wenn Sie diesen Befehl verwenden.

Die erste Option verwendet den lokalen Typ EXT und wird während der Hostinstallation erstellt. Die zweite Option verwendet die SR, die in der Befehlszeile angegeben ist.

> **Warnhinweis:**
>
> Diese Schritte sind nur für Benutzer erforderlich, die mehrere lokale SR konfiguriert haben.

F: Wann wird der lokale Cache gelöscht?

A: Eine VDI-Cache-Datei wird nur gelöscht, wenn der VDI selbst gelöscht wird. Der Cache wird zurückgesetzt, wenn ein VDI an eine VM angeschlossen ist (z. B. beim Start der VM). Wenn der Host offline ist, wenn Sie den VDI löschen, sammelt die SR-Synchronisation, die beim Start Garbage ausgeführt wird, die Cache-Datei.

> **Hinweis:**
>
> Die Cache-Datei wird nicht vom Host gelöscht, wenn eine VM auf einen anderen Host migriert oder heruntergefahren wird.

Kopiert!
Failed!

Speicher-Lese-Caching

October 16, 2019

Lese-Caching verbessert die Festplattenleistung einer VM, da nach dem ersten Lesen von externen Datenträgern Daten 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 dadurch die Anzahl der von der Festplatte gelesenen Blöcke drastisch reduziert wird. Beispielsweise in Umgebungen mit Citrix Virtual Desktops (Machine Creation Service, MCS).

Die Leistungssteigerung kann angezeigt werden, wenn Daten mehrmals von der Festplatte gelesen werden, da sie im Speicher zwischengespeichert werden. Diese Änderung ist am deutlichsten in der Verschlechterung des Dienstes, der während schwerer 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 beträchtliche Anzahl von VMs geplant ist, dass Malware-Scans gleichzeitig ausgeführt werden (Virenschutzstürme).

Die Lesezwischenspeicherung ist standardmäßig aktiviert, wenn Sie über den entsprechenden Lizenztyp verfügen.

> **Hinweis:**
>
> Storage Read Caching ist für Citrix Hypervisor Premium Edition-Kunden verfügbar.
>
> Storage Read Caching ist auch für Kunden verfügbar, die über ihre Berechtigung für Citrix Virtual Apps and Desktops auf Citrix Hypervisor zugreifen.

Aktivieren und Deaktivieren von Lese-Caching

Bei dateibasierten SRs wie NFS- und EXT3-SR-Typen ist das Lese-Caching standardmäßig aktiviert. Lese-Caching ist für alle anderen SRs deaktiviert.

Führen Sie den folgenden Befehl aus, um die Lesezwischenspeicherung für eine bestimmte SR zu deaktivieren:

```
1 xe sr-param-set uuid=sr-uuid other-config:o_direct=true
```


Einschränkungen

- Lese-Caching ist nur für NFS- und EXT3-SRs verfügbar. Es ist nicht für andere SR Typen verfügbar.
- Lese-Caching 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 sind zu erkennen, wenn viele VMs aus einem einzigen „goldenen" Image geklont werden.
- Die Leistungsverbesserungen hängen von der Menge des freien Arbeitsspeichers in der Steuerdomäne des Hosts (dom0) ab. Durch das Erhöhen der Menge an dom0-Speicher kann dem Lese-Cache mehr Speicher zugewiesen werden. Informationen zum Konfigurieren des dom0-Speichers finden Sie unterCTX134951.

Vergleich mit IntelliCache

IntelliCache und speicherbasiertes Lese-Caching sind in gewisser Hinsicht komplementär. IntelliCache speichert nicht nur auf einer anderen Ebene, sondern speichert auch Schreibvorgänge zusätzlich zu Lesevorgängen. IntelliCache speichert Lesevorgänge aus dem Netzwerk auf einen lokalen Datenträger. In-Memory-Lese-Caching speichert die Lesevorgänge vom Netzwerk oder vom Datenträger in den Hostspeicher. Der Vorteil des In-Memory-Lese-Cachings besteht darin, dass der Speicher immer noch um eine Größenordnung schneller ist als eine Solid-State-Festplatte (SSD). Die Leistung bei Boot-Stürmen und anderen schweren E/A-Situationen verbessert sich.

Sowohl das Lese-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.

Festlegen der Lesecachegröße

Die Lesecache-Performance kann optimiert werden, indem der Steuerdomäne von Citrix Hypervisor (dom0) mehr Arbeitsspeicher zur Verfügung steht.

> **Wichtig:**
>
> Legen Sie die Lese-Cache-Größe auf ALLE Hosts im Pool individuell zur Optimierung fest. Alle nachfolgenden Änderungen an der Größe des Lesecaches müssen auch auf allen Hosts im Pool festgelegt werden.

Öffnen Sie auf dem Citrix Hypervisor or-Server eine lokale Shell, und melden Sie sich als Root an.

Führen Sie den folgenden Befehl aus, um die Größe des Lesecache festzulegen:


```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
```

Legen Sie sowohl den Anfangs- als auch den Maximalwert auf denselben Wert fest. Zum Beispiel, um dom0 Speicher auf 2.048 MiB zu setzen:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
```

> **Wichtig:**
>
> Starten Sie alle Hosts neu, nachdem Sie die Lese-Cache-Größe geändert haben.

Wie kann ich die aktuelle dom0-Speicherzuweisung anzeigen?

Um die aktuellen dom0-Speichereinstellungen anzuzeigen, geben Sie Folgendes ein:

```
free -m
```

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 mit dom0 auf 2.6 GiB

	Gesamtsumme	Gebraucht	Frei	Geteilt	Puffer/Cache	Verfügbar
Mem:	2450	339	1556	9	554	2019
Tauschen:	1023	0	1023			

Welcher Wertebereich kann verwendet werden?

Da die Citrix Hypervisor Control Domain (dom0) 64-Bit ist, können große Werte verwendet werden, z. B. 32768 MiB. Wir empfehlen jedoch, **den dom0-Speicher nicht unter 1 GiB zu reduzieren**.

XenCenter Anzeigenotizen

Der gesamte Speicher des Hosts kann als Xen Hypervisor, dom0, VMs und freier 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 zählen die Anzahl der VMs, die auf dem Host zu jeder Zeit ausgeführt werden, und wie diese VMs konfiguriert werden. Es ist nicht möglich, die Menge an Speicher zu begrenzen, die Xen verwendet. Die Begrenzung der Speichermenge kann dazu führen,

dass Xen nicht mehr genügend Arbeitsspeicher hat und verhindert wird, 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** .

Im Feld Citrix Hypervisor wird die *Summe* des Speichers angezeigt, der dem Speicher dom0 *und* Xen zugewiesen ist. Daher kann die angezeigte Speichermenge höher sein als vom Administrator angegeben. Die Speichergröße kann beim Starten und Beenden von VMs variieren, selbst wenn der Administrator eine feste Größe für dom0 festgelegt hat.

Kopiert!
Failed!

PVS-Beschleuniger

October 16, 2019

Die Citrix Hypervisor PVS-Accelerator-Funktion bietet erweiterte Funktionen für Kunden, die Citrix Hypervisor mit Citrix Provisioning verwenden. Citrix Provisioning ist eine beliebte Wahl für die Image-Verwaltung und -Hosting für Citrix Virtual Apps and Desktops. PVS-Accelerator verbessert die bereits ausgezeichnete Kombination von Citrix Hypervisor und Citrix Provisioning erheblich. Einige der Vorteile, die diese neue Funktion bietet, sind:

- **Datenlokalität:** Verwenden Sie die Leistung und die Lokalität von Speicher, SSD und NVM-Geräten für Leseanforderungen, während die Netzwerkauslastung erheblich reduziert wird.
- **Verbesserte Benutzererfahrung:** Die Datenlokalität ermöglicht eine Reduzierung der Lese-E/A-Latenz für zwischengespeicherte Zielgeräte (VMs) und beschleunigt die Endbenutzeranwendungen weiter.
- **Beschleunigte VM-Boots und Boot-Stürme:** Reduzierte Lese-I/O-Latenz und verbesserte Effizienz können die Startzeiten von virtuellen Rechnern beschleunigen und eine schnellere Leistung ermöglichen, wenn viele Geräte innerhalb eines engen Zeitrahmens hochfahren.
- **Vereinfachtes Skalieren durch Hinzufügen von mehr Hypervisor-Hosts:** Möglicherweise sind weniger Citrix Provisioning -Server erforderlich, da die Speicherlast effizient auf alle Citrix Hypervisor or-Server verteilt wird. Spitzenlasten werden mit dem Cache innerhalb der ursprünglichen Hosts behandelt.
- **Geringere Gesamtbetriebskosten und vereinfachte Infrastrukturanforderungen:** Weniger Citrix Provisioning -Server bedeutet eine Reduzierung der Hardware- und Lizenzanforderungen sowie reduzierten Verwaltungsaufwand. Freigabe von Kapazität ist für Arbeitslasten verfügbar.

> **Hinweis:**
>
> PVS-Accelerator ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Um die PVS-Accelerator-Funktion zu verwenden, aktualisieren Sie den Lizenzserver auf Version 11.14.

Wie funktioniert PVS-Accelerator?

PVS-Accelerator verwendet einen Proxy-Mechanismus, der sich in der Control Domain (dom0) von Citrix Hypervisor befindet. Wenn diese Funktion aktiviert ist, werden Leseanforderungen für Citrix Provisioning Targets Device (VM) direkt auf dem Citrix Hypervisor or-Servercomputer zwischengespeichert. Diese Anforderungen werden im physischen Speicher oder in einem Speicher-Repository zwischengespeichert. Wenn nachfolgende VMs auf diesem Citrix Hypervisor or-Server 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.

PVS-Beschleuniger aktivieren

Kunden müssen die folgenden Konfigurationseinstellungen in Citrix Hypervisor und Citrix Provisioning ausführen, um die PVS-Accelerator-Funktion zu aktivieren:

1. Installieren Sie das PVS-Accelerator Supplemental Pack auf jedem Citrix Hypervisor or-Server im Pool. Das Ergänzungspaket kann von derCitrix Hypervisor ProduktdownloadsSeite heruntergeladen werden. Sie können das Zusatzpaket mit XenCenter oder der xe CLI installieren. Informationen zum Installieren eines Zusatzpakets mit XenCenter finden Sie in der XenCenter-Hilfe. CLI-Anweisungen finden Sie imCitrix Hypervisor Zusatzpakete und DDK-Handbuch.
2. Konfigurieren Sie den PVS-Accelerator in Citrix Hypervisor mithilfe von XenCenter oder der XE CLI. Diese Konfiguration umfasst das Hinzufügen einer Citrix Provisioning -Site und die Angabe des Speicherorts für Citrix Provisioning-Cachespeicher.
   - CLI-Anweisungen finden Sie unter *Konfigurieren von PVS-Accelerator in Citrix Hypervisor mithilfe der CLI* im folgenden Abschnitt.
   - Informationen zum Konfigurieren von PVS-Accelerator mit XenCenter finden Sie in der XenCenter-Hilfe.
3. Nachdem Sie den PVS-Accelerator in Citrix Hypervisor konfiguriert haben, schließen Sie die Cache-Konfiguration für die PVS-Site mit der PVS-Benutzeroberfläche ab. Ausführliche Anweisungen finden Sie unter Abschluss der Cache-Konfiguration in Citrix Provisioning.

Konfigurieren des PVS-Accelerators in Citrix Hypervisor mithilfe der CLI

1. Führen Sie den folgenden Befehl aus, um eine Citrix Provisioning Standortkonfiguration auf Citrix Hypervisor zu erstellen:

```
PVS_SITE_UUID=$ (xe pvs-site-introduce name-label=Meine PVS-
    Website)
```

2. Geben Sie für jeden Host im Pool an, welcher Cache verwendet werden soll. Sie können den Cache in einem Speicher-Repository (SR) oder im Control Domain Memory speichern.

Konfigurieren des Cachespeichers in einem Speicher-Repository

Berücksichtigen Sie bei der Auswahl eines Speicher-Repository (SR) für den Cache-Speicher die folgenden Merkmale:

Vorteile:

- Zuletzt gelesene Daten werden auf bestem Aufwand im Speicher zwischengespeichert. Der Zugriff auf die Daten kann so schnell erfolgen wie die Verwendung des Kontrolldomänen-Speichers.
- Der Cache kann viel größer sein, wenn er sich auf einem SR befindet. Die Kosten für den SR-Speicherplatz sind in der Regel ein Bruchteil der Kosten des Speicherplatzes. Durch das Caching auf einem SR kann der Citrix Provisioning -Server mehr Last entlastet werden.
- Sie müssen die Speichereinstellung „Steuerdomäne“ nicht ändern. Der Cache verwendet automatisch den in der Steuerungsdomäne verfügbaren Speicher und bewirkt nie, dass die Kontrolldomäne nicht genügend Arbeitsspeicher hat.
- Die Cache-VDIs können im gemeinsam genutzten Speicher gespeichert werden. Diese Wahl des Speichers macht jedoch selten Sinn. Dieser Ansatz ist nur dann sinnvoll, wenn der freigegebene Speicher deutlich schneller ist als der Citrix Provisioning -Server.
- Sie können entweder eine dateibasierte oder eine blockbasierte SR für die Cache-Speicherung verwenden.

Nachteile:

- Wenn der SR langsam ist und sich die angeforderten Daten nicht auf der Speicherebene befinden, kann der Caching-Prozess langsamer sein als ein Remote-Server für Citrix Provisioning.
- Zwischengespeicherte VDIs, die im freigegebenen 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 Speicher-Repository zu konfigurieren:

1. Führen Sie den folgenden Befehl aus, um die UUID der SR zu finden, die für das Caching verwendet werden soll:

```
xe sr-list name-label=Local storage host=host-name-label --minimal
    )
```

2. Erstellen Sie den Cache-Speicher.

```
xe pvs-cache-storage-create host=host-name-label pvs-site-uuid=
    PVS_SITE_UUID \
          sr-uuid=SR_UUID size=10GiB
```

> **Hinweis:**
>
> Bei der Auswahl eines Speicher-Repository (SR) verwendet das Feature bis zur angegebenen Cachegröße auf der SR. Es verwendet auch implizit verfügbaren Control Domain Speicher als bestmögliche Cache-Ebene.

Konfigurieren des Cachespeichers im Steuerdomänenspeicher

Berücksichtigen Sie die folgenden Merkmale, wenn Sie den Speicher für die Steuerdomäne für den Cachespeicher auswählen:

Vorteile:

Die Verwendung von Speicher bedeutet konstant schnelle Lese-/Schreibleistung beim Zugriff auf den Cache oder beim Füllen des Caches.

Nachteile:

- Hardware muss entsprechend dimensioniert werden, da der für den Cachespeicher verwendete RAM für VMs nicht verfügbar ist.
- Kontrolldomänenspeicher muss **vor** der Konfiguration des Cachespeichers erweitert werden.

  > **Hinweis:**
  >
  > Wenn Sie den Cache im Speicher der Steuerdomäne speichern, verwendet das Feature bis zur angegebenen Cachegröße im Speicher der Steuerdomäne. Diese Option ist nur verfügbar, nachdem der Steuerdomäne zusätzlicher Speicher zugewiesen wurde. Hinweise zum Erhöhen des Arbeitsspeichers der Steuerdomäne finden Sie unterÄndern der Speichermenge, die der Steuerdomäne zugewiesen ist.

  Nachdem Sie die Speichermenge erhöht haben, die der Steuerdomäne des Hosts zugewiesen ist, kann der zusätzliche Speicher explizit für PVS-Accelerator zugewiesen werden.

  Führen Sie die folgenden Schritte aus, um den Cachespeicher im Speicher der Steuerdomäne 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
```

2. Erstellen Sie eine SR des speziellen Typs `tmpfs`:

```
xe sr-create type=tmpfs name-label=MemorySR host-uuid=
   HOST_UUID device-config:uri=""
```

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
```

   Wo `SR_UUID` ist die UUID der SR, die in Schritt b erstellt wurde

Schließen Sie die Cache-Konfiguration in Citrix Provisioning ab

Führen Sie nach der Konfiguration von PVS-Accelerator in Citrix Hypervisor die folgenden Schritte aus, um die Cache-Konfiguration für die Citrix Provisioning-Site abzuschließen.

Verwenden Sie in der Citrix Provisioning Administratorkonsole den Setup-Assistenten für Citrix Virtual Desktops oder den Streaming-VM-Assistenten (je nach Bereitstellungstyp), um auf die Proxy-Funktion zuzugreifen. Obwohl beide Assistenten ähnlich sind und viele der gleichen Bildschirme teilen, gibt es folgende Unterschiede:

- Der **Setup-Assistent für Citrix virtuelle Desktops** wird verwendet, um VMs zu konfigurieren, die auf dem Citrix 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 betroffen.

Starten Sie die Citrix Provisioning Administratorkonsole:

1. Navigieren Sie zur Citrix Provisioning Website.
2. Select die Citrix Provisioning -Site aus, klicken Sie mit der rechten Maustaste, um ein Kontextmenü anzuzeigen.
3. Wählen Sie basierend auf der Bereitstellung den entsprechenden Assistenten aus. Select die Option **PVS-Beschleuniger für alle virtuellen Maschinen** aktivieren, um die PVS-Beschleunigerfunktion zu aktivieren.
4. Wenn Sie das Caching virtueller Datenträger zum ersten Mal aktivieren, wird der Bildschirm **Citrix Hypervisor** im Setup-Assistenten für gestreamte virtuelle Maschinen angezeigt. Es zeigt die

Liste aller Citrix Provisioning -Sites an, die auf Citrix Hypervisor konfiguriert sind, die noch nicht mit einer Citrix Provisioning -Site verknüpft sind. Wählen Sie in 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 Citrix Hypervisor or-Server ausführen.

5. Klicken Sie auf **Weiter** , um die Caching-Konfiguration abzuschließen.
6. Klicken Sie auf **Fertig stellen** , um Citrix Virtual Desktops oder gestreamte VMs bereitzustellen und die ausgewählte Citrix Provisioning -Site mit dem PVS Accelerator in Citrix Hypervisor zu verknüpfen. Wenn dieser Schritt abgeschlossen ist, ist die Schaltfläche **PVS-Server anzeigen** im **Konfigurationsfenster PVS-Beschleuniger** 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.

Zwischenspeichervorgang

Berücksichtigen Sie Folgendes, wenn Sie die PVS-Beschleunigerfunktion verwenden:

- Die PVS-Accelerator-Benutzeroberflächen in XenCenter und Citrix Provisioning werden nur verfügbar gemacht, wenn das Zusatzpaket PVS-Accelerator installiert ist.
- Citrix Provisioning Zielgeräte kennen ihren Proxystatus. Nach der Installation der Funktion ist keine zusätzliche Konfiguration erforderlich.
- In Umgebungen, in denen mehrere Citrix Provisioning -Server mit derselben virtuellen Festplatte bereitgestellt werden, aber unterschiedliche Dateisystemzeitstempel aufweisen, werden Daten möglicherweise mehrmals zwischengespeichert. Aufgrund dieser Einschränkung empfehlen wir, VHDX-Format anstelle von VHD für virtuelle Laufwerke zu verwenden.
- Verwenden Sie keinen großen Portbereich für die PVS-Serverkommunikation. Die Einstellung einer Reichweite von mehr als 20 Ports ist selten notwendig. Ein großer Portbereich kann die Paketverarbeitung verlangsamen und die Startzeit der Citrix Hypervisor or-Steuerdomäne bei Verwendung von PVS-Accelerator erhöhen.
- Nachdem Sie eine VM mit aktiviertem PVS-Accelerator gestartet haben, wird der Caching-Status für die VM in XenCenter angezeigt:
  - Auf der Registerkarte **PVS** des Pools oder des Hosts
  - Auf der Registerkarte **Allgemein** für die VM
- Kunden können den korrekten Betrieb des PVS-Accelerators mithilfe von RRD-Metriken auf der Registerkarte **Leistung** des Hosts in XenCenter bestätigen. Weitere Informationen finden Sie unter Überwachen und Verwalten Ihrer Bereitstellung.

> **Wichtig:**
>
> - PVS-Accelerator erfordert Citrix Provisioning 7.13 oder höher.
> - PVS-Accelerator ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Desktops und Citrix Virtual Apps-Berechtigung Zugriff auf Citrix Hypervisor haben.
> - PVS-Accelerator benötigt Lizenzserver 11.14.
> - PVS-Accelerator verwendet Funktionen von OVS und ist daher nicht auf Hosts verfügbar, die Linux Bridge als Netzwerk-Back-End verwenden.
> - PVS-Accelerator wird in Verbindung mit dem vSwitch Controller nicht unterstützt.
> - PVS-Accelerator arbeitet an der ersten virtuellen Netzwerkschnittstelle (VIF) einer zwischengespeicherten VM. Verbinden Sie daher die erste VIF mit dem Citrix Provisioning -Speichernetzwerk, damit das Caching funktioniert.
> - PVS-Accelerator kann derzeit nicht auf Netzwerkports 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 können PVS-Ziele nicht mit dem Fehler „Anmeldeanforderung Timeout¡‘ gestartet werden. nach dem Aktivieren des PVS-Beschleunigers.

Die Funktionalität des PVS-Beschleunigers wird zwischengeschlitzt:

- **Liest** von virtuellen Laufwerken, aber nicht schreibt oder liest aus einem Schreibcache
- **Basierend auf Bildversionen**. Mehrere VMs teilen zwischengespeicherte Blöcke, wenn sie dieselbe Image-Version verwenden
- Geräte mit einem **nicht persistenten** Schreib-Cache-Typ
- Virtuelle Laufwerke mit dem **Zugriffsmodus Standard Image**. Es funktioniert nicht für virtuelle Laufwerke mit dem Zugriffsmodus Private Image
- Geräte, die als **Typ Production oder Test**markiert sind. Geräte, die als Typ Wartung gekennzeichnet sind, werden nicht zwischengespeichert

PVS-Beschleuniger CLI-Vorgänge

Im folgenden Abschnitt werden die Vorgänge beschrieben, die Kunden ausführen können, wenn sie PVS-Accelerator mit der CLI verwenden. Kunden können diese Vorgänge auch mit XenCenter ausführen. Weitere Informationen finden Sie in der XenCenter Hilfe.

Anzeigen von Citrix Provisioning-Serveradressen und -ports, die von Citrix Provisioning konfiguriert wurden

PVS-Accelerator optimiert den Netzwerkverkehr zwischen einer VM und dem Citrix Provisioning -Server. Beim Abschluss der Konfiguration auf dem Citrix Provisioning -Server füllt der Citrix Provisioning-Server die`pvs-server` Objekte auf Citrix Hypervisor mit ihren IPs und Ports. PVS-Accelerator verwendet diese Informationen später, um den Datenverkehr zwischen einer VM und ihren Citrix Provisioning-Servern zu optimieren. Die konfigurierten Citrix Provisioning -Server können mit dem folgenden Befehl aufgelistet werden:

```
1 xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
```

Konfigurieren einer VM für das Caching

PVS-Accelerator kann für die VM mit einem der folgenden Tools aktiviert werden:

- Citrix Provisioning CLI
- Setup-Assistent für Citrix Virtual Desktops
- Setup-Assistent 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 die erste VIF der VM, um das Caching zu aktivieren:

   ```
   1 VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
       minimal)
   ```

2. Erstellen des Citrix Provisioning Proxy

   ```
   1 xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
   ```

Caching für eine VM deaktivieren

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 die erste VIF der VM:


```
VIF_UUID=$(xe vif-list vm-name-label=pvsdevice_1 device=0 --
    minimal)
```

2. Suchen Sie den Citrix Provisioning Proxy der VM:

```
PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
```

3. Zerstören Sie den Citrix Provisioning Proxy:

```
xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
```

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 zerstören möchten:

```
HOST_UUID=$(xe host-list name-label=HOST_NAME --minimal)
```

2. Suchen Sie die uuid des Objekts:

```
PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=
    $HOST_UUID --minimal)
```

3. Objekt zerstören:

```
xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
```

Vergessen Sie die PVS-Accelerator-Konfiguration für eine Site

So vergessen Sie die PVS-Accelerator-Konfiguration für eine Site:

1. Suchen Sie die Citrix Provisioning Website:

```
PVS_SITE_UUID=$(xe pvs-site-list name-label=My PVS Site)
```

2. Führen Sie den folgenden Befehl aus, um die Citrix Provisioning-Site zu vergessen:

```
xe pvs-site-forget uuid=$PVS_SITE_UUID
```

Kopiert!
Failed!

Grafikübersicht

October 16, 2019

Dieser Abschnitt bietet einen Überblick über die virtuelle Bereitstellung von professionellen 3D-Grafikanwendungen und -Workstations von Citrix Hypervisor. Das Angebot umfasst GPU-Pass-Through (für NVIDIA, AMD und Intel GPUs) und hardwarebasierte GPU-Sharing mit NVIDIA GRID™ vGPU™, AMD MxGPU™ und Intel GVT-G™.

GPU-Pass-Through

In einem virtualisierten System werden die meisten physischen 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 eine eigene dedizierte GPU, wodurch die Softwareverstraktion und die damit einhergehende Leistungseinbuße eliminiert werden.

Mit Citrix Hypervisor können Sie einer Windows oder HVM-Linux-VM, die auf demselben Host ausgeführt wird, eine physische GPU (im Citrix Hypervisor or-Server) zuweisen. Diese GPU-Pass-Through-Funktion ist für Grafik-Power-Benutzer wie CAD-Designer gedacht.

Gemeinsame GPU

Gemeinsame GPU ermöglicht die gleichzeitige Verwendung einer physischen GPU von mehreren VMs. Da ein Teil einer physischen GPU verwendet wird, ist die Leistung größer als die emulierte Grafik, und es besteht keine Notwendigkeit für eine Karte pro VM. Diese Funktion ermöglicht Ressourcenoptimierung und steigert die Leistung der VM. Die Grafikbefehle jeder virtuellen Maschine werden direkt an die GPU übergeben, ohne dass der Hypervisor übersetzt wird.

Lizenzierungshinweis

Die Grafikvirtualisierung ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Berechtigung für virtuelle Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie auf der Citrix Websitehier. Weitere Informationen finden Sie unter Lizenzierung.

Anbieter-Support

In der folgenden Tabelle sind GPU- und gemeinsam genutzte GPU-Unterstützung für Gäste aufgeführt:

	GPU für Windows VMs	GPU für HVM Linux-VMs	Gemeinsame GPU für Windows VMs	Virtuelle GPU für Linux-VMs
AMD	JA		JA	
Intel	JA		JA	
NVIDIA	JA	JA	JA	JA

Je nach verwendeter Grafikkarte benötigen Sie möglicherweise ein Anbieterabonnement oder eine Lizenz.

vGPU Livemigration

Die vGPU Livemigration ermöglicht eine VM, die eine virtuelle GPU verwendet, um Live-Migration, Speicher-Livemigration oder VM Suspend durchzuführen. VMs mit vGPU -Live-Migrationsfunktionen können migriert werden, um Ausfallzeiten zu vermeiden.

Mit der vGPU Livemigration können Sie auch Rolling-Pool-Upgrades auf Pools durchführen, die VGPU-fähige VMs hosten. Weitere Informationen finden Sie unter Upgrades für rollende Schwimmbecken.

Um die vGPU Livemigration zu verwenden, muss die VM auf einer Grafikkarte ausgeführt werden, die diese Funktion unterstützt und die unterstützten Treiber vom GPU-Hersteller installiert sind.

Bei der vGPU Livemigration gelten die folgenden Einschränkungen:

- Die Livemigration von VMs aus früheren Versionen von Citrix Hypervisor wird nicht unterstützt.
- Live-Migration ist nicht mit GPU-Pass-Through kompatibel.
- VMs müssen die entsprechenden vGPU -Treiber installiert sein, damit sie mit allen vGPU-Live-Migrationsfunktionen unterstützt werden können. Die In-Gast-Treiber müssen für alle Gäste installiert werden, die vGPU verwenden.
- Neustart- und Herunterfahrvorgänge auf einer VM werden während einer Migration nicht unterstützt. Diese Vorgänge können dazu führen, dass die Migration fehlschlägt.
- Linux-VMs werden mit vGPU -Live-Migrationsfunktionen nicht unterstützt.
- Die Livemigration durch die Workload Balancing-Appliance wird für VGPU-fähige VMs nicht unterstützt. Die Workload Balancing-Appliance kann keine Kapazitätsplanung für VMs mit einer vGPU durchführen.

- Nach der Migration einer VM mit vGPU Livemigration kann die Gast-VNC-Konsole beschädigt werden. Verwenden Sie ICA, RDP oder eine andere netzwerkbasierte Methode für den Zugriff auf VMs, nachdem eine vGPU Livemigration durchgeführt wurde.
- Die VDI-Migration verwendet Live-Migration, daher erfordert genügend vGPU Speicherplatz auf dem Host, um eine Kopie der vGPU-Instanz auf dem Host zu erstellen. Wenn die physischen GPUs vollständig genutzt werden, ist die VDI-Migration möglicherweise nicht möglich.

Anbieter-Support

In der folgenden Tabelle sind die Unterstützung für vGPU Live-Migration aufgeführt:

	GPRU für Windows VMs	GPU für HVM Linux-VMs	Gemeinsame GPU für Windows VMs	Virtuelle GPU für Linux-VMs
NVIDIA			JA	

Weitere Informationen zu den Grafikkarten, die diese Funktion unterstützen, finden Sie in den herstellerspezifischen Abschnitten dieses Handbuchs. Je nach verwendeter Grafikkarte benötigen Kunden möglicherweise ein Anbieterabonnement oder eine Lizenz.

Gast-Support und Einschränkungen

Citrix Hypervisor 8.0 unterstützt die folgenden Gastbetriebssysteme für virtuelle GPU.

NVIDIA vGPU

Windows Gäste:

- Windows 7 (32-Bit/64-Bit)
- Windows 8.1 (32-Bit/64-Bit)
- Windows 10 (64 Bit)
- Windows Server 2008 R2 SP1 (64 Bit)
- Windows Server 2012 (64 Bit)
- Windows Server 2012 R2 (64 Bit)
- Windows Server 2016 (64 Bit)
- Windows Server 2019 (64 Bit)

HVM Linux-Gäste:

- RHEL 7.x

- CentOS 7.x
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 18.04

AMD MxGPU

Windows Gäste:

- Windows 7 SP1 (64 Bit)
- Windows 10 (64 Bit)
- Windows Server 2016 (64 Bit)
- Windows Server 2019 (64 Bit)

Intel GVT-G

Windows Gäste:

- Windows 7 (32-Bit/64-Bit)
- Windows 8.1 (32-Bit/64-Bit)
- Windows 10 (64 Bit)
- Windows Server 2008 R2 SP1 (64 Bit)
- Windows Server 2012 R2 (64 Bit)
- Windows Server 2016 (64 Bit)

Einschränkungen

- Citrix Hypervisor unterstützt nur eine GPU pro VM.
- VMs mit einer virtuellen GPU werden von Dynamic Memory Control nicht unterstützt.
- Citrix Hypervisor erkennt und gruppiert automatisch identische physische GPUs auf Hosts im selben Pool. Wenn 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, AMD MxGPU und vGPU Pass-Through) können in einer Umgebung verwendet werden, die hohe Verfügbarkeit nutzt. VMs, die diese Grafiklösungen verwenden, können jedoch nicht mit hoher Verfügbarkeit geschützt werden. Diese VMs können nach bestem Aufwand neu gestartet werden, während Hosts mit den entsprechenden freien Ressourcen vorhanden sind.

Kopiert!
Failed!

Vorbereiten des Hosts für Grafiken

October 16, 2019

Dieser Abschnitt enthält schrittweise Anweisungen zum Vorbereiten von Citrix Hypervisor für unterstützte grafische Virtualisierungstechnologien. Zu den Angeboten gehören NVIDIA GRID vGPU, AMD MxGPU und Intel GVT-d und GVT-G.

NVIDIA GRID vGPU

Mit der NVIDIA GRID vGPU können mehrere virtuelle Maschinen (VM) gleichzeitig direkten Zugriff auf eine einzelne physische GPU haben. Es verwendet NVIDIA-Grafiktreiber, die auf nicht virtualisierten Betriebssystemen bereitgestellt werden. GRID physische GPUs können mehrere virtuelle GPU-Geräte (VGPUs) unterstützen. Um diese Unterstützung zu bieten, muss die physische GPU unter der Kontrolle des GRID Virtual GPU Managers von NVIDIA stehen, der in Citrix Hypervisor Control Domain (dom0) ausgeführt wird. Die VGPUs können VMs direkt zugewiesen werden.

VMs verwenden virtuelle GRID-GPUs wie eine physische GPU, die der Hypervisor durchlaufen hat. Ein in die VM geladener NVIDIA-Treiber ermöglicht direkten Zugriff auf die GPU für leistungskritische schnelle Pfade. Es bietet auch eine paravirtualisierte Schnittstelle zum GRID Virtual GPU Manager.

NVIDIA GRID ist mit der HDX 3D Pro Funktion von Citrix Virtual Apps and Desktops kompatibel. Weitere Informationen finden Sie unter HDX 3D Pro.

Lizenzierungshinweis

NVIDIA vGPU ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie auf der Citrix Websitehier. 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 imWebsite von NVIDIA.

Verfügbare NVIDIA GRID vGPU ypen

NVIDIA GRID-Karten enthalten mehrere Grafikprozessoren (GPU). Beispielsweise enthalten TESLA M10-Karten vier GM107GL-GPUs und TESLA M60-Karten zwei GM204GL-GPUs. Jede physische GPU kann mehrere verschiedene Typen virtueller GPU (vGPU) hosten. vGPU-Typen haben eine feste

Menge an Frame-Puffer, Anzahl der unterstützten Anzeigeköpfe und maximale Auflösungen und sind auf verschiedene Klassen von Arbeitslasten ausgerichtet.

Eine Liste der zuletzt unterstützten NVIDIA-Karten finden Sie unter Hardwarekompatibilitätsliste und NVIDIA-Produktinformationen.

> **Hinweis:**
>
> Die vGPUs, die gleichzeitig auf einer physischen GPU gehostet werden, **müssen alle vom gleichen Typ sein.** Es gibt jedoch keine entsprechende Einschränkung für physische GPUs auf derselben Karte. Diese Einschränkung ist automatisch und kann zu unerwarteten Kapazitätsplanungsproblemen führen.
>
> Beispielsweise verfügt eine TESLA M60-Karte über zwei physische GPUs und kann 11 vGPU -Typen unterstützen:
>
> - GITTER M60-1A
> - GITTER M60-2A
> - GITTER M60-4A
> - GITTER M60-8A
> - GITTER M60-0B
> - GITTER M60-1B
> - GITTER M60-0Q
> - GITTER M60-1Q
> - GITTER M60-2Q
> - GITTER M60-4Q
> - GRID M60-8Q
>
> In dem Fall, in dem Sie sowohl eine VM mit vGPU Typ M60-1A als auch eine VM mit vGPU Typ M60-2A starten:
>
> - Eine physische GPU unterstützt nur M60-1A-Instanzen
> - Die andere unterstützt nur M60-2A-Instanzen
>
> Auf dieser Karte können keine M60-4A-Instanzen gestartet werden.

NVIDIA GRID-Systemanforderungen

- NVIDIA GRID-Karte:
  - Eine Liste der zuletzt unterstützten NVIDIA-Karten finden Sie unter Hardwarekompatibilitätsliste und NVIDIA-Produktinformationen.
- Je nach verwendeter NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-Abonnement oder eine Lizenz. Weitere Informationen finden Sie unter NVIDIA-Produktinformationen.

- Citrix Hypervisor Premium Edition (oder Zugriff auf Citrix Hypervisor über eine Berechtigung für Citrix Virtual Apps and Desktops).
- Ein Server, der Citrix Hypervisor und NVIDIA GRID-Karten hosten kann.
- NVIDIA GRID vGPU -Softwarepaket für Citrix Hypervisor, bestehend aus GRID Virtual GPU Manager für Citrix Hypervisor und NVIDIA-Treibern.
- Zum Ausführen von Citrix Virtual Desktops mit VMs mit NVIDIA vGPU benötigen Sie außerdem: Citrix Virtual Desktops 7.6 oder höher, vollständige Installation.

> **Hinweis:**
>
> Lesen Sie das NVIDIA GRID Virtual GPU Benutzerhandbuch (Ref: DU-06920-001), das im verfügbar istWebsite von NVIDIA. Registrieren Sie sich bei NVIDIA, um auf diese Komponenten zuzugreifen.

vGPU Livemigration

Citrix Hypervisor ermöglicht die Verwendung von Livemigration, Speicher-Livemigration und die Möglichkeit, für NVIDIA GRID VGPU-fähige VMs anzuhalten und wieder aufzunehmen.

Um die vGPU Livemigration, die Speicher-Livemigration oder die Suspend-Funktionen zu verwenden, erfüllen Sie die folgenden Anforderungen:

- Eine NVIDIA GRID-Karte, Maxwell Familie oder höher.
- Ein NVIDIA GRID Virtual GPU-Manager für Citrix Hypervisor mit aktivierter Livemigration. Weitere Informationen finden Sie in der NVIDIA-Dokumentation.
- Eine Windows VM, auf der NVIDIA Live-Migrationsfähige vGPU -Treiber installiert sind.

vGPU Livemigration ermöglicht die Verwendung von Live-Migration innerhalb eines Pools, Live-Migration zwischen Pools, Speicher-Livemigration und Suspend/Resume von VGPU-fähigen VMs.

Vorbereitungsübersicht

1. Installieren von Citrix Hypervisor
2. Installieren Sie den NVIDIA GRID Virtual GPU-Manager für Citrix Hypervisor
3. Starten Sie den Citrix Hypervisor -Server neu

Installation auf Citrix Hypervisor

Citrix Hypervisor steht auf der Citrix Hypervisor Downloads Seite zum Download bereit.

Installieren Sie Folgendes:

- **Citrix Hypervisor Basisinstallations-ISO**
- **XenCenter Windows Verwaltungskonsole**

Weitere Informationen finden Sie unter Installieren.

Lizenzierungshinweis

vGPU ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie auf der Citrix Websitehier. 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.

Weitere Informationen zur Lizenzierung von NVIDIA-Karten finden Sie imWebsite von NVIDIA.

Installieren Sie den NVIDIA GRID vGPU Manager für Citrix Hypervisor

Installieren Sie die NVIDIA GRID vGPU -Software, die von verfügbar istNVIDIA. Die NVIDIA GRID Software besteht aus:

- GRID vGPU Manager

  (Beispiel: NVIDIA-VGPU-Citrix Hypervisor-7.2-367.64.x86_64.rpm)

- Windows Anzeigetreiber (Der Windows Anzeigetreiber hängt von der Windows-Version ab)

  (Beispiel: 369.71_grid_win10_server2016_64bit_international.exe)

Der *GRID vGPU Manager* wird in der Citrix Hypervisor Control Domain (dom0) ausgeführt. Es wird entweder als ergänzendes Paket oder als RPM-Datei bereitgestellt. Weitere Informationen zur Installation finden Sie im Benutzerhandbuch der NVIDIA GRID vGPU -Software.

> **Hinweis:**
>
> Update, RPM Namen und Versionen sind Beispiele und unterscheiden sich in Ihrer Umgebung.

Das Update kann mit einer der folgenden Methoden installiert werden:

- XenCenter verwenden (**ToolsUpdate > installieren > ****Select ein Update oder ein zusätzliches Paket von der Festplatte aus**)
- Verwenden Sie den Befehl xe CLI`xe-install-update`.

Das Update hat den Namen`NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.iso` oder ähnliches.

> **Hinweis:**
>
> Wenn Sie den GRID vGPU Manager mithilfe einer RPM-Datei installieren, stellen Sie sicher, dass Sie die RPM-Datei nach dom0 kopieren und installieren.

1. Verwenden Sie den Befehl rpm, um das Paket zu installieren:

```
rpm -iv NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.rpm
```

2. Starten Sie den Citrix Hypervisor -Server neu:

```
shutdown -r now
```

3. Überprüfen Sie nach dem Neustart des Citrix Hypervisor or-Servers, ob das GRID-Paket ordnungsgemäß installiert und geladen wurde, indem Sie den NVIDIA-Kerneltreiber überprüfen:

```
[root@xenserver ~]#lsmod |grep nvidia
    nvidia            8152994 0
    i2c_core            20294 2 nvidia,i2c_i801
```

4. Stellen Sie sicher, dass der NVIDIA-Kerneltreiber erfolgreich mit den GRID-physischen GPUs in Ihrem Host kommunizieren kann. Führen Sie dennvidia-smi Befehl aus, um eine Auflistung 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 |
+-----------------------------------------------------------------------------
```

> **Hinweis:**
>
> Wenn Sie NVIDIA vGPU mit Citrix Hypervisor or-Servern mit mehr als 768 GB RAM verwenden, fügen Sie den Parameter der Xen Befehlszeile`iommu=dom0-passthrough`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.

AMD MxGPU

Mit AMDs MxGPU können mehrere virtuelle Maschinen (VM) über Single Root I/O-Virtualisierung direkten Zugriff auf einen Teil einer einzelnen physischen GPU haben. Der gleiche AMD-Grafiktreiber, der auf nicht virtualisierten Betriebssystemen bereitgestellt wird, kann innerhalb des Gastes verwendet werden.

VMs verwenden MxGPU-GPUs auf die gleiche Weise wie eine physische GPU, die der Hypervisor durchlaufen hat. Ein in die VM geladener AMD-Grafiktreiber bietet direkten Zugriff auf die GPU für leistungskritische schnelle Pfade.

Weitere Informationen zur Verwendung von AMD MxGPU mit Citrix Hypervisor finden Sie imAMD Dokumentation.

Lizenzierungshinweis

MxGPU ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zu Citrix Hypervisor Editionen und zum Upgrade finden Sie auf der Citrix Websitehier. Ausführliche Informationen zur Lizenzierung finden Sie imHäufig gestellte Fragen zur Citrix Hypervisor or-Lizenzierung.

Verfügbare AMD MxGPU-vGPU ypen

AMD MxGPU-Karten können mehrere GPUs enthalten. S7150-Karten enthalten beispielsweise eine physische GPU und S7150x2-Karten zwei GPUs. Jede physische GPU kann mehrere verschiedene Typen virtueller GPU (vGPU) hosten. vGPU-Typen teilen eine physische GPU in eine vordefinierte Anzahl von vGPU auf. Jede dieser VGPUs hat einen gleichen Anteil an den Frame-Puffer- und Grafikverarbeitungsfähigkeiten. Die verschiedenen vGPU ypen richten sich an verschiedene Klassen von Arbeitslasten. vGPU ypen, die eine physische GPU in weniger Teile aufteilen, eignen sich besser für intensive Arbeitslasten.

> **Hinweis:**
>
> Die gleichzeitig auf einer physischen GPU gehosteten VGPUs **müssen alle vom gleichen Typ sein**. Es gibt jedoch keine entsprechende Einschränkung für physische GPUs auf derselben Karte. Diese Einschränkung ist automatisch und kann zu unerwarteten Kapazitätsplanungsproblemen führen.

AMD MxGPU-Systemanforderungen

- AMD FirePro S7100-Serie GPUs
- Citrix Hypervisor Premium Edition (oder Zugriff auf Citrix Hypervisor über eine Citrix Virtual Desktops oder Citrix Virtual Apps Berechtigung)
- Ein Server, der Citrix Hypervisor und AMD MxGPU-Karten hosten kann. Die Liste der von AMD validierten Server finden Sie aufdie AMD Website.
- AMD MxGPU-Hosttreiber für Citrix Hypervisor. Diese Treiber sind verfügbar von die AMD Download-Site.
- AMD FirePro In-Gast-Treiber, geeignet für MxGPU auf Citrix Hypervisor. Diese Treiber sind verfügbar von die AMD Download-Site.
- Zum Ausführen von Citrix Virtual Desktops mit VMs mit AMD MxGPU benötigen Sie außerdem eine vollständige Installation von Citrix Virtual Desktops 7.13 oder höher.
- System-BIOS für die Unterstützung von SR-IOV und der als sekundärer Adapter konfigurierten MxGPU

Vorbereitungsübersicht

1. Installieren von Citrix Hypervisor
2. Installieren der AMD MxGPU-Hosttreiber für Citrix Hypervisor
3. Starten Sie den Citrix Hypervisor -Server neu

Installation auf Citrix Hypervisor

Citrix Hypervisor steht auf der Citrix Hypervisor Downloads Seite zum Download bereit.

Installieren Sie Folgendes:

- **Citrix Hypervisor 8.0 Basisinstallations-ISO**
- **XenCenter 8.0 Windows Verwaltungskonsole**

Weitere Informationen zur Installation finden Sie unterCitrix Hypervisor Installationshandbuch.

Installieren des AMD MxGPU-Hosttreibers für Citrix Hypervisor

Führen Sie die folgenden Schritte aus, um den Hosttreiber zu installieren.

1. Das Update, das den Treiber enthält, kann mithilfe von XenCenter oder mithilfe der XE CLI installiert werden.
   - Um mithilfe von XenCenter zu installieren, gehen Sie zu **Extras > Update installieren > Update oder Zusatzpaket von der Festplatte Select**
   - Um mithilfe der xe-CLI zu installieren, kopieren Sie das Update auf den Host und führen Sie den folgenden Befehl in dem Verzeichnis aus, in dem sich das Update befindet:

     ```
     xe-install-supplemental-pack mxgpu-1.0.5.amd.iso
     ```

2. Starten Sie den Citrix Hypervisor -Server neu.
3. Überprüfen Sie nach dem Neustart des Citrix Hypervisor or-Servers, ob das MxGPU-Paket ordnungsgemäß installiert und geladen wurde. Überprüfen Sie, ob der`gim` Kerneltreiber geladen wird, indem Sie die folgenden Befehle in der Citrix Hypervisor or-Serverkonsole ausführen:

   ```
   modinfo gim
   modprobe gim
   ```

4. Stellen Sie sicher, dass der`gim` Kerneltreiber MxGPU Virtual Functions erfolgreich erstellt hat, die den Gästen zur Verfügung gestellt werden. Führen Sie den folgenden Befehl aus:


```
lspci | grep "FirePro S7150"
```

Die Ausgabe des Befehls zeigt virtuelle Funktionen mit dem Bezeichner „S7150V“ an.

5. Verwenden Sie die Registerkarte „GPU“ in XenCenter, um zu bestätigen, dass virtuelle MxGPU-GPU-Typen als verfügbar auf dem System aufgeführt werden.

Nach der Installation der AMD MxGPU-Treiber ist die **Passthrough-Option** für die GPUs nicht mehr verfügbar. Verwenden Sie stattdessen die Option **MxGPU.1** .

Erstellen einer MxGPU-fähigen VM

Bevor Sie eine VM für die Verwendung von MxGPU konfigurieren, installieren Sie die VM. Stellen Sie sicher, dass AMD MxGPU das VM-Betriebssystem unterstützt. Weitere Informationen finden Sie unter Gast-Support und Einschränkungen.

Führen Sie nach der Installation der VM die Konfiguration durch, indem Sie die Anweisungen unter befolgenErstellen von vGPU fähigen VMs.

Intel GVT-D und GVT-G

Citrix Hypervisor unterstützt Intels Virtual GPU (GVT-G), eine Grafikbeschleunigungslösung, die keine zusätzliche Hardware erfordert. Es verwendet die Intel Iris Pro-Funktion, die in bestimmte Intel-Prozessoren eingebettet ist, und einen standardmäßigen Intel GPU-Treiber, der in der VM installiert ist.

Intel GVT-d und GVT-G sind mit den HDX 3D Pro Funktionen von Citrix Virtual Apps and Desktops 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 kommt es möglicherweise nicht zu einer vollständigen Grafikbeschleunigung wie bei rein GPU-intensiven Arbeitslasten.

Intel GVT-G Systemanforderungen und -konfiguration

Um Intel GVT-G verwenden zu können, muss Ihr Citrix Hypervisor or-Server über die folgende Hardware verfügen:

- Eine CPU mit Iris Pro-Grafik. Diese CPU muss auf derHardwarekompatibilitätslisteSeite

- Ein Motherboard, das über einen Grafikchipsatz verfügt. 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-Pass-Through (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 Citrix Hypervisor or-Server unterstützt werden, von der Größe der GPU-Leiste ab. Die GPU-Balkengröße wird im BIOS als „Blendengröße“ bezeichnet. Es wird empfohlen, die Aperture-Größe auf 1.024 MB festzulegen, 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 gestartet werden. Die Einstellung auf 512 MB kann dazu führen, dass nur drei VMs auf dem Citrix Hypervisor or-Server gestartet werden. Eine Aperture-Größe größer als 1.024 MB wird nicht unterstützt und erhöht **nicht** die Anzahl der VMs, die auf einem Host gestartet werden.

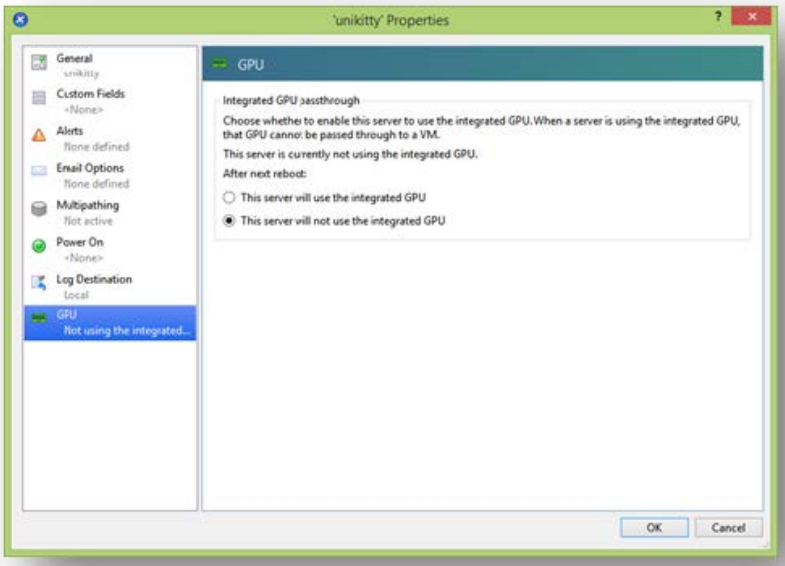
Intel GPU-Pass-Through aktivieren

Citrix Hypervisor unterstützt die GPU-Pass-Through-Funktion für Windows 7 und Windows 8.1 (32-/64-Bit) VMs mit einem integrierten Intel GPU-Gerät. Weitere Informationen zu unterstützter Hardware finden Sie imHardwarekompatibilitätsliste.

Wenn Sie Intel GPU auf Intel-Servern verwenden, hat die Control Domain (dom0) des Citrix Hypervisor or-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 an die VM übergeben.

Führen Sie die folgenden Schritte aus, um diese Verbindung zu deaktivieren:

1. Wählen Sie im Bereich **Ressourcen** den Citrix Hypervisor -Server 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 Citrix Hypervisor or-Server neu, damit die Änderungen wirksam werden.

   Die Intel GPU ist jetzt in der Liste der GPU-Typen während der Erstellung neuer VM und auf der Registerkarte **Eigenschaften** der VM sichtbar.

   > **Hinweis:**
   >
   > Der externe Konsolenausgang des Citrix Hypervisor or-Servers (z. B. VGA, HDMI, DP) ist nach dem Deaktivieren der Verbindung zwischen dom0 und der GPU nicht verfügbar.

Kopiert!
Failed!

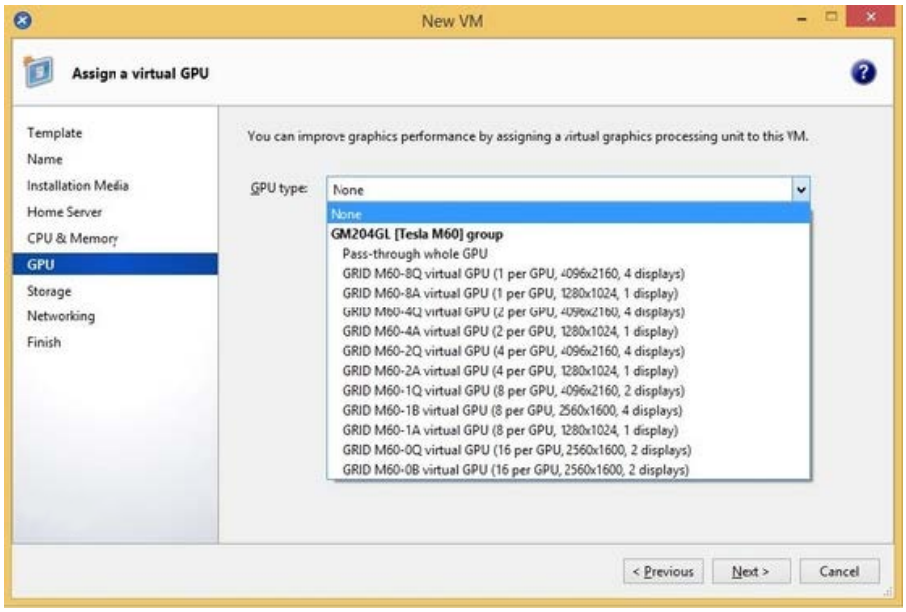
Erstellen von vGPU fähigen VMs

October 16, 2019

Dieser Abschnitt enthält 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 *Enabling Intel GPU-Pass-Through*für weitere Konfigurationen, und führen Sie dann die folgenden Schritte aus.

1. Erstellen Sie eine VM mit XenCenter. Select den Host im Bereich Ressourcen und dann im Menü **VM die Option Neue** VM aus.
2. Folgen Sie den Anweisungen in der Konfiguration „ **Neue VM** “, und wählen Sie das **Installationsmedium** , den **Heimserver** , die **CPU** und den **Arbeitsspeicher** aus.
3. GPU-fähige Server zeigen eine **GPU-Konfigurationsseite** an:



4. Wählen Sie in der Liste **GPU-Typ** entweder **GPU-Through GPU-Typ** oder einen virtuellen GPU-Typ aus.

   Nicht verfügbare virtuelle GPU-Typen sind ausgegraut.
5. Klicken Sie auf **Weiter** , um **Speicher** und **Netzwerk** zu konfigurieren.
6. Klicken Sie nach Abschluss der Konfiguration auf **Jetzt erstellen**.

Installieren der Citrix VM-Tools

1. Installieren der Citrix VM-Tools

   Ohne die optimierten Netzwerk- und Speichertreiber der Citrix VM Tools bieten Remote-Grafikanwendungen, die auf GRID vGPU ausgeführt werden, **keine** maximale Leistung.

a) Select die VM im **Ressourcenbereich** aus, klicken Sie mit der rechten Maustaste, und klicken Sie dann im Kontextmenü auf **Citrix VM-Tools installieren**. Alternativ klicken Sie im Menü **VM** auf **Citrix VM Tools installieren** .

b) Klicken Sie im Meldungsdialog auf **Citrix VM Tools installieren** , um zur Konsole der VM zu wechseln und mit der Installation zu beginnen.

c) Wenn die automatische Wiedergabe für das CD/DVD-Laufwerk der VM aktiviert ist, wird die Installation nach wenigen Augenblicken automatisch gestartet. Dieser Prozess installiert die E/A-Treiber und den Management Agent. Starten Sie die VM neu, wenn Sie aufgefordert werden, Ihre VM in einen optimierten Zustand zu versetzen. Wenn die automatische Wiedergabe nicht aktiviert ist, zeigt das Citrix VM Tools-Installationsprogramm die Installationsoptionen an. Klicken Sie auf **Citrix VM-Tools installieren**, um mit der Installation fortzufahren. Mit diesem Vorgang wird das Citrix VM Tools-ISO (guest-tools.iso) auf dem CD/DVD-Laufwerk der VM bereitgestellt.

d) Klicken Sie auf **Setup.exe ausführen** , um die Installation von Citrix VM Tools zu starten und die VM neu zu starten, wenn Sie aufgefordert werden, die VM in einen optimierten Zustand zu versetzen.

Installieren der In-Gast-Treiber

Beim Anzeigen der VM-Konsole in XenCenter wird die VM normalerweise im VGA-Modus mit einer Auflösung von 800 x 600 auf dem Desktop gestartet. Die standardmäßigen Windows Bildschirmauflösungssteuerungen können verwendet werden, um die Auflösung auf andere Standardauflösungen zu erhöhen. (Systemsteuerung > Anzeige > Bildschirmauflösung)

> **Hinweis:**
>
> Wenn Sie GPU-Pass-Through oder MxGPU verwenden, empfehlen wir, die In-Gast-Treiber über RDP oder VNC über das Netzwerk zu installieren. Das heißt, nicht über XenCenter.

Installieren Sie die NVIDIA-Treiber

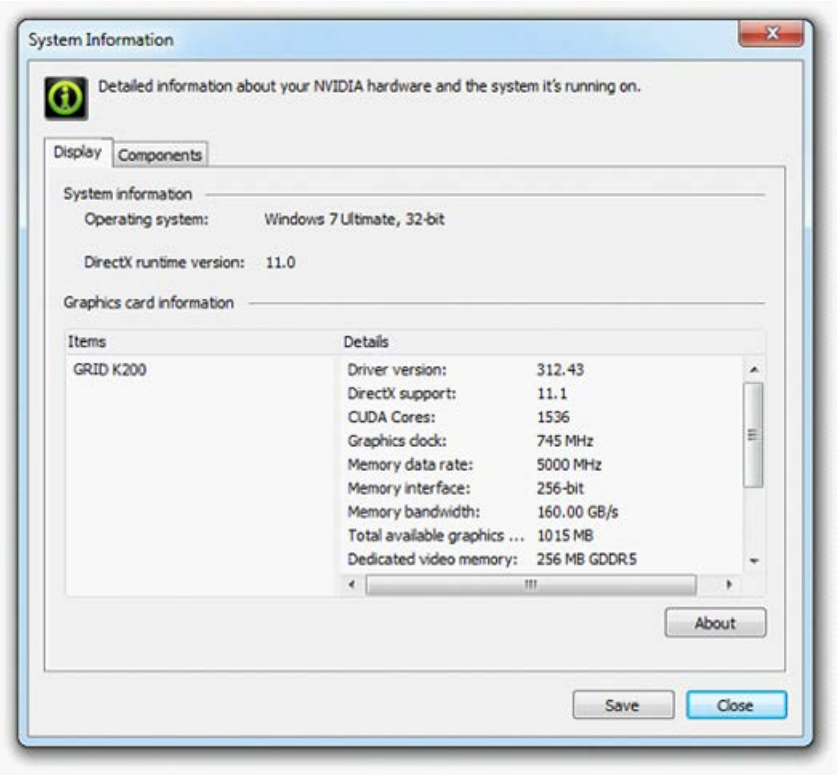
Um den vGPU Betrieb (wie bei einer physischen NVIDIA-GPU) zu aktivieren, installieren Sie NVIDIA-Treiber in der VM.

Der folgende Abschnitt bietet einen Überblick über die Vorgehensweise. Ausführliche Anweisungen finden Sie in den NVIDIA-Benutzerhandbüchern.

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 Citrix Hypervisor der VM dynamisch eine vGPU zu.

2. Folgen Sie den Installationsbildschirmen des Windows Betriebssystems.
3. Starten Sie die VM nach Abschluss der Installation des Betriebssystems 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 32-Bit- oder 64-Bit-NVIDIA-Windows -Treiberpaket auf die VM, öffnen Sie die ZIP-Datei, und führen Sie setup.exe aus.
6. Führen Sie die Installationsschritte aus, um den Treiber zu installieren.
7. Nach Abschluss der Treiberinstallation werden Sie möglicherweise aufgefordert, die VM neu zu starten. Select **Jetzt neu starten** , um die VM sofort neu zu starten, alternativ beenden Sie das Installationspaket und starten Sie die VM neu, wenn sie bereit ist. Wenn die VM gestartet wird, wird sie auf einem Windows Desktop gestartet.
8. Um zu überprüfen, ob der NVIDIA-Treiber ausgeführt wird, klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie **NVIDIA-Systemsteuerung**aus.
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:



> **Hinweis:**
>
> Je nach verwendeter NVIDIA-Grafikkarte benötigen Sie möglicherweise ein NVIDIA-

> Abonnement oder eine Lizenz. Weitere Informationen finden Sie unter NVIDIA-Produktinformationen.

Die VM ist nun bereit, die gesamte Palette von DirectX- und OpenGL-Grafikanwendungen auszuführen, die von der GPU unterstützt werden.

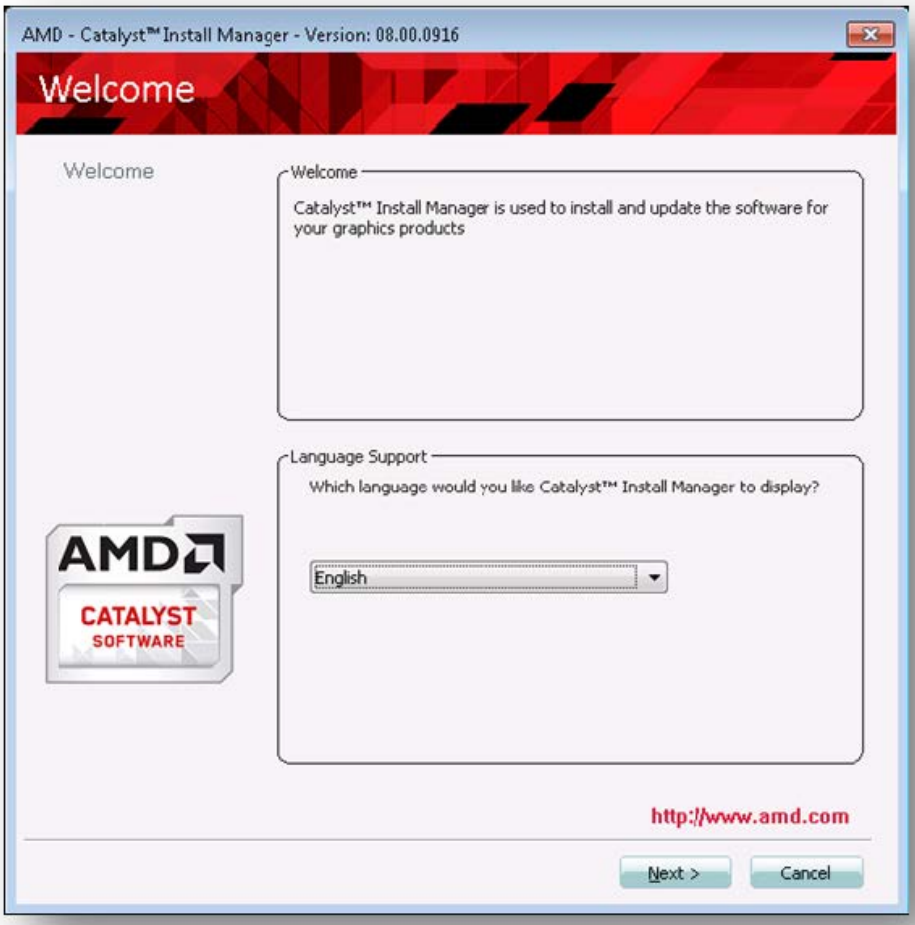
Installieren Sie die AMD-Treiber

Um den GPU-Betrieb zu aktivieren, installieren Sie AMD-Treiber in der VM.

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 Citrix Hypervisor der VM dynamisch eine GPU zu.

2. Folgen Sie den Installationsbildschirmen des Windows Betriebssystems.
3. Starten Sie die VM nach Abschluss der Installation des Betriebssystems neu.
4. Kopieren Sie die 32-Bit- oder 64-Bit-AMD-Windows -Treiber (AMD Catalyst Install Manager) auf die VM.
5. Führen Sie den AMD Catalyst Install Manager aus, wählen Sie Ihren **Zielordner**aus, und klicken Sie dann auf **Installieren**.



6. Führen Sie die Installationsschritte aus, um den Treiber zu installieren.
7. Starten Sie die VM neu, um die Installation abzuschließen.
8. Überprüfen Sie nach dem Neustart der VM, ob die Grafik ordnungsgemäß funktioniert. Öffnen Sie den **Windows Device Manager**, erweitern Sie **Displayadapter**, und stellen Sie sicher, dass der AMD Graphics Adapter keine Warnsymbole enthält.

Installieren Sie die Intel Treiber

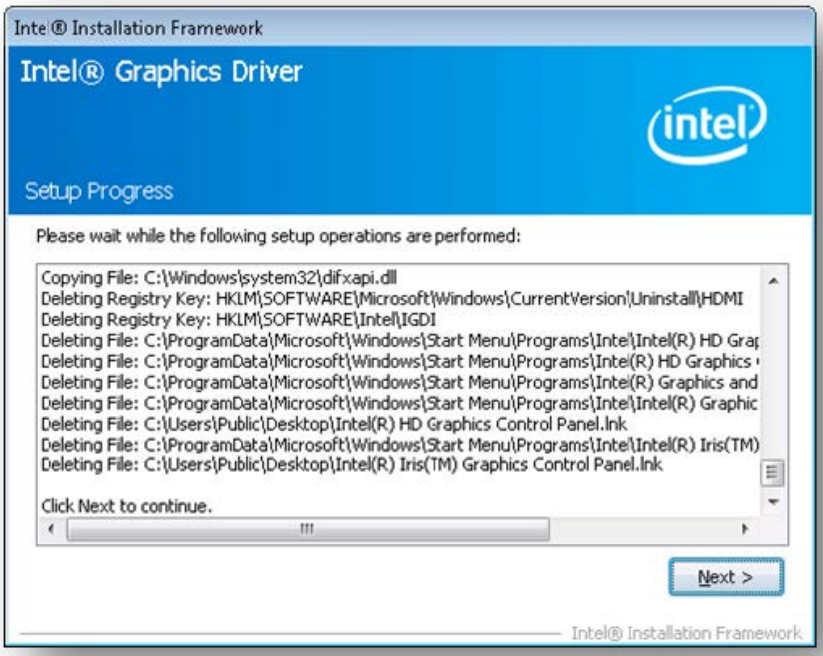
Um den GPU-Betrieb zu aktivieren, installieren Sie Intel-Treiber in der VM.

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 Citrix Hypervisor der VM dynamisch eine GPU zu.

2. Folgen Sie den Installationsbildschirmen des Windows Betriebssystems.
3. Starten Sie die VM nach Abschluss der Installation des Betriebssystems neu.
4. Kopieren Sie den 32-Bit- oder 64-Bit-Intel Windows -Treiber (Intel Grafiktreiber) auf die VM.
5. Führen Sie das Setup-Programm **für Intel Grafiktreiber** aus.
6. Select **WinSAT automatisch ausführen**aus, und klicken Sie dann auf **Weiter**.

7. Um die Lizenzvereinbarung zu akzeptieren, klicken Sie auf **Ja**, und klicken Sie im Fenster Informationen zur Readme-Datei auf **Weiter**.
8. Warten Sie, bis die Setup-Vorgänge abgeschlossen sind. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**.



9. Um die Installation abzuschließen, werden Sie aufgefordert, die VM neu zu starten. Select **Ja**, ich möchte diesen Computer jetzt neu starten, und klicken Sie auf **Fertig stellen**.
10. Überprüfen Sie nach dem Neustart der VM, ob die Grafik ordnungsgemäß funktioniert. Öffnen Sie den Windows Device Manager, erweitern Sie **Displayadapter**, und stellen Sie sicher, dass der Intel Grafikadapter keine Warnsymbole enthält.

> **Hinweis:**
>
> Sie können die neuesten Treiber von der erhaltenIntel Website.

Kopiert!
Failed!

Speichernutzung

October 16, 2019

Zwei Komponenten tragen zum Speicherbedarf des Citrix Hypervisor or-Servers bei. Zuerst der Speicher, der vom Xen Hypervisor selbst verbraucht wird. Zweitens gibt es den Speicher, der von der *Steuerungsdomäne* des Hosts belegt wird. Die Control Domain ist eine sichere, privilegierte Linux-VM, auf der der Citrix Hypervisor Verwaltungstoolstack (XAPI) ausgeführt wird. Neben der Bereitstellung

von Citrix Hypervisor Verwaltungsfunktionen führt die Steuerdomäne auch den Treiberstapel aus, der vom Benutzer erstellte VM-Zugriff auf physische Geräte bereitstellt.

Domänenspeicher steuern

Die der Control Domain zugewiesene Speichermenge wird automatisch angepasst und basiert auf der Menge des physischen Speichers auf dem physischen Host. Standardmäßig weist Citrix Hypervisor der Steuerdomäne **1 GiB plus 5% des gesamten physischen Speichers** zu, bis zu einem Maximum von 8 GiB.

> **Hinweis:**
>
> Der im Citrix Hypervisor Abschnitt in XenCenter gemeldete Betrag umfasst den Speicher, der von der Control Domain (dom0), dem Xen Hypervisor selbst und dem Absturzkernel verwendet wird. Daher kann die Menge des in XenCenter gemeldeten Speichers 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, mithilfe von XenCenter oder mithilfe der Befehlszeile ändern. Wenn Sie die der Kontrolldomäne zugewiesene Menge an Speicher über den standardmäßig zugewiesenen Betrag hinaus erhöhen, wird für VMs weniger Arbeitsspeicher zur Verfügung gestellt.

Ändern des dom0-Speichers mithilfe von XenCenter

Informationen zum Ändern des dom0-Speichers mithilfe von XenCenter finden SieÄndern des Kontrolldomänenspeichersin der XenCenter-Dokumentation.

> **Hinweis:**
>
> Sie können XenCenter nicht verwenden, um dom0-Speicher unter den Wert zu reduzieren, der ursprünglich während der Citrix Hypervisor Installation festgelegt wurde. Um diese Änderung vorzunehmen, müssen Sie die Befehlszeile verwenden.

Ändern des dom0-Speichers mithilfe der Befehlszeile

> **Hinweis:**
>
> Auf Hosts mit kleinerem Speicher (weniger als 16 GiB) sollten Sie den Speicher, der der Steuerdomäne zugewiesen wurde, auf niedriger als der bei der Installation festgelegte Standardwert

> 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 Citrix Hypervisor or-Server 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
   ```

   Wo`<nn>` repräsentiert die Menge des Speichers, in MiB, die dom0 zugewiesen werden soll.
3. Starten Sie den Citrix Hypervisor or-Server mit XenCenter oder dem`reboot` Befehl auf der xs-console neu.

   Führen Sie beim Neustart des Hosts auf der xsconsole den`free` Befehl aus, um die neuen Speichereinstellungen zu überprüfen.

Wie viel Arbeitsspeicher steht virtuellen Rechnern zur Verfügung?

Um herauszufinden, wie viel Hostspeicher verfügbar ist, um VMs zuzuweisen, suchen 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. Zum Beispiel:

```
xe host-list uuid=host_uuid params=memory-free
xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
```

Kopiert!
Failed!

Überwachen und Verwalten Ihrer Bereitstellung

October 16, 2019

Citrix Hypervisor bietet eine detaillierte Überwachung der Leistungsmetriken, einschließlich CPU, Arbeitsspeicher, Festplatte, Netzwerk, C-State/P-State-Informationen und Speicher. Gegebenenfalls sind diese Metriken auf Host- und VM-Basis verfügbar. Diese Metriken sind direkt verfügbar oder können in XenCenter oder anderen Anwendungen von Drittanbietern auf grafische Weise aufgerufen und angezeigt werden.

Citrix Hypervisor stellt außerdem System- und Leistungswarnungen bereit. Warnungen sind Benachrichtigungen, die als Reaktion auf ausgewählte Systemereignisse auftreten. Diese Benachrichtigungen treten auch auf, wenn einer der folgenden Werte einen angegebenen Schwellenwert auf einem verwalteten Host, VM oder Speicher-Repository überschreitet: CPU-Auslastung, Netzwerkauslastung, Speicherauslastung, Domänenspeicherauslastung, Speicherdurchsatz oder VM-Festplattenauslastung. Sie können die Warnungen mithilfe der xe-CLI oder mithilfe von XenCenter konfigurieren. Informationen zum Erstellen von Benachrichtigungen auf der Grundlage einer der verfügbaren Host- oder VM-Performance-Metriken finden Sie unterLeistungswarnungen.

Überwachung der Leistung von Citrix Hypervisor

Kunden können die Leistung ihrer Citrix Hypervisor or-Server und virtuellen Maschinen (VMs) mithilfe der Metriken überwachen, die über Round Robin Databases (RRDs) bereitgestellt werden. Diese Metriken können über HTTP oder über das RRD2CSV-Tool abgefragt werden. Darüber hinaus verwendet XenCenter diese Daten, um Systemleistungsdiagramme 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:**
>
> - Latenz über einen Zeitraum ist definiert als die durchschnittliche Latenz von Operationen während dieser Periode.
> - Die Verfügbarkeit und der Nutzen bestimmter Metriken sind SR und CPU abhängig.
> - Leistungsmetriken sind für GFS2 SRs und Festplatten auf diesen SRs nicht verfügbar.

Verfügbare Host-Metriken

Metrikname	Beschreibung	Bedingung	XenCenter Name
avgqu_sz_<sr-uuid-**short**>	Durchschnittliche E/A-Warteschlangengröße (Anforderungen).	Mindestens eine eingesteckte VBD in SR <sr-uuid-**short**> auf dem Host	sr-uuid-**short** Queue-Größe
cpu<cpu>-C<cstate>	Zeit-CPU, die im C-Zustandcpu in Millisekundencstate verbracht wird.	C-Zustand ist auf der CPU vorhanden	CPUcpu C-Zustandcstate

Metrikname	Beschreibung	Bedingung	XenCenter Name
cpu<cpu>-P<pstate>	Zeit-CPU, die im P-Zustandcpu in Millisekundenpstate verbracht wird.	P-Status ist auf der CPU vorhanden	CPUcpu P-Zustandpstate
cpu<cpu>	Auslastung der physischen CPUcpu (Bruchteil). Standardmäßig aktiviert.	CPUcpu existiert	CPUcpu
cpu_avg	Mittlere Auslastung physischer CPUs (Fraktion). Standardmäßig aktiviert.	Keine	Durchschnittliche CPU
inflight_<sr-uuid-**short**>	Anzahl der E/A-Anfragen, die derzeit im Flug sind. Standardmäßig aktiviert.	Mindestens eine eingesteckte VBD in SR sr auf dem Host	sr Bordanfragen
io_throughput_read<sr-uuidshort>	Daten, die von SR gelesen werden (MIB/s).	Mindestens eine eingesteckte VBD in SR sr auf dem Host	sr Lese-Durchsatz
io_throughput_write<sr-uuidshort>	Daten in die SR geschrieben (MIB/s).	Mindestens eine eingesteckte VBD in SR sr auf dem Host	sr Schreibdurchsatz
io_throughput_total<sr-uuidshort>	Alle SR I/O (MIB/s).	Mindestens eine eingesteckte VBD in SR sr auf dem Host	sr Gesamtdurchsatz
iops_read_<sr-uuid-**short**>	Lesen Sie Anforderungen pro Sekunde.	Mindestens eine eingesteckte VBD in SR sr auf dem Host	IOPSsr lesen
iops_write_<sr-uuid-**short**>	Schreiben Sie Anfragen pro Sekunde.	Mindestens eine eingesteckte VBD in SR sr auf dem Host	IOPSsr schreiben

Metrikname	Beschreibung	Bedingung	XenCenter Name
iops_total_<sr-uuid-**short**>	E/A-Anforderungen pro Sekunde.	Mindestens eine eingesteckte VBD in SR sr auf dem Host	IOPSsr insgesamt
iowait_<sr-uuid-**short**>	Prozentsatz der Wartezeit auf E/A.	Mindestens eine eingesteckte VBD in SR sr auf dem Host	sr I/A Warten
latency_<sr-uuid-**short**>	Durchschnittliche E/A-Latenz (Millisekunden).	Mindestens eine eingesteckte VBD in SR sr auf dem Host	srLatenz
loadavg	Domain0 Ladedurchschnitt. Standardmäßig aktiviert	Keine	Domänenlast steuern
memory_free_kib	Gesamtmenge des freien Speichers (KiB). Standardmäßig aktiviert.	Keine	Freier Speicher
memory_reclaimed	Host-Speicher, der durch Squeeze (B) wiederhergestellt wird.	Keine	Rückgewinnter Speicher
memory_reclaimed_max	Host-Speicher zur Rückgewinnung mit Squeeze (B).	Keine	Potentieller wiedergewinnter Speicher
memory_total_kib	Gesamtspeicher (KiB) im Host. Standardmäßig aktiviert.	Keine	Gesamtspeicher
network/latency	Intervall in Sekunden zwischen den letzten beiden Heartbeats, die vom lokalen Host an alle Online-Hosts übertragen werden. Standardmäßig deaktiviert.	HA aktiviert	Netzwerklatenz

Metrikname	Beschreibung	Bedingung	XenCenter Name
statefile/<t>/latency	Umlaufzeit in Sekunden des aktuellen State-File-Zugriffs vom lokalen Host. Standardmäßig deaktiviert.	HA aktiviert	HA-Statefile Latenz
pif_<pif>_rx	Bytes pro Sekunde, die auf der physischen Schnittstelle empfangenpif werden. Standardmäßig aktiviert.	PIF existiert	XenCenter-pifname Empfangen (siehe Hinweis)
pif_<pif>_tx	Bytes pro Sekunde, die auf der physischen Schnittstelle gesendetpifwerden. Standardmäßig aktiviert.	PIF existiert	XenCenter-pifname Senden (siehe Hinweis)
pif_<pif>_rx_errors	Empfangen von Fehlern pro Sekunde auf der physischen Schnittstellepif. Standardmäßig deaktiviert.	PIF existiert	XenCenter-pifname Empfangen von Fehlern (siehe Hinweis)
pif_<pif>_tx_errors	Übertragen Sie Fehler pro Sekunde auf der physischen Schnittstellepif . Standardmäßig deaktiviert	PIF existiert	FehlerXenCenter-pifname senden (siehe Hinweis)

Metrikname	Beschreibung	Bedingung	XenCenter Name
pif_aggr_rx	Auf allen physischen Schnittstellen empfangene Bytes pro Sekunde. Standardmäßig aktiviert.	Keine	NIC-Empfang insgesamt
pif_aggr_tx	Bytes pro Sekunde, die auf allen physischen Schnittstellen gesendet werden. Standardmäßig aktiviert.	Keine	Senden von Netzwerkkarten insgesamt
pvsaccelerator_evicted	Bytes pro Sekunde aus dem Cache entfernt	PVSAccelerator aktiviert	PVS-Beschleuniger Räumungsrate
pvsaccelerator_rea	Lesevorgänge pro Sekunde aus dem Cache	PVSAccelerator aktiviert	PVS-Beschleuniger Trefferrate
pvsaccelerator_read_misses	Lesevorgänge pro Sekunde, die nicht aus dem Cache bereitgestellt werden können	PVSAccelerator aktiviert	PVS-Beschleuniger Fehlerrate
pvsaccelerator_tra	Bytes pro Sekunde, die von zwischengespeicherten PVS-Clients gesendet werden	PVSAccelerator aktiviert	PVS-Beschleuniger beobachtete Netzwerkverkehr von Clients
pvsaccelerator_traffic_from_host	Bytes pro Sekunde, die von gecachten PVS-Servern gesendet werden	PVSAccelerator aktiviert	PVS-Beschleuniger beobachtete Netzwerkverkehr von Servern

Metrikname	Beschreibung	Bedingung	XenCenter Name
pvsaccelerator_rea	Lesevorgänge pro Sekunde, die vom Cache beobachtet werden	PVSAccelerator aktiviert	PVS-Beschleuniger beobachtete Leserate
pvsaccelerator_traffic_bytes_secured	Bytes pro Sekunde, die von PVSAccelerator anstelle des PVS-Servers gesendet werden	PVSAccelerator aktiviert	PVS-Beschleuniger gesicherter Netzwerkverkehr
pvsaccelerator_spa	Prozentsatz des von PVSAccelerator auf diesem Host belegten Speicherplatzes im Vergleich zur Gesamtgröße des Cachespeichers	PVSAccelerator aktiviert	PVS-Beschleuniger Raumauslastung
sr_<sr>_cache_size	Größe in Bytes der IntelliCache SR. Standardmäßig aktiviert.	IntelliCache aktiviert	IntelliCache-Cache-Größe
sr_<sr>_cache_hits	Cache-Treffer pro Sekunde. Standardmäßig aktiviert.	IntelliCache aktiviert	IntelliCache-Cache-Treffer
sr_<sr>_cache_misses	Cache-Fehlschläge pro Sekunde. Standardmäßig aktiviert.	IntelliCache aktiviert	IntelliCache-Cache-Fehler
xapi_allocation_ki	Speicherzuweisung (KiB) durch den XAPI-Daemon. Standardmäßig aktiviert.	Keine	Agent-Speicherzuweisung

Metrikname	Beschreibung	Bedingung	XenCenter Name
xapi_free_memory_kib	Freier Speicher (KiB) für den XAPI-Daemon verfügbar. Standardmäßig aktiviert.	Keine	Agentenspeicher frei
xapi_healthcheck/latency_health	Umlaufzeit in Sekunden nach dem letzten Aufruf der XAPI-Statusüberwachung auf dem lokalen Host. Standardmäßig deaktiviert	Hochverfügbarkeit aktiviert	Citrix Hypervisor prüfungslatenz
xapi_live_memory_kib	Live-Speicher (KiB), der vom XAPI-Daemon verwendet wird. Standardmäßig aktiviert.	Keine	Agentenspeicher Live
xapi_memory_usage_	Gesamtspeicher (KiB), der vom XAPI-Daemon verwendet wird. Standardmäßig aktiviert.	Keine	Verwendung des Agentenspeichers

Verfügbare VM-Metriken

Metrikname	Beschreibung	Bedingung	XenCenter Name
cpu<cpu>	Auslastung der vCPUcpu (Bruchteil). Standardmäßig aktiviert	vCPUcpu existiert	CPU

Metrikname	Beschreibung	Bedingung	XenCenter Name
memory	Aktuell zugewiesener Arbeitsspeicher (Bytes) .Standardmäßig aktiviert	Keine	Gesamtspeicher
memory_target	Ziel des VM-Sprechblasentreibers (Bytes). Standardmäßig aktiviert	Keine	Speicherziel
memory_internal_free	Der vom Gastagenten (KiB) gemeldete Speicher wird verwendet. Standardmäßig aktiviert	Keine	Freier Speicher
runstate_fullrun	Bruchteil der Zeit, in der alle vCPUs ausgeführt werden.	Keine	vCPUs Vollausführung
runstate_full_contention	Bruchteil der Zeit, in der alle vCPUs ausgeführt werden können (dh auf CPU warten)	Keine	VCPUs voller Konflikt
runstate_concurrency	Bruchteil der Zeit, in der einige vCPUs ausgeführt werden und einige ausführbar sind	Keine	Parallelitätsrisiko für vCPUs
runstate_blocked	Bruchteil der Zeit, dass alle vCPUs blockiert oder offline sind	Keine	vCPUs im Leerlauf

Metrikname	Beschreibung	Bedingung	XenCenter Name
runstate_partial_r	Bruchteil der Zeit, dass einige vCPUs ausgeführt werden und einige blockiert sind	Keine	vCPUs partieller Ausführung
runstate_partial_contention	Bruchteil der Zeit, dass einige vCPUs ausführbar sind und einige blockiert sind	Keine	VCPUs partieller Streitigkeit
vbd_<vbd>_write	Schreibt auf das Gerätvbd in Bytes pro Sekunde. Standardmäßig aktiviert	VBD vbd existiert	vbd “Datenträger-schreibvorgang
vbd_<vbd>_read	Liest vom Gerätvbd in Bytes pro Sekunde. Standardmäßig aktiviert.	VBD vbd existiert	vbd Datenträgerlesen
vbd_<vbd> _write_latency	Schreibtvbd in Mikrosekunden auf das Gerät.	VBD vbd existiert	vbd Datenträger-Latenz
vbd_<vbd> _read_latency	Liest vom Gerätvbd in Mikrosekunden.	VBD vbd existiert	vbd Datenträger-Lese-Latenz
vbd <vbd> _iops_read	Lesen Sie Anforderungen pro Sekunde.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	vbd Datenträgerlese-IOPs
vbd <vbd> _iops_write	Schreiben Sie Anfragen pro Sekunde.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	vbd Datenträgerschreib-IOPS
vbd <vbd> _iops_total	E/A-Anforderungen pro Sekunde.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	Volume E/A\ Sek.vbd gesamt

Metrikname	Beschreibung	Bedingung	XenCenter Name
vbd <vbd>_iowait	Prozentsatz der Wartezeit auf I/0.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	vbd Festplatten-E/A-Warten
vbd <vbd> _inflight	Anzahl der E/A-Anfragen, die derzeit im Flug sind.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	vbd Datenträgeranfragen
vbd <vbd> _avgqu_sz	Durchschnittliche E/A-Warteschlangengröße.	Mindestens ein eingesteckter VBD für Nicht-ISO-VDI auf dem Host	vbd“ Datenträger-warteschlangengröße
vif_<vif>_rx	Bytes pro Sekunde, die auf der virtuellen Schnittstellennum-mer empfangenvif werden. Standardmäßig aktiviert.	VIF vif existiert	vifEmpfangen
vif_<vif>_tx	Bytes pro Sekunde, die auf der virtuellen Schnittstelle übertragenvif werden. Standardmäßig aktiviert.	VIF vif existiert	vifAbsenden
vif_<vif> _rx_errors	Empfangen von Fehlern pro Sekunde auf der virtuellen Schnittstellevif. Standardmäßig aktiviert.	VIF vif existiert	vif Empfangen von Fehlern

Metrikname	Beschreibung	Bedingung	XenCenter Name
vif_<vif>_tx_errors	Übertragungsfehler pro Sekunde auf der virtuellen Schnittstelle standardmäßigvif aktiviert.	VIF vif existiert	Fehlervif senden

> **Hinweis:**
>
> Der Wert von<XenCenter-pif-name> kann eine der folgenden sein:
>
> | | |
> |—|—|
> | NIC <pif> | Wenn <pif> pif_eth# enthält, wobei ## 0—9 ist |
> | <pif> | Wenn <pif> pif_eth#.## oder pif_xenbr## oder pif_bond## enthält | | <Internal> Netzwerk <pif> | Wenn <pif> pif_xapi## enthält, (Hinweis, die <Internal> wie vorhanden erscheint) |
> | TAP <tap> | Wenn <pif> enthält pif_tap## |
> | xapi Loopback | Wenn<pif> pif_lo enthält |

Analysieren und Visualisieren von Metriken

Die Registerkarte „Leistung“ in XenCenter bietet die Echtzeitüberwachung von Leistungsstatistiken über Ressourcenpools hinweg sowie grafische Trends bei der Leistung virtueller und physischer Maschinen. Diagramme mit CPU, Arbeitsspeicher, Netzwerk und Festplatten-E/A 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 unter *Konfigurieren von Metriken* im folgenden Abschnitt.

- Sie können Leistungsdaten von bis zu 12 Monaten anzeigen und vergrößern, um die Leistungsspitzen genauer zu betrachten.
- XenCenter kann Leistungswarnungen generieren, wenn CPU, Arbeitsspeicher, Netzwerk-E/A, Speicher-E/A oder Festplatten-E/A-Auslastung einen angegebenen Schwellenwert auf einem Server, VM oder SR überschreiten. Weitere Informationen finden Sie unter *Warnungen* im folgenden Abschnitt.

> **Hinweis:**
>
> Installieren Sie die Citrix VM-Tools (paravirtualisierte Treiber), um vollständige VM-Leistungsdaten anzuzeigen.

Leistungsdiagramme konfigurieren

So fügen Sie ein Diagramm hinzu:

1. Klicken Sie auf der Registerkarte **Leistung** auf **Aktionen** und dann auf **Neues Diagramm**. Das Dialogfeld Neue Grafik wird angezeigt.
2. Geben Sie im Feld **Name** einen Namen für das Diagramm ein.
3. Aktivieren Sie in der Liste der **Datenquellen**die Kontrollkästchen für die Datenquellen, 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**aus, 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**.

Diagrammtyp konfigurieren

Daten in den Performance-Graphen können als Linien oder als Flächen angezeigt werden. So ändern Sie den Diagrammtyp:

1. Klicken Sie im Menü **Extras** auf **Optionen** , und wählen Sie **Diagramme** aus.
2. Um Performance-Daten als Liniendiagramm anzuzeigen, klicken Sie auf die Option **Liniendiagramm** .
3. Um Performance-Daten als Flächendiagramm anzuzeigen, klicken Sie auf die Option **Flächendiagramm** .
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ausführliche Details zum Konfigurieren und Anzeigen von XenCenter Leistungsdiagrammen finden Sie in der XenCenter-Hilfe im Abschnitt *Systemleistung überwachen*.

Konfigurieren von Metriken

> **Hinweis:**
>
> C-Zustände und P-Zustände sind Energieverwaltungsfunktionen einiger Prozessoren. Der Bereich der verfügbaren Zustände hängt von den physischen Fähigkeiten des Hosts sowie von der

> Konfiguration der Energieverwaltung ab.

Sowohl Host- als auch VM-Befehle geben Folgendes zurück:

- Eine vollständige Beschreibung der Datenquelle
- Die Einheiten, die auf die Metrik angewendet werden
- Der Bereich der möglichen Werte, die verwendet werden können

Zum 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
```

Aktivieren einer bestimmten Metrik

Die meisten Metriken sind standardmäßig aktiviert und gesammelt. Geben Sie Folgendes ein, um die Metriken zu aktivieren, die nicht sind:

```
xe host-data-source-record data-source=metric name host=hostname
```

Deaktivieren einer bestimmten Metrik

Sie möchten bestimmte Metriken möglicherweise 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
```

Anzeigen einer Liste der aktuell aktivierten Host-Metriken

Um die aktuell erfassten Host-Metriken aufzulisten, geben Sie Folgendes ein:

```
xe host-data-source-list host=hostname
```

Anzeigen einer Liste der aktuell aktivierten VM-Metriken

Um die aktuell erfassten VM-Metriken hosten zu können, geben Sie Folgendes ein:

```
xe vm-data-source-list vm=vm_name
```


RRDs verwenden

Citrix Hypervisor verwendet RRDs zum Speichern von Leistungsmetriken. Diese RRDs bestehen aus mehreren Round Robin Archives (RRAs) in einer Datenbank mit fester Größe.

Jedes Archiv in der Datenbank nimmt seine bestimmte Metrik auf einer angegebenen Granularität ab:

- Alle 5 Sekunden für 10 Minuten
- Jede Minute für die letzten zwei Stunden
- Jede Stunde für die letzte Woche
- Jeden Tag für das vergangene Jahr

Die Abtastung, die alle fünf Sekunden stattfindet, zeichnet tatsächliche Datenpunkte auf, jedoch verwenden die folgenden RRAs stattdessen Konsolidierungsfunktionen. Die von Citrix Hypervisor unterstützten Konsolidierungsfunktionen sind:

- DURCHSCHNITT
- MIN
- MAX

RRDs sind für einzelne VMs (einschließlich dom0) und den Citrix Hypervisor or-Server vorhanden. VM-RRDs werden auf dem Host gespeichert, auf dem sie ausgeführt werden, oder auf dem Pool-Master, wenn sie nicht ausgeführt werden. Daher muss der Speicherort einer VM bekannt sein, um die zugehörigen Leistungsdaten abzurufen.

Ausführliche Informationen zur Verwendung von Citrix Hypervisor RRDs finden Sie im Citrix Hypervisor Software Development Kit — Handbuch.

Analysieren von RRDs mit HTTP

Sie können RRDs über HTTP vom Citrix Hypervisor-Server herunterladen, der mit dem unter oder registrierten HTTP-Handler angegeben wurde `/host_rrd` `./vm_rrd` Beide Adressen erfordern die Authentifizierung entweder durch HTTP-Authentifizierung oder durch Bereitstellung eines gültigen Management-API-Sitzungsreferenzs als Abfrageargument. Zum Beispiel:

Laden Sie eine Host-RRD herunter.

```
1 wget http://server/host_rrd?session_id=OpaqueRef:SESSION HANDLE>
```

Laden Sie eine virtuelle RRD herunter.

```
1 wget http://server/vm_rrd?session_id=OpaqueRef:SESSION HANDLE>&uuid=VM
    UUID>
```

Beide Aufrufe laden XML in einem Format herunter, das `rrdtool` zur Analyse importiert oder direkt analysiert werden kann.

Analysieren von RRDs mit rrd2csv

Neben der Anzeige von Leistungsmetriken in XenCenter protokolliert das Tool rd2csv RDs im CSV-Format (Comma Separated Value). Man und Hilfeseiten werden zur Verfügung gestellt. Führen Sie den folgenden Befehl aus, um den Werkzeugmann oder die Hilfeseiten des rrd2csv anzuzeigen:

```
man rrd2csv
```

Oder

```
rrd2csv --help
```

> **Hinweis:**
>
> Wenn mehrere Optionen verwendet werden, geben Sie sie einzeln an. Zum Beispiel: Um sowohl die UUID als auch die Namensbezeichnung, die einer VM oder einem Host zugeordnet ist, zurückzugeben, rufen Sie rrd2csv wie unten dargestellt auf:
>
> `rrd2csv -u -n`
>
> Die zurückgegebene UUID ist eindeutig und eignet sich als Primärschlüssel, jedoch ist die Namensbezeichnung einer Entität möglicherweise nicht unbedingt eindeutig.

Die Manpage (`rrd2csv --help`) ist der definitive Hilfetext des Tools.

Warnungen

Sie können Citrix Hypervisor so konfigurieren, dass Warnungen basierend auf einer der verfügbaren Host- oder VM-Metriken generiert werden. Darüber hinaus stellt Citrix Hypervisor vorkonfigurierte Alarme bereit, die ausgelöst werden, wenn Hosts bestimmte Bedingungen und Zustände durchlaufen. Sie können diese Warnungen mit XenCenter oder der xe CLI anzeigen.

Anzeigen von Warnungen mit XenCenter

Sie können verschiedene Warnungen in XenCenter anzeigen, indem Sie auf **Benachrichtigungen** und dann auf **Warnungen** klicken. In der Ansicht Warnungen werden verschiedene Warnungen angezeigt, einschließlich Leistungswarnungen, Systemwarnungen und Softwareupdate-Warnungen.

Leistungswarnungen

Leistungswarnungen können generiert werden, wenn einer der folgenden Werte einen angegebenen Schwellenwert auf einem verwalteten Host, VM oder Speicher-Repository (SR) überschreitet: CPU-

Auslastung, Netzwerkauslastung, Speicherauslastung, Domänenspeicherauslastung, Speicherdurchsatz oder VM-Festplattenauslastung.

Standardmäßig ist das Alert-Wiederholungsintervall auf 60 Minuten eingestellt, es 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 bestimmte Leistungswarnungen zusammen mit anderen schwerwiegenden Systemwarnungen gesendet wird.

Alle benutzerdefinierten Warnungen, die mit der xe-CLI konfiguriert werden, werden auch auf der Seite Warnungen in XenCenter angezeigt.

Jeder Alert hat eine entsprechende Priorität/Schweregrad. Sie können diese Ebenen ändern und optional eine E-Mail erhalten, wenn die Warnung ausgelöst wird. Die Standardwarnpriorität/Schweregrad wird auf festgelegt3.

Priorität	Name	Beschreibung	Standard-E-Mail-Benachrichtigung
1	Kritisch	Handeln Sie jetzt, oder Daten können dauerhaft verloren gehen oder beschädigt werden.	Ja
2	Major	Handeln Sie jetzt, oder einige Dienste können fehlschlagen.	Ja
3	Warnung	Handeln Sie jetzt oder ein Dienst kann leiden.	Ja
4	Moll	Beachten Sie, dass sich etwas gerade verbessert hat.	Nein
5	Information	Tagesinformationen (VM Start, Stop, Fortsetzen usw.)	Nein
?	Unbekannt	Unbekannter Fehler	Nein

Konfigurieren von Leistungswarnungen

1. Wählen Sie im Bereich **Ressourcen** den entsprechenden Host, die VM oder die SR aus, und klicken Sie dann auf die Registerkarte **Allgemein** und dann auf **Eigenschaften** .

2. Klicken Sie auf die Registerkarte **Warnungen** . Sie können die folgenden Warnungen konfigurieren:

   - **CPU-Auslastungswarnungen** für einen Host oder VM: Aktivieren Sie das Kontrollkästchen **CPU-Auslastungswarnungen generieren** , und legen Sie dann den CPU-Auslastung und den Zeitschwellenwert fest, der die Warnung auslöst.
   - **Netzwerkauslastungswarnungen** für einen Host oder eine VM: Aktivieren Sie das Kontrollkästchen **Netzwerkauslastungswarnungen generieren** , und legen Sie dann den Netzwerkauslastungs- und Zeitschwellenwert fest, der die Warnung auslöst.
   - **Speicherauslastungswarnungen** für einen Host: Aktivieren Sie das Kontrollkästchen **Speicherauslastung generieren** , und legen Sie dann den Schwellenwert für freien Speicher und Zeit fest, die die Warnung auslösen.
   - **Domänenspeicherverwendungswarnungen** für einen Host steuern: Aktivieren Sie das Kontrollkästchen **Warnungen zur Speichernutzung der Kontrolldomäne generieren** , und legen Sie dann die Speichernutzung und den Zeitschwellenwert für die Steuerdomäne fest, die die Warnung auslösen.
   - Warnungen zur**Datenträgerverwendung** für eine VM: Aktivieren Sie das Kontrollkästchen **Warnungen für die Datenträgerverwendung generieren** , und legen Sie dann den Schwellenwert fest, der die Warnung auslöst.
   - **Speicherdurchsatzwarnungen** für einen SR: Aktivieren Sie das Kontrollkästchen **Speicherdurchsatzwarnungen generieren, und legen** Sie dann den Speicherdurchsatz und den Zeitschwellenwert fest, der die Warnung auslöst.

     > **Hinweis:**
     >
     > Physical Block Devices (PBD) stellen die Schnittstelle zwischen einem bestimmten Citrix Hypervisor or-Server und einem angeschlossenen SR dar. Wenn die gesamte SR-Durchsatzaktivität mit Lese-/Schreibzugriff auf einer PBD den angegebenen Schwellenwert überschreitet, werden Warnungen auf dem mit der PBD verbundenen Host generiert. Im Gegensatz zu anderen Citrix Hypervisor or-Serverwarnungen muss diese Warnung auf der SR konfiguriert werden.

3. Um das Warnungswiederholintervall zu ändern, geben Sie die Anzahl der Minuten in das Feld **Warnungswiederholungsintervall** ein. Wenn ein Alarmschwellenwert erreicht und ein Alert generiert wurde, wird erst nach Ablauf des Alert-Wiederholungsintervalls ein weiterer Alert generiert.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ausführliche Informationen zum Anzeigen, Filtern und Konfigurieren von Schweregraden für Leistungswarnungen finden Sie in der XenCenter Hilfe.

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	Citrix Hypervisor Lizenzvertrag läuft in Kürze ab.
ha-statefile_lost	2	Kontakt mit dem Speicher-Repository mit hoher Verfügbarkeit verloren, handeln Sie bald.
ha-heartbeat_approaching_timeou	5	Hochverfügbarkeit nähert sich dem Timeout, Host kann neu starten, es sei denn, eine Aktion wird ausgeführt.
ha_statefile_approaching_timeout	5	Hochverfügbarkeit nähert sich dem Timeout, Host kann neu starten, es sei denn, eine Aktion wird ausgeführt.
haxapi_healthcheck_approachi	5	Hochverfügbarkeit nähert sich dem Timeout, Host kann neu starten, es sei denn, eine Aktion wird ausgeführt.
ha_network_bonding_error	3	Möglicher Service-Verlust. Verlust des Netzwerks, das Hochverfügbarkeits-Heartbeat sendet.
ha_pool_overcommited	3	Möglicher Service-Verlust. Hochverfügbarkeit kann den Schutz für konfigurierte VMs nicht garantieren.

Name	Priorität/Schweregrad	Beschreibung
ha_poor_drop_in_plan_exists_for	3	Die Abdeckung mit hoher Verfügbarkeit ist gesunken, wahrscheinlich fehlgeschlagen, noch kein Verlust vorhanden.
ha_protected_vm_restart_failed	2	Dienstverlust. Hochverfügbarkeit konnte eine geschützte VM nicht neu starten.
ha_host_failed	3	Hohe Verfügbarkeit hat festgestellt, dass ein Host fehlgeschlagen ist.
ha_host_was_fenced	4	Hochverfügbarkeit hat einen Host neu gestartet, um vor VM-Beschädigung zu schützen.
redo_log_healthy	4	Das XAPI-Redo-Protokoll wurde von einem vorherigen Fehler wiederhergestellt.
redo_log_broken	3	Im XAPI-Redo-Protokoll ist ein Fehler aufgetreten.
ip_configured_pif_can_unplug	3	Eine IP-konfigurierte Netzwerkkarte kann von XAPI entfernt werden, wenn Hochverfügbarkeit verwendet wird, was möglicherweise zu einem Ausfall der hohen Verfügbarkeit führt.
host_sync_data_failed	3	Fehler beim Synchronisieren der Citrix Hypervisor Leistungsstatistiken.
host_clock_skew_detected	3	Die Host-Uhr wird nicht mit anderen Hosts im Pool synchronisiert.
host_clock_went_backwards	1	Die Host-Uhr ist beschädigt.

Name	Priorität/Schweregrad	Beschreibung
pool_master_transition	4	Ein neuer Host wurde als Poolmaster angegeben.
pbd_plug_failed_on_server_sta	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_nicht-homogen	2	Hosts in einem Pool haben unterschiedliche AD-Authentifizierungskonfiguration.
multipath_period_alert	3	Ein Pfad zu einem SR ist fehlgeschlagen oder wiederhergestellt.
Anleihestatus geändert	3	Eine Verbindung in einer Bindung wurde getrennt oder wieder verbunden.

Softwareupdate-Warnungen

- **XenCenter alt:** Citrix Hypervisor erwartet eine neuere Version, kann aber trotzdem eine Verbindung zur aktuellen Version herstellen
- **XenCenter veraltet:** XenCenter ist zu alt, um eine Verbindung mit Citrix Hypervisor herzustellen
- **Citrix Hypervisor veraltet:** Citrix Hypervisor ist eine alte Version, mit der das aktuelle XenCenter keine Verbindung herstellen kann
- **Warnung abgelaufen:** Citrix Hypervisor-Lizenz ist abgelaufen
- **Fehlende IQN-Warnung:** Citrix Hypervisor verwendet iSCSI-Speicher, aber der Host-IQN ist leer
- **Doppelte IQN-Warnung:** Citrix Hypervisor verwendet iSCSI-Speicher, und es gibt doppelte Host-IQNs

Konfigurieren von Leistungswarnungen mithilfe der XE CLI

> **Hinweis:**
>
> Trigger für Warnungen werden in einem Mindestintervall von fünf Minuten überprüft. Dieses Intervall vermeidet eine übermäßige Belastung des Systems, um auf diese Bedingungen zu über-

> prüfen und Fehlalarme zu melden. Wenn Sie ein Alert-Wiederholungsintervall kleiner als fünf Minuten festlegen, werden die Alerts weiterhin mit dem Mindestintervall von fünf Minuten generiert.

Das`perfmon` Leistungsüberwachungstool wird alle fünf Minuten ausgeführt und fordert Aktualisierungen von Citrix Hypervisor an, die durchschnittlich über eine Minute liegen. Diese Standardwerte können in geändert werden `/etc/sysconfig/perfmon`.

Das`perfmon` Tool liest alle fünf Minuten Aktualisierungen von Leistungsvariablen, die auf demselben Host ausgeführt werden. Diese Variablen sind in eine Gruppe, die sich auf den Host selbst bezieht, und eine Gruppe für jede VM, die auf diesem Host ausgeführt wird, getrennt. `perfmon` Lesen Sie für jede VM und jeden Host den Parameter`other-config:perfmon` und verwenden Sie 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 „CPU-Auslastung“ -Warnung durch Schreiben einer XML-Zeichenfolge in den Parameter gezeigt`other-config:perfmon`:

```
xe vm-param-set uuid=vm_uuid other-config:perfmon=\

'<config>
    <variable>
        <name value="cpu_usage"/>
        <alarm_trigger_level value="0.5"/>
    </variable>
 </config>'
```

> **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
```

Wenn diese Aktualisierung nicht durchgeführt wird, kommt es zu einer Verzögerung, bevor die neue Konfiguration wirksam wird, da standardmäßig alle 30 Minuten nach einer neuen Konfiguration`perfmon` sucht. Dieser Standardwert kann in geändert werden `/etc/sysconfig/perfmon`.

Gültige VM-Elemente

- `name`: Der Name der Variablen (kein Standard). Wenn der Namenswert entwedercpu_usagenetwork_usage“ oder lautetdisk_usage, `sind diealarm_trigger_sense`Parameterrrd_regex“und nicht als Standardwerte für diese Werte verwendet werden.

- `alarm_priority`: Die Priorität der generierten Alerts (Standard `3`).
- `alarm_trigger_level`: Die Wertstufe, die eine Warnung auslöst (kein Standardwert).
- `alarm_trigger_sense`: Der Wert`high`ist`alarm_trigger_level`, wenn ein Maximalwert ansonsten`low`, wenn der`alarm_trigger_level`ein Mindestwert (Standardwert`high`).
- `alarm_trigger_period`: Die Anzahl der Sekunden, in denen Werte (oberhalb oder unterhalb des Alert-Schwellenwerts) empfangen werden können, bevor ein Alert gesendet wird (der Standardwert ist`60`).
- `alarm_auto_inhibit_period`: Die Anzahl der Sekunden, die dieser Alarm deaktiviert wird, nachdem ein Alarm gesendet wurde (der Standardwert ist`3600`).
- `consolidation_fn`: Kombiniert Variablen aus rrd_updates zu einem Wert. Für`cpu-usage` den Standard ist`average` , für`fs_usage` den Standard ist`get_percent_fs_usage` und für alle anderen -`sum` .
- `rrd_regex`: Entspricht den Namen von Variablen aus`xe vm-data-sources-list uuid= vm_uuid`, um Performance-Werte zu berechnen. Dieser Parameter hat Standardwerte für die benannten Variablen:
  - cpu_usage
  - network_usage
  - disk_usage

Wenn angegeben, werden die Werte aller Elemente, die von`xe vm-data-source-list` deren Namen mit dem angegebenen regulären Ausdruck übereinstimmen, unter Verwendung der Methode konsolidiert, die als angegeben wird`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 Wertestufe, die einen Alarm auslöst (kein Standard).
- `alarm_trigger_sense`: Der Wert ist`high`, wenn ein Maximalwert`alarm_trigger_level`ist andernfalls`low`, wenn`alarm_trigger_level`es sich um ein Mindestwert. (Standard`high`)
- `alarm_trigger_period`: Die Anzahl der Sekunden, in denen Werte (oberhalb oder unterhalb des Alarmschwellens) empfangen werden können, bevor ein Alarm gesendet wird (Standard`60`).
- `alarm_auto_inhibit_period`: Die Anzahl der Sekunden, für die die Warnung deaktiviert wird, nachdem eine Warnung gesendet wurde. (Standard`3600`).
- `consolidation_fn`: Kombiniert Variablen aus`rrd_updates`einem Wert (Standard`sum`- oder`average`)

- `rrd_regex`: Ein regulärer Ausdruck, der den Namen der Variablen entspricht, die vom`xe vm-data-source-list uuid=vm_uuid`Befehl zurückgegeben werden, um den statistischen Wert zu berechnen. Dieser Parameter hat Standardwerte für die folgenden benannten Variablen:
  - cpu_usage
  - network_usage
  - memory_free_KB
  - sr_io_throughput_total_xxxxxxxx (wobei`xxxxxxxx`die ersten acht Zeichen der SR-UUID sind).

SR-Durchsatz: Speicherdurchsatzwarnungen müssen auf der SR und nicht auf dem Host konfiguriert werden. Zum 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>'
```

Generische Beispielkonfiguration

Das folgende Beispiel zeigt eine generische Konfiguration:

```
<config>
  <variable>
    <name value="NAME_CHOSEN_BY_USER"/>
    <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALARM"/>
    <alarm_trigger_period value="
       RAISE_ALARM_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_ALARMS_FROM_THIS_MONITOR"/>
    <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
    <rrd_regex value="
       REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
  </variable>

  <variable>
    ...
  </variable>

```



```
17          ...
18      </config>
```

Konfigurieren von E-Mail-Benachrichtigungen

Sie können Citrix Hypervisor so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, wenn Citrix Hypervisor or-Server Warnungen generieren. Diese Konfiguration kann entweder mithilfe von XenCenter oder mithilfe der xe-Befehlszeilenschnittstelle erfolgen.

Aktivieren von E-Mail-Warnungen mithilfe von XenCenter

1. Klicken Sie im Bereich Ressourcen mit der rechten Maustaste auf einen Pool, und wählen Sie **Eigenschaften**aus.
2. Wählen Sie im Eigenschaftenfenster **E-Mail-Optionen**aus.
3. Select das Kontrollkästchen E-Mail-Warnbenachrichtigungen senden, und geben Sie die E-Mail-Adresse und den SMTP-Server ein.

   > **Hinweis:**
   >
   > Geben Sie die Details eines SMTP-Servers ein, der keine Authentifizierung erfordert.

4. Wählen Sie die bevorzugte Sprache aus der **Mail-Sprachliste** aus, um eine E-Mail mit Leistungswarnungen zu erhalten. Die drei verfügbaren Sprachen sind Englisch, Chinesisch und Japanisch.

   Die Standardsprache für die Konfiguration der E-Mail-Sprache für Leistungswarnungen für XenCenter ist Englisch.

Aktivieren von E-Mail-Warnungen mithilfe der XE-CLI

> **Wichtig:**
>
> Wenn Sie XenCenter oder die xe-CLI zum Aktivieren von E-Mail-Benachrichtigungen verwenden, geben Sie die Details eines SMTP-Servers ein, der keine Authentifizierung erfordert. E-Mails, die über SMTP-Server gesendet werden, die eine Authentifizierung erfordern, werden nicht zugestellt.

Um E-Mail-Warnungen zu konfigurieren, geben Sie die E-Mail-Adresse und den SMTP-Server an:

```
1   xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.
       bloggs@domain.tld
2   xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
       domain.tld[:port]
```


Sie können auch den Mindestwert der Priorität (in XenCenter als Schweregrad bezeichnet) in der Nachricht angeben, bevor die E-Mail gesendet wird:

```
xe pool-param-set uuid=pool_uuid other-config:mail-max-priority=
   level
```

Die Standardprioritätsstufe ist4.

> **Hinweis:**
>
> Einige SMTP-Server leiten nur E-Mails mit Adressen weiter, die FQDNs verwenden. Wenn Sie feststellen, dass E-Mails nicht weitergeleitet werden, könnte dies aus diesem Grund sein. In diesem Fall können Sie den Serverhostnamen auf den FQDN festlegen, damit diese Adresse beim Herstellen einer Verbindung mit Ihrem Mail-Server verwendet wird.

So konfigurieren Sie die E-Mail-Sprache der Leistungswarnung:

```
xe pool-param-set uuid=pool_uuid other-config:mail-language=en-US |
    zh-CN | ja-JP
```

Senden von E-Mail-Benachrichtigungen über authentifizierte SMTP-Server

Das E-Mail-Alarmdienstprogramm in Citrix Hypervisor verwendet SSmtp, um E-Mail-Benachrichtigungen zu senden. Vor dem Senden von E-Mail-Benachrichtigungen sucht das E-Mail-Alarm-Dienstprogramm nach der Konfigurationsdatei`mail-alarm.conf`. Wenn die Konfigurationsdatei vorhanden ist, wird der Inhalt der Datei verwendet, um SSmtp zu konfigurieren. Andernfalls werden die in der XAPI-Datenbank verfügbaren Details (wie mit XenCenter oder der XE-CLI konfiguriert) zum Senden von E-Mail-Benachrichtigungen verwendet. Um E-Mail-Benachrichtigungen über authentifizierte SMTP-Server zu senden, erstellen Sie eine`mail-alarm.conf` Datei`/etc/` mit folgendem Inhalt:

```
root=postmaster
authUser=<username>
authPass=<password>
mailhub=<server address>:<port>
```

> **Hinweis:**
>
> Diese Konfigurationsdatei wird für alle Warnungen verwendet, die von Citrix Hypervisor or-Servern generiert werden.

Zusätzliche Konfigurationsoptionen

Jeder SMTP-Server kann sich in seinem Setup geringfügig unterscheiden und erfordert möglicherweise eine zusätzliche Konfiguration. 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.

    Mailhub
        The host to send mail to, in the form host | IP_addr port [:
        port]. The default port is 25.

    RewriteDomain
    The domain from which mail seems to come. For user authentication.

    Hostname
        The full qualified name of the host. If not specified, the host
        is queried for its hostname.

    FromLineOverride
        Specifies whether the From header of an email, if any, may over-
        ride the default domain. The default is "no".

    UseTLS
    Specifies whether ssmtp uses TLS to talk to the SMTP server.
    The default is "no".

    UseSTARTTLS
        Specifies whether ssmtp does a EHLO/STARTTLS before
```



```
                starting SSL
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".
```

Benutzerdefinierte Felder und Tags

XenCenter unterstützt die Erstellung von Tags und benutzerdefinierten Feldern, was die Organisation und schnelle Suche von VMs, Speicher usw. ermöglicht. Weitere Informationen finden Sie in der XenCenter Hilfe.

Benutzerdefinierte Suchvorgänge

XenCenter unterstützt die Erstellung benutzerdefinierter Suchvorgänge. Suchen können exportiert und importiert werden, und die Ergebnisse einer Suche können im Navigationsbereich angezeigt werden. Weitere Informationen finden Sie in der XenCenter Hilfe.

Ermitteln des Durchsatzes von physischen Busadaptern

Bei FC-, SAS- und iSCSI-HBAs können Sie den Netzwerkdurchsatz Ihrer PBDs anhand des folgenden Verfahrens ermitteln.

1. Listen Sie die PBDs auf einem Host auf.
2. Bestimmen Sie, welche LUNs über welche PBDs weitergeleitet werden.
3. Listen Sie für jede PBD und SR die VBDs auf, die VDIs auf der SR referenzieren.

4. Berechnen Sie für alle aktiven VBDs, die VMs auf dem Host zugeordnet sind, den kombinierten Durchsatz.

Überprüfen Sie für iSCSI- und NFS-Speicher Ihre Netzwerkstatistiken, um festzustellen, ob ein Durchsatzengpass am Array vorliegt oder ob die PBD gesättigt ist.

Kopiert!
Failed!

Verwalten virtueller Maschinen

October 16, 2019

Dieser Abschnitt enthält eine Übersicht darüber, wie virtuelle Maschinen (VMs) mithilfe von Vorlagen erstellt werden. Darüber hinaus werden weitere Vorbereitungsmethoden erläutert, darunter die physische in virtuelle Konvertierung (P2V), das Klonen von Vorlagen und das Importieren von zuvor exportierten VMs.

Was ist eine virtuelle Maschine?

Eine virtuelle Maschine (VM) ist ein Software-Computer, der wie ein physischer Computer ein Betriebssystem und Anwendungen ausführt. Die VM besteht aus einer Reihe von Spezifikations- und Konfigurationsdateien, die von den physischen Ressourcen eines Hosts gesichert werden. Jede VM verfügt über virtuelle Geräte, die dieselben Funktionen wie physische Hardware bereitstellen. VMs können die Vorteile bieten, dass sie mobiler, verwaltbarer und sicherer sind. Darüber hinaus können Sie das Boot-Verhalten jeder VM an Ihre spezifischen Anforderungen anpassen. Weitere Informationen finden Sie unter VM-Startverhalten.

Citrix Hypervisor unterstützt Gäste mit einer beliebigen Kombination von IPv4- oder IPv6-konfigurierten Adressen.

Typen von virtuellen Maschinen

In Citrix Hypervisor können VMs in einem von zwei Modi betrieben werden:

- Paravirtualisiert (PV): Der Kernel der virtuellen Maschine verwendet spezifischen Code, der bewusst ist, dass er auf einem Hypervisor läuft, um Geräte und Speicher zu verwalten.
- Vollständig virtualisiert (HVM): Spezifische Prozessorfunktionen werden verwendet, um privilegierte Anweisungen zu „trapping“, die die virtuelle Maschine ausführt. Mit dieser Funktion

können Sie ein unverändertes Betriebssystem verwenden. Für den Netzwerk- und Speicherzugriff werden emulierte Geräte der virtuellen Maschine angezeigt. Alternativ können PV-Treiber aus Gründen der Leistung und Zuverlässigkeit verwendet werden.

VMs erstellen

Verwenden von VM-Vorlagen

VMs werden aus Vorlagen vorbereitet. Eine Vorlage ist ein *Gold-Image* , das alle verschiedenen Konfigurationseinstellungen enthält, um eine Instanz einer bestimmten VM zu erstellen. Citrix Hypervisor wird mit einem Basissatz von Vorlagen ausgeliefert, bei denen es sich um *rohe* VMs handelt, auf denen Sie ein Betriebssystem installieren können. Unterschiedliche Betriebssysteme erfordern unterschiedliche Einstellungen, um optimal ausgeführt werden zu können. Citrix Hypervisor Vorlagen werden optimiert, um die Leistung des Betriebssystems zu maximieren.

Es gibt zwei grundlegende Methoden, mit denen Sie VMs aus Vorlagen erstellen können:

- Verwendung einer komplett vorkonfigurierten Vorlage, zum Beispiel der virtuellen Demo Linux Appliance.
- Installieren eines Betriebssystems von einer CD, einem ISO-Image oder einem Netzwerk-Repository auf die entsprechende bereitgestellte Vorlage.

Windows VMsbeschreibt, wie Windows Betriebssysteme auf VMs installiert werden.

Linux-VMsbeschreibt, wie Linux-Betriebssysteme auf VMs installiert werden.

> **Hinweis:**
>
> Vorlagen, die mit älteren Versionen von Citrix Hypervisor erstellt wurden, können in neueren Versionen von Citrix Hypervisor verwendet werden. Vorlagen, die in neueren Versionen von Citrix Hypervisor erstellt wurden, sind jedoch nicht mit älteren Versionen von Citrix Hypervisor kompatibel. Wenn Sie eine VM-Vorlage mithilfe von Citrix Hypervisor 8.0 erstellt haben, exportieren Sie die VDIs separat, und erstellen Sie die VM erneut.

Andere Methoden der VM-Erstellung

Zusätzlich zum Erstellen von VMs aus den bereitgestellten Vorlagen können Sie VMs mithilfe der folgenden Methoden erstellen.

Physisch-virtuelle Konvertierung

Physical to Virtual Conversion (P2V) ist der Prozess, der ein vorhandenes Windows Betriebssystem auf einem physischen Server in eine virtualisierte Instanz von sich selbst konvertiert. Die Konvertierung

umfasst das Dateisystem, die Konfiguration usw. Diese virtualisierte Instanz wird dann als VM auf dem Citrix Hypervisor or-Server übertragen, instanziiert und gestartet.

Klonen einer vorhandenen VM

Sie können eine Kopie einer vorhandenen VM erstellen, indem Sie aus einer Vorlage *klonen* . Vorlagen sind gewöhnliche VMs, die als Master-Kopien verwendet werden sollen, um Instanzen von VMs zu erstellen. Eine VM kann angepasst und in eine Vorlage konvertiert 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 VMs verwendet werden.

Citrix Hypervisor verfügt über zwei Mechanismen zum Klonen von VMs:

- Eine vollständige Kopie
- Copy-on-Write

  Der schnellere Kopiermodus schreibt nur *geänderte* Blöcke auf den Datenträger. Copy-on-Write wurde entwickelt, um Speicherplatz zu sparen und schnelle Klone zu ermöglichen, verlangsamt jedoch die normale Festplattenleistung etwas. Eine Vorlage kann mehrmals ohne Verlangsamung schnell geklont werden.

  > **Hinweis:**
  >
  > Wenn Sie eine Vorlage in eine VM klonen und dann den Klon in eine Vorlage konvertieren, kann die Datenträgerleistung abnehmen. Der Grad der Abnahme hat eine lineare Beziehung zu der Häufigkeit, wie oft dieser Prozess passiert ist. In diesem Fall kann der`vm-copy` CLI-Befehl verwendet werden, um eine vollständige Kopie der Festplatten durchzuführen und die erwartete Festplattenleistung wiederherzustellen.

Hinweise für Ressourcenpools

Wenn Sie eine Vorlage von virtuellen VM-Laufwerken auf einem freigegebenen SR erstellen, wird der Vorlagenklonvorgang an jeden Server im Pool weitergeleitet, der auf die freigegebenen 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 Server 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 das Klonen, Exportieren und Importieren einer VM ist 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 Serverkonfiguration, die Sie oft verwenden. Nachdem Sie eine VM nach Bedarf eingerichtet haben, exportieren Sie sie und importieren Sie sie später, um eine weitere Kopie der speziell konfigurierten VM zu erstellen. Sie können auch den Export und Import verwenden, um eine VM auf den Citrix Hypervisor or-Server zu verschieben, der sich in einem anderen Ressourcenpool befindet.

Einzelheiten und Verfahren zum Importieren und Exportieren von VMs finden Sie unterImportieren und Exportieren von VMs.

Citrix VM-Tools

Citrix VM-Tools bieten leistungsstarke E/A-Dienste ohne den Aufwand herkömmlicher Geräteemulation. Citrix VM Tools bestehen aus E/A-Treibern (auch als paravirtualisierte Treiber oder PV-Treiber bezeichnet) und dem Management Agent. Installieren Sie Citrix VM Tools auf jeder Windows VM, damit diese VM über eine vollständig unterstützte Konfiguration verfügt und die xe CLI oder XenCenter verwenden kann. Die auf der VM installierte Version von Citrix VM Tools muss mit der neuesten verfügbaren Version übereinstimmen, die auf dem Citrix Hypervisor or-Server installiert ist. Einige Hotfixes enthalten beispielsweise eine aktualisierte Citrix VM Tools-ISO, die die auf dem Host installierte Version aktualisiert.

Die E/A-Treiber enthalten Speicher- und Netzwerktreiber sowie Low-Level-Management-Schnittstellen. Diese Treiber ersetzen die emulierten Geräte und ermöglichen den Hochgeschwindigkeitsverkehr zwischen Windows und der Citrix Hypervisor Produktfamilie. Bei der Installation eines Windows Betriebssystems verwendet Citrix Hypervisor herkömmliche Geräteemulation, um der VM einen Standard-IDE-Controller und eine Standard-Netzwerkkarte zu präsentieren. Diese Emulation ermöglicht es Windows, mithilfe von integrierten Treibern zu installieren, jedoch mit reduzierter Leistung aufgrund des Overhead, der mit der Emulation der Controllertreiber verbunden ist.

Der Management Agent, auch als Gast-Agent bezeichnet, ist für Verwaltungsfunktionen der virtuellen Maschine auf hoher Ebene verantwortlich und stellt XenCenter einen vollständigen Satz von Funktionen bereit. Diese Funktionen umfassen stillschweigte Snapshots.

Sie müssen Citrix VM Tools auf jeder Windows VM installieren, damit die VM über eine vollständig unterstützte Konfiguration verfügt. Die auf der VM installierte Version von Citrix VM Tools muss mit der auf dem Citrix Hypervisor or-Server installierten Version übereinstimmen. Eine VM funktioniert ohne Citrix VM Tools, aber die Leistung wird beeinträchtigt, wenn die E/A-Treiber (PV-Treiber) nicht installiert sind. Sie müssen Citrix VM Tools 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 ausgeführten VM (mit Livemigration oder Storage Livemigration)
- Erstellen stillschweigter Snapshots oder Snapshots mit Arbeitsspeicher (Prüfpunkte) oder Wiederherstellen von Snapshots
- Anpassen der Anzahl der vCPUs auf einer laufenden Linux-VM (Windows VMs erfordern einen Neustart, damit diese Änderung wirksam wird)

Finden Sie den Virtualisierungsstatus einer VM heraus

XenCenter meldet den Virtualisierungsstatus einer VM auf der Registerkarte **Allgemein** der VM. Sie können herausfinden, ob Citrix VM Tools (E/A-Treiber und der Management Agent) 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:

E/A-optimiert (nicht optimiert): Dieses Feld zeigt an, ob die E/A-Treiber auf der VM installiert sind. Klicken Sie auf den Link **E/A-Treiber installieren und Management Agent** , um die E/A-Treiber von Citrix VM Tools ISO zu installieren.

> **Hinweis:**
>
> E/A-Treiber werden automatisch auf einer Windows VM installiert, die Updates von Windows Update erhalten kann. Weitere Informationen finden Sie unter Aktualisieren von Citrix VM-Tools.

Management Agent installiert (nicht installiert): Dieses Feld zeigt an, ob der Management Agent auf der VM installiert ist. Klicken Sie auf den Link **E/A-Treiber und Management Agent** installieren, um den Management Agent über die Citrix VM Tools-ISO zu installieren.

Kann Updates von Windows Update empfangen (kann nicht): Gibt an, ob die VM E/A-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 auf der Citrix VM Tools-ISO.

Installieren von E/A-Treibern und Management Agent: Diese Meldung wird angezeigt, wenn auf der VM keine E/A-Treiber oder der Management Agent installiert sind. Klicken Sie auf den Link, um Citrix VM Tools zu installieren. Bei Linux-VMs wechselt das Klicken auf den Statuslink zur Konsole der VM und lädt die Citrix VM Tools-ISO. Anschließend können Sie die ISO mounten und die Installation manuell ausführen, wie unter beschriebenInstallieren von Citrix VM-Tools.

Unterstützte Gäste und Zuweisung von Ressourcen

Eine Liste der unterstützten Gastbetriebssysteme finden Sie unterUnterstützte Gäste, virtuelle Arbeitsspeicher und Datenträgergrößenbeschränkungen

In diesem Abschnitt werden die Unterschiede bei der Unterstützung virtueller Geräte für die Mitglieder der Citrix Hypervisor Produktfamilie beschrieben.

Unterstützung virtueller Geräte der Citrix Hypervisor Produktfamilie

Die aktuelle Version der Citrix Hypervisor Produktfamilie hat einige allgemeine Einschränkungen für virtuelle Geräte für VMs. Bestimmte Gastbetriebssysteme haben möglicherweise niedrigere Grenzwerte für bestimmte Funktionen. Der Abschnitt zur individuellen Gastinstallation stellt die Einschränkungen fest. Ausführliche Informationen zu Konfigurationslimits finden Sie unterKonfigurationsbeschränkungen.

Faktoren wie Hardware und Umgebung können die Einschränkungen beeinflussen. Weitere Informationen zur unterstützten Hardware finden Sie im Citrix HypervisorHardwarekompatibilitätsliste.

VM-Blockgeräte

Im para-virtualisierten (PV) Linux-Fall werden Blockgeräte als PV-Geräte übergeben. Citrix Hypervisor versucht nicht, SCSI oder IDE zu emulieren, sondern stellt stattdessen eine geeignetere Schnittstelle in der virtuellen Umgebung bereit. Diese Schnittstelle ist in Form von`xvd*` Geräten. Manchmal ist es auch möglich, ein`sd*` Gerät mit demselben Mechanismus zu erhalten, bei dem der PV-Treiber innerhalb der VM den SCSI-Gerätenamespace übernimmt. Dieses Verhalten ist nicht wünschenswert, daher ist es am besten,`xvd*` wenn möglich für PV-Gäste zu verwenden. Die`xvd*` Geräte sind standardmäßig für Debian und RHEL.

Für Windows oder andere vollständig virtualisierte Gäste emuliert Citrix Hypervisor einen IDE-Bus in Form eines`hd*` Geräts. Wenn Sie Windows verwenden, wird bei der Installation der Citrix VM Tools ein spezieller E/A-Treiber installiert, der ähnlich wie Linux funktioniert, außer in einer vollständig virtualisierten Umgebung.

Kopiert!
Failed!

Windows VMs

October 16, 2019

Die Installation von Windows VMs auf dem Citrix Hypervisor or-Server erfordert Hardware-Virtualisierungsunterstützung (Intel VT oder AMD-V).

Grundlegendes Verfahren zum Erstellen einer Windows VM

Die Installation eines Windows auf einer VM besteht aus den folgenden Schritten:

1. Auswählen der entsprechenden Windows Vorlage
2. Installieren des Windows Betriebssystems
3. Installieren der Citrix VM-Tools (*E/A-Treiber* und *Management Agent*)

> **Warnhinweis:**
>
> Windows VMs werden nur unterstützt, wenn auf den VMs die Citrix VM-Tools installiert sind. Weitere Informationen finden Sie unter Citrix VM-Tools.

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. Die Vorlagen für einzelne Gäste haben vordefinierte Plattformkennzeichen gesetzt, die die Konfiguration der virtuellen Hardware definieren. Beispielsweise werden alle Windows VMs mit aktiviertem ACPI-Modus (Hardware Abstraction Layer, HAL) installiert. Wenn Sie später einen dieser VMs auf mehrere virtuelle CPUs ändern, wechselt Windows die HAL automatisch in den Mehrprozessormodus.

Die verfügbaren Windows Vorlagen sind unten aufgeführt:

Vorlagenname	Beschreibung
Citrix XenApp unter Windows Server 2008 (32-Bit)	Wird verwendet, um Windows Server 2008 SP2 (32-Bit) zu installieren. Alle Editionen werden unterstützt. Diese Vorlage wurde speziell auf die Optimierung der Citrix XenApp Leistung abgestimmt.
Citrix XenApp unter Windows Server 2008 (64-Bit)	Wird verwendet, um Windows Server 2008 SP2 (64-Bit) zu installieren. Alle Editionen werden unterstützt. Diese Vorlage wurde speziell auf die Optimierung der Citrix XenApp Leistung abgestimmt.

Vorlagenname	Beschreibung
Citrix XenApp unter Windows Server 2008 R2 (64-Bit)	Wird verwendet, um Windows Server 2008 R2 und Windows Server 2008 R2 SP1 (64-Bit) zu installieren. Alle Editionen werden unterstützt. Diese Vorlage wurde speziell auf die Optimierung der Citrix XenApp Leistung abgestimmt.
Windows 7 (32-Bit)	Wird verwendet, um Windows 7 und Windows 7 SP1 (32-Bit) zu installieren.
Windows 7 (64 Bit)	Wird verwendet, um Windows 7 und Windows 7 SP1 (64-Bit) zu installieren.
Windows 8.1 (32-Bit)	Wird verwendet, um Windows 8.1 (32-Bit) zu installieren. (Siehe Anmerkung)
Windows 8.1 (64 Bit)	Wird verwendet, um Windows 8.1 (64-Bit) zu installieren. (Siehe Anmerkung)
Windows 10 (32-Bit)	Wird verwendet, um Windows 10 zu installieren.
Windows 10 (64 Bit)	Wird verwendet, um Windows 10 (64-Bit) zu installieren.
Windows Server 2008 (32-bit)	Wird verwendet, um Windows Server 2008 SP2 (32-Bit) zu installieren. Alle Editionen werden unterstützt.
Windows Server 2008 (64 Bit)	Wird verwendet, um Windows Server 2008 SP2 (64-Bit) zu installieren. Alle Editionen werden unterstützt.
Windows Server 2008 R2 (64 Bit)	Wird verwendet, um Windows Server 2008 R2 und Windows Server 2008 R2 SP1 (64-Bit) zu installieren. Alle Editionen werden unterstützt.
Windows Server 2012 (64 Bit)	Wird verwendet, um Windows Server 2012 (64-Bit) zu installieren.
Windows Server 2012 R2 (64 Bit)	Wird verwendet, um Windows Server 2012 R2 (64-Bit) zu installieren.
Windows Server 2016 (64 Bit)	Wird verwendet, um Windows Server 2016 oder Windows Server Core 2016 (64-Bit) zu installieren

Vorlagenname	Beschreibung
Windows Server 2019 (64 Bit)	Wird verwendet, um Windows Server 2019 oder Windows Server Core 2019 (64-Bit) zu installieren

> **Hinweis:**
>
> Windows 8 wird nicht mehr unterstützt. Benutzer, die Windows 8 installieren, werden auf Windows 8.1 aktualisiert.
>
> **Warnhinweis:**
>
> Experimentelle Gastbetriebssysteme haben eingeschränkte Tests erhalten, sind möglicherweise nicht in zukünftigen Produktversionen vorhanden und dürfen nicht auf Produktionssystemen aktiviert werden. Wir reagieren möglicherweise nicht auf Support-Anfragen bezüglich experimenteller Funktionen.

Anfügen einer ISO-Image-Bibliothek

Das Windows Betriebssystem kann entweder von einer Installations-CD in einem physischen CD-ROM-Laufwerk auf dem Citrix Hypervisor-Server oder von einem ISO-Image installiert werden. InformationenErstellen von ISO-Imageszum Erstellen eines ISO-Abbilds von einer Windows Installations-CD und zur Verwendung finden Sie unter.

Erstellen einer virtuellen Maschine mit XenCenter

> **Hinweis:**
>
> Das folgende Verfahren enthält ein Beispiel für das Erstellen von Windows 7 (32-Bit-) VM. Die Standardwerte können je nach verwendetem Betriebssystem variieren.

So erstellen Sie eine Windows 7 (32-Bit) -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. Select eine VM-Vorlage aus, 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 enthält die Vorlagen, die von Citrix Hypervisor derzeit unterstützt werden.

> **Hinweis:**
>
> Wenn das Betriebssystem, das Sie auf Ihrer VM installieren, nur mit der ursprünglichen Hardware kompatibel ist, aktivieren Sie das Kontrollkästchen **Host-BIOS-Zeichenfolgen in VM kopieren** . Sie können diese Option beispielsweise für eine Betriebssystem-Installations-CD verwenden, die mit einem bestimmten Computer verpackt wurde.

Informationen zum Kopieren von BIOS-Zeichenfolgen mithilfe der CLI finden Sie unterInstallieren von HVM-VMs von Reseller Option Kit (BIOS-gesperrte) Medien. Die Option zum Festlegen benutzerdefinierter BIOS-Zeichenfolgen ist für HVM-VMs nicht verfügbar.

3. Geben Sie einen Namen und eine optionale Beschreibung für die neue VM ein.
4. Wählen Sie die Quelle des Betriebssystemmediums aus, das auf der neuen VM installiert werden soll.

   Die Installation von einer CD/DVD ist die einfachste Möglichkeit, um loszulegen.

   a) Wählen Sie die Standardinstallationsquellenoption (DVD-Laufwerk)
   b) Legen Sie den Datenträger in das DVD-Laufwerk des Citrix Hypervisor or-Servers ein
   c) Wählen Sie **Weiter**, um fortzufahren.

   Mit Citrix Hypervisor können Sie außerdem 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 CD (CD, DVD usw.) enthalten würde. In diesem Fall würde ein ISO-Abbild die gleichen 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 die spezifischen ISO-Medien des Betriebssystems aus der Liste auswählen.
5. Select einen Home-Server für die VM aus.

   Ein Home-Server ist der Server, der die Ressourcen für eine VM in einem Pool bereitstellt. Wenn Sie einen Home-Server für eine VM nominieren, versucht Citrix Hypervisor, die VM auf diesem Server zu starten. Wenn diese Aktion nicht möglich ist, wird automatisch ein alternativer Server innerhalb desselben Pools ausgewählt. Um einen Heimserver auszuwählen, klicken Sie auf **Die VM auf diesem Server platzieren** , und wählen Sie einen Server aus der Liste aus.

   > **Hinweise:**
   >
   > ```
   > 1 - In WLB-fähigen Pools wird der nominierte Home-Server nicht
   >     zum Starten, Neustarten, Fortsetzen oder Migrieren der VM
   >     verwendet. Stattdessen nominiert WLB den besten Server für
   >     die VM, indem die Metriken des Citrix Hypervisor
   >     Ressourcenpools analysiert und Optimierungen empfohlen
   > ```



```
        werden. -  Wenn einer VM eine virtuelle GPU zugewiesen ist,
         wird die Nominierung des Home-Servers nicht wirksam.
        Stattdessen basiert die Server-Nominierung auf der vom
        Benutzer festgelegten virtuellen GPU-Platzierungsrichtlinie
        .
```

Wenn Sie keinen Home-Server nominieren möchten, klicken Sie auf **Dieser VM keinen Home-Server zuweisen**. Die VM wird auf jedem Server mit den erforderlichen Ressourcen gestartet.

Klicken Sie auf **Weiter**, um fortzufahren.

6. Weisen Sie Prozessor- und Speicherressourcen für die VM zu. Für eine Windows 10-VM ist der Standardwert 1 virtuelle CPU und 2.048 MB RAM. Sie können auch die Standardeinstellungen ändern. Klicken Sie auf **Weiter**, um fortzufahren.
7. Weisen Sie eine virtuelle GPU zu. Der Assistent für neue VM fordert Sie auf, der VM eine dedizierte GPU oder eine virtuelle GPU zuzuweisen. Mit dieser Option kann die VM die Verarbeitungsleistung der GPU nutzen. Mit dieser Funktion haben Sie bessere Unterstützung für professionelle High-End-3D-Grafikanwendungen wie CAD/CAM, GIS und Medical Imaging-Anwendungen.
8. Weisen Sie Speicher für die neue VM zu und konfigurieren Sie sie.

   Klicken Sie auf **Weiter** , um die Standardzuweisung (24 GB) und -konfiguration auszuwählen, oder Sie möchten die folgende zusätzliche Konfiguration vornehmen:

   - Ändern Sie den Namen, die Beschreibung oder die Größe des virtuellen Laufwerks, indem Sie auf **Eigenschaften** klicken.
   - Fügen Sie ein neues virtuelles Laufwerk hinzu, indem Sie **Hinzufügen**auswählen.
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 NIC. Alternativ können Sie die folgende zusätzliche Konfiguration vornehmen:

   - Ändern Sie die physische Netzwerk-, MAC-Adresse oder QoS-Priorität (Quality of Service) des virtuellen Laufwerks, indem Sie auf **Eigenschaften** klicken.
   - Fügen Sie eine neue virtuelle Netzwerkkarte hinzu, indem Sie **Hinzufügen**auswählen.
10. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Jetzt erstellen**, um die VM zu erstellen und zur Registerkarte **Suchen** zurückzukehren.

    Im **Ressourcenbereich** wird unter dem Host ein Symbol für Ihre neue VM 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 Betriebssysteminstallationsbildschirmen und treffen Sie Ihre Auswahl.

12. Nachdem die Installation des Betriebssystems abgeschlossen und die VM neu gestartet wurde, installieren Sie die Citrix VM-Tools.

Installieren von Citrix VM-Tools

Citrix Hypervisor verfügt über einen einfacheren Mechanismus zum Installieren und Aktualisieren von Citrix VM Tools (E/A-Treiber und Verwaltungsagent) auf Windows VMs.

Citrix VM-Tools bieten leistungsstarke E/A-Dienste ohne den Aufwand herkömmlicher Geräteemulation. Citrix VM Tools bestehen aus E/A-Treibern (auch als paravirtualisierte Treiber oder PV-Treiber bezeichnet) und dem Management Agent. Citrix VM Tools müssen auf jeder Windows VM installiert sein, damit die VM über eine vollständig unterstützte Konfiguration verfügt. Eine VM funktioniert ohne sie, aber die Leistung wird erheblich behindert.

> **Hinweis:**
>
> Um Citrix VM Tools auf einer Windows VM zu installieren, muss auf der VM Microsoft .NET Framework Version 4.0 oder höher ausgeführt werden.

So installieren Sie Citrix VM-Tools:

1. Select die VM im **Ressourcenbereich** aus, klicken Sie mit der rechten Maustaste, und klicken Sie dann im Kontextmenü auf **Citrix VM-Tools installieren**. Alternativ klicken Sie im Menü **VM** auf **Citrix VM Tools installieren** oder auf der Registerkarte **Allgemein** der VM auf **E/A-Treiber und Management Agent installieren** .

   > **Hinweis:**
   >
   > Wenn Sie Citrix VM Tools auf Ihrer VM installieren, installieren Sie sowohl E/A-Treiber (PV-Treiber) als auch den Management Agent.

2. Wenn die automatische Wiedergabe für das CD/DVD-Laufwerk der VM aktiviert ist, wird die Installation nach wenigen Augenblicken automatisch gestartet. Der Prozess installiert die E/A-Treiber und den Management Agent. Starten Sie die VM neu, wenn Sie aufgefordert werden, Ihre VM in einen optimierten Zustand zu versetzen.

3. Wenn die automatische Wiedergabe nicht aktiviert ist, klicken Sie auf **Citrix VM-Tools installieren** , um mit der Installation fortzufahren. Mit dieser Aktion wird die Citrix VM Tools ISO (`guest-tools.iso`) auf dem CD/DVD-Laufwerk der VM bereitgestellt.

   Wenn Sie dazu aufgefordert werden, wählen Sie eine der folgenden Optionen aus, um festzulegen, was mit dem Citrix VM Tools-ISO geschieht:

   - Klicken Sie auf **Setup.exe ausführen** , um die Installation von Citrix VM Tools zu starten. Mit dieser Aktion wird der **Setup-Assistent für Citrix Hypervisor für Windows Management Agent** geöffnet. Befolgen Sie die Anweisungen des Assistenten, um die VM in einen

optimierten Zustand zu versetzen und alle Aktionen auszuführen, die zum Abschluss des Installationsvorgangs erforderlich sind. Wenn Sie Citrix VM Tools mit dieser Methode installieren, wird der Management Agent so konfiguriert, dass Updates automatisch abruft. Der Verwaltungsagent-Aktualisierungsmechanismus aktualisiert jedoch nicht automatisch die E/A-Treiber. Dieses Verhalten ist die Standardeinstellung. Wenn Sie das Standardverhalten ändern möchten, installieren Sie Citrix VM Tools mit der folgenden Methode:

- Klicken Sie auf **Ordner öffnen, um Dateien anzuzeigen** und dann`Setup.exe` vom CD-Laufwerk aus auszuführen. Mit dieser Option wird der **Setup-Assistent für den Citrix Hypervisor für Windows Management Agent** geöffnet und Sie können die Installation von Citrix VM Tools und die Update-Einstellungen für den Management Agent anpassen.
- 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. Der **Setup-Assistent für Citrix Hypervisor Windows Management Agent** zeigt die Standardeinstellungen an. Standardmäßig zeigt der Assistent die folgenden Einstellungen an:
  - E/A-Treiber jetzt installieren
  - Automatische Management-Agent-Updates zulassen
  - Automatische E/A-Treiberaktualisierungen durch den Management-Agent nicht zulassen
  - Anonyme Nutzungsinformationen an Citrix senden

  Wenn Sie die automatische Aktualisierung des Management Agents nicht zulassen möchten, wählen Sie **Automatische Management-Agent-Updates nicht zulassen** aus der Liste aus.

  Wenn Sie zulassen möchten, dass der Management Agent die E/A-Treiber automatisch aktualisieren kann, wählen Sie **Automatische E/A-Treiberaktualisierungen durch den Management-Agent zulassen**aus.

  > **Hinweis:**
  >
  > Wenn Sie E/A-Treiberupdates über den Windows Update-Mechanismus erhalten möchten, erlauben Sie dem Management Agent nicht, die E/A-Treiber automatisch zu aktualisieren.

  Wenn Sie keine anonymen Nutzungsinformationen für Citrix freigeben möchten, deaktivieren **Sie das Kontrollkästchen Anonyme Nutzungsinformationen an Citrix senden** . Die an Citrix übertragenen Informationen enthalten die UUID der VM, die das Update

anfordert. Es werden keine weiteren Informationen über die VM erfasst oder an Citrix übertragen.

- Klicken Sie auf **Weiter** und anschließend auf **Installieren** , um mit der Installation von Citrix VM Tools zu beginnen.
- Wenn Sie dazu aufgefordert werden, führen Sie alle Aktionen aus, die zum Abschließen des Installationsvorgangs erforderlich sind.

  > **Hinweis:**
  >
  > Die Citrix VM-Tools können einen Neustart mit`/quiet /norestart` oder`/quiet /forcerestart` angeben, nachdem die VM bereits einmal im Rahmen der Installation neu gestartet wurde.

- Klicken Sie auf **Fertig stellen** , um den Assistenten zu beenden.

> **Hinweis:**
>
> E/A-Treiber werden automatisch auf einer Windows VM installiert, die Updates von Windows Update erhalten kann. Es wird jedoch empfohlen, das Citrix VM Tools-Paket zu installieren, um den Management Agent zu installieren und die unterstützte Konfiguration beizubehalten.

Um die E/A-Treiber und den Management Agent auf vielen Windows VMs zu installieren, installieren`managementagentx86.msi` oder`managementagentx64.msi` verwenden Sie das bevorzugte MSI-Installationstool. Diese Dateien finden Sie auf der Citrix VM Tools ISO.

Kunden, die die Citrix VM Tools oder den Management Agent über RDP installieren, werden möglicherweise die Aufforderung zum Neustart nicht angezeigt, da sie nur in der Windows Konsolensitzung angezeigt wird. Um sicherzustellen, dass Sie die VM (falls erforderlich) neu starten und die VM in einen optimierten Zustand 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.

Geräuschlose Installation

Führen Sie einen der folgenden Befehle aus, um die Citrix VM-Tools automatisch zu installieren und den Neustart des Systems zu verhindern:

```
Msiexec.exe /package managementagentx86.msi /quiet /norestart
Msiexec.exe /package managementagentx64.msi /quiet /norestart
```

Oder

```
Setup.exe /quiet /norestart
```


Eine nicht interaktive, aber nicht unbeaufsichtigte Installation kann erhalten werden, indem Sie Folgendes ausführen:

```
Msiexec.exe managementagentx86.msi /passive
Msiexec.exe managementagentx64.msi /passive
```

Oder

```
Setup.exe /passive
```

Bei interaktiven, unbeaufsichtigten und passiven Installationen können nach dem nächsten Systemneustart mehrere automatische Neustarts durchgeführt werden, bevor die Citrix VM-Tools vollständig installiert sind. Dieses Verhalten ist auch bei Installationen mit dem angegebenen `/norestart` Flag der Fall. Bei Installationen, bei denen das `/norestart` Flag bereitgestellt wird, kann der erste Neustart jedoch manuell initiiert werden.

Die Citrix VM-Tools werden standardmäßig im `C:\Program Files\Citrix\XenTools` Verzeichnis auf der VM installiert.

> **Hinweise:**
>
> - Um Citrix VM Tools auf einer Windows VM zu installieren, muss auf der VM Microsoft .NET Framework Version 4.0 oder höher ausgeführt werden.
> - Der `/quiet` Parameter gilt nur für die Installationsdialoge, nicht aber für die Gerätetreiberinstallation. Wenn der `/quiet` Parameter angegeben ist, fordert die Installation des Gerätetreibers bei Bedarf die Berechtigung zum Neustart an.
>   - Wenn angegeben `/quiet /norestart` ist, wird das System nach Abschluss der Installation der gesamten Tools nicht neu gestartet. Dieses Verhalten ist unabhängig von dem, was der Benutzer im Neustartdialog angibt.
>   - Wenn angegeben `/quiet /forcerestart` ist, wird das System neu gestartet, nachdem die gesamte Installation der Tools abgeschlossen ist. Dieses Verhalten ist unabhängig von dem, was der Benutzer im Neustartdialog angibt.
>   - Wenn die Installation des Gerätetreibers die Berechtigung zum Neustart anfordert, kann eine Toolinstallation mit dem angegebenen `quiet` Parameter noch ausgeführt werden. Verwenden Sie den Task-Manager, um zu bestätigen, ob das Installationsprogramm noch ausgeführt wird.
>
> **Warnhinweis:**
> Das
> Installieren oder Aktualisieren der Citrix VM-Tools kann dazu führen, dass sich der Anzeigename und der Bezeichner einiger Netzwerkadapter ändern. Jede Software, die für die Verwendung eines bestimmten Adapters konfiguriert ist, muss möglicherweise nach der Installation oder Aktualisierung von Citrix VM Tools neu konfiguriert werden.

Erstellen einer Windows VM mithilfe der CLI

So erstellen Sie eine Windows VM aus einem ISO-Repository mithilfe der xe-CLI:

1. Erstellen einer virtuellen Maschine aus einer Vorlage:

   ```
   xe vm-install new-name-label=vm_name template=template_name
   ```

   Dieser Befehl gibt die UUID der neuen VM zurück.

2. Erstellen Sie ein ISO-Speicher-Repository:

   ```
   xe-mount-iso-sr path_to_iso_sr
   ```

3. Alle verfügbaren ISOs auflisten:

   ```
   xe cd-list
   ```

4. Legen Sie die angegebene ISO in das virtuelle CD-Laufwerk der angegebenen VM ein:

   ```
   xe vm-cd-add vm=vm_name cd-name=iso_name device=3
   ```

5. Starten Sie die VM und installieren Sie das Betriebssystem:

   ```
   xe vm-start vm=vm_name
   ```

Zu diesem Zeitpunkt ist die VM-Konsole in XenCenter sichtbar.

Weitere Hinweise zur Verwendung der CLI finden Sie unterBefehlszeilenschnittstelle.

Aktualisieren Windows Betriebssystemen

In diesem Abschnitt werden die Aktualisierung von Windows VMs mit aktualisierten Betriebssystemen und die Neuinstallation von Citrix VM Tools erläutert.

Upgrades auf VMs sind normalerweise erforderlich, wenn Sie auf eine neuere Version von Citrix Hypervisor wechseln. Beachten Sie die folgenden Einschränkungen beim Upgrade Ihrer VMs auf eine neuere Version von Citrix Hypervisor:

- Bevor Sie Windows VMs mit Live-Migration migrieren, müssen Sie die Citrix VM-Tools auf jeder VM aktualisieren.
- Der Vorgang „Aussetzen/Fortsetzen“ wird auf Windows VMs erst unterstützt, wenn die Citrix VM-Tools aktualisiert wurden.
- Die Verwendung bestimmter Antiviren- und Firewallanwendungen kann Windows VMs abstürzen, es sei denn, die Citrix VM-Tools werden aktualisiert.

> **Warnhinweis:**
>
> Deinstallieren Sie vor dem Aktualisieren von Windows Betriebssystemen die Citrix VM-Tools. Wenn sie während des Aktualisierungsversuchs vorhanden sind, schlägt das Update fehl.

Windows-Installationsdatenträger bieten normalerweise eine Upgrade-Option, wenn Sie sie auf einem Server starten, auf dem bereits eine frühere Version von Windows installiert ist.

Sie können das Betriebssystem von Windows VMs auf ähnliche Weise aktualisieren.

So deinstallieren Sie die Citrix VM-Tools:

1. Wählen **Sie auf der Schaltfläche Start** die Option **Systemsteuerung** aus.
2. Select **Programme**und dann **Programme und Funktionen**aus.
3. Select alle folgenden Elemente aus (die Liste hängt von Ihrem Betriebssystem und der auf Ihrer VM installierten Version der Citrix VM Tools ab):
   - Citrix Hypervisor Windows Verwaltungsagent
   - Citrix Tools für virtuelle Maschinen
   - Installationsprogramm für Citrix VM Tools
   - Citrix Hypervisor Windows Gast-Agent
   - Citrix Hypervisor Xen Windows x64 PV Treiber
   - Citrix Hypervisor Xen Windows x86 PV Treiber
   - Citrix Hypervisor VSS-Anbieter
4. Select **Deinstallieren**aus.

   Mit dieser Option werden die Citrix VM-Tools entfernt. Wenn der Vorgang abgeschlossen ist, wird eine Meldung angezeigt. Klicken Sie auf **OK** , um das Meldungsfeld zu schließen.

Nachdem das Update des Betriebssystems abgeschlossen ist, installieren Sie die Citrix VM-Tools wie nach der Installation einer neuen Windows VM neu.

Citrix VM-Tools neu installieren

Die Citrix VM-Tools sind in XenCenter auf dem integrierten verfügbar`guest-tools.iso`. Wählen Sie im Menü **VM** die Option **Citrix VM Tools installieren** . Mit dieser Option wird das CD-Image, das die Citrix VM-Tools enthält, an die VM angehängt.

Wenn die automatische Wiedergabe für das CD/DVD-Laufwerk der VM aktiviert ist, wird die Installation nach wenigen Augenblicken automatisch gestartet. Der Prozess installiert die E/A-Treiber und den Management Agent. Starten Sie die VM neu, wenn Sie aufgefordert werden, Ihre VM in einen optimierten Zustand zu versetzen.

Wenn die automatische Wiedergabe nicht aktiviert ist, zeigt das Citrix VM Tools-Installationsprogramm die Installationsoptionen an. Klicken Sie auf **Citrix VM-Tools installieren**, um mit der Installation

fortzufahren. Mit dieser Option wird die Citrix VM Tools-ISO (guest-tools.iso) auf dem CD/DVD-Laufwerk der VM bereitgestellt. Klicken Sie auf **Setup.exe ausführen** , um die Installation von Citrix VM Tools zu starten und die VM neu zu starten, wenn Sie aufgefordert werden, die VM in einen optimierten Zustand zu versetzen.

Aktualisieren von Citrix VM-Tools

Citrix Hypervisor verfügt über einen einfacheren Mechanismus, um E/A-Treiber (PV-Treiber) und den Verwaltungs-Agent für Windows VMs automatisch zu aktualisieren. Mit diesem Mechanismus können Kunden Updates installieren, sobald sie verfügbar sind, ohne auf einen Hotfix warten zu müssen.

Der Abschnitt **Virtualisierungsstatus** auf der Registerkarte **Allgemein** einer virtuellen Maschine 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 E/A-Treiberupdates von Windows Update erhalten möchten, deaktivieren Sie Windows Update auf der VM, oder geben Sie eine Gruppenrichtlinie an.

Die folgenden Abschnitte enthalten Informationen zur automatischen Aktualisierung der E/A-Treiber und des Management Agents.

Aktualisieren der E/A-Treiber

Sie können I/O-Treiberupdates automatisch von Microsoft Windows Update abrufen, vorausgesetzt:

- Sie führen Citrix Hypervisor 8.0 Premium Edition aus oder haben Zugriff auf Citrix Hypervisor über die Berechtigung für Citrix Virtual Apps and Desktops.
- Sie haben eine Windows VM mit XenCenter erstellt, die mit Citrix Hypervisor 8.0 ausgestellt wurde.

  > **Wichtig:**
  >
  > VMs, die aus früheren Versionen von Citrix Hypervisor importiert **wurden, können keine** E/A-Treiber von Windows Update empfangen.

- Windows Update ist innerhalb der VM aktiviert
- Die VM hat Zugriff auf das Internet, oder sie kann eine Verbindung zu einem WSUS-Proxyserver herstellen

> **Hinweis:**
>
> Windows Server Core unterstützt nicht die Verwendung von Windows Update zum Installieren oder Aktualisieren der E/A-Treiber. Verwenden Sie stattdessen das Installationsprogramm auf der Citrix VM Tools-ISO.

> **Hinweis:**
>
> Kunden können E/A-Treiber-Updates auch automatisch über den automatischen Management-Agent-Aktualisierungsmechanismus erhalten. Sie können diese Einstellung während der Installation von Citrix VM Tools konfigurieren. Weitere Informationen finden Sie unter *Installieren von Citrix VM-Tools*.

Suchen der E/A-Treiberversion

So ermitteln Sie die Version der auf der VM installierten E/A-Treiber:

1. Navigieren Sie zu `C:\Windows\System32\drivers`.
2. Suchen Sie den Treiber aus der Liste.
3. Klicken Sie mit der rechten Maustaste auf den Treiber, und wählen Sie **Eigenschaften** und dann **Details** aus.

   Im Feld **Dateiversion** wird die Version des Treibers angezeigt, der auf der VM installiert ist.

Aktualisieren des Management-Agents

Mit Citrix Hypervisor können Sie den Management Agent automatisch auf neuen und vorhandenen Windows VMs aktualisieren. Standardmäßig ermöglicht Citrix Hypervisor 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 Citrix VM Tools anpassen. Die automatische Aktualisierung des Management Agents erfolgt nahtlos und startet die VM nicht neu. In Szenarien, in denen ein Neustart der virtuellen Maschine erforderlich ist, wird auf der Registerkarte Konsole der VM eine Meldung angezeigt, in der die Benutzer über die erforderliche Aktion benachrichtigt werden.

Sie können die Management-Agent-Updates automatisch abrufen, vorausgesetzt:

- Sie führen Citrix Hypervisor 8.0 Premium Edition aus oder haben Zugriff auf Citrix Hypervisor über die Berechtigung für Citrix Virtual Apps and Desktops.
- Sie haben Citrix VM Tools installiert, die mit Citrix Hypervisor 7.0 oder höher ausgestellt sind.
- Die Windows VM hat Zugriff auf das Internet

> **Wichtig:**
>
> Updates für Citrix VM Tools können auch über den standardmäßigen Citrix Hypervisor Update-Mechanismus (Hotfix) ausgegeben werden. Solche Hotfixes enthalten Updates sowohl für E/A-Treiber als auch für den Management Agent. Es gibt keine Lizenzbeschränkung für die Aktualisierung von Citrix VM Tools, die als Hotfix ausgestellt wurden.

Suchen der Management-Agent-Version

So ermitteln Sie die auf der VM installierte Version des Management Agents:

1. Navigieren Sie zu `C:\Program Files\Citrix\XenTools`.
2. Klicken Sie mit`XenGuestAgent` der rechten Maustaste in der Liste, und klicken Sie auf **Eigenschaften** und dann auf **Details** .

   Im Feld **Dateiversion** wird die auf der VM installierte Version des Management Agents angezeigt.

Verwalten von automatischen Updates mithilfe der CLI

Mit Citrix Hypervisor können Sie mithilfe der Befehlszeile die automatische Aktualisierung der E/A-Treiber und des Management-Agents verwalten. Sie können`setup.exe` oder`msiexec.exe` mit den in der folgenden Tabelle aufgeführten Argumenten ausführen, um anzugeben, ob die E/A-Treiber und der Management Agent automatisch aktualisiert werden. Informationen zum Installieren von Citrix VM Tools mit`setup.exe` oder`msiexec.exe` finden Sie unterGeräuschlose Installation .

> **Hinweis:**
>
> Bei VMs, die entweder mit PVS oder MCS verwaltet werden, werden automatisierte Updates automatisch deaktiviert, wenn der VDA für Citrix Virtual Desktops vorhanden ist und dass der Computer als nicht persistent gemeldet wird.

Argument	Werte	Beschreibung
ALLOWAUTOUPDATE	JA/NEIN	Automatische Aktualisierung des Management-Agents erlaubt/nicht zulassen
ALLOWDRIVERINSTALL	JA/NEIN	Zulassen/Verlassen des Citrix VM Tools-Installationsprogramms die Installation von PARTIALURLPLACEHOLDER Treibern
ALLOWDRIVERUPDATE	JA/NEIN	Zulassen/Verbieten des Management Agents, die PARTIALURLPLACEHOLDER Treiber automatisch zu aktualisieren

Argument	Werte	Beschreibung
IDENTIFIZIERUNGAUTOUPDATE	JA/NEIN	Zulassen/Verwehren des automatischen Aktualisierungsmechanismus für das Senden anonymer Verwendungsinformationen an Citrix

Zum Beispiel:

```
setup.exe  /passive /forcerestart ALLOWAUTOUPDATE=YES
    ALLOWDRIVERINSTALL=NO \
      ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Oder

```
msiexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES
    ALLOWDRIVERINSTALL=NO \
     ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Umleiten der Management Agent-Updates

Mit Citrix Hypervisor können Kunden Management Agent-Updates vor der Installation auf einen internen Webserver umleiten. Mit dieser Umleitung können Kunden die Updates überprüfen, bevor sie automatisch auf der VM installiert werden.

So leiten Sie die Management-Agent-Updates um:

1. Laden Sie die JSON-Datei von herunter https://pvupdates.vmd.citrix.com/updates.json.
2. Laden Sie die MSI-Dateien des Management Agent herunter, auf die in der JSON-Datei verwiesen wird.
3. Laden Sie die MSI-Dateien auf einen internen Webserver hoch, auf den Ihre VMs zugreifen können.
4. Aktualisieren Sie die JSON-Datei so, dass sie auf die MSI-Dateien auf dem internen Webserver verweist.
5. Laden Sie die JSON-Datei auf den Webserver hoch.

> **Hinweis:**
>
> Diese Datei ist auch im TSV-Format für ältere Versionen des Management Agents verfügbar. https://pvupdates.vmd.citrix.com/updates.tsv

Automatische Updates können auch pro VM oder Pool umgeleitet werden. So leiten Sie Updates pro VM um:

1. Öffnen Sie auf der VM eine Eingabeaufforderung als Administrator.
2. Führen Sie den Befehl aus

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url
   /d \
    url of the JSON file on the web server
```

Führen Sie den folgenden Befehl aus, um die automatische Aktualisierung des Management Agents auf Poolbasis umzuleiten:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url
   of the JSON file on the web server
```

Management-Agent-Updates deaktivieren

So deaktivieren Sie die automatische Aktualisierung des Management Agents pro VM:

1. Öffnen Sie auf der VM eine Eingabeaufforderung als Administrator.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_DWORD /v
   DisableAutoUpdate /d 1
```

Führen Sie den folgenden Befehl aus, um die automatische Aktualisierung des Management Agents pro Pool zu deaktivieren:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=
   false
```

Ändern der Einstellungen für die automatische E/A-Treiberaktualisierung

Während der Installation von Citrix VM Tools können Sie angeben, ob der Management Agent die E/A-Treiber automatisch aktualisieren kann. Wenn Sie diese Einstellung nach Abschluss der Installation von Citrix VM Tools aktualisieren möchten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf der VM eine Eingabeaufforderung als Administrator.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v
    \
     InstallDrivers /d YES/NO
```

So senden Sie anonyme Nutzungsinformationen an Citrix:

Während der Installation von Citrix VM Tools können Sie angeben, ob Sie anonyme Verwendungsinformationen an Citrix senden möchten. Wenn Sie diese Einstellung nach Abschluss der Installation von Citrix VM Tools aktualisieren möchten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie auf der VM eine Eingabeaufforderung als Administrator.
2. Führen Sie den folgenden Befehl aus:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \
     IDENTIFYAUTOUPDATE /d YES/NO
```

Vorbereiten des Klonens einer Windows VM mithilfe von Sysprep

Die einzige unterstützte Methode zum Klonen einer Windows VM besteht darin, die VM mit dem Windows-Dienstprogramm`sysprep` vorzubereiten.

Das`sysprep` Dienstprogramm ändert die SID des lokalen Computers, um sie für jeden Computer eindeutig zu machen. Die`sysprep` Binärdateien befinden sich im`C:\Windows\System32\Sysprep` Ordner.

> **Hinweis:**
>
> Bei älteren Versionen von Windows befinden sich die`sysprep` Binärdateien auf den Windows-Produkt-CDs in der`\support\tools\deploy.cab` Datei. Diese Binärdateien müssen vor der Verwendung auf Ihre Windows VM kopiert werden.

So klonen Sie Windows VMs:

1. Erstellen, installieren und konfigurieren Sie die Windows VM wie gewünscht.
2. Wenden Sie alle relevanten Service Packs und Updates an.
3. Installieren Sie die Citrix VM-Tools.
4. Installieren Sie alle Anwendungen und führen Sie eine andere Konfiguration durch.
5. Lauf`sysprep`! Dieses Dienstprogramm fährt die VM herunter, wenn sie abgeschlossen ist.
6. Konvertieren Sie die VM mit XenCenter in eine Vorlage.

7. Klonen Sie die neu erstellte Vorlage nach Bedarf in neue VMs.
8. Wenn die geklonte VM gestartet wird, werden die folgenden Aktionen ausgeführt, bevor sie zur Verwendung verfügbar ist:
    - Es erhält eine neue SID und Name
    - Es führt ein Mini-Setup aus, um bei Bedarf Konfigurationswerte einzugeben.
    - Schließlich wird es neu gestartet

    > **Hinweis:**
    >
    > Starten Sie die ursprüngliche, sys-vorbereitete VM (die „Quelle“ -VM) nach der`sysprep` Bühne nicht erneut neu. Konvertieren Sie es anschließend sofort in eine Vorlage, um Neustarts zu verhindern. Wenn die Quell-VM neu gestartet wird,`sysprep` muss sie erneut ausgeführt werden, bevor sie sicher verwendet werden kann, um mehr Klone zu erstellen.

Weitere Informationen zur Verwendung`sysprep`finden Sie auf der folgenden Microsoft-Website:

- Das Windows Automated Installation Kit (AIK)

Windows VM Versionshinweise

Es gibt viele Versionen und Varianten von Windows mit unterschiedlicher Unterstützung für die von Citrix Hypervisor bereitgestellten Funktionen. In diesem Abschnitt werden Notizen und Errata zu den bekannten Unterschieden aufgeführt.

Allgemeine Windows Probleme

- Starten Sie bei der Installation von Windows VMs mit nicht mehr als drei virtuellen Laufwerken. Nachdem die VM und die Citrix VM Tools installiert wurden, können Sie zusätzliche virtuelle Laufwerke hinzufügen. Stellen Sie sicher, dass das Startgerät immer eine der ersten Festplatten ist, damit die VM ohne die Citrix VM-Tools erfolgreich gestartet werden kann.
- Wenn der Startmodus für eine Windows VM BIOS-Start ist, formatiert Windows die primäre Festplatte mit einem Master Boot Record (MBR). MBR begrenzt den maximal adressierbaren Speicherplatz einer Festplatte auf 2 TiB. Führen Sie eine der folgenden Schritte aus, um einen Datenträger mit einer Windows VM zu verwenden, die größer als 2 TiB ist:
    - Wenn UEFI-Boot 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-Partitionstabelle (GPT) aus.
- Mehrere vCPUs werden Windows Gästen als CPU-Sockets bereitgestellt und unterliegen den in der VM vorhandenen Lizenzierungsbeschränkungen. Die Anzahl der im Gast vorhandenen CPUs

kann durch Überprüfung des Device Manager bestätigt werden. Die Anzahl der tatsächlich von Windows verwendeten CPUs kann im Task-Manager angezeigt werden.

- Die Reihenfolge der Datenträgeraufzählung in einem Windows Gast kann von der Reihenfolge abweichen, in der sie ursprünglich hinzugefügt wurden. Dieses Verhalten ist aufgrund der Interaktion zwischen den E/A-Treibern und dem Plug-and-Play-Subsystem in Windows. Zum Beispiel kann der erste Datenträger als angezeigt werden`Disk 1`, der nächste Hot Plug als`Disk 0`, ein nachfolgender Datenträger als`Disk 2`und dann in der erwarteten Art und Weise nach oben.
- Ein Fehler im VLC-Player-DirectX-Back-End ersetzt Gelb durch Blau bei der Videowiedergabe, wenn die Windows Anzeigeeigenschaften auf 24-Bit-Farbe eingestellt sind. VLC mit OpenGL als Back-End funktioniert korrekt, und jeder andere DirectX-basierte oder OpenGL-basierte Video-Player funktioniert auch. Es ist kein Problem, wenn der Gast so eingestellt ist, 16-Bit-Farbe anstelle von 24 zu verwenden.
- Der PV-Ethernet-Adapter meldet eine Geschwindigkeit von 1 Gbit/s in Windows VMs. Diese Geschwindigkeit ist ein fest codierter Wert und ist in einer virtuellen Umgebung nicht relevant, da die virtuelle Netzwerkkarte mit einem virtuellen Switch verbunden ist. Die Datenrate wird nicht durch die angekündigte Netzwerkgeschwindigkeit begrenzt.

Windows 7

Microsoft unterstützt die Verwendung von Windows 7 nur, wenn Service Pack 1 installiert ist. Damit eine Windows 7-VM auf Citrix Hypervisor unterstützt wird, stellen Sie sicher, dass SP1 oder höher installiert ist.

Windows 8

Windows 8-Gäste werden nicht mehr unterstützt. Wenn Sie eine Windows 8-VM installieren, wird sie auf Windows 8.1 aktualisiert.

Windows Server 2008 R2

Microsoft unterstützt nur die Verwendung von Windows Server 2008 R2, wenn Service Pack 1 installiert ist. Damit eine Windows Server 2008 R2-VM auf Citrix Hypervisor unterstützt wird, stellen Sie sicher, dass SP1 oder höher installiert ist.

Kopiert!
Failed!

Linux-VMs

October 16, 2019

Wenn Sie eine Linux-VM erstellen möchten, erstellen Sie die VM mit einer Vorlage für das Betriebssystem, das Sie auf der VM ausführen möchten. Sie können eine Vorlage verwenden, die Citrix Hypervisor für Ihr Betriebssystem bereitstellt, oder eine Vorlage, 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:**
>
> Führen Sie die folgenden Schritte aus, um eine VM eines neueren kleineren Updates einer RHEL-Version zu erstellen, als für die Installation von Citrix Hypervisor unterstützt wird:
>
> - Installieren von den neuesten unterstützten Medien
> - Verwenden`yum update`, um die VM auf dem neuesten Stand zu bringen
>
> Dieser Prozess gilt auch für RHEL-Derivate wie CentOS und Oracle Linux.

Es wird empfohlen, die Citrix VM Tools unmittelbar nach der Installation des Betriebssystems zu installieren. Weitere Informationen finden Sie unter Installieren des Linux-Gast-Agents. Bei einigen Betriebssystemen enthalten die Citrix VM-Tools einen für Citrix Hypervisor spezifischen Kernel, der den vom Hersteller bereitgestellten Kernel ersetzt. Andere Betriebssysteme wie RHEL 5.x erfordern die Installation einer bestimmten Version eines vom Hersteller bereitgestellten Kernels.

Die Übersicht zum Erstellen einer Linux-VM lautet wie folgt:

1. Erstellen Sie die VM für Ihr Zielbetriebssystem mithilfe von XenCenter oder der CLI.
2. Installieren Sie das Betriebssystem mit dem Installationsmedium des Herstellers.
3. Installieren Sie die Citrix VM-Tools (empfohlen).
4. Konfigurieren Sie die korrekte Zeitzone auf der VM und VNC wie in einer normalen nicht-virtuellen Umgebung.

Citrix Hypervisor unterstützt die Installation vieler Linux-Distributionen als VMs. Es gibt drei Installationsmechanismen:

- Installieren von einem Internet-Repository
- Installation von einer physischen CD
- Installation von einer ISO-Bibliothek

> **Warnhinweis:**
>
> Die Vorlage **Andere Installationsmedien richtet** sich an fortgeschrittene Benutzer, die ver-

> suchen möchten, VMs zu installieren, auf denen nicht unterstützte Betriebssysteme ausgeführt werden. Citrix Hypervisor wurde getestet, wenn nur die unterstützten Distributionen und spezifischen Versionen ausgeführt werden, die von den standardmäßigen Vorlagen abgedeckt werden. VMs, die mit der Vorlage **Andere Installationsmedien installiert** wurden, werden *nicht* unterstützt.
>
> VMs, die mit der Vorlage **Andere Installationsmedien** erstellt wurden, werden als HVM-Gäste erstellt. Dieses Verhalten kann bedeuten, dass einige Linux-VMs langsamer emulierte Geräte anstelle der leistungsstärkeren E/A-Treiber verwenden.

Hinweise zu bestimmten Linux-Distributionen finden Sie unterInstallationshinweise für Linux-Distributionen.

PV-Linux-Distributionen

Die unterstützten PV-Linux-Distributionen sind:

- Debian Wheezy 7 (32-/64-Bit)
- Red Hat Enterprise Linux 5.x (32-/64-Bit)

  Unterstützt, vorausgesetzt, Sie verwenden den Kernel 5.4 oder höher.
- Red Hat Enterprise Linux 6.x (32-/64-Bit)
- CentOS 5.x (32-/64-Bit)
- CentOS 6.x (32-/64-Bit)
- Oracle Linux 5.x (32-/64-Bit)
- Oracle Linux 6.x (32-/64-Bit)
- Scientific Linux 6.6—6.9 (32-/64-Bit)
- SUSE Linux Enterprise Server 11 SP3, SP4 (32-/64-bit)
- SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64 Bit)
- SUSE Linux Enterprise Desktop 11 SP3 (64 Bit)
- SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64 Bit)
- NeoKylin Linux Advanced Server 6.5 (64-bit)
- NeoKylin Linux Advanced Server 7.2 (64-bit)

Andere PV-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.

Hinweise:

- Das Ausführen von 32-Bit-PV-Linux-VMs auf einem Host mit mehr als 128 GB Arbeitsspeicher wird nicht unterstützt.
- Die Hardwaresicherheitsfunktionen von Citrix Hypervisor können die Gesamtleistung von 32-Bit-PV-VMs reduzieren. Wenn sich dieses Problem auf Sie auswirkt, können Sie eine der folgenden Schritte ausführen:
  - Ausführen einer 64-Bit-Version der PV-Linux-VM
  - Boot Xen mit der`no-smep no-smap` Option.

  Wir empfehlen diese Option nicht, da sie die Tiefe der Sicherheit des Hosts verringern kann

HVM-Linux-Distributionen

Diese VMs können die Vorteile der x86-Virtual-Container-Technologien in neueren Prozessoren nutzen, um die Leistung zu verbessern. Netzwerk- und Speicherzugriff von diesen Gästen wird immer noch im PV-Modus betrieben, wobei Treiber verwendet werden, die in die Kernel integriert sind.

Die unterstützten HVM Linux-Distributionen sind:

- Debian Jessie 8 (32-/64-Bit)
- Debian Stretch 9 (32-/64-Bit)
- Red Hat Enterprise Linux 7.x (64-Bit)
- CentOS 7.x (64-Bit)
- Oracle Enterprise Linux 7.x (64-Bit)
- Scientific Linux 7.x (64-bit)
- SUSE Linux Enterprise Server 12 SP3 (64 Bit)
- SUSE Linux Enterprise Desktop 12 SP3 (64 Bit)
- SUSE Linux Enterprise Server 15 (64 Bit)
- SUSE Linux Enterprise Desktop 15 (64 Bit)
- Ubuntu 14.04 (32-/64-bit)
- Ubuntu 16.04 (32-/64-bit)
- Ubuntu 18.04 (64-bit)
- CoreOS-Stable (64-Bit)

Andere HVM-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 durch die Installation von einem Internet-Repository

Dieser Abschnitt zeigt die xe CLI-Prozedur für die Erstellung einer Linux-VM unter Verwendung eines Debian Squeeze-Beispiels, indem das Betriebssystem von einem Internet-Repository installiert wird.

1. Erstellen Sie eine VM aus der Debian Squeeze-Vorlage. Die UUID der VM wird zurückgegeben:

```
xe vm-install template=template-name new-name-label=squeeze-vm
```

2. Geben Sie das Installations-Repository an. Dieses Repository ist ein Debian-Spiegel mit den für die Installation des Basissystems erforderlichen Paketen und dem zusätzlichen, das Sie während des Debian-Installationsprogramms auswählen:

```
xe vm-param-set uuid=UUID other-config:install-repository=
    path_to_repository
```

   Ein Beispiel für einen gültigen Repository-Pfad ist,`http://ftp.xx.debian.org/debian` wo`xx` ist Ihr Ländercode (eine Liste dieser Codes finden Sie in der Debian-Spiegelliste). Bei mehreren Installationen empfehlen wir die Verwendung eines lokalen Spiegels oder eines apt-Proxys, um zu vermeiden, dass übermäßiger Netzwerkverkehr oder Last auf den zentralen Repositories generiert wird.

   > **Hinweis:**
   >
   > Das Debian-Installationsprogramm unterstützt nur HTTP und FTP apt Repos. NFS wird nicht unterstützt.

3. Suchen Sie die UUID des Netzwerks, mit dem Sie eine Verbindung herstellen möchten. Wenn es beispielsweise derjenige ist, der an *xenbr0*angehängt ist:

```
xe network-list bridge=xenbr0 --minimal
```

4. Erstellen Sie eine VIF, um die neue VM mit diesem Netzwerk zu verbinden:

```
xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random
    device=0
```

5. Starten Sie die VM. Es bootet direkt in den Debian-Installer:

```
xe vm-start uuid=UUID
```

6. Folgen Sie dem Debian-Installationsprogramm, um die VM in der von Ihnen gewünschten Konfiguration zu installieren.
7. Installieren Sie den Gast-Agent und konfigurieren Sie die grafische Anzeige. Weitere Informationen finden Sie unter Installieren des Linux-Gast-Agents.

Erstellen einer Linux-VM durch Installation von einer physischen CD oder DVD

In diesem Abschnitt wird das CLI-Verfahren zum Erstellen einer Linux-VM anhand eines Debian-Squeeze-Beispiels durch die Installation des Betriebssystems von einer physischen CD/DVD gezeigt.

1. Erstellen Sie eine VM aus der Debian Squeeze-Vorlage. Die UUID der VM wird zurückgegeben:

```
xe vm-install template=template-name new-name-label=vm-name
```

2. Holen Sie sich die UUID des Stammdatenträgers der neuen VM:

```
xe vbd-list vm-uuid=vm_uuid userdevice=0 params=uuid --minimal
```

3. Legen Sie mithilfe der zurückgegebenen UUID die Root-Festplatte so fest, dass sie nicht bootfähig ist:

```
xe vbd-param-set uuid=root_disk_uuid bootable=false
```

4. Rufen Sie den Namen des physischen CD-Laufwerks auf dem Citrix Hypervisor or-Server ab:

```
xe cd-list
```

   Das Ergebnis dieses Befehls gibt Ihnen etwas wie SCSI 0:0:0:0 für dasname-**label** Feld.

5. Fügen Sie der neuen VM eine virtuelle CD-ROM hinzu, indem Sie den Parameter des Citrix Hypervisor or-Server-CD-Laufwerks alsname-labelcd-name““ Parameter verwenden:

```
xe vm-cd-add vm=vm_name cd-name=”host_cd_drive_name_label” device
    =3
```

6. Holen Sie sich die UUID des VBD entsprechend dem neuen virtuellen CD-Laufwerk:

```
xe vbd-list vm-uuid=vm_uuid type=CD params=uuid --minimal
```

7. Machen Sie die VBD der virtuellen CD bootfähig:

```
xe vbd-param-set uuid=cd_drive_uuid bootable=true
```

8. Legen Sie das Installations-Repository der VM als CD-Laufwerk fest:

```
xe vm-param-set uuid=vm_uuid other-config:install-repository=cdrom
```

9. Legen Sie die Debian Squeeze-Installations-CD in das CD-Laufwerk des Citrix Hypervisor or-Servers ein.
10. Öffnen Sie eine Konsole für die VM mit XenCenter oder einem SSH-Terminal, und führen Sie die Schritte zum Ausführen der Betriebssysteminstallation durch.
11. Starten Sie die VM. Es bootet direkt in den Debian-Installer:

```
xe vm-start uuid=UUID
```


12. Installieren Sie die Gast-Dienstprogramme und konfigurieren Sie die grafische Anzeige. Weitere Informationen finden Sie unter Installieren des Linux-Gast-Agents.

Erstellen einer Linux-VM durch Installation von einem ISO-Image

In diesem Abschnitt wird das CLI-Verfahren zum Erstellen einer Linux-VM durch die Installation des Betriebssystems von einem netzwerkfähigen ISO beschrieben.

1. Führen Sie den Befehl aus

```
xe vm-install template=template new-name-label=name_for_vm sr-uuid
   =storage_repository_uuid
```

   Dieser Befehl gibt die UUID der neuen VM zurück.

2. Suchen Sie die UUID des Netzwerks, mit dem Sie eine Verbindung herstellen möchten. Wenn es beispielsweise derjenige ist, der an *xenbr0*angehängt ist:

```
xe network-list bridge=xenbr0 --minimal
```

3. Erstellen Sie eine VIF, um die neue VM mit diesem Netzwerk zu verbinden:

```
xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random
    device=0
```

4. Legen Sie den`install-repository` Schlüssel des`other-config` Parameters auf den Pfad Ihres Netzwerk-Repositorys fest. Um beispielsweise`http://mirror.centos.org/centos/6/os/x86_64` als URL der Herstellermedien zu verwenden:

```
xe vm-param-set uuid=vm_uuid other-config:install-repository=http:
   //mirror.centos.org/centos/6/os/x86_64
```

5. Starten der VM

```
xe vm-start uuid=vm_uuid
```

6. Stellen Sie mithilfe von XenCenter oder VNC eine Verbindung zur VM-Konsole her, und führen Sie die Betriebssysteminstallation durch.

Netzwerkinstallationshinweise

Mit dem Citrix Hypervisor Gastinstallationsprogramm können Sie ein Betriebssystem von einem auf das Netzwerk zugänglichen ISO-Image auf einer VM installieren. Um die Installation von einem ISO

vorzubereiten, erstellen Sie ein explodiertes Netzwerk-Repository Ihrer Herstellermedien (*nicht* ISO-Images). Exportieren Sie es über NFS, HTTP oder FTP, so dass es über die Administrationsoberfläche des Citrix Hypervisor or-Servers zugänglich ist.

Auf das Netzwerk-Repository muss über die Steuerdomäne des Citrix Hypervisor or-Servers zugegriffen werden, normalerweise über die Verwaltungsschnittstelle. Die URL muss auf die Basis des CD/DVD-Abbilds auf dem Netzwerkserver verweisen und die folgende Form haben:

- **HTTP:** `http://<server>/<path>`
- **FTP:** `ftp://<server>/<path>`
- **NFS:** `nfs://<server>/<path>`
- **NFS:** `nfs:<server>/<path>`

Weitere Informationen zur Vorbereitung einer netzwerkbasierten Installation finden Sie in den Installationsanweisungen Ihres Herstellers, z. B. wo Sie die ISO entpacken möchten.

> **Hinweis:**
>
> Verwenden Sie bei Verwendung der NFS-Installationsmethode von XenCenter immer den`nfs://` Pfadstil.

Beim Erstellen von VMs aus Vorlagen werden Sie vom XenCenter Assistenten für **neue VM** aufgefordert, die Repository-URL einzugeben. Wenn Sie die CLI verwenden, installieren Sie die Vorlage wie gewohnt mit`vm-install` und setzen Sie dann den`other-config:install-repository` Parameter auf den Wert der URL. Wenn die VM dann gestartet wird, wird die Netzwerkinstallation gestartet.

> **Warnhinweis:**
>
> Bei der Installation einer neuen Linux-basierten VM ist es wichtig, die Installation abzuschließen und neu zu starten, bevor Sie weitere Vorgänge ausführen. Dieser Vorgang ist analog dazu, eine Windows Installation nicht zu unterbrechen — was Ihnen eine nicht funktionierende VM überlassen würde.

Erweiterte Startparameter des Betriebssystems

Beim Erstellen einer virtuellen Maschine können Sie erweiterte Startparameter des Betriebssystems mithilfe von XenCenter oder der xe-CLI angeben. Die Angabe erweiterter Parameter kann hilfreich sein, wenn Sie beispielsweise automatisierte Installationen paravirtualisierter Gäste konfigurieren. Beispielsweise könnten Sie eine Debian-Preseed- oder RHEL-Kickstart-Datei wie folgt verwenden.

So installieren Sie Debian mithilfe einer Preseed Datei:

1. Erstellen Sie eine Vorabdatei. Informationen zum Erstellen von Preseed-Dateien finden Sie in der Debian-Dokumentation für Details.

2. Legen Sie die Kernel-Befehlszeile für die VM richtig fest, bevor Sie sie starten. Verwenden Sie den Assistenten für neue virtuelle Rechner in XenCenter, oder führen Sie einen xe-CLI-Befehl wie folgt aus:

```
xe vm-param-set uuid=uuid PV-args=preseed_arguments
```

So installieren Sie RHEL mithilfe einer Kickstart-Datei:

> **Hinweis:**
>
> Eine Red Hat Kickstart-Datei ist eine automatisierte Installationsmethode, ähnlich einer Antwortdatei, mit der Sie Antworten auf die RHEL-Installationsaufforderungen bereitstellen können. Um diese Datei zu erstellen, installieren Sie RHEL manuell. Die Kickstart-Datei befindet sich in `/root/anaconda-ks.cfg`.

1. Wählen Sie in XenCenter die entsprechende RHEL-Vorlage aus.
2. Geben Sie die Kickstart-Datei an, die als Kernel-Befehlszeilenargument im XenCenter Assistenten für neue VM verwendet werden soll. Geben Sie diesen Wert genau so an, wie er in der PXE-Konfigurationsdatei angegeben würde. Zum Beispiel:

```
ks=http://server/path ksdevice=eth0
```

3. Verwenden Sie in der Befehlszeile, `vm-param-set` um den `PV-args` Parameter für die Verwendung einer Kickstart-Datei festzulegen.

```
xe vm-param-set uuid=vm_uuid PV-args="ks=http://server/path
    ksdevice=eth0"
```

4. Legen Sie den Repository-Speicherort so fest, dass Citrix Hypervisor weiß, woher der Kernel und `initrd` vom Installationsprogramm gestartet werden soll:

```
xe vm-param-set uuid=vm_uuid other-config:install-repository=http:
    //server/path
```

> **Hinweis:**
>
> Wenn Sie eine Kickstart-Datei ohne den Assistenten für **neue VM** installieren möchten, können Sie dem Textfeld **Erweiterte Betriebssystemstartparameter** das entsprechende Argument hinzufügen.

Installieren des Linux-Gastagenten

Obwohl alle unterstützten Linux-Distributionen nativ paravirtualisiert sind (und keine speziellen Treiber für die volle Leistung benötigen), enthält Citrix Hypervisor einen Gast-Agent. Dieser Gastagent

stellt dem Host zusätzliche Informationen über die VM bereit. Installieren Sie den Gast-Agent auf jeder Linux-VM, um Dynamic Memory Control (DMC) zu aktivieren.

Es ist wichtig, den Linux-Gast-Agent beim Upgrade des Citrix Hypervisor or-Servers auf dem neuesten Stand zu halten. Weitere Informationen finden Sie unter Aktualisieren von Linux-Kernels und Gast-Dienstprogrammen.

> **Hinweis:**
>
> Stellen Sie vor der Installation des Gastagenten auf einem SUSE Linux Enterprise Desktop oder Server 15 Gast sicher, dass dieser auf dem Gast installiert `insserv-compat-0.1-2.15.noarch.rpm` ist.

So installieren Sie den Gast-Agent:

1. Die erforderlichen Dateien befinden sich auf dem integrierten`guest-tools.iso` CD-Image oder können alternativ installiert werden, indem Sie in XenCenter die Option **VMund Citrix VM Tools installieren** auswählen.
2. Hängen Sie das Bild auf den Gast ein, indem Sie den folgenden Befehl ausführen:

```
mount -o ro,exec /dev/disk/by-label/Citrix VM Tools /mnt
```

> **Hinweis:**
>
> Wenn das Mounten des Abbilds fehlschlägt, können Sie das Abbild folgendermaßen suchen:
>
> ```
> blkid -t label="Citrix VM-Tools "
> ```

3. Führen Sie das Installationsskript als Root-Benutzer aus:

```
/mnt/Linux/install.sh
```

4. Heben Sie die Bereitstellung des Abbilds vom Gast auf, indem Sie den folgenden Befehl ausführen:

```
umount /mnt
```

5. Wenn der Kernel aktualisiert wurde oder die VM von einer früheren Version aktualisiert wurde, starten Sie die VM jetzt neu.

> **Hinweis:**
>
> CD-ROM-Laufwerke und ISOs, die an virtuelle Linux-Maschinen angeschlossen sind, werden als Geräte angezeigt`/dev/xvdd` , z. B.`/dev/sdd` oder, anstatt`/dev/cdrom` wie erwartet. Dieses Verhalten liegt daran, dass es sich nicht um echte CD-ROM-Geräte, son-

> dern um normale Geräte handelt. Wenn Sie entweder XenCenter oder die CLI zum Auswerfen der CD verwenden, wird das Gerät von der VM abgezogen, und das Gerät wird ausgeblendet. In Windows VMs ist das Verhalten unterschiedlich, und die CD verbleibt in der VM in einem leeren Zustand.

Installationshinweise für Linux-Distributionen

In diesem folgenden Abschnitt werden herstellerspezifische Konfigurationsinformationen aufgeführt, die vor dem Erstellen der angegebenen Linux-VMs berücksichtigt werden müssen.

Ausführlichere Versionshinweise zu allen Distributionen finden Sie unterLinux VM Versionshinweise.

CentOS 5.x (32-/64-Bit)

Stellen Sie bei einer CentOS 5.x-VM sicher, dass das Betriebssystem den CentOS 5.4-Kernel oder höher verwendet, der vom Distributionshersteller verfügbar ist. Enterprise Linux-Kernelversionen vor 5.4 enthalten Probleme, die verhindern, dass Citrix Hypervisor VMs ordnungsgemäß ausgeführt werden. Aktualisieren Sie den Kernel mit dem normalen Kernel-Upgrade-Verfahren des Herstellers.

Red Hat Enterprise Linux 5.x (32-/64-Bit)

Stellen Sie bei RHEL 5.x-VMs sicher, dass das Betriebssystem den RHEL 5.4-Kernel (2.6.18-164.el5) oder höher verwendet, der vom Distributionshersteller verfügbar ist.
Enterprise Linux-Kernelversionen vor 5.4 enthalten Probleme, die verhindern, dass Citrix Hypervisor VMs ordnungsgemäß ausgeführt werden. Aktualisieren Sie den Kernel mit dem normalen Kernel-Upgrade-Verfahren des Herstellers.

Red Hat Enterprise Linux* 7.x (32-/64-bit)

Die neue Vorlage für diese Gäste gibt 2 GB RAM an. Diese Menge an RAM ist eine Voraussetzung für eine erfolgreiche Installation von v7.4 und höher. Für v7.0 - v7.3 gibt die Vorlage 2 GB RAM an, aber wie bei früheren Versionen von Citrix Hypervisor ist 1 GB RAM ausreichend.

> **Hinweis:**
>
> Diese Informationen gelten sowohl für Red Hat als auch für Red Hat Derivate.

Oracle Linux 5.x (32-/64-Bit)

Stellen Sie bei einer OEL 5.x-VM sicher, dass das Betriebssystem den OEL 5.4-Kernel oder höher verwendet, der vom Distributionshersteller verfügbar ist.

Enterprise-Linux-Kernelversionen vor 5.4 enthalten Probleme, die verhindern, dass Citrix Hypervisor VMs ordnungsgemäß ausgeführt werden. Aktualisieren Sie den Kernel mit dem normalen Kernel-Upgrade-Verfahren des Herstellers.

Für OEL 5.6 64-Bit unterstützt der Unbreakable Enterprise Kernel (UEK) die Xen Plattform nicht. Wenn Sie versuchen, UEK mit diesem Betriebssystem zu verwenden, kann der Kernel nicht ordnungsgemäß gestartet werden.

Oracle Linux 6.9 (64-Bit)

Bei OEL 6.9 VMs mit mehr als 2 GB Arbeitsspeicher legen Sie den Boot-Parameter fest, `crashkernel=no` um den Absturzkernel zu deaktivieren. Die VM wird nur erfolgreich neu gestartet, wenn dieser Parameter festgelegt ist. Wenn Sie eine frühere Version von OEL 6.x verwenden, setzen Sie diesen Startparameter, bevor Sie auf OEL 6.9 aktualisieren.

Um den Parameter mithilfe von XenCenter festzulegen, fügen Sie ihn dem Feld **Erweiterte Betriebssystemstartparameter** auf der Seite **Installationsmedien** des Assistenten **Neue VM** hinzu.

Um eine vorhandene VM mithilfe von XenCenter zu ändern, klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie **Eigenschaften > Startoptionen > Betriebssystemstartparameter**.

Debian 6.0 (Squeeze) (32-/64-bit)

Wenn in XenCenter eine private Spiegelung angegeben wird, wird diese Spiegelung nur zum Abrufen des Installationskernel verwendet. Wenn das Installationsprogramm ausgeführt wird, müssen Sie erneut die Adresse des Spiegels eingeben, der für den Paketabruf verwendet werden soll.

Debian 7 (Wheezy) (32-/64-Bit)

Wenn in XenCenter eine private Spiegelung angegeben wird, wird diese Spiegelung nur zum Abrufen des Installationskernel verwendet. Wenn das Installationsprogramm ausgeführt wird, müssen Sie erneut die Adresse des Spiegels eingeben, der für den Paketabruf verwendet werden soll.

Apt-Repositories (Debian)

Bei seltenen oder einmaligen Installationen ist es sinnvoll, einen Debian-Spiegel direkt zu verwenden. Wenn Sie jedoch mehrere VM-Installationen durchführen möchten, empfehlen wir, einen Caching-Proxy oder einen lokalen Spiegel zu verwenden. Beide der folgenden Tools können in einer VM installiert werden.

- `Apt-cacher`: Eine Implementierung des Proxy-Servers, der einen lokalen Cache von Paketen aufbewahrt
- `debmirror`: Ein Tool, das einen teilweisen oder vollständigen Spiegel eines Debian-Repositorys erstellt

Vorbereiten des Klonvorbereitung einer Linux-VM

Wenn Sie eine VM oder einen Computer klonen, werden in der Regel Attribute, die für diesen Computer eindeutig sind, in Ihren Umgebungen dupliziert, sofern Sie das geklonte Image nicht generalisieren. Einige der eindeutigen Attribute, die beim Klonen dupliziert werden, sind die IP-Adresse, die SID oder die MAC-Adresse.

Daher ändert Citrix Hypervisor beim Klonen einer Linux-VM automatisch einige Parameter der virtuellen Hardware. Wenn Sie die VM mit XenCenter kopieren, ändert XenCenter automatisch die MAC-Adresse und die IP-Adresse für Sie. Wenn diese Schnittstellen dynamisch in Ihrer Umgebung 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 zu machen. Anweisungen zu bestimmten unterstützten Linux-Distributionen finden Sie unterLinux VM Versionsh-inweise.

Computername

Eine geklonte VM ist ein anderer Computer, und wie jeder neue Computer in einem Netzwerk muss sie einen eindeutigen Namen innerhalb der Netzwerkdomäne haben.

IP-Adresse

Eine geklonte VM muss über eine eindeutige IP-Adresse innerhalb der Netzwerkdomäne verfügen, zu der sie gehört. Im Allgemeinen ist diese Anforderung kein Problem, wenn DHCP verwendet wird, um Adressen zuzuweisen. Wenn die VM gestartet wird, weist der DHCP-Server ihr eine IP-Adresse zu. Wenn die geklonte VM eine statische IP-Adresse hatte, muss dem Klon eine nicht verwendete IP-Adresse zugewiesen werden, bevor er gestartet wird.

MAC-Adresse

Es gibt zwei Situationen, in denen wir empfehlen, 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. Beim Klonen einer virtuellen Maschine weist XenCenter der neuen geklonten VM jedoch eine andere MAC-Adresse zu. Wenn die neue VM zum ersten Mal gestartet wird, erkennt das Netzwerk die neue VM und wird nicht automatisch angezeigt.

2. Einige Linux-Distributionen verwendenudev Regeln, um die MAC-Adresse jeder Netzwerkschnittstelle zu speichern und einen Namen für diese Schnittstelle beizubehalten. Dieses Verhalten ist so vorgesehen, dass die gleiche physische NIC immer der gleichen*eth n-Schnittstelle*zugeordnet wird, was bei Wechsel-Netzwerkkarten (wie Laptops) nützlich ist. Dieses Verhalten ist jedoch im Kontext von VMs problematisch.

   Betrachten Sie beispielsweise das Verhalten im folgenden Fall:

   ```
   1.  Konfigurieren von zwei virtuellen Netzwerkkarten bei der
      Installation einer VM
   1. VM herunterfahren
   1.  Entfernen der ersten NIC
   ```

   Wenn die VM neu gestartet wird, zeigt XenCenter nur eine Netzwerkkarte an, ruft sie aber aufeth0. Inzwischen zwingt die VM bewusst diese NIC zu seineth1. Das Ergebnis ist, dass die Vernetzung nicht funktioniert.

Deaktivieren Sie für VMs, die persistente Namen verwenden, diese Regeln vor dem Klonen. Wenn Sie persistente Namen nicht deaktivieren 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 von Linux-Kernels und Gast-Dienstprogrammen

Die Linux-Gast-Dienstprogramme können aktualisiert werden, indem dasLinux/install.sh Skript vom integriertenguest-tools.iso CD-Image erneut ausgeführt wird (sieheInstallieren des Linux-Gast-Agents).

Füryum-aktivierte Distributionen CentOS 5.x, RHEL 5.x und höherxe-guest-utilitiesinstalliert eineyumKonfigurationsdatei, um nachfolgende Aktualisierungen mit yumin der Standardweise.

Für Debian/etc/apt/sources.list wird standardmäßig aufgefüllt, um Aktualisierungen mit apt zu aktivieren.

Beim Upgrade wird empfohlen, dass Sie immer erneut ausführenLinux/install.sh. Dieses Skript bestimmt automatisch, ob Ihre VM Updates benötigt, und wird bei Bedarf installiert.

Upgrade auf Ubuntu 14.04, RHEL 7 und CentOS 7 Gäste

Um *vorhandene* Linux-Gäste auf Versionen zu aktualisieren, die im **HVM-Modus** betrieben werden (z. B. RHEL 7.x, CentOS 7.x und Ubuntu 14.04), führen Sie ein In-Gast-Upgrade durch. Zu diesem Zeitpunkt wird der aktualisierte Gast nur im PV-Modus ausgeführt - der nicht unterstützt wird und bekannte Probleme aufweist. Führen Sie das folgende Skript aus, um den neu aktualisierten Gast in den unterstützten HVM-Modus zu konvertieren.

Öffnen Sie auf dem Citrix Hypervisor or-Server eine lokale Shell, melden Sie sich als root an, und geben Sie den folgenden Befehl ein:

```
1 /opt/xensource/bin/pv2hvm vm_name
```

Oder

```
1 /opt/xensource/bin/pv2hvm vm_uuid
```

Starten Sie die VM neu, um den Vorgang abzuschließen.

Linux VM Versionshinweise

Die meisten modernen Linux-Distributionen unterstützen Xen Paravirtualisierung direkt, haben aber unterschiedliche Installationsmechanismen und einige Kernel-Einschränkungen.

Unterstützung für grafische Installation von RHEL

Um das grafische Installationsprogramm zu verwenden, führen Sie in XenCenter den Assistenten für **neue virtuelle Computer** durch. Fügen Sie auf der Seite **Installationsmedien** im Abschnitt **Erweiterte Betriebssystemstartparametervnc“** zu den Listenparametern hinzu:

```
1 graphical utf8 vnc
```

! [Ein Screenshot des Assistenten für neue VM. Auf der Seite Installationsmedien`graphical utf8 vnc` wird der Wert in das Feld Erweiterte Betriebssystemstartparameter eingegeben.] (/de-de/citrix-hypervisor/media/rhel-graphical-network-install.png)

Sie werden aufgefordert, Netzwerkkonfiguration für die neue VM bereitzustellen, um die VNC-Kommunikation zu aktivieren. Arbeiten Sie den Rest des Assistenten für neue VM. 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 startet zunächst im Textmodus und kann eine Netzwerkkonfiguration anfordern. Nach der Bereitstellung wird die Schaltfläche **Zur grafischen Konsole wechseln** in der oberen rechten Ecke des XenCenter Fensters angezeigt.

Red Hat Enterprise Linux 5

Citrix Hypervisor erfordert, dass Sie den RHEL 5.4 Kernel oder höher ausführen. Ältere Kernel haben die folgenden bekannten Probleme:

- RHEL 5.0 64-Bit-Gastbetriebssysteme mit ihren ursprünglichen Kerneln können unter Citrix Hypervisor 8.0 nicht gestartet werden. Bevor Sie versuchen, den Citrix Hypervisor or-Server auf Version 8.0 zu aktualisieren, aktualisieren Sie den Kernel auf Version 5.4 (2.6.18-164.el5xen) oder höher. Wenn Sie diese Gäste ausführen und Ihren Host bereits auf Citrix Hypervisor 8.0 aktualisiert haben, finden Sie weitere InformationenCTX134845zum Aktualisieren des Kernel.
- Wenn eine angehaltene VM fortgesetzt wird, können Zuweisungen vorgenommen werden, die Auslagerungsaktivitäten verursachen können, die nicht ausgeführt werden können, da der Auslagerungsdatenträger noch neu angeschlossen wird. Dieses Vorkommen ist selten. (Red Hat Problem429102).
- Wenn Sie RHEL 5.3 oder 5.4 (32/64-bit) ausführen, verwenden Sie nicht Dynamic Memory Control (DMC), da diese Funktion den Gast zum Absturz führen kann. Wenn Sie DMC verwenden möchten, empfehlen wir, ein Upgrade auf neuere Versionen von RHEL oder CentOS durchzuführen. [EXT-54]
- In RHEL 5.3 gibt es manchmal, wenn viele Geräte an eine VM angeschlossen sind, nicht genug Zeit für alle diese Geräte, um eine Verbindung herzustellen. In diesem Fall schlägt der Start fehl. [EXT-17]
- In RHEL 5.0—5.3 kann die Verwendung des XFS-Dateisystems unter außergewöhnlichen Umständen zu Kernel-Panik führen. Wenn Sie den Red Hat RHEL 5.4 Kernel weiter anwenden, wird dieses Problem behoben. [EXT-16]
- In RHEL 5.2, 5.3 können VMs abstürzen, wenn ein Host 64 GiB RAM oder höher konfiguriert hat. Wenn Sie den Red Hat RHEL 5.4 Kernel weiter anwenden, wird dieses Problem behoben. [EXT-30]
- In RHEL 5.0—5.3 enthält der Netzwerktreiber ein Problem, das in seltenen Fällen zu einem Kernel-Deadlock führen kann. Wenn Sie den Red Hat RHEL 5.4 Kernel weiter anwenden, wird dieses Problem behoben. [EXT-45]

> **Hinweis:**
>
> In früheren Versionen enthielt Citrix Hypervisor einen Ersatz-Kernel RHEL 5, der kritische Probleme behoben hat, durch die RHEL 5 nicht effektiv als virtuelle Maschine ausgeführt werden konnte. Red Hat hat diese Probleme in RHEL 5.4 und höher behoben. Daher enthält Citrix Hypervisor keinen spezifischen RHEL 5-Kernel mehr.

Bereiten Sie einen RHEL 5-Gast für das Klonen vor

Um einen RHEL 5.x-Gast für das Klonen vorzubereiten, bearbeiten Sie`/etc/sysconfig/network-scripts/ifcfg-eth0` vor dem Konvertieren der VM in eine Vorlage und entfernen Sie die`HWADDR` Zeile. Weitere Informationen finden Sie unter Vorbereiten des Klonvorbereitung einer Linux-VM.

> **Hinweis:**
>
> Red Hat empfiehlt die Verwendung von Kickstart, um automatisierte Installationen durchzuführen, anstatt Disk-Images direkt zu klonen (sieheRed Hat KB Artikel 1308).

Red Hat Enterprise Linux 6

> **Hinweis:**
>
> Red Hat Enterprise Linux 6.x enthält auch Red Hat Enterprise Linux Workstation 6.6 (64-Bit) und Red Hat Enterprise Linux Client 6.6 (64-Bit).

- Der RHEL 6.0-Kernel hat einen Fehler, der die Festplatten-E/A auf mehreren Virtualisierungsplattformen beeinflusst. Dieses Problem bewirkt, dass VMs, auf denen RHEL 6.0 ausgeführt wird, Interrupts verlieren. [Weitere Informationen finden Sie unter Red Hat Probleme681439[]und603938[]652262().]
- Versuche, ein Virtual Disk Image (VDI) von einer RHEL 6.1 und 6.2 (32-/64-Bit) VM zu trennen, sind möglicherweise nicht erfolgreich. Diese erfolglosen Versuche führen zu einem Gast-Kernel-Absturz mit einer`NULL pointer dereference at <xyz>` Fehlermeldung. Aktualisieren Sie den Kernel auf Version 6.3 (2.6.32-238.el6) oder höher, um dieses Problem zu beheben. Weitere Informationen finden Sie unter Red Hat Ausgabe 773219.

Red Hat Enterprise Linux 7

Nach der Migration oder dem Anhalten der VM können RHEL 7.x-Gäste während des Lebenslaufs einfrieren. Weitere Informationen finden Sie unter Red Hat Problem1141249.

CentOS 5

Eine Liste der CentOS 5.x-Versionshinweise finden Sie unterRed Hat Enterprise Linux 5.

CentOS 6

Eine Liste der CentOS 6.x-Versionshinweise finden Sie unterRed Hat Enterprise Linux 6.

CentOS 7

Eine Liste der CentOS 7.x-Versionshinweise finden Sie unterRed Hat Enterprise Linux 7.

Oracle Linux 5

Eine Liste der Versionshinweise zu Oracle Linux 5.x finden Sie unterRed Hat Enterprise Linux 5.

Oracle Linux 6

Oracle Linux 6.x-Gäste, die auf einem Host installiert sind, auf dem Versionen vor v6.5 ausgeführt werden, führen den Red Hat Kernel nach einem Upgrade auf v6.5 weiter aus. Um zum UEK-Kernel zu wechseln (standardmäßig mit einer sauberen Installation), löschen Sie die`/etc/pygrub/rules.d/oracle-5.6` Datei in dom0. Sie können auswählen, welcher Kernel für eine einzelne VM verwendet werden soll, indem Sie die Bootloader-Konfiguration innerhalb der VM bearbeiten.

Bei OEL 6.9 VMs mit mehr als 2 GB Arbeitsspeicher legen Sie den Boot-Parameter fest, `crashkernel=no` um den Absturzkernel zu deaktivieren. Die VM wird nur erfolgreich neu gestartet, wenn dieser Parameter festgelegt ist. Wenn Sie eine frühere Version von OEL 6.x verwenden, setzen Sie diesen Startparameter, bevor Sie auf OEL 6.9 aktualisieren. Weitere Informationen finden Sie unter Installationshinweise für Linux-Distributionen

Eine Liste der Versionshinweise zu Oracle Linux 6.x finden Sie unterRed Hat Enterprise Linux 6.

Oracle Linux 7

Eine Liste der Versionshinweise zu Oracle Linux 7.x finden Sie unterRed Hat Enterprise Linux 7.

Wissenschaftliches Linux 6

Eine Liste der Versionshinweise für Scientific Linux 6.x finden Sie unterRed Hat Enterprise Linux 6.

Wissenschaftliches Linux 7

Eine Liste der Versionshinweise für Scientific Linux 7.x finden Sie unterRed Hat Enterprise Linux 7.

SUSE Linux Enterprise 12

SUSE Linux Enterprise 12 VMs werden standardmäßig in den folgenden Modi unterstützt:

PV-Modus:

- SUSE Linux Enterprise Desktop 12, 12 SP1 und 12 SP2
- SUSE Linux Enterprise Server 12, 12 SP1 und 12 SP2

HVM-Modus:

- SUSE Linux Enterprise Desktop 12 SP3
- SUSE Linux Enterprise Server 12 SP3

SLES-Gast für das Klonen vorbereiten

> **Hinweis:**
>
> Bevor Sie einen SLES-Gast für das Klonen vorbereiten, müssen Sie die`udev` Konfiguration für Netzwerkgeräte wie folgt löschen:
>
> ```
> 1 cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
> ```

So bereiten Sie einen SLES-Gast auf das Klonen vor:

1. Öffnen Sie die Datei`/etc/sysconfig/network/config`
2. Bearbeiten Sie die Zeile, die lautet:

   ```
   1 FORCE_PERSISTENT_NAMES=yes
   ```

   Zu

   ```
   1 FORCE_PERSISTENT_NAMES=no
   ```

3. Speichern Sie die Änderungen und starten Sie die VM neu.

Weitere Informationen finden Sie unter Vorbereiten des Klonvorbereitung einer Linux-VM.

Ubuntu 14.04

Versuche, einen PV-Gast zu starten, können dazu führen, dass der Gast mit dem folgenden Fehler abstürzt:`kernel BUG at /build/buildd/linux-3.13.0/arch/x86/kernel/paravirt.c :239!`. Dieser Fehler wird beim unsachgemäßen Aufruf einer nicht-atomaren Funktion aus dem Interrupt-Kontext verursacht. Aktualisieren Sie das Paket linux-image auf Version 3.13.0-35.62, um dieses Problem zu beheben. Weitere Informationen finden Sie unter Ubuntu Launchpad1350373.

Kopiert!
Failed!

VM-Speicher

October 16, 2019

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 Citrix Hypervisor Umgebung zu verbessern. DMC ist eine Speicherverwaltungsfunktion, die eine dynamische Neuzuweisung von Speicher zwischen VMs ermöglicht.

XenCenter bietet eine grafische Anzeige der Speichernutzung auf der Registerkarte „ **Speicher** “. Weitere Informationen finden Sie in der XenCenter Hilfe.

Dynamic Memory Control (DMC) bietet folgende Vorteile:

- Sie können Speicher hinzufügen oder löschen, ohne die VMs neu zu starten, was dem Benutzer eine nahtlose Erfahrung bietet.
- Wenn die Server voll sind, können Sie mit DMC mehr VMs auf diesen Servern starten, wodurch der Arbeitsspeicher, der den ausgeführten VMs zugewiesen wird, proportional reduziert wird.

Was ist Dynamic Memory Control (DMC)?

Citrix Hypervisor DMC passt automatisch den Arbeitsspeicher ausgeführter VMs an, wobei die Speichermenge, die jeder VM zugewiesen wird, zwischen festgelegten Mindest- und Maximalspeicherwerten bleibt, die Leistung garantiert und eine größere Dichte von VMs pro Server ermöglicht wird.

Wenn ein Server voll ist, schlägt das Starten zusätzlicher VMs ohne DMC fehl und „Out of Memory“ -Fehler. Um die vorhandene VM-Speicherzuweisung zu reduzieren und Platz für weitere VMs zu schaffen, bearbeiten Sie die Speicherzuweisung jeder VM, und starten Sie die VM neu. Bei Verwendung von DMC versucht Citrix Hypervisor, Speicher zurückzufordern, indem die aktuelle Speicherzuweisung ausgeführter VMs innerhalb ihrer definierten Speicherbereiche automatisch reduziert wird. Citrix Hypervisor versucht, Speicher zurückzugeben, selbst wenn der Server voll ist.

> **Hinweis:**
>
> Dynamic Memory Control wird nicht von VMs unterstützt, die über eine virtuelle GPU verfügen.

Das Konzept des Dynamikbereiches

Für jede VM kann der Administrator einen dynamischen Speicherbereich festlegen. Der dynamische Speicherbereich ist der Bereich, innerhalb dessen Speicher der VM hinzugefügt oder entfernt werden kann, ohne dass ein Neustart erforderlich ist. Wenn eine VM ausgeführt wird, kann der Administrator den Dynamikbereich anpassen. Citrix Hypervisor garantiert immer, dass der VM zugewiesene Arbeitsspeicher innerhalb des dynamischen Bereichs bleibt. Daher kann Citrix Hypervisor dazu führen, dass die VM zugewiesene Speichermenge angepasst wird, während die VM ausgeführt wird. Der extremste Fall ist, dass der Administrator die dynamische Min/Max auf den gleichen Wert setzt und Citrix Hypervisor dazu zwingt, sicherzustellen, dass diese Menge an Arbeitsspeicher der VM zugewiesen wird. Wenn neue VMs auf „vollen“ Servern gestartet werden müssen, wird der Arbeitsspeicher für ausgeführte VMs „gequetscht“, um neue zu starten. Der erforderliche zusätzliche Speicher wird erhalten, indem die vorhandenen laufenden VMs proportional innerhalb ihrer vordefinierten Dynamikbereiche quetscht werden.

Mit DMC können Sie dynamische Mindest- und Maximalspeicherstufen konfigurieren und einen Dynamic Memory Range (DMR) erstellen, in dem die VM arbeitet.

- Dynamischer Mindestspeicher: Eine niedrigere Speichergrenze, die Sie der VM zuweisen.
- Dynamic Higher Limit: Eine obere Speichergrenze, die Sie der VM zuweisen.

Wenn der dynamische Mindestspeicher beispielsweise auf 512 MB festgelegt wurde und der dynamische Maximalspeicher auf 1.024 MB festgelegt wurde, erhält der VM einen Dynamic Memory Range (DMR) von 512 bis 1024 MB, innerhalb dessen er arbeitet. Citrix Hypervisor *garantiert* , dass jeder VM-Speicher innerhalb der angegebenen DMR bei Verwendung von DMC immer zugewiesen wird.

Das Konzept der statischen Reichweite

Viele von Citrix Hypervisor unterstützte Betriebssysteme verstehen den Begriff des dynamischen Hinzufügens oder Löschens von Arbeitsspeicher nicht vollständig. Daher muss Citrix Hypervisor die maximale Speichermenge deklarieren, die eine VM zum Zeitpunkt des Neustarts benötigt. Durch die Deklaration der maximalen Speichermenge kann das Gastbetriebssystem seine Seitentabellen und andere Speicherverwaltungsstrukturen entsprechend skalieren. Dies führt das Konzept eines statischen Speicherbereichs innerhalb von Citrix Hypervisor ein. Der statische Speicherbereich kann nicht angepasst werden, wenn die VM ausgeführt wird. Bei einem bestimmten Boot wird der Dynamikbereich so eingeschränkt, dass er immer innerhalb dieses statischen Bereichs enthalten ist. Das statische Minimum (die untere Grenze des statischen Bereichs) schützt den Administrator und ist auf die niedrigste Speichermenge festgelegt, die das Betriebssystem mit Citrix Hypervisor ausführen kann.

> **Hinweis:**
>
> Es wird empfohlen, die statische Mindeststufe nicht zu ändern, da die statische Mindeststufe auf der unterstützten Stufe pro Betriebssystem festgelegt ist. Weitere Informationen finden Sie in der Tabelle Speichereinschränkungen.
>
> 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

Automatische VM-Quetschung

- Wenn DMC nicht aktiviert ist und die Hosts voll sind, schlagen neue VM-Starter mit Fehlern „außerhalb des Arbeitsspeichers“ fehl.
- Wenn DMC aktiviert ist, selbst wenn Hosts voll sind, versucht Citrix Hypervisor, Speicher zurückzufordern, indem die Speicherzuweisung ausgeführter VMs innerhalb ihrer definierten dynamischen Bereiche reduziert wird. Auf diese Weise werden ausgeführte VMs proportional im gleichen Abstand zwischen dem dynamischen Minimum und dem dynamischen Maximum für alle VMs auf dem Host gequetscht.

Wenn DMC aktiviert ist

- Wenn der Speicher des Hosts reichlich vorhanden ist, erhalten alle laufenden VMs ihre dynamische Maximalspeicherstufe
- Wenn der Speicher des Hosts knapp ist, erhalten alle ausgeführten VMs ihre dynamische Mindestspeicherstufe.

Denken Sie beim Konfigurieren von DMC daran, dass die Zuweisung nur einer kleinen Menge Speicher zu einer VM negativ beeinflussen kann. Beispiel: Zuweisen zu wenig Speicher:

- Die Verwendung von Dynamic Memory Control, um den physischen Speicher zu reduzieren, der einer VM zur Verfügung steht, kann dazu führen, dass er langsam neu gestartet wird. Wenn Sie einer VM zu wenig Speicher zuweisen, kann diese langsam gestartet werden.
- Das Festlegen des minimalen dynamischen Arbeitsspeichers für eine zu niedrige VM kann zu Leistungsproblemen oder Stabilitätsproblemen führen, wenn die VM gestartet wird.

Wie funktioniert DMC?

Mit DMC ist es möglich, einen virtuellen Gastcomputer in einem von zwei Modi zu betreiben:

1. **Zielmodus:** Der Administrator gibt ein Speicherziel für den Gast an. Citrix Hypervisor passt die Speicherzuweisung des Gastes an das Ziel an. Die Angabe eines Ziels ist in virtuellen

Serverumgebungen und in Situationen nützlich, in denen Sie genau wissen, wie viel Speicher ein Gast verwenden soll. Citrix Hypervisor passt die Speicherzuweisung des Gastes an das angegebene Ziel an.

2. **Dynamischer Bereichsmodus:** Der Administrator gibt einen dynamischen Speicherbereich für den Gast an. Citrix Hypervisor wählt ein Ziel aus dem Bereich aus und passt die Speicherzuweisung des Gastes an das Ziel an. Das Angeben eines dynamischen Bereichs ist in virtuellen Desktopumgebungen und in allen Situationen nützlich, in denen Citrix Hypervisor den Hostspeicher dynamisch neu partitionieren soll, wenn sich die Anzahl der Gäste ändert oder der Druck des Hostspeichers ändert. Citrix Hypervisor wählt ein Ziel innerhalb des Bereichs aus und passt die Speicherzuweisung des Gastes an das Ziel an.

> **Hinweis:**
>
> Für jeden laufenden Gast ist es jederzeit möglich, zwischen Ziel- und Dynamikbereichsmodus zu wechseln. Geben Sie ein neues Ziel oder einen neuen Dynamikbereich an, und Citrix Hypervisor kümmert sich um den Rest.

Speicherbeschränkungen

Mit Citrix Hypervisor können Administratoren alle Speichersteuerungsvorgänge mit jedem Gastbetriebssystem verwenden. Citrix Hypervisor erzwingt jedoch die folgende Sortierbeschränkung für Speichereigenschaft für alle Gäste:

```
0 memory-static-min memory-dynamic-min memory-dynamic-max memory-static-max
```

Citrix Hypervisor ermöglicht Administratoren, Gastspeichereigenschaften auf Werte zu ändern, die diese Einschränkung erfüllen, vorbehaltlich einer Überprüfung. Zusätzlich zu der vorherigen Einschränkung unterstützen wir jedoch nur bestimmte Gastspeicherkonfigurationen für jedes unterstützte Betriebssystem. Der Umfang der unterstützten Konfigurationen hängt vom verwendeten Gastbetriebssystem ab. Citrix Hypervisor hindert Administratoren nicht daran, Gäste so zu konfigurieren, dass sie das unterstützte Limit überschreiten. Kunden werden jedoch empfohlen, Speichereigenschaften innerhalb der unterstützten Grenzen zu halten, um Performance- oder Stabilitätsprobleme zu vermeiden. Ausführliche Richtlinien zu den minimalen und maximalen Speicherlimits für jedes unterstützte Betriebssystem finden Sie unterUnterstützung für Gastbetriebssysteme.

> **Warnhinweis:**
>
> Bei der Konfiguration des Gastspeichers empfehlen wir, die maximale Menge an physischem Speicher, die von Ihrem Betriebssystem adressierbar ist, NICHT zu überschreiten. Wenn Sie ein Speichermaximum festlegen, das größer als das vom Betriebssystem unterstützte Limit ist, kann es zu Stabilitätsproblemen innerhalb Ihres Gastes kommen.

> Das dynamische Minimum muss größer oder gleich einem Viertel des statischen Maximums für alle unterstützten Betriebssysteme sein. Die Untergrenze unterhalb des dynamischen Minimums kann auch zu Stabilitätsproblemen führen. Administratoren werden aufgefordert, die Größe ihrer VMs sorgfältig zu kalibrieren und sicherzustellen, dass ihre Arbeitsgruppe von Anwendungen auf dynamischem Minimum zuverlässig funktioniert.

xe CLI-Befehle

Anzeigen der statischen Speichereigenschaften einer VM

1. Suchen Sie die uuid der erforderlichen VM:

```
xe vm-list
```

2. Notieren Sie sich die uuid, und führen Sie dann den Befehl`param-name=memory-static`

```
xe vm-param-get uuid=uuid param-name=memory-static-{
 min,max }
```

Im Folgenden werden beispielsweise die statischen Maximalspeichereigenschaften für die VM mit der uuid beginnend ec77 angezeigt:

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-static-max;
    268435456
```

Das Beispiel zeigt, dass der statische maximale Arbeitsspeicher für diese VM 268.435.456 Byte (256 MB) beträgt.

Anzeigen der dynamischen Speichereigenschaften einer VM

Um die dynamischen Speichereigenschaften anzuzeigen, gehen Sie wie oben beschrieben vor, verwenden Sie jedoch den Befehl`param-name=memory-dynamic`:

1. Suchen Sie die uuid der erforderlichen VM:

```
xe vm-list
```

2. Notieren Sie sich die uuid, und führen Sie dann den Befehl aus`param-name=memory-dynamic`:

```
xe vm-param-get uuid=uuid param-name=memory-dynamic-{
 min,max }
```


Im Folgenden werden beispielsweise die dynamischen maximalen Speichereigenschaften für die VM mit uuid ab ec77 angezeigt.

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-dynamic-max;
    134217728
```

Das Beispiel zeigt, dass der dynamische maximale Arbeitsspeicher für diese VM 134.217.728 Byte (128 MB) beträgt.

Speichereigenschaften aktualisieren

> **Warnhinweis:**
>
> Verwenden Sie die korrekte Reihenfolge, wenn Sie die statischen/dynamischen Minimum/Maximum-Parameter festlegen. 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=valuemax=value
```

Aktualisieren Sie den dynamischen Speicherbereich einer virtuellen Maschine:

```
xe vm-memory-dynamic-range-set \
      uuid=uuid min=value \
      max=value
```

Die Angabe eines Ziels ist in virtuellen Serverumgebungen und in jeder Situation nützlich, in der Sie genau wissen, wie viel Speicher ein Gast verwenden soll. Citrix Hypervisor passt die Speicherzuweisung des Gastes an das angegebene Ziel an. Zum Beispiel:

```
xe vm-target-set target=value vm=vm-name
```

Aktualisieren Sie alle Speichergrenzen (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
```


> **Hinweise:**
>
> - Um einer virtuellen Maschine eine bestimmte Menge Speicher zuzuweisen, die sich nicht ändert, legen Sie Dynamisches Maximum und Dynamisches 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

> **Warnhinweis:**
>
> Ändern Sie die statische Mindeststufe nicht, 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
```

2. Notieren Sie sich die uuid, und verwenden Sie dann den Befehl`memory-dynamic-{ min,max } =value`

```
xe vm-param-set uuid=uuidmemory-dynamic-{
 min,max }
 =value
```

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
```

Kopiert!
Failed!

Migrieren von VMs

October 16, 2019

Sie können ausgeführte VMs mithilfe von *Livemigration und Speicher-Livemigration**migrieren* und ein VMs Virtual Disk Image (VDI) ohne Ausfallzeiten von virtuellen Rechnern verschieben.

Livemigration und Livemigration von Speicher

In den folgenden Abschnitten werden die Kompatibilitätsanforderungen und Einschränkungen der Livemigration und der Livemigration von Speicher beschrieben.

Live-Migration

Die Live-Migration ist in allen Versionen von Citrix Hypervisor verfügbar. Mit dieser Funktion können Sie eine ausgeführte VM von einem Host auf einen anderen Host verschieben, wenn sich die VMs auf einem von beiden Hosts gemeinsam genutzten Speicher befinden. Pool-Wartungsfunktionen wie Hochverfügbarkeit und Rolling Pool Upgrade (RPU) können VMs automatisch mithilfe der Live-Migration verschieben. Diese Funktionen ermöglichen die Ausgleichung der Arbeitslasten, die Ausfallsicherheit der Infrastruktur und das Upgrade der Serversoftware ohne Ausfallzeiten der virtuellen Rechner.

> **Hinweis:**
>
> Speicher kann nur zwischen Hosts im selben Pool freigegeben werden. Daher können VMs nur auf Hosts im selben Pool migriert werden.
>
> Virtuelle GPU und Intel GVT-G sind nicht mit Livemigration, Storage Livemigration oder VM Suspend kompatibel. VMs, die GPU-Pass-Through oder vGPU verwenden, können jedoch weiterhin auf jedem Host gestartet werden, der über die entsprechenden Ressourcen verfügt. Hinweise zur NVIDIA vGPU Kompatibilität mit diesen Funktionen finden Sie unterGrafik.

Live-Migration von Massenspeicher

> **Hinweise:**
>
> - Verwenden Sie keine Storage-Livemigration in Citrix Virtual Desktops Bereitstellungen.
> - Storage-Livemigration kann nicht auf VMs verwendet werden, für die die Blockverfolgung aktiviert wurde. Deaktivieren Sie die geänderte Blockverfolgung, bevor Sie versuchen, die Livemigration zu speichern.
> - Storage-Livemigration kann nicht auf VMs verwendet werden, deren VDIs sich auf einem GFS2 SR befinden.

Die Massenspeicher-Livemigration ermöglicht außerdem, VMs von einem Host auf einen anderen zu verschieben, wobei sich die VMs nicht auf einem Speicher befinden, der zwischen den beiden Hosts gemeinsam genutzt wird. Daher können VMs, die auf dem lokalen Speicher gespeichert sind, ohne Ausfallzeiten migriert werden, und VMs können von einem Pool in einen anderen verschoben werden. Diese Funktion ermöglicht Systemadministratoren Folgendes:

- Neuverteilung von VMs zwischen Citrix Hypervisor Pools (z. B. von einer Entwicklungsumgebung zu einer Produktionsumgebung).

- Aktualisieren und Aktualisieren von eigenständigen Citrix Hypervisor or-Servern ohne Ausfallzeiten von VMs.
- Aktualisieren Sie die Hardware des Citrix Hypervisor or-Servers.

> **Hinweis:**
>
> Das Verschieben einer VM von einem Host auf einen anderen behält den *VM-Status*bei. Die Statusinformationen enthalten Informationen, die die VM und die historischen Leistungsmetriken definieren und identifizieren, z. B. CPU- und Netzwerkauslastung.

Kompatibilitätsanforderungen

Bei der Migration einer VM mit Livemigration oder Storage Livemigration müssen VM und der Zielhost die folgenden Kompatibilitätsanforderungen erfüllen, damit die Migration fortgesetzt werden kann:

- Auf dem Zielhost muss dieselbe oder eine neuere Version von Citrix Hypervisor als Quellhost installiert sein.
- Citrix VM Tools müssen auf jeder Windows VM installiert sein, die Sie migrieren möchten. Die auf der VM installierte Version von Citrix VM Tools muss mit der auf dem Citrix Hypervisor or-Zielserver installierten Version übereinstimmen.
- Nur Storage-Livemigration: Wenn die CPUs auf dem Quell- und Zielhost unterschiedlich sind, muss die Ziel-CPU mindestens den gesamten Featuresatz als Quell-CPU bereitstellen. Daher ist es unwahrscheinlich, dass eine VM zwischen AMD- und Intel-Prozessoren verschoben werden kann.
- VMs mit Checkpoint können nicht migriert werden.
- Nur Massenspeicher-Livemigration: VMs mit mehr als sechs angeschlossenen VDIs können nicht migriert werden.
- Der Zielhost muss über ausreichende Speicherkapazität verfügen oder über eine ausreichende Kapazität mit Dynamic Memory Control freigeben können. Wenn nicht genügend Arbeitsspeicher vorhanden ist, kann die Migration nicht abgeschlossen werden.
- Nur Massenspeicher-Livemigration: Der Zielspeicher muss genügend freier Festplattenspeicher für die eingehenden VMs zur Verfügung stehen. Der erforderliche freie Speicherplatz kann das Dreifache der VDI-Größe (ohne Snapshots) sein. Wenn nicht genügend Speicherplatz vorhanden ist, kann die Migration nicht abgeschlossen werden.

Einschränkungen und Vorbehalte

Live-Migration und Speicher-Livemigration unterliegen den folgenden Einschränkungen und Vorbehalte:

- VMs, die PCI-Pass-Through verwenden, können nicht migriert werden.
- Die VM-Leistung wird während der Migration reduziert.
- Bei der Massenspeicher-Livemigration deaktivieren Sie Pools, die durch hohe Verfügbarkeit geschützt sind, die hohe Verfügbarkeit, bevor Sie die VM-Migration versuchen.
- Die Zeit bis zum Abschluss der VM-Migration hängt vom Speicherbedarf der VM und ihrer Aktivität ab. Darüber hinaus wirken sich die Größe des VDI und seine Speicheraktivität auf VMs aus, die mit der Livemigration von Speicher migriert werden.
- IPv6-Linux-VMs benötigen einen Linux-Kernel größer als 3.0.

Migrieren einer virtuellen Maschine mit XenCenter

1. Wählen Sie im Bereich Ressourcen die VM aus, und führen Sie eine der folgenden Aktionen aus:
   - Um eine ausgeführte oder angehaltene VM mit Livemigration oder Storage Livemigration zu **migrieren, klicken Sie im Menü **VM** auf Zu Server**migrieren und dann VM migrieren** . Mit dieser Aktion wird der Assistent zum **Migrieren von virtuellen Rechnern** geöffnet.
   - So verschieben Sie eine gestoppte VM: Wählen Sie im Menü **VM** die Option **VM verschieben** aus. Mit dieser Aktion wird der Assistent zum **Verschieben von virtuellen Rechnern** geöffnet.
2. Wählen Sie in der Liste **Ziel** einen eigenständigen Server oder einen Pool aus.
3. Wählen Sie in der Liste **Home-Server** einen Server aus, der als Home-Server für die VM zugewiesen werden soll, und klicken Sie auf **Weiter** .
4. Geben Sie auf der Registerkarte **Speicher** das Speicher-Repository an, in dem die virtuellen Laufwerke der migrierten VM platziert werden sollen, und klicken Sie dann auf **Weiter** .
   - Das Optionsfeld **Alle migrierten virtuellen Laufwerke auf demselben SR platzieren** ist standardmäßig aktiviert und zeigt die standardmäßige freigegebene SR im Zielpool an.
   - Klicken Sie auf **Migrierte virtuelle Laufwerke auf bestimmte SRs platzieren** , um einen SR aus der Liste **Speicher-Repository** anzugeben. Mit dieser Option können Sie für jedes virtuelle Laufwerk auf der migrierten VM unterschiedliche SR auswählen.
5. Wählen Sie in der Liste **Speichernetzwerk** ein Netzwerk im Zielpool aus, das für die Live-Migration der virtuellen Laufwerke der VM verwendet wird. Klicken Sie auf **Weiter**.

   > **Hinweis:**

> Aus Leistungsgründen wird empfohlen, das Verwaltungsnetzwerk nicht für die Live-Migration zu verwenden.

6. Überprüfen Sie die Konfigurationseinstellungen, und klicken Sie auf **Fertig stellen** , um mit der Migration der VM zu beginnen.

Live-VDI-Migration

Mit der Live-VDI-Migration kann der Administrator das virtuelle Laufwerk (Virtual Disk Image, VDI) verschieben, 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.
- Verschieben zwischen Speicherstufen, wenn eine VM durch die Speicherkapazität begrenzt ist.
- Durchführung von Speicher-Array-Upgrades.

Einschränkungen und Vorbehalte

Live-VDI-Migration unterliegt den folgenden Einschränkungen und Vorbehalte

- Verwenden Sie keine Storage-Livemigration in Citrix Virtual Desktops Bereitstellungen.
- IPv6-Linux-VMs benötigen einen Linux-Kernel größer als 3.0.
- Wenn Sie Live-VDI-Migration auf einer VM mit einer vGPU durchführen, wird vGPU-Livemigration verwendet. Der Host muss über genügend vGPU -Speicherplatz verfügen, um eine Kopie der vGPU-Instanz auf dem Host zu erstellen. Wenn die PGPU voll eingesetzt sind, ist eine VDI-Migration möglicherweise nicht möglich.

So verschieben Sie virtuelle Laufwerke

1. Wählen Sie im Bereich **Ressourcen** die SR aus, in der das virtuelle Laufwerk 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 **Virtuelles Laufwerk verschieben** die Ziel-SR aus, in die Sie den VDI verschieben möchten.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass der SR genügend Speicherplatz für ein anderes virtuelles Laufwerk

> hat: Der verfügbare Speicherplatz wird in der Liste der verfügbaren SRs angezeigt.

4. Klicken Sie auf **Verschieben**, um das virtuelle Laufwerk zu verschieben.

Kopiert!
Failed!

Importieren und Exportieren von VMs

October 16, 2019

Mit Citrix Hypervisor können Sie VMs importieren und in verschiedene Formate exportieren. Mit dem XenCenter Importassistenten können Sie VMs aus Disk-Images (VHD und VMDK), Open Virtualization Format (OVF und OVA) und Citrix Hypervisor XVA-Format importieren. Sie können sogar VMs importieren, die auf anderen Virtualisierungsplattformen erstellt wurden, z. B. von VMware und Microsoft.

> **Hinweis:**
>
> Beim Importieren von VMs, die mit anderen Virtualisierungsplattformen erstellt wurden, konfigurieren oder *reparieren* Sie das Gastbetriebssystem, um sicherzustellen, dass es auf Citrix Hypervisor gestartet wird. Die Funktion „Betriebssystemfixup“ in XenCenter zielt darauf ab, diese grundlegende Interoperabilität bereitzustellen. Weitere Informationen finden Sie unter Betriebssystemfixup.

Mit dem XenCenter Export-Assistenten können Sie VMs in das Open Virtualization Format (OVF und OVA) und das Citrix Hypervisor XVA-Format exportieren.

Beim Importieren und Exportieren von VMs wird eine temporäre VM — die Transfer-VM — für den Import/Export von OVF/OVA-Paketen und Festplatten-Images verwendet. Konfigurieren Sie Netzwerkeinstellungen für die Übertragung von VM in den XenCenter Import- und Export-Assistenten. Weitere Informationen finden Sie unter Die Transfer-VM.

Sie können die xe-CLI auch verwenden, um VMs aus dem Citrix Hypervisor XVA-Format zu importieren und in das 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)	Imagedateien für virtuelle Festplatten (Virtual Hard Disk, VHD) und Virtual Machine Disk (VMDK) können mit dem Import-Assistenten importiert werden. Das Importieren eines Datenträgerabbilds ist möglicherweise sinnvoll, wenn ein virtuelles Datenträgerabbild verfügbar ist und keine OVF-Metadaten zugeordnet sind.
Citrix Hypervisor 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 lautet `.xva`.
Citrix Hypervisor XVA Version 1 Format	XVA Version 1 ist das Originalformat, das für XEN-basierte Hypervisoren spezifisch ist. Dieses Format packt eine einzelne VM als einzelnes Dateiarchiv, einschließlich eines Deskriptors und Disk-Images. Die Dateinamenerweiterung lautet `ova.xml`.

Welches Format soll verwendet werden?

Verwenden Sie das OVF/OVA-Format, um:

- Freigeben von Citrix Hypervisor 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
- Eine Lizenzvereinbarung einschließen
- Vereinfachen Sie die vApp-Verteilung durch Speichern eines OVF-Pakets in einer OVA-Datei

Verwenden Sie das XVA-Format, um:

- Freigeben von VMs mit Versionen von Citrix Hypervisor vor 6.0
- Importieren und Exportieren von VMs aus einem Skript mit einer CLI

Offenes Virtualisierungsformat (OVF und OVA)

OVF ist ein von der Distributed Management Task Force spezifizierter offener Standard für das 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 offene Virtualisierungsformat
- Open Virtualization Format-Spezifikation

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu importieren oder zu exportieren, müssen Sie als root angemeldet sein oder die Rolle Pooladministrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.

Ein **OVF-Paket** ist die Gruppe von Dateien, die 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. Sie kann auch andere Informationen angeben, darunter:

- Beschreibungen der virtuellen Laufwerke, des Pakets selbst und der Gastbetriebssysteme
- Eine Lizenzvereinbarung
- Anweisungen zum Starten und Beenden von VMs 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`): Das Manifest ermöglicht es Ihnen, die Integrität des Paketinhalts zu überprüfen. Es enthält die SHA-1-Digests jeder Datei im Paket.

Virtuelle Laufwerke: OVF gibt kein Disk-Image-Format 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. Citrix Hypervisor produziert OVF-Pakete mit Festplatten-Images im dynamischen VHD-Format; VMware Produkte und Virtual Box produzieren OVF-Pakete mit virtuellen Laufwerken im Stream-optimierten VMDK-Format.

OVF-Pakete unterstützen auch andere nicht Metadaten-bezogene Funktionen wie Komprimierung, Archivierung, EULA-Anhänge und Anmerkungen.

> **Hinweis:**
>
> Wenn Sie ein OVF-Paket importieren, das komprimiert wurde oder komprimierte Dateien enthält, müssen Sie möglicherweise zusätzlichen Speicherplatz auf dem Citrix Hypervisor or-Server freigeben, um es ordnungsgemäß zu importieren.

Ein **Open Virtual Appliance (OVA) -Paket** ist eine einzelne Archivdatei im Format Tape Archive (.tar), die die Dateien enthält, die ein OVF-Paket enthalten.

OVF- oder OVA-Format Select

OVF-Pakete enthalten eine Reihe von unkomprimierten 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 nützlich für bestimmte Anwendungen, für die es vorteilhaft ist, nur eine Datei zu haben, z. B. das Erstellen von Paketen für Web-Downloads. Verwenden Sie OVA nur als Option, um die Handhabung des Pakets zu erleichtern. Die Verwendung dieses Formats verlängert sowohl den Export- als auch den Importvorgang.

Disk-Image-Formate (VHD und VMDK)

Mit XenCenter können Sie Datenträgerabbilder in die Formate Virtual Hard Disk (VHD) und Virtual Machine Disk (VMDK) importieren. Das Exportieren von eigenständigen Disk-Images wird nicht unterstützt.

> **Hinweis:**
>
> Stellen Sie zum Importieren von Datenträgerabbildern sicher, dass Sie als root angemeldet sind oder die Rolle Pooladministrator RBAC mit Ihrem Benutzerkonto verknüpft ist.

Sie können ein Datenträgerabbild importieren, wenn ein virtuelles Datenträgerabbild ohne zugeordnete OVF-Metadaten verfügbar ist. Diese Option kann in 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, die es Ihnen nicht erlaubt, ein OVF-Paket zu erstellen (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

Wenn verfügbar, empfehlen wir, Appliance-Pakete zu importieren, die OVF-Metadaten und nicht ein einzelnes Disk-Image enthalten. Die OVF-Daten enthalten Informationen, die der Import-Assistent benötigt, um eine VM von seinem Datenträgerabbild neu zu erstellen. Diese Informationen umfassen die Anzahl der Datenträgerabbilder, die mit der VM, dem Prozessor, dem Speicher, dem Netzwerk, den Speicheranforderungen usw. verknüpft sind. Ohne diese Informationen kann es viel komplexer und fehleranfälliger sein, die VM neu zu erstellen.

XVA-Format

XVA ist ein virtuelles Appliance-Format, das für Citrix Hypervisor spezifisch ist, das eine einzelne VM als einen einzigen Satz von Dateien, einschließlich eines Deskriptors und Datenträgerabbildern, verpackt. 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 rohen Binärformat und hat keine Erweiterung. Die zweite Datei ist eine Prüfsumme der ersten Datei mit der Erweiterung `.checksum`.

> **Wichtig:**
>
> Wenn eine VM vom Citrix Hypervisor or-Server exportiert und dann in einen anderen Citrix Hypervisor-Server mit einem anderen CPU-Typ importiert wird, wird sie möglicherweise nicht ordnungsgemäß ausgeführt. Beispielsweise kann eine Windows VM, die von einem Host mit einer Intel® VT-fähigen CPU exportiert wird, nicht ausgeführt werden, wenn sie in einen Host mit einer AMD-VTM-CPU importiert werden.

XVA Version 1 Format

XVA Version 1 ist das Originalformat, das für XEN-basierte Hypervisoren spezifisch ist. Dieses Format packt eine einzelne VM als einzelnes Dateiarchiv, einschließlich eines Deskriptors und Disk-Images. Die Dateinamenerweiterung ist ova.xml.

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 eine Datei für jeden 1 GB Abschnitt des Disk-Images. Der Basisname jeder Datei enthält die Chunk-Nummer in Dezimalzahl. Es enthält einen Block des Disk-Images im Raw-Binärformat, komprimiert mit gzip.

> **Wichtig:**
>
> Wenn eine VM vom Citrix Hypervisor or-Server exportiert und dann in einen anderen Citrix Hypervisor-Server mit einem anderen CPU-Typ importiert wird, wird sie möglicherweise nicht ordnungsgemäß ausgeführt. Beispielsweise kann eine Windows VM, die von einem Host mit einer Intel® VT-fähigen CPU exportiert wird, nicht ausgeführt werden, wenn sie in einen Host mit einer AMD-VTM-CPU importiert werden.

Betriebssystemfixup

Beim Importieren einer virtuellen Appliance oder eines Datenträgerabbilds, die von einer anderen Virtualisierungsplattform als Citrix Hypervisor erstellt und exportiert werden, müssen Sie die VM möglicherweise konfigurieren, bevor sie auf dem Citrix Hypervisor-Server ordnungsgemäß gestartet wird.

XenCenter enthält eine erweiterte Hypervisor-Interoperabilitätsfunktion (Betriebssystemfixup), die darauf abzielt, eine grundlegende Interoperabilität für VMs sicherzustellen, die Sie in Citrix Hypervisor importieren. Verwenden Sie Betriebssystemfixup, wenn Sie VMs aus OVF/OVA-Paketen und Disk-Images importieren, die auf anderen Virtualisierungsplattformen erstellt wurden.

Der Betriebssystemfixup-Prozess behebt die Betriebssystemgeräte- und Treiberprobleme, die beim Wechsel von einem Hypervisor zum anderen auftreten. Der Prozess versucht, Probleme mit dem Startgeräteproblem mit der importierten VM zu beheben, die möglicherweise verhindern, dass das Betriebssystem in der Citrix Hypervisor Umgebung gestartet wird. Diese Funktion dient nicht dazu, Konvertierungen von einer Plattform in eine andere durchzuführen.

> **Hinweis:**
>
> Für diese Funktion ist ein ISO-Speicher-Repository mit 40 MB freiem Speicherplatz und 256 MB virtuellem Speicher erforderlich.

Betriebssystemfixup wird als automatisch startendes ISO-Image bereitgestellt, 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 dann wird die VM heruntergefahren. Beim nächsten Start der neuen VM wird das Startgerät zurückgesetzt und die VM wird normal gestartet.

Wenn Sie Betriebssystemfixup auf importierten Datenträgerabbildern oder OVF/OVA-Paketen verwenden möchten, aktivieren Sie das Feature auf der Seite Erweiterte Optionen des XenCenter Importassistenten. Geben Sie einen Speicherort an, an den das Fixup-ISO kopiert wird, damit Citrix Hypervisor es verwenden kann.

Was macht das Betriebssystemfixup mit der VM?

Die Option Betriebssystemfixup ist so konzipiert, dass minimale Änderungen möglich sind, damit ein virtuelles System gestartet werden kann. Abhängig vom Gastbetriebssystem und dem Hypervisor des ursprünglichen Hosts sind nach der Verwendung von Betriebssystemfixup möglicherweise weitere Aktionen erforderlich. Diese Aktionen können Konfigurationsänderungen und Treiberinstallation umfassen.

Während des Fixup-Prozesses wird ein ISO in eine ISO SR kopiert. Die ISO ist an eine VM angehängt. Die Startreihenfolge ist so eingestellt, dass sie vom virtuellen DVD-Laufwerk gestartet wird, und die VM startet in das ISO. 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 ermittelt. Alle Zeiger auf SCSI-Festplattenstartgeräte werden so geändert, dass sie auf IDE-Festplatten verweisen. Wenn GRUB beispielsweise einen Eintrag enthält, in dem der erste Datenträger auf dem ersten SCSI-Controller `/dev/sda1` dargestellt wird, wird dieser Eintrag in die `/dev/hda1` Darstellung des ersten Datenträgers auf dem ersten IDE-Controller geändert.

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 IDE-Schnittstelle geändert wird.

Wenn bestimmte Virtualisierungstools in der VM erkannt werden, werden diese deaktiviert, um Leistungsprobleme und unnötige Ereignismeldungen zu vermeiden.

Die Transfer-VM

Die Transfer-VM ist eine integrierte VM, die nur während des Imports oder Exports eines virtuellen Datenträgerabbilds ausgeführt wird. Es wird verwendet, um seinen Inhalt zwischen dem Speicherort der Disk-Image-Datei und dem Citrix Hypervisor or-Speicher-Repository zu übertragen.

Für jeden Import oder Export eines Disk-Images wird eine Transfer-VM ausgeführt. Beim Importieren oder Exportieren einer virtuellen Appliance mit mehr als einem Disk-Image wird jeweils nur ein Disk-Image übertragen.

Die Ausführung einer Transfer-VM hat folgende Anforderungen:

Virtuelle CPU	1
Virtueller Speicher	256 MB

Speicher	8 MB
Netzwerk	Vom Citrix Hypervisor or-Server erreichbar; statische oder dynamische IP-Adresse (dynamisch, empfohlen)

Das Standardübertragungsprotokoll ist iSCSI. In diesem Fall erfordert die Übertragungs-VM einen iSCSI-Initiator auf dem Citrix Hypervisor or-Server. Ein alternatives Übertragungsprotokoll ist RawVDI.

So verwenden Sie das RawVDI-Übertragungsprotokoll:

1. Sichern Sie die`XenCenterMain.exe.config` Datei, die sich im Installationsordner befindet.
2. Öffnen Sie die`XenCenterMain.exe.config` Datei mit einem Texteditor.
3. Fügen Sie die folgende Abschnittsgruppe zur hinzu`configSection`:

```
<sectionGroup name=”applicationSettings”
    type=”System.Configuration.ApplicationSettingsGroup, System,
       Version=2.0.0.0,
    Culture=neutral, PublicKeyToken=b77a5c561934e089” >
    <section name=”XenOvfTransport.Properties.Settings”
       type=”System.Configuration.ClientSettingsSection, System,
          Version=2.0.0.0,
      Culture=neutral, PublicKeyToken=b77a5c561934e089”
         requirePermission=”false”/>
</sectionGroup>
```

4. Fügen Sie zum Ende der Datei den folgenden Abschnitt hinzu:

```
<applicationSettings>
    <XenOvfTransport.Properties.Settings>
        <setting name=”TransferType” serializeAs=”String”> <value>
           UploadRawVDI</value>
        </setting>
    </XenOvfTransport.Properties.Settings>
</applicationSettings>
```

5. Speichern Sie die`XenCenterMain.exe.config` Datei.

> **Hinweis:**
>
> Wenn XenCenter nicht ordnungsgemäß gestartet wird, überprüfen Sie, ob die neue Ab-

> schnittsgruppe und der neue Abschnitt korrekt hinzugefügt wurden.

VMs importieren

Wenn Sie eine VM importieren, erstellen Sie effektiv eine VM und verwenden viele der gleichen Schritte, die zum Bereitstellen einer neuen VM erforderlich sind. Diese Schritte umfassen die Nominierung eines Hosts sowie die Konfiguration 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.

Importieren von VMs aus OVF/OVA

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu importieren, müssen Sie als root angemeldet sein oder die Rolle Pooladministrator 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 Import-Assistent führt Sie durch die üblichen Schritte zum Erstellen einer VM in XenCenter: Nominieren eines Hosts und dann Konfigurieren von Speicher und Netzwerk für die neue VM. Beim Importieren von OVF- und OVA-Dateien sind möglicherweise zusätzliche Schritte erforderlich, z. B.:

- Wenn Sie VMs importieren, die mit anderen Virtualisierungsplattformen erstellt wurden, führen Sie die Funktion „Betriebssystemfixup“ aus, um eine grundlegende Interoperabilität für die VM sicherzustellen. Weitere Informationen finden Sie unter Betriebssystemfixup.
- Es ist notwendig, das Netzwerk für die Transfer-VM zu konfigurieren, die für den Importvorgang verwendet wird. Weitere Informationen finden Sie unter Die Transfer-VM.

> **Tipp:**
>
> Stellen Sie sicher, dass der Zielhost über genügend Arbeitsspeicher verfügt, um die zu importierenden virtuellen Maschinen zu unterstützen. Ein Mangel an verfügbarem RAM führt zu einem fehlgeschlagenen Import. Weitere Informationen zum Beheben dieses Problems finden Sie unterCTX125120 - Appliance-Importassistent schlägt aufgrund von Arbeitsspeicher fehl.

Importierte OVF-Pakete werden beim Importieren mit XenCenter als vApps angezeigt. Wenn der Import abgeschlossen ist, werden die neuen VMs im XenCenter **Ressourcenbereich** angezeigt, und die neue vApp wird im Dialogfeld „ **vApps verwalten** “ angezeigt.

So importieren Sie VMs aus OVF/OVA mithilfe von XenCenter:

1. Öffnen Sie den Import-Assistenten, indem Sie eine der folgenden Aktionen ausführen:

- Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü **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, und klicken Sie dann auf **Weiter**, um fortzufahren.

3. Überprüfen und akzeptieren Sie die EULAs, falls zutreffend.

   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 springt direkt zur nächsten Seite.

4. Geben Sie den Pool oder den Host an, in den Sie die VMs importieren möchten, und weisen Sie die VMs dann (optional) einem Citrix Hypervisor or-Server zu.

   Um einen Host oder Pool auszuwählen, wählen Sie aus der Liste Zu **importierende VM (s)** aus.

   Um jeder VM einen Citrix Hypervisor or-Server zuzuweisen, wählen Sie einen Server aus der Liste im **Home-Server**aus. Wenn Sie keinen Home-Server zuweisen möchten, wählen Sie **Einen Home-Server nicht zuweisen**aus.

   Klicken Sie auf **Weiter**, um fortzufahren.

5. Konfigurieren des Speichers für die importierten VMs: Wählen Sie ein oder mehrere Speicher-Repositories aus, auf denen die importierten virtuellen Festplatten platziert werden sollen, und klicken Sie dann auf **Weiter** , um fortzufahren.

   Um alle importierten virtuellen Laufwerke auf derselben SR zu **platzieren, wählen Sie Alle importierten VMs auf dieser Ziel-SR**platzieren aus. Select eine 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 die Ziel-SR aus der Liste in der Spalte SR aus.

6. Konfigurieren des Netzwerkes für die importierten VMs: Ordnen Sie die virtuellen Netzwerkschnittstellen in den VMs zu, die Sie importieren, den Zielnetzwerken im Zielpool zu. Die Netzwerk- und MAC-Adresse, die in der Liste der eingehenden VMs angezeigt wird, 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 auf **Weiter**, um fortzufahren.

7. Sicherheitseinstellungen angeben: Wenn das ausgewählte OVF/OVA-Pakete mit Sicherheitsfunktionen wie Zertifikaten oder einem Manifest konfiguriert ist, geben Sie die erforderlichen Informationen an, und klicken Sie dann auf **Weiter** , um fortzufahren.

Je nachdem, welche Sicherheitsfunktionen auf der OVF-Appliance konfiguriert wurden, werden auf der Seite „Sicherheit“ verschiedene Optionen angezeigt:

- 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, das zum Signieren des Pakets verwendet wurde. Wenn das Zertifikat als nicht vertrauenswürdig angezeigt wird, ist es wahrscheinlich, dass entweder das Stammzertifikat oder die ausstellende Zertifizierungsstelle auf dem lokalen Computer nicht vertrauenswürdig ist. 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. Select dieses Kontrollkästchen, damit der Assistent die Liste der Dateien im Paket überprüft.

Wenn Pakete digital signiert sind, wird das zugehörige Manifest automatisch überprüft, sodass das Kontrollkästchen **Manifestinhalt** überprüfen nicht auf der Seite Sicherheit angezeigt wird.

> **Hinweis:**
>
> VMware Workstation 7.1.x OVF-Dateien können nicht importiert werden, wenn Sie das Manifest überprüfen. 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 Citrix Hypervisor basieren, aktivieren Sie das Kontrollkästchen **Betriebssystemfixup verwenden** . Select eine ISO-SR aus, in die das Fixup-ISO kopiert werden kann, damit Citrix Hypervisor darauf zugreifen kann. Weitere Informationen zu diesem Feature finden Sie unter Betriebssystemfixup.

   Klicken Sie auf **Weiter**, um fortzufahren.

9. Konfigurieren Sie die Übertragung von VM-Netzwerken.

   Select ein Netzwerk aus der Liste der Netzwerkschnittstellen aus, die im Zielpool oder Host verfügbar sind. Wählen Sie, ob die Netzwerkeinstellungen automatisch oder manuell konfiguriert werden sollen.

   - Wenn Sie das automatisierte Dynamic Host Configuration Protocol verwenden möchten, um Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske und Gateway zuzuweisen, wählen Sie **Netzwerkeinstellungen automatisch mit DHCP abrufen** aus.
   - Um Netzwerkeinstellungen manuell zu konfigurieren, wählen Sie **Diese Netzwerkeinstellungen verwenden**aus, und geben Sie dann die erforderlichen Werte ein. Geben Sie eine IP-Adresse ein. Legen Sie optional die Subnetzmaske und die Gatewayeinstellungen fest.

Klicken Sie auf **Weiter**, um fortzufahren.

10. 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 in Anspruch nehmen, 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 mit Windows Betriebssystemen verwendet haben, müssen Sie den`platform` Parameter festlegen.
>
> 1. Setzen Sie den `platform` Parameter auf `device_id=0002`. Zum Beispiel:
>
> ```
> xe vm-param-set UUID=VM uuid-Plattform:device_id=0002
> ```
>
> 2. Setzen Sie den `platform` Parameter auf `viridian=true`. Zum Beispiel:
>
> ```
> xe vm-param-set UUID=VM uuid-Plattform:viridian=true
> ```

Importieren von Disk-Images

Mit dem XenCenter Importassistenten können Sie ein Datenträgerabbild als VM in einen Pool oder einen bestimmten Host importieren. Der Import-Assistent führt Sie durch die üblichen Schritte zum Erstellen einer VM in XenCenter: Nominieren eines Hosts und dann 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 im Verwaltungsnetzwerk ausgeführt wird, das Citrix Hypervisor verwendet.
- Der Import-Assistent erfordert lokalen Speicher auf dem Server, auf dem Sie ihn ausführen.

So importieren Sie VMs aus einem Disk-Image mithilfe von XenCenter:

1. Öffnen Sie den Import-Assistenten, indem Sie eine der folgenden Aktionen ausführen:

- Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü **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, 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 Datenträgerabbild erstellt werden soll, und weisen Sie dann die Anzahl der CPUs und die Speichermenge zu. Klicken Sie auf **Weiter**, um fortzufahren.
4. Geben Sie den Pool oder den Host an, in den Sie die VMs importieren möchten, und weisen Sie die VMs dann (optional) einem Citrix Hypervisor or-Server zu.

   Um einen Host oder Pool auszuwählen, wählen Sie aus der Liste Zu **importierende VM (s)** aus.

   Um jeder VM einen Citrix Hypervisor or-Server zuzuweisen, wählen Sie einen Server aus der Liste im **Home-Server**aus. Wenn Sie keinen Home-Server zuweisen möchten, wählen Sie **Einen Home-Server nicht zuweisen**aus.

   Klicken Sie auf **Weiter**, um fortzufahren.
5. Speicher für die importierten VMs konfigurieren: Select ein oder mehrere Speicher-Repositories aus, auf denen die importierten virtuellen Festplatten platziert werden sollen, und klicken Sie dann auf **Weiter** , um fortzufahren.

   Um alle importierten virtuellen Laufwerke auf derselben SR zu **platzieren, wählen Sie Alle importierten VMs auf dieser Ziel-SR**platzieren aus. Select eine 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 die Ziel-SR aus der Liste in der Spalte SR aus.
6. Konfigurieren des Netzwerkes für die importierten VMs: Ordnen Sie die virtuellen Netzwerkschnittstellen in den VMs zu, die Sie importieren, den Zielnetzwerken im Zielpool zu. Die Netzwerk- und MAC-Adresse, die in der Liste der eingehenden VMs angezeigt wird, 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 auf **Weiter**, um fortzufahren.
7. Betriebssystemfixup aktivieren: Wenn die importierten Datenträgerabbilder auf einer anderen Virtualisierungsplattform als Citrix Hypervisor erstellt wurden, aktivieren Sie das Kontrollkästchen Betriebssystemfixup verwenden. Select eine ISO-SR aus, in die das Fixup-ISO kopiert

werden kann, damit Citrix Hypervisor darauf zugreifen kann. Weitere Informationen zu diesem Feature finden Sie unter Betriebssystemfixup.

Klicken Sie auf **Weiter**, um fortzufahren.

8. Konfigurieren Sie die Übertragung von VM-Netzwerken.

   Select ein Netzwerk aus der Liste der Netzwerkschnittstellen aus, die im Zielpool oder Host verfügbar sind. Wählen Sie, ob die Netzwerkeinstellungen automatisch oder manuell konfiguriert werden sollen.

   - Wenn Sie das automatisierte Dynamic Host Configuration Protocol verwenden möchten, um Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske und Gateway zuzuweisen, wählen Sie **Netzwerkeinstellungen automatisch mit DHCP abrufen** aus.
   - Um Netzwerkeinstellungen manuell zu konfigurieren, wählen Sie Diese Netzwerkeinstellungen verwenden aus, und geben Sie dann die erforderlichen Werte ein. Geben Sie eine IP-Adresse ein. Legen Sie optional die Subnetzmaske und die Gatewayeinstellungen fest.

   Klicken Sie auf **Weiter**, um fortzufahren.

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 in Anspruch nehmen, 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 Datenträgerabbilds mit Windows Betriebssystemen verwendet haben, müssen Sie den`platform` Parameter festlegen. Der Wert dieses Parameters variiert je nach Windows Version, die im Disk-Image enthalten ist:

- Legen Sie für Windows Server 2008 und höher den`platform` Parameter auf fest`device_id=0002` . Zum Beispiel:

  ```
  xe vm-param-set uuid=VM uuid platform:device_id=0002
  ```

- Setzen Sie für alle anderen Windows Versionen den`platform` Parameter auf`viridian=true` . Zum Beispiel:

  ```
  xe vm-param-set uuid=VM uuid platform:viridian=true
  ```


Importieren von VMs aus XVA

Sie können VMs, Vorlagen und Snapshots importieren, die zuvor exportiert und lokal im XVA-Format (`.xva`) oder XVA-Version 1 (`ova.xml`) gespeichert wurden. Führen Sie dazu die üblichen Schritte aus, um eine VM zu erstellen: Nominieren eines Hosts und dann Konfigurieren von Speicher und Netzwerk für die neue VM.

> **Warnhinweis:**
>
> Möglicherweise ist es nicht immer möglich, eine importierte VM auszuführen, die von einem anderen Server mit einem anderen CPU-Typ exportiert wurde. Beispielsweise wird eine Windows VM, die von einem Server mit einer Intel VT-fähigen CPU exportiert wurde, möglicherweise nicht ausgeführt, wenn sie auf einen Server mit einer AMD-VTM-CPU importiert wird.

So importieren Sie VMs aus XVA mithilfe von XenCenter:

1. Öffnen Sie den Import-Assistenten, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste, und wählen Sie dann im Kontextmenü **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 im Feld **Dateiname**einen URL-Speicherort (httphttpsfile“““„ oderftp“) eingeben. Klicken Sie auf **Weiter**, das Dialogfeld Paket herunterladen wird geöffnet, und Sie müssen einen Ordner auf dem XenCenter Host angeben, in den die Datei kopiert wird.
3. Select einen Pool oder einen Host aus, auf dem die importierte VM gestartet werden soll, und klicken Sie dann auf **Weiter** , um fortzufahren.
4. Select die Speicher-Repositories aus, auf denen das importierte virtuelle Laufwerk abgelegt werden soll, und klicken Sie dann auf **Weiter** , um fortzufahren.
5. Konfigurieren des Netzwerkes für die importierte VM: Ordnen Sie die virtuelle Netzwerkschnittstelle in der zu importierenden VM zu, um ein Netzwerk im Zielpool zu erreichen. Die Netzwerk- und MAC-Adresse, die in der Liste der eingehenden VMs angezeigt wird, 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 auf **Weiter**, um fortzufahren.
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 in Anspruch nehmen, 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 mithilfe der xe-CLI:

Um die VM in die Standard-SR auf dem Citrix Hypervisor or-Zielserver zu importieren, geben Sie Folgendes ein:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file
```

Um die VM in eine andere SR auf dem Citrix Hypervisor or-Zielserver zu importieren, fügen Sie den optionalen`sr-uuid` Parameter hinzu:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
```

Wenn Sie die MAC-Adresse der ursprünglichen VM beibehalten möchten, fügen Sie den optionalen`preserve` Parameter hinzu und legen Sie Folgendes fest**`true`** :

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file preserve=true
```

> **Hinweis:**
>
> Das Importieren einer VM kann einige Zeit in Anspruch nehmen, 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.

VMs exportieren

Sie können OVF/OVA- und XVA-Dateien mit dem XenCenter Exportassistenten exportieren. Sie können XVA-Dateien auch über die xe-CLI exportieren.

Exportieren von VMs als OVF/OVA

Mit dem XenCenter Export-Assistenten können Sie einen oder mehrere VMs als OVF/OVA-Pakete exportieren. Wenn Sie VMs als OVF/OVA-Pakete exportieren, werden die Konfigurationsdaten zusammen mit den virtuellen Festplatten jeder VM exportiert.

> **Hinweis:**
>
> Um OVF- oder OVA-Pakete zu exportieren, müssen Sie als root angemeldet sein oder die Rolle Pooladministrator Role Based Access Control (RBAC) mit Ihrem Benutzerkonto verknüpft sein.

So exportieren Sie VMs als OVF/OVA mithilfe von XenCenter:

1. Fahren Sie die VMs, die Sie exportieren möchten, herunter oder halten Sie sie an.
2. Öffnen Sie den Export-Assistenten: Klicken Sie im Bereich **Ressourcen** mit der rechten Maustaste auf den Pool oder den Host, der die VMs enthält, 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.
   - Select **OVF/OVA-Pakete (*.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-Pakete aufnehmen möchten, und klicken Sie dann auf **Weiter** , um fortzufahren.
5. Falls erforderlich, können Sie dem Paket ein zuvor vorbereitetes Endbenutzer-Lizenzvertrag (EULA) Dokument (.rtf, .txt) hinzufügen.

   Um einen 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 in der Liste der **EULA-Dateien** auswählen und dann auf **Anzeigen** klicken.

   EULAs können die rechtlichen Bedingungen für die Verwendung der Appliance und der in der Appliance gelieferten Anwendungen bereitstellen.

   Durch die Möglichkeit, eine oder mehrere EULAs einzuschließen, können Sie die Software auf der Appliance rechtlich schützen. Wenn Ihre Appliance beispielsweise ein proprietäres Betriebssystem auf ihren VMs enthält, sollten Sie den EULA-Text dieses Betriebssystems einfügen. Der Text wird angezeigt, und die Person, die die Appliance importiert, muss sie akzeptieren.

   > **Hinweis:**
   >
   > Der Versuch, EULA-Dateien hinzuzufügen, die nicht in unterstützten Formaten enthalten

> sind, einschließlich XML- oder Binärdateien, kann dazu führen, dass die ImportEULA-Funktionalität fehlschlägt.

Select **Weiter** aus, um fortzufahren.

6. Geben Sie auf der Seite **Erweiterte Optionen** ein Manifest, Signatur und Ausgabedateioptionen 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 stellt eine Bestandsaufnahme oder eine Liste der anderen Dateien in einem Paket bereit. Das Manifest wird verwendet, um sicherzustellen, dass die Dateien, die ursprünglich beim Erstellen des Pakets enthalten waren, dieselben Dateien sind, die beim Eintreffen des Pakets vorhanden sind. Beim Importieren der Dateien wird eine Prüfsumme verwendet, um zu überprüfen, ob sich die Dateien seit der Erstellung des Pakets nicht geändert haben.

   b) Um dem Paket eine digitale Signatur hinzuzufügen, aktivieren Sie das Kontrollkästchen **OVF-Paket signieren** , und suchen Sie nach einem Zertifikat. Geben Sie den mit dem Zertifikat verknüpften privaten Schlüssel in das Feld **Kennwort für den privaten Schlüssel ein** .

   Wenn ein signiertes Paket importiert wird, kann der Benutzer die Identität des Erstellers überprüfen, indem er den öffentlichen Schlüssel zur Validierung der digitalen Signatur verwendet. Verwenden Sie ein X.509-Zertifikat, das Sie von einer vertrauenswürdigen Behörde erstellt und als `.pem` Datei `.pfx` oder exportiert haben. Das Zertifikat muss die Signatur der Manifestdatei und das Zertifikat enthalten, das zum Erstellen dieser Signatur verwendet wird.

   c) Um die ausgewählten VMs als einzelne (tar-) Datei im OVA-Format auszugeben, aktivieren Sie das Kontrollkästchen **OVA-Paket (einzelne OVA-Exportdatei) erstellen** . Weitere Informationen zu den verschiedenen Dateiformaten finden Sie unterOffenes Virtualisierungsformat.

   d) Aktivieren Sie das Kontrollkästchen OVF-Dateien komprimieren, um virtuelle Festplattenabbilder (.VHD-Dateien) zu komprimieren, die im Paket enthalten sind.

   Wenn Sie ein OVF-Paket erstellen, werden den virtuellen Festplatten-Images standardmäßig die gleiche Menge an Speicherplatz zugewiesen wie die exportierte VM. Beispielsweise verfügt eine VM, der 26 GB Speicherplatz zugewiesen ist, über ein Festplattenabbild, das 26 GB Speicherplatz verbraucht. Das Festplattenabbild verwendet diesen Speicherplatz, unabhängig davon, ob die VM diesen tatsächlich benötigt.

> **Hinweis:**
>
> Durch das Komprimieren der VHD-Dateien dauert der Exportvorgang länger. Das Importieren eines Pakets mit komprimierten VHD-Dateien dauert ebenfalls länger, da der Import-Assistent beim Importieren alle VHD-Bilder extrahieren muss.

Wenn sowohl **OVF-Dateien erstellen (einzelne OVA-Exportdatei)** als auch **OVF-Dateien komprimieren** aktiviert sind, ergibt sich eine komprimierte OVA-Datei mit der Erweiterung `.ova.gz` .

7. Konfigurieren Sie die Übertragung von VM-Netzwerken.

   Select ein Netzwerk aus der Liste der Netzwerkschnittstellen aus, die im Zielpool oder Host verfügbar sind. Wählen Sie, ob die Netzwerkeinstellungen automatisch oder manuell konfiguriert werden sollen.

   - Wenn Sie das automatisierte Dynamic Host Configuration Protocol verwenden möchten, um Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske und Gateway zuzuweisen, wählen Sie **Netzwerkeinstellungen automatisch mit DHCP abrufen** aus.
   - Um Netzwerkeinstellungen manuell zu konfigurieren, wählen Sie **Diese Netzwerkeinstellungen verwenden**aus, und geben Sie dann die erforderlichen Werte ein. Geben Sie eine IP-Adresse ein. Legen Sie optional die Subnetzmaske und die Gatewayeinstellungen fest.

   Klicken Sie auf **Weiter**, um fortzufahren.

8. Überprüfen Sie die Exporteinstellungen.

   Wenn der Assistent das exportierte Paket überprüfen soll, aktivieren Sie das Kontrollkästchen **Export bei 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 in Anspruch nehmen, 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**.

Exportieren von VMs als XVA

Sie können eine vorhandene VM als XVA-Datei mit dem XenCenter Exportassistenten oder der xe-CLI exportieren. Es wird empfohlen, eine VM auf einen anderen Computer als den Citrix Hypervisor or-Server zu exportieren, auf dem Sie eine Bibliothek mit Exportdateien verwalten können. Beispielsweise können Sie die VM auf den Computer exportieren, auf dem XenCenter ausgeführt wird.

> **Warnhinweis:**
>
> Möglicherweise ist es nicht immer möglich, eine importierte VM auszuführen, die von einem anderen Server mit einem anderen CPU-Typ exportiert wurde. Beispielsweise wird eine Windows VM, die von einem Server mit einer Intel VT-fähigen CPU exportiert wurde, möglicherweise nicht ausgeführt, wenn sie auf einen Server mit einer AMD-VTM-CPU importiert wird.

So exportieren Sie VMs als XVA-Dateien mithilfe von XenCenter:

1. Fahren Sie die VM, die Sie exportieren möchten, herunter oder halten Sie sie an.
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.
   - Select **XVA-Datei (*.xva)** aus der Liste **Format** aus.
   - 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. Überprüfen Sie die Exporteinstellungen.

   Wenn der Assistent das exportierte Paket überprüfen soll, aktivieren Sie das Kontrollkästchen **Export bei 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 in Anspruch nehmen, 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 mithilfe 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
```


> **Hinweis:**
>
> Achten Sie darauf, die `.xva` Erweiterung 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.

Kopiert!
Failed!

Sichere Bromium-Plattform

October 16, 2019

Citrix Hypervisor unterstützt Bromium Secure Platform auf Windows VMs. Diese Funktion schützt Ihr Unternehmen vor Verstößen und ermöglicht es Benutzern, alle Vorgänge auszuführen, ohne die Sicherheit zu beeinträchtigen.

> **Hinweis:**
>
> Die mindestens unterstützte Bromium-Version ist 4.0.4.

Mit dieser Funktion können Sie:

- Schützen Sie Ihr Unternehmen vor bekannten und unbekannten Bedrohungen.
- Erkennung und Überwachung der Bedrohungsaktivität.
- Reagieren Sie auf eine Visualisierung des Angriffs und sehen Sie die ergriffenen Abhilfemaßnahmen an.

Kompatibilitätsanforderungen und Vorbehalte

Citrix Hypervisor unterstützt Bromium auf:

- **CPU**: Intel Core i3, i5, i7 v3 (Haswell) oder höher mit Intel Virtualization Technology (Intel VT) und Extended Page Tables (EPT) im System-BIOS aktiviert.

  AMD CPUs werden nicht unterstützt.

- **VMs**: Windows 7 SP1 (32-Bit und 64-Bit), Windows 8.1 (64-Bit) und Windows 10 (64-Bit).
- **VM-Ressourcen**: Mindestens 2 vCPUs, 4 GB RAM und 32 GB Festplattenspeicher.

Für VMs, auf denen Bromium ausgeführt wird, unterstützt Citrix Hypervisor nicht und verhindert die Verwendung der folgenden Funktionen:

- Jede Form der VM-Bewegung (zum Beispiel: Live-Migration, Speicher-Live-Migration).
- Verwendung von Dynamic Memory Control (DMC).

> **Hinweis:**
>
> Es ist möglich, PCI-Pass-Through und vGPU für eine VM zu verwenden, die geschachtelte Virtualisierung aktiviert hat. Citrix unterstützt solche Konfigurationen jedoch nicht.
>
> **Wichtig:**
>
> Bromium Secure Platform verwendet Unterstützung für verschachtelte Virtualisierung. Citrix unterstützt diese Funktion nur für die Verwendung mit Bromium Secure Platform. Verschachtelte Virtualisierung wird für andere Anwendungsfälle nicht unterstützt. Um dieses Feature nutzen zu können, müssen Sie Citrix Hypervisor Premium Edition ausführen oder über eine Berechtigung für Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.

Konfiguration

So bereiten Sie Ihr Citrix Hypervisor or-System für die Verwendung mit Bromium Secure Platform vor:

1. Erzwingen Sie auf jedem Host die Verwendung von Software VMCS Shadowing, indem Sie den folgenden Befehl an der Eingabeaufforderung ausführen:

```
/opt/xensource/libexec/xen-cmdline --set-xen
   force_software_vmcs_shadow
```

2. Starten Sie den Host neu.
3. Aktivieren Sie auf jeder VM die virtualisierte Unterstützung mit den folgenden Befehlen:

```
xe vm-list name-label='vm_name' --minimal

xe vm-param-set uuid=$VM platform:nested-virt=1
```

> **Hinweis:**
>
> Verwenden Sie für Citrix Virtual Desktops das Gold-Image für verschachtelte Virtualisierung.

4. Installieren Sie Bromium Secure Platform auf der VM, indem Sie die Installationsanweisungen befolgen.

Kopiert!
Failed!

Containermanagement

October 16, 2019

Citrix Hypervisor enthält zwei neue Funktionen zur Verbesserung der Bereitstellung von Docker Containern auf Citrix Hypervisor

- Unterstützung für CoreOS Linux VMs und Konfigurieren von Cloud Config Drives
- Containerverwaltung für CoreOS, Debian 8, Ubuntu 14.04 und RHEL/Centos/OEL 7
- Vorschau der Containerverwaltung für Windows Server-Container unter Windows Server 2016 Technologievorschau

CoreOS ist eine minimalistische Linux-Distribution, die für das Hosten von Docker Anwendungen populär geworden ist. Das CoreOS Cloud Config Drive ermöglicht die Anpassung verschiedener Betriebssystemkonfigurationsoptionen. Wenn die Containerverwaltung auf einer VM aktiviert ist, erkennt Citrix Hypervisor alle Docker Container, die auf der VM ausgeführt werden.

> **Hinweis:**
>
> Informationen zum Installieren von CoreOS-Gästen, zum Konfigurieren von Cloud-Config-Parametern und zum Verwalten von Docker Containern finden Sie in der XenCenter er-Hilfe. Drücken Sie **F1** oder klicken Sie auf **Hilfe** .

Der Container Management Supplemental Park ermöglicht Citrix Hypervisor die folgenden Aktionen:

- Abfragen der VMs
- Interagieren mit Cloud-Konfigurationslaufwerken
- Entdecken Sie Anwendungscontainer
- Zeigen Sie Anwendungscontainer in der Infrastrukturansicht von XenCenter an.

XenCenter ermöglicht auch die Interaktion mit den Containern, um Start-, Stopp- und Pausevorgänge sowie andere Überwachungsfunktionen zu ermöglichen. Weitere Informationen finden Sie unter Ergänzungspaket für die Containerverwaltung.

Was ist Docker?

Docker ist eine offene Plattform für Entwickler und Systemadministratoren, um verteilte Anwendungen zu erstellen, zu versenden und auszuführen. Ein Docker Container umfasst nur die Anwendung und ihre Abhängigkeiten. Es läuft als isolierter Prozess im Benutzerbereich auf dem Host-Betriebssystem und teilt den Kernel und das Basisdateisystem mit anderen Containern. Weitere Informationen finden Sie unter https://www.docker.com/whatisdocker.

> **Hinweis:**
>
> Das Feature Citrix Hypervisor Container Management ergänzt, ersetzt jedoch nicht die Docker Umgebung. Sie können eines der vielen verfügbaren Docker er-Verwaltungstools verwenden, um einzelne Docker Engine-Instanzen in den VMs zu verwalten.

Ergänzungspaket für die Containerverwaltung

Das Container Management Supplemental Pack bietet:

Überwachung und Sichtbarkeit: Hier können Sie sehen, welche VMs für das Docker Hosting verwendet werden und welche Container auf der VM ausgeführt werden.

Diagnose: Zugriff auf grundlegende Containerinformationen wie weitergeleitete Netzwerkports und den ursprünglichen Docker Imagenamen. Diese Funktion kann dazu beitragen, die Untersuchungen zu Problemen zu beschleunigen, bei denen die Infrastruktur- und Anwendungsebenen möglicherweise betroffen sind.

Performance: Gibt einen Einblick in die Container, die auf dieser VM ausgeführt werden. Abhängig von den vom Betriebssystem bereitgestellten Informationen werden Informationen zu den Prozessen und Anwendungen bereitgestellt, die auf dem Container ausgeführt werden, und der verbrauchten CPU-Ressource.

Steuerungsanwendungen: Mit XenCenter können Sie Anwendungscontainer starten, stoppen und pausieren (falls vom Betriebssystem unterstützt), wodurch problematische Anwendungen schnell beendet werden können.

> **Hinweis:**
>
> Citrix Hypervisor unterstützt die Installation von Supplemental Packs mit XenCenter. Informationen zum Installieren eines Zusatzpakets mit XenCenter finden Sie in der XenCenter-Hilfe. Wenn Sie lieber mit der XE CLI installieren möchten, lesen Sie dieCitrix Hypervisor Supplemental Packs und DDK-Handbuch.

Verwalten von Docker Containern mithilfe von XenCenter

Dieser Abschnitt enthält Informationen zum Verwalten Ihrer CoreOS-VMs mit XenCenter. Führen Sie die folgenden Schritte aus, um CoreOS-VMs zu verwalten:

1. Installieren oder aktualisieren Sie Ihren Host auf Citrix Hypervisor 8.0.
2. Installieren Sie XenCenter, das im Lieferumfang von Citrix Hypervisor 8.0 enthalten ist.
3. Installieren Sie das Container Management Supplemental Pack, das über die verfügbar istCitrix Website.

4. Erstellen Sie eine CoreOS-VM und schließen Sie ein Konfigurationslaufwerk für die VM ein.

   Wenn Sie eine CoreOS-VM in XenCenter erstellen, werden Sie vom Assistenten für **neue VM** aufgefordert, cloud-config-Parameter für Ihre VM anzugeben. Das Konfigurationslaufwerk stellt Benutzerdaten für die VM-Instanz bereit. Wenn Sie planen, Citrix Hypervisor für die Verwaltung von Containern zu verwenden, die innerhalb der VM ausgeführt werden, erstellen Sie ein Konfigurationslaufwerk.

   Standardmäßig enthält XenCenter einen vordefinierten Satz von Parametern auf der Seite „Cloud-Config-Parameter“. Sie können diese Parameter basierend auf Ihren Anforderungen ändern. Ausführliche Informationen zu unterstützten Konfigurationsparametern finden Sie in der CoreOS-Dokumentation.

   > **Warnhinweis:**
   >
   > Die Containerverwaltung funktioniert möglicherweise nicht, wenn Sie kein Konfigurationslaufwerk für die VM erstellen.

5. Aktivieren Sie die Containerverwaltung für die VM. Sie können diese Einstellung auf der Registerkarte **Eigenschaften** der VM in XenCenter aktualisieren.

> **Hinweis:**
>
> Wenn Sie eine Container-verwaltete VM zwischen Pools migrieren, funktioniert die Container-Verwaltung nicht mehr für die VM. Dieses Verhalten liegt daran, dass Container-Management mit einem pool-spezifischen Schlüssel implementiert wird. Um die Container-Management-Funktionalität für die VM wieder zu aktivieren, aktualisieren Sie die Konfiguration des Cloud Config Drive-Laufwerks in den VM-Voreinstellungen.

Verwalten von Containern auf anderen Linux-Gästen

CoreOS-VMs, die mit der standardmäßigen Cloud Config Drive-Konfiguration erstellt werden, werden automatisch für die Container-Verwaltung vorbereitet. Nur müssen Sie die Funktion aktivieren. Andere Linux-Gäste können manuell vorbereitet werden. Diese Funktion wird nur für VMs von Debian 8, Ubuntu 14.04 und RHEL/Centos/OEL 7.x unterstützt.

So bereiten Sie einen Linux-Gast manuell vor:

1. Stellen Sie sicher, dass auf der VM Citrix VM Tools installiert sind und dass das VM-Netzwerk wie unter beschrieben konfiguriert ist Netzwerkanforderungen und -sicherheit.
2. Installieren Sie Docker, Ncat und SSHD in der VM.

   Für Ubuntu 14.04:

   ```
   1 apt-get install docker.io nmap openssh-server
   ```


Für RHEL/Centos/OEL 7.x:

```
yum install docker nmap openssh-server
```

3. Autostart für docker.service aktivieren:

```
systemctl enable docker.service
```

4. docker.service starten

```
systemctl start docker.service
```

Verwenden Sie einen Nicht-Root-Benutzer für die Containerverwaltung. Fügen Sie den Benutzer zur Gruppe „Docker“ hinzu, um den Zugriff auf Docker zu ermöglichen.

5. Bereiten Sie die VM für die Containerverwaltung vor; führen Sie den folgenden Befehl für die Steuerdomäne (dom0) auf einem der Hosts im Pool aus:

```
xscontainer-prepare-vm -v vm_uuid -u username
```

Wo`vm_uuid` ist die zu vorbereitende VM und`username` der Benutzername auf der VM, die die Containerverwaltung für den Verwaltungszugriff verwendet.

Das Vorbereitungsskript führt Sie durch den Prozess und ermöglicht automatisch die Containerverwaltung für diese VM.

> **Hinweis:**
>
> Wenn Sie eine Container-verwaltete VM zwischen Pools migrieren, funktioniert die Container-Verwaltung nicht mehr für die VM. Dieses Verhalten liegt daran, dass Container-Management mit einem pool-spezifischen Schlüssel implementiert wird. Um die Container-Management-Funktionalität für die VM wieder zu aktivieren, führen Sie den`xscontainer-prepare-vm` Befehl erneut auf der VM aus. Selbst nach dem Ausführen dieses Befehls kann der ursprüngliche Citrix Hypervisor Pool weiterhin auf die VM zugreifen.

Zugriff auf die Docker Container-Konsole und Protokolle

Bei Linux-VMs ermöglicht XenCenter Kunden den Zugriff auf die Containerkonsole und das Anzeigen von Protokollen zur Verwaltung und Überwachung von Anwendungen, die auf Docker Containern ausgeführt werden. So greifen Sie mit XenCenter auf die Containerkonsole und die Protokolle zu:

1. Select den Container im Bereich **Ressourcen** aus.
2. Klicken Sie im Abschnitt **Allgemeine Containereigenschaften** auf **View Console** , um die Containerkonsole anzuzeigen. Klicken Sie auf Protokoll anzeigen, um die **Konsolenprotokolle**

anzuzeigen. Diese Aktion öffnet einen SSH-Client auf dem Computer, auf dem XenCenter ausgeführt wird.

3. Melden Sie sich bei entsprechender Aufforderung am SSH-Client mit dem Benutzernamen und dem Kennwort der VM an.

> **Hinweis:**
>
> Kunden können den Authentifizierungsprozess automatisieren, indem sie ihre öffentlichen/privaten SSH-Schlüssel konfigurieren. Weitere Informationen finden Sie im folgenden Abschnitt.

Automatisieren des Authentifizierungsprozesses (optional)

Beim Zugriff auf die Containerkonsole und die Protokolle müssen Kunden die Anmeldeinformationen der VM eingeben, um SSH-Verbindungen zu authentifizieren. Kunden können jedoch den Authentifizierungsprozess automatisieren, um die Eingabe der Anmeldeinformationen zu vermeiden. Befolgen Sie die folgenden Anweisungen, um den automatischen Authentifizierungsprozess zu konfigurieren:

1. Generieren Sie ein öffentliches/privates Schlüsselpaar.
2. Fügen Sie den öffentlichen SSH-Schlüssel zum Benutzerverzeichnis auf der VM hinzu, auf der der Container ausgeführt wird.
   - Fügen Sie bei Containern, die auf einer CoreOS-VM ausgeführt werden, den öffentlichen Schlüssel zum Abschnitt **Cloud-Config-Parameter** auf der Registerkarte **Allgemein** der VM in XenCenter hinzu.
   - Fügen Sie für Container, die unter Ubuntu 14.04, RHEL/Centos/Oracle Linux 7 und Debian 8 ausgeführt werden, den öffentlichen Schlüssel manuell hinzu`~/.ssh/authorized_keys`.
3. Fügen Sie den privaten SSH-Schlüssel dem`%userprofile%` Verzeichnis auf dem Computer hinzu, auf dem XenCenter ausgeführt wird, und benennen Sie den Schlüssel um`ContainerManagement.ppk`.

Verwalten von Windows Server-Containern

Windows Server-Container sind Teil des Windows Server 2016-Gastbetriebssystems. Sie ermöglichen die Kapselung von Windows Anwendungen, indem Prozesse in ihren eigenen Namespace isoliert werden. Citrix Hypervisor Container Management unterstützt die Überwachung und Verwaltung von Windows Server Containern unter Windows Server 2016-Gastbetriebssystemen.

> **Hinweis:**
>
> Windows Server 2016-VMs müssen mit einer oder mehreren statischen IP-Adressen für die TLS-Kommunikation konfiguriert werden, da TLS-Serverzertifikate an bestimmte IP-Adressen gebunden sind.

So bereiten Sie Windows Server-Container für die Containerverwaltung vor:

1. Stellen Sie sicher, dass auf der VM Citrix VM Tools installiert sind und dass das VM-Netzwerk wie unter beschrieben konfiguriert ist Netzwerkanforderungen und -sicherheit.
2. Installieren Sie Windows Server Container-Unterstützung innerhalb der VM wie unter beschriebenMicrosoft-Dokumentation. Windows Server-Container sind keine Hyper-V-Container.
3. Erstellen Sie eine Datei, die`daemon.json` im Ordner`C:\ProgramData\docker\config` mit dem Inhalt aufgerufen wird:

```
{

    ”hosts”: [”tcp://0.0.0.0:2376”, ”npipe://”],
    ”tlsverify”: true,
    ”tlscacert”: ”C:\ProgramData\docker\certs.d\ca.pem”,
    ”tlscert”: ”C:\ProgramData\docker\certs.d\server-cert.pem”,
    ”tlskey”: ”C:\ProgramData\docker\certs.d\server-key.pem”
 }
```

4. Bereiten Sie die VM für die Containerverwaltung vor; führen Sie einen der folgenden Befehle in der Steuerdomäne (dom0) auf einem der Hosts im Pool aus:

   Option 1 (für Einzelbenutzer-VMs): Citrix Hypervisor soll TLS-Zertifikate für diese VM generieren.

   > **Wichtig:**
   >
   > Diese Option ist nur dann sicher, wenn nur ein einzelner Benutzer Zugriff auf die VM hat. Der TLS-Server und die Clientschlüssel werden mithilfe einer virtuellen CD in die VM injiziert. Diese Informationen können von böswilligen Benutzern während der Vorbereitung kopiert werden.

```
xscontainer-prepare-vm -v vm_uuid -u root --mode tls --generate-
    certs
```

   Wobei *vm_uuid* die VM ist, die vorbereitet werden soll. Befolgen Sie die Anweisungen auf dem Bildschirm, um das Vorbereiten von Windows Server-Containern abzuschließen. Es beinhaltet die Interaktion mit dom0 und der VM.

   Option 2: Konfigurieren von Citrix Hypervisor mit extern generierten TLS-Zertifikaten


```
xscontainer-prepare-vm -v vm_uuid -u root --mode tls \
    --client-cert client_cert --client-key client_key --ca-cert
       ca_cert
```

Dabei steht *vm_uuid* für die VM, die vorbereitet werden soll, *client_cert* für das TLS-Clientzertifikat, *client_key* für den TLS-Clientschlüssel und *ca_cert* für das Zertifizierungsstellenzertifikat. Bei dieser Option wird davon ausgegangen, dass Docker bereits für TLS innerhalb der VM konfiguriert ist.

Netzwerkanforderungen und -sicherheit

> **Wichtig:**
>
> Damit das Containermanagement funktioniert, kann es notwendig sein, die Sicherheitsanforderungen hinsichtlich der Netzwerkisolierung zu lockern.

Für maximale Sicherheit von Virtualisierungsumgebungen empfehlen Administratoren, das Netzwerk zu partitionieren, indem sie das Verwaltungsnetzwerk von Citrix Hypervisor (mit Citrix Hypervisor Control Domain) von den VMs isolieren.

Das Aktivieren der Containerverwaltung erfordert eine Route zwischen diesen beiden Netzwerken, wodurch das Risiko erhöht wird, dass bösartige VMs das Verwaltungsnetzwerk angreifen (d. h. dom0). Um das Risiko zu verringern, dass der Datenverkehr zwischen VM und dem Verwaltungsnetzwerk zugelassen wird, empfehlen wir die Konfiguration von Firewallregeln, damit nur vertrauenswürdige Quellen eine Verbindung zwischen den beiden Netzwerken initiieren können.

Verwenden Sie diese Funktion in den folgenden Fällen nicht in der Produktion:

- Wenn diese empfohlene Netzwerkkonfiguration nicht mit Ihrem Risikoprofil übereinstimmt
- Wenn Ihnen das erforderliche Know-how im Netzwerk oder in der Firewall fehlt, um diese Route ausreichend für Ihren speziellen Anwendungsfall zu sichern.

Netzwerkpartitionierung und Firewalls

Wie bei anderen VMs können Sie Containerverwaltete VMs nicht direkt mit dem Verwaltungsnetzwerk von Citrix Hypervisor verbinden, um die erforderliche Isolation zu gewährleisten.

Damit die Container-Verwaltung funktioniert, müssen verwaltete VMs über die Control Domain (dom0) des Citrix Hypervisors erreichbar sein. Um Container auf Linux-basierten Betriebssystemen zu überwachen, müssen die Netzwerktopologie und Firewalls ausgehende SSH-Verbindungen von dom0 zu Container-verwalteten VMs zulassen. Um Windows Server-Container zu überwachen, müssen die Netzwerktopologie und Firewalls ausgehende Docker er-TLS-Verbindungen (Ziel-TCP-Port 2376) von dom0 zu Containerverwalteten VMs zulassen.

Um das Risiko zu verringern, dass der Datenverkehr zwischen VM und dem Verwaltungsnetzwerk zugelassen wird, leiten Sie den gesamten Datenverkehr über eine externe statusbehaftete Firewall. Diese Firewall muss manuell von einem Experten entsprechend Ihren geschäftlichen und Sicherheitsanforderungen eingerichtet und konfiguriert werden.

Der folgende Abschnitt enthält eine Beispielkonfiguration:

So sichern Sie Verbindungen zwischen den Netzwerken:

- Verhindern Sie alle Verbindungen zwischen dem Citrix Hypervisor Verwaltungsnetzwerk (einschließlich dom0) und dem VM-Netzwerk (einschließlich containerverwalteten VMs) in beiden Richtungen.

Fügen Sie Ausnahmen für die Aktivierung der Container-Verwaltung hinzu:

- Um das Linux-basierte Betriebssystem zu überwachen, erlauben Sie dom0 ausgehende SSH-Verbindungen (TCP-Port 22) (sowohl NEW als auch ESTINESTIERT) zu Container-verwalteten VMs.
- Zum Überwachen von Windows Server-Containern erlauben Sie dom0 ausgehende Docker er-TLS-Verbindungen (TCP-Port 2376) (sowohl NEW als auch ESTEBUD) mit Containerverwalteten VMs.
- Behälterverwaltete VMs können auf SSH- und Docker er-TLS-Verbindungen antworten, die von dom0 initiiert wurden.

Authentifizierung auf Linux-basierten Betriebssystemen

Das Container-Management von Citrix Hypervisor verwendet ein pool-spezifisches 4096-Bit-private/öffentliches RSA-Schlüsselpaar zur Authentifizierung auf Container-verwalteten VMs. Der private Schlüssel wird in der Citrix Hypervisor Control Domain (dom0) gespeichert. Der jeweilige Public-Key wird während der Vorbereitung auf Container Managed VMs registriert, entweder über das Cloud Config Drive oder die`~user/.ssh/authorized_keys` Datei. Wie bei allen privaten/öffentlichen Schlüsselpaaren üblich muss der private Schlüssel sicher aufbewahrt werden, da er einen passwortlosen Zugriff auf alle Container Managed VMs ermöglicht. Dieser Zugriff umfasst sowohl derzeit verwaltete VMs als auch VMs, die in der Vergangenheit verwaltet wurden.

Die Containerverwaltung von Citrix Hypervisor versucht, Container Managed VMs über eine der IP-Adressen zu erreichen, die von den Citrix VM-Tools angekündigt werden, die innerhalb der VM ausgeführt werden. Nach einer ersten Verbindung speichert Citrix Hypervisor den öffentlichen Schlüssel von Container-verwalteten VMs und überprüft, ob der Schlüssel bei jeder nachfolgenden Verbindung übereinstimmt. Stellen Sie sicher, dass nur die Container Managed VM über die angekündigte IP kontaktiert werden kann (mit IP Source Guard oder ähnlichen Mitteln). Wenn die Netzwerktopologie dieses Verhalten nicht gewährleisten kann, empfehlen wir Administratoren, den SSH-Hostschlüssel

zu bestätigen, den die Containerverwaltung beim Herstellen der ersten Verbindung mit der VM erhalten hat.

Auf den Schlüssel kann mit dem folgenden Befehl zugegriffen werden:

```
xe vm-parm-get-uuid=vm_uuid param-name=other-config  /
  param-key=xscontainer-sshhostkey
```

vm_uuid ist die UUID der VM

Authentifizierung für Windows Server-Container

Citrix Hypervisor verwendet SSL oder TLS, um Windows Server-Container zu überwachen und zu steuern. In diesem Fall fungiert Citrix Hypervisor als SSL/TLS-Client, und Windows Server-VMs fungieren als SSL/TLS-Server. Schlüssel werden sowohl in Dom0 als auch in der VM gespeichert.

> **Wichtig:**
>
> - Der Clientschlüssel muss sicher aufbewahrt werden, da er einen passwortlosen Zugriff auf Docker auf der VM ermöglicht
> - Der Serverschlüssel muss sicher aufbewahrt werden, da er zur Authentifizierung der Überwachungsverbindung zur VM dient

Wenn Citrix Hypervisor Container Management TLS-Zertifikate und -Schlüssel mithilfe der `-generate-certs` Option generiert, werden temporäre Zertifizierungsstellen-, Server- und Clientzertifikate für einen bestimmten Pool und eine bestimmte VM generiert. Zertifikate verwenden sha256-Hash und sind bis zu 2*365 Tage gültig. Nach dieser Zeit wiederholen Sie die Vorbereitung. Die TLS-Verbindung wird immer mit einer AES128-SHA-Verschlüsselung hergestellt.

Notizen

Wenn Sie Citrix Hypervisor Container Management und Docker verwenden, beachten Sie die folgenden Verhaltensweisen:

- Durch das Umbenennen eines Containers wird die Containerverwaltungsansicht nicht aktualisiert. Darüber hinaus löst das Anhalten oder Aufheben eines Containers von außerhalb XenCenter unter Ubuntu 14.04 die Ansicht nicht zum Aktualisieren aus. Dieses Verhalten kann bedeuten, dass Citrix Hypervisor möglicherweise nicht den aktuellen Container-Status (umbenannt/angehalten) anzeigt. Die zugrunde liegende Ursache ist, dass die Ansicht nur nach Docker Ereignisbenachrichtigungen aktualisiert wird. Als Problemumgehung kann die Aktualisierung ausgelöst werden, indem eine Aktion (d. h. Start oder Stop) für einen nicht verwandten Container auf derselben VM ausgeführt wird.

Kopiert!
Failed!

vApps

October 16, 2019

Eine vApp ist eine logische Gruppe von einer oder mehreren verwandten virtuellen Maschinen (VMs), die als einzelne Entität gestartet werden kann. Wenn eine vApp gestartet wird, werden die in der vApp enthaltenen VMs in einer vom Benutzer vordefinierten Reihenfolge gestartet. Mit dieser Funktion können VMs, die voneinander abhängig sind, automatisch sequenziert werden. Ein Administrator muss den Start abhängiger VMs nicht mehr manuell sequenzieren, wenn ein ganzer Dienst neu gestartet werden muss (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 Disaster Recovery-Situation nützlich. Sie können alle VMs, die sich im selben Speicher-Repository befinden, oder alle VMs, die sich auf dieselbe Service Level Agreement (SLA) beziehen, gruppieren.

> **Hinweis:**
>
> vApps können sowohl mit XenCenter als auch mit der xe-CLI erstellt und geändert werden. Informationen zum Arbeiten mit vApps mithilfe der CLI finden Sie unterBefehlszeilenschnittstelle.

Verwalten von vApps in XenCenter

Im Dialogfeld „ **vApps verwalten** “ können Sie vApps erstellen, löschen, ändern, starten und herunterfahren sowie vApps im ausgewählten Pool importieren und exportieren. Wenn Sie eine vApp in der Liste auswählen, werden die darin enthaltenen VMs im Detailbereich auf der rechten Seite aufgeführt.

Sie können **vApps verwalten** verwenden, um die folgenden Aktionen auszuführen:

- So ändern Sie den Namen oder die Beschreibung einer vApp
- So fügen Sie VMs der vApp hinzu oder entfernen sie daraus
- So ändern Sie die Startsequenz der VMs in der vApp

So ändern Sie vApps:

1. Select den Pool aus, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus.

   Alternativ können Sie mit der rechten Maustaste im **Ressourcenbereich** klicken und im Kontextmenü **vApps verwalten** auswählen.

2. Select die vApp aus, und wählen Sie **Eigenschaften** , um das Dialogfeld Eigenschaften zu öffnen.

3. Select die Registerkarte **Allgemein** , um den vApp-Namen oder die Beschreibung zu ändern.
4. Select die Registerkarte **Virtuelle Maschinen** , um VMs der vApp hinzuzufügen oder daraus zu entfernen.
5. Select die Registerkarte **VM-Startsequenz** , um die Werte für die Startreihenfolge und das Verzögerungsintervall für einzelne VMs in der vApp zu ändern.
6. Klicken Sie auf **OK** , um die Änderungen zu speichern und **Eigenschaften** zu schließen.

Weitere Informationen finden Sie in der XenCenter Hilfe. Drücken Sie **F1** , oder klicken Sie auf **Hilfe** , um die XenCenter Hilfe anzuzeigen.

Erstellen von vApps

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, das Erstellen mehrerer vApps mit demselben Namen zu vermeiden, 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, die einen Startreihenwert von 0 (Null) haben, werden zuerst gestartet. VMs, die einen Startauftragswert von 1 haben, werden als nächstes gestartet. Dann werden VMs mit einem Startreihenwert von 2 gestartet usw.

Wert	Beschreibung
Versuchen Sie, die nächste VM nach	Gibt an, wie lange nach dem Starten 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, die eine niedrigere Startreihenfolge aufweisen.

1. Auf der letzten Seite von „ **vApps verwalten**“ können Sie die vApp-Konfiguration überprüfen. Klicken Sie auf **Zurück** , um die Einstellungen zu ändern, oder auf **Fertig stellen** , um die vApp zu erstellen und **vApps verwalten** zu schließen.

   > **Hinweis:**
   >
   > Eine vApp kann sich über mehrere Server in einem einzigen Pool erstrecken, kann sich jedoch nicht über mehrere Pools erstrecken.

Löschen von vApps

Gehen Sie folgendermaßen vor, um eine vApp zu löschen:

1. Wählen Sie den Pool aus, und wählen Sie im Menü **Pool** die Option **vApps verwalten** aus.
2. Select die vApp, die Sie löschen möchten, aus der Liste aus. Klicken Sie auf **Löschen**.

> **Hinweis:**
>
> Die VMs in der vApp werden **nicht** gelöscht.

Starten und Herunterfahren von vApps mithilfe von XenCenter

Verwenden Sie zum Starten oder Herunterfahren einer vApp die Option **„vApps verwalten“**, auf die über das Menü „Pool“ zugegriffen wird. Wenn Sie eine vApp starten, werden alle darin eingesetzten VMs automatisch nacheinander gestartet. Die für jede einzelne VM angegebenen Werte für die Startreihenfolge und das Verzögerungsintervall steuern die Startsequenz. Diese Werte können beim ersten Erstellen der vApp festgelegt werden. Ändern Sie diese Werte jederzeit im Dialogfeld „vApp-Eigenschaften“ oder im Dialogfeld „VM-Eigenschaften“.

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. Alternativ können

Sie mit der rechten Maustaste im **Ressourcenbereich** 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. Alternativ können Sie mit der rechten Maustaste im **Ressourcenbereich** 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.

   Auf allen VMs wird versucht, ein weiches Herunterfahren durchzuführen. 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. Möglicherweise werden nicht immer alle laufenden Prozesse heruntergefahren. Wenn Sie eine VM auf diese Weise herunterfahren, riskieren Sie, Daten zu verlieren. Verwenden Sie ein erzwungenes Herunterfahren nur, wenn ein Soft-Shutdown nicht möglich ist.

Importieren und Exportieren von 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 die unter beschriebenen Schritte Exportieren von VMs als OVF/OVA.

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 die unter beschriebenen Schritte VMs als OVF/OVA importieren.

Nachdem der Import abgeschlossen ist, wird die neue vApp in der Liste der vApps unter **vApps verwalten**angezeigt.

Kopiert!
Failed!

Virtuelle Demo-Linux-Appliance

October 16, 2019

Wir bieten eine voll funktionsfähige Installation einer Demo Linux Virtual Appliance, basierend auf einer CentOS 7.5-Distribution.

Die Appliance steht zum Download in einer einzigen`xva` Datei auf derCitrix Hypervisor Herunterladen Seite zur Verfügung.

Die`xva` Datei kann schnell in XenCenter importiert werden, um eine voll funktionsfähige virtuelle Linux-Maschine zu erstellen. Es sind keine zusätzlichen Konfigurationsschritte erforderlich.

Mit der virtuellen Demo Linux Appliance können Sie eine VM schnell und einfach bereitstellen. Mit dieser Appliance können Sie Citrix Hypervisor Produktfunktionen wie Live-Migration, dynamische Speichersteuerung und hohe Verfügbarkeit testen. Citrix VM-Tools sind in der virtuellen Demo-Linux-Appliance vorinstalliert. Die Appliance umfasst außerdem vorkonfigurierte Netzwerkkonnektivität und einen Webserver für Testzwecke.

> **Warnhinweis:**
>
> Verwenden Sie die virtuelle Demo-Linux-Appliance nicht zum Ausführen von Produktions-Workloads.

Importieren der virtuellen Demo-Linux-Appliance

1. Laden Sie die virtuelle Demo Linux Appliance von derCitrix Hypervisor HerunterladenSeite herunter.

   Kunden benötigen Zugriff auf **My Account** , um auf diese Seite zugreifen zu können. Wenn Sie kein Konto haben, können Sie sich auf der Citrix Homepage registrieren.

2. Wählen Sie im Bereich **Ressourcen** einen Host oder einen Pool aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Importieren** aus. Der Import-Assistent wird angezeigt.

3. Klicken Sie auf **Durchsuchen** , und navigieren Sie zum Speicherort der heruntergeladenen Demo Linux Virtual`xva` Appliance-Datei auf Ihrem Computer.

4. Klicken Sie auf **Weiter**.
5. Select den Citrix Hypervisor-Zielserver oder -Pool aus, und klicken Sie dann auf **Weiter**.
6. Select ein Speicher-Repository aus, auf dem die Festplatte der virtuellen Appliance erstellt werden soll, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Fertig stellen** , um die virtuelle Appliance zu importieren.

> **Hinweis:**
>
> Wenn Sie die VM zum ersten Mal starten, werden Sie aufgefordert, ein Root-Kennwort einzugeben. Anschließend wird die IP-Adresse der VM angezeigt. Stellen Sie sicher, dass Sie die IP-Adresse aufzeichnen, da sie für Testzwecke nützlich ist.

Nützliche Tests

In diesem Abschnitt werden einige nützliche Tests aufgeführt, die durchgeführt werden müssen, um sicherzustellen, dass Ihre virtuelle Demo Linux Appliance korrekt konfiguriert ist.

1. Testen Sie, ob Sie über externe Netzwerkkonnektivität verfügen.

   Melden Sie sich über die XenCenter Konsole bei der VM an. Führen Sie diesen Kommentar aus, um Ping-Pakete an Google und zurück zu senden:

   ```
   1 ping -c 10 google.com
   ```

   Weitere installierte Netzwerkwerkzeuge sind ifconfig, netstat und tracepath.

2. Testen Sie anhand der beim Starten der virtuellen Maschine angezeigten IP-Adresse, ob Sie die VM von einem externen Computer aus pingen können.
3. Testen Sie, ob der Webserver konfiguriert ist.

   Geben Sie in einem Webbrowser die VM-IP-Adresse ein. Die Seite „Demonstration Linux Virtual Machine“ wird geöffnet. Auf dieser Seite werden einfache Informationen zu den bereitgestellten VM-Datenträgern, ihrer Größe, ihrem Standort und ihrer Verwendung angezeigt.

Sie können die Webseite auch zum Bereitstellen eines Datenträgers verwenden.

Bereitstellen eines Datenträgers mit der Webseite der virtuellen Demonstration Linux Machine

1. Fügen Sie Ihrer VM in XenCenter ein virtuelles Laufwerk hinzu. Select die VM im Bereich **Ressourcen** aus, öffnen Sie die Registerkarte **Speicher** , und klicken Sie dann auf **Hinzufügen** .
2. Geben Sie den Namen des neuen virtuellen Laufwerks und optional eine Beschreibung ein.

3. Geben Sie die Größe des neuen virtuellen Laufwerks ein.

   Stellen Sie sicher, dass das Speicher-Repository, in dem das virtuelle Laufwerk gespeichert ist, genügend Speicherplatz für das neue virtuelle Laufwerk hat.

4. Select die SR aus, in der das neue virtuelle Laufwerk gespeichert ist.
5. Klicken Sie auf **Erstellen** , um das neue virtuelle Laufwerk hinzuzufügen und das Dialogfeld zu schließen.
6. Klicken Sie auf die Registerkarte **Konsole** , und verwenden Sie Ihre normalen Tools, um die Festplatte nach Bedarf zu partitionieren und zu formatieren.
7. Aktualisieren Sie die Demo Linux Virtual Machine Webseite, die neue Festplatte wird angezeigt.
8. Klicken Sie auf **Einhängen**. Diese Aktion mountet den Datenträger, und Dateisysteminformationen werden angezeigt.

Weitere Informationen zum Hinzufügen virtueller Laufwerke finden Sie in der XenCenter Hilfe.

Kopiert!
Failed!

Erweiterte Notizen für virtuelle Maschinen

October 16, 2019

Dieser Abschnitt enthält einige erweiterte Hinweise zu virtuellen Maschinen.

VM-Startverhalten

Es gibt zwei Optionen für das Verhalten des VDI einer virtuellen Maschine, wenn die VM gestartet wird:

> **Hinweis:**
>
> Die VM muss heruntergefahren werden, bevor Sie die Einstellung des Startverhaltens ändern können.

Persistieren (Citrix Virtual Desktops - Privatdesktop-Modus)

Dieses Verhalten ist die Standardeinstellung beim Starten von VMs. Der VDI befindet sich in dem Zustand, in dem er sich beim letzten Herunterfahren befand.

Select diese Option aus, wenn Sie Benutzern erlauben möchten, dauerhafte Änderungen an ihren Desktops vorzunehmen. Um persist auszuwählen, fahren Sie die VM herunter, und geben Sie dann den folgenden Befehl ein:


```
xe vdi-param-set uuid=vdi_uuid on-boot=persist
```

Zurücksetzen (Citrix Virtual Desktops - Freigegebener Desktopmodus)

Beim Starten der virtuellen Maschine wird der VDI in den Zustand zurückgesetzt, in dem er sich beim vorherigen Start befand. Alle Änderungen, die während der Ausführung der VM vorgenommen werden, gehen beim nächsten Starten der VM verloren.

Select diese Option aus, wenn Sie standardisierte Desktops bereitstellen möchten, die Benutzer nicht dauerhaft ändern können. Um „Zurücksetzen“ auszuwählen, fahren Sie die VM herunter, und geben Sie dann den folgenden Befehl ein:

```
xe vdi-param-set uuid=vdi_uuid on-boot=reset
```

> **Warnhinweis:**
>
> Nach dem Ändernon-boot=resetwerden alle im VDI gespeicherten Daten nach dem nächsten Herunterfahren/Starten oder Neustart verworfen.

Bereitstellung der ISO-Bibliothek für Citrix Hypervisor -Server

Um eine ISO-Bibliothek für Citrix Hypervisor or-Server zur Verfügung zu stellen, erstellen Sie ein externes NFS- oder SMB/CIFS-Freigabeverzeichnis. Der NFS- oder SMB/CIFS-Server muss Root-Zugriff auf die Freigabe zulassen. Erlauben Sie für NFS-Freigaben den Zugriff, indem Sie dasno_root_squash Flag festlegen, wenn Sie den Freigabeeintrag/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
```

Für die erweiterte Verwendung können Sie zusätzliche Argumente an den Befehl mount übergeben.

Um eine Windows SMB/CIFS-Freigabe für den Host zur Verfügung zu stellen, verwenden Sie 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
```

Ersetzen Sie hintere Schrägstriche imunc_path Argument durch Schrägstriche. Zum Beispiel:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
```


Nach dem Einhängen der Freigabe sind alle verfügbaren ISOs in XenCenter in der Liste **Install from ISO-Bibliothek oder DVD-Laufwerk** verfügbar. Diese ISOs sind auch als CD-Images über die CLI-Befehle verfügbar.

Fügen Sie das ISO an eine entsprechende Windows Vorlage an.

VSS (Windows Volume Shadow Copy Service) -Anbieter

Die Windows Tools enthalten auch einen VSS-Anbieter für Citrix Hypervisor, mit dem das Gastdateisystem zur Vorbereitung eines VM-Snapshots stillgelegt wird. Der VSS-Anbieter wird als Teil der Installation des PV-Treibers installiert, ist aber standardmäßig nicht aktiviert.

So aktivieren Sie den Windows Citrix Hypervisor VSS-Anbieter:

1. Installieren Sie die Windows PV-Treiber.
2. Navigieren Sie zu dem Verzeichnis`c:\Program Files\Citrix\XenTools`, in dem die Treiber installiert sind (standardmäßig oder`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\Install_dir`in der Windows Registrierung).
3. Doppelklicken Sie auf den`install-XenProvider.cmd` Befehl, um den VSS-Provider zu aktivieren.

> **Hinweise:**
>
> - Der VSS-Anbieter wird automatisch deinstalliert, wenn die PV-Treiber deinstalliert werden. Aktivieren Sie den VSS-Anbieter erneut, wenn er erneut installiert wird. Sie können separat von den PV-Treibern deinstalliert werden, indem Sie`uninstall-XenProvider.cmd` im selben Verzeichnis verwenden.
> - Die Verwendung von VSS-Snapshots auf GFS2-SRs wird nicht unterstützt.

Herstellen einer Verbindung mit einer Windows VM mithilfe von Remotedesktop

Sie können eine der folgenden Möglichkeiten zum Anzeigen einer Windows VM-Konsole verwenden, die beide die volle Nutzung von Tastatur und Maus unterstützen.

- Verwenden von XenCenter. Diese Methode stellt eine standardmäßige grafische Konsole bereit und verwendet die in Citrix Hypervisor integrierte VNC-Technologie, um den Remotezugriff auf die Konsole der virtuellen Maschine zu ermöglichen.
- Herstellen einer Verbindung mit Windows Remote Desktop. Diese Methode verwendet die Remote Desktop Protocol-Technologie

In XenCenter auf der Registerkarte **Konsole** befindet sich die Schaltfläche **Zu Remote Desktop wechseln** . Diese Schaltfläche deaktiviert die standardmäßige grafische Konsole in XenCenter und wechselt zu Remote Desktop.

Wenn Remotedesktop in der VM nicht aktiviert ist, ist diese Schaltfläche deaktiviert. Um es zu aktivieren, installieren Sie die Citrix VM-Tools. Gehen Sie folgendermaßen vor, um sie auf jeder VM zu aktivieren, die Sie mit Remotedesktop verbinden möchten.

So aktivieren Sie den Remotedesktop auf einer Windows VM:

1. Öffnen Sie **System** , indem Sie auf die Schaltfläche **Start** klicken, mit der rechten Maustaste auf **Computer** , und wählen Sie dann **Eigenschaften** aus.
2. Klicken Sie auf **Remoteeinstellungen**. Wenn Sie zur Eingabe eines Administratorkennworts aufgefordert werden, geben Sie das Kennwort ein, das Sie während der VM-Einrichtung erstellt haben.
3. Klicken Sie im Bereich **Remotedesktop** auf das Kontrollkästchen **Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird** (Windows 7).
4. Um Nicht-Administratorbenutzer Select, 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 für die Windows Domäne können standardmäßig eine Verbindung herstellen.

Sie können jetzt über Remote Desktop eine Verbindung zu dieser VM herstellen. Weitere Informationen finden Sie im Microsoft Knowledge Base-ArtikelHerstellen einer Verbindung mit einem anderen Computer mithilfe der Remotedesktopverbindung.

> **Hinweis:**
>
> Sie können keine Verbindung zu einer virtuellen Maschine herstellen, die im Ruhezustand oder im Ruhezustand ist. Legen Sie die Einstellungen für den Ruhezustand und den Ruhezustand auf dem Remotecomputer auf **Nie**fest.

Zeitverarbeitung in Windows VMs

Für Windows Gäste steuert zunächst die Kontrolldomänenuhr die Zeit. Die Zeit wird während der VM-Lebenszyklusvorgänge wie Suspendieren und Neustart aktualisiert.Wir empfehlen, einen zuverlässigen NTP-Dienst in der Steuerdomäne und allen Windows VMs auszuführen.

Wenn Sie manuell festlegen, dass eine VM zwei Stunden vor der Steuerdomäne liegt, bleibt sie erhalten. Sie können die VM voraussetzen, indem Sie einen Zeitzonenoffset innerhalb der VM verwenden. Wenn Sie später die Zeit der Steuerdomäne ändern (entweder manuell oder über NTP), wird die VM entsprechend verschoben, behält jedoch den Abstand von zwei Stunden bei. Das Ändern der Zeitzone der Steuerdomäne wirkt sich nicht auf VM-Zeitzonen oder Offset aus. Citrix Hypervisor verwendet die Hardware-Uhreinstellung der VM, um die VM zu synchronisieren. Citrix Hypervisor verwendet die Systemtakteinstellung der VM nicht.

Stellen Sie beim Aussetzen und Fortsetzen von Vorgängen oder bei der Livemigration sicher, dass die aktuellen Citrix VM-Tools installiert sind. Citrix VM-Tools benachrichtigen den Windows Kernel, dass nach dem Fortsetzen (möglicherweise auf einem anderen physischen Host) eine Zeitsynchronisierung erforderlich ist.

> **Hinweis:**
>
> Wenn Sie Windows VMs in Citrix Virtual Desktops Umgebung ausführen, müssen Sie sicherstellen, dass die Hostuhr dieselbe Quelle wie die Active Directory Domäne (AD) hat. Ein Fehler beim Synchronisieren der Uhren kann dazu führen, dass die VMs eine falsche Zeit anzeigen und die Windows PV-Treiber zum Absturz bringen.

Zeitverarbeitung in Linux-VMs

Das Zeitverarbeitungsverhalten von Linux-VMs in Citrix Hypervisor hängt davon ab, ob es sich bei der VM um einen PV-Gast oder einen HVM-Gast handelt.

Zusätzlich zu dem von Citrix Hypervisor definierten Verhalten können Betriebssystemeinstellungen und -verhalten das Zeitverarbeitungsverhalten Ihrer Linux-VMs beeinflussen. Einige Linux-Betriebssysteme synchronisieren möglicherweise die Systemuhr und die Hardware-Uhr in regelmäßigen Abständen, oder das Betriebssystem verwendet standardmäßig einen eigenen NTP-Dienst. Weitere Informationen finden Sie in der Dokumentation zum Betriebssystem Ihrer Linux-VM.

> **Hinweis:**
>
> Stellen Sie bei der Installation einer neuen Linux-VM sicher, dass Sie die Zeitzone von der Standard-UTC in Ihren lokalen Wert ändern. Spezifische Anweisungen zur Verteilung finden Sie unterLinux Versionshinweise.

Zeitverarbeitung in PV-Linux-VMs

Es gibt zwei *Wanduhr-Verhalten* für paravirtualisierte Linux-Distributionen — *abhängig* und *unabhängig* .

Abhängige Wanduhr: Die Systemuhren in PV-Linux-VMs werden mit der auf der Steuerdomäne ausgeführten Uhr synchronisiert und können nicht unabhängig voneinander geändert werden. Dieser Modus ist praktisch, da nur die Steuerdomäne den NTP-Dienst (Network Time Protocol) ausführen muss, um die genaue Zeit auf allen VMs zu halten.

Unabhängige Wanduhr: Systemuhren in PV-Linux-VMs werden **nicht** mit der auf der Steuerdomäne laufenden Uhr synchronisiert und können geändert werden. Wenn die VM gestartet wird, wird die Kontrolldomänenzeit verwendet, um die Anfangszeit der Systemuhr festzulegen.

Einige PV-Linux-VMs können die`independent_wallclock` Einstellung verwenden, um das Wanduhrverhalten der VM zu ändern.

Die folgende Tabelle listet das Wanduhrverhalten für PV-Linux-VMs auf:

Gastbetriebssystem	Standard-Wanduhrverhalten	Ist`independent_wallclock` die Einstellung verfügbar?
CentOS 5.x (32-/64-Bit)	Abhängig	Ja
CentOS 6.x (32-/64-Bit)	Unabhängig	
Red Hat Enterprise Linux 5.x (32-/64-Bit)	Abhängig	Ja
Red Hat Enterprise Linux 6.x (32-/64-Bit)	Unabhängig	
Oracle Linux 5.x (32-/64-Bit)	Abhängig	Ja
Oracle Linux 6.x (32-/64-Bit)	Unabhängig	
Scientific Linux 6.x (32-/64-Bit)	Unabhängig	
SLES 11 SP3, SP4 (32-/64-Bit)	Unabhängig	Ja (No-op)
SLES 12 SP1, SP2 (64 Bit)	Unabhängig	Ja (No-op)
SED 11 SP3, SP4 (64 Bit)	Unabhängig	Ja (No-op)
SED 12 SP1, SP2 (64 Bit)	Unabhängig	Ja (No-op)
Debian 7 (32-/64-Bit)	Unabhängig	
NeoKylin Linux Advanced Server 6.5 (64-bit)	Unabhängig	
NeoKylin Linux Advanced Server 7.2 (64-bit)	Unabhängig	

Bei PV-Linux-VMs, auf denen die`independent_wallclock` Einstellung verfügbar ist, können Sie mit dieser Einstellung festlegen, ob die VM ein abhängiges oder unabhängiges Wanduhrverhalten hat.

> **Wichtig:**
>
> Es wird empfohlen, die`independent_wallclock` Einstellung zu verwenden, um ein unabhängiges Wanduhrverhalten zu aktivieren und einen zuverlässigen NTP-Dienst auf den Linux-VMs und dem Citrix Hypervisor or-Server auszuführen.

So richten Sie einzelne Linux-VMs auf ein unabhängiges Wanduhrverhalten ein:

1. Führen Sie an einer Root-Eingabeaufforderung auf der VM den folgenden Befehl aus:`echo 1 > /proc/sys/xen/independent_wallclock`
2. Diese Einstellung kann bei Neustarts beibehalten werden, indem Sie die `/etc/sysctl.conf` Konfigurationsdatei ändern und Folgendes hinzufügen:

```
## Set independent wall clock time
xen.independent_wallclock=1
```

3. Als dritte Alternative `independent_wallclock=1` kann auch als Boot-Parameter an die VM übergeben werden.

So richten Sie einzelne Linux-VMs auf ein abhängiges Wanduhrverhalten ein:

1. Führen Sie an einer Root-Eingabeaufforderung auf der VM den folgenden Befehl aus:`echo 0 > /proc/sys/xen/independent_wallclock`
2. Diese Einstellung kann bei Neustarts beibehalten werden, indem Sie die `/etc/sysctl.conf` Konfigurationsdatei ändern und Folgendes hinzufügen:

```
## Set independent wall clock time
xen.independent_wallclock=0
```

3. Als dritte Alternative `independent_wallclock=0` kann auch als Boot-Parameter an die VM übergeben werden.

HVM-Linux-VMs

Hardware-Uhren in HVM Linux-VMs werden **nicht** mit der auf der Steuerdomäne ausgeführten Uhr synchronisiert und können geändert werden. Wenn die VM zum ersten Mal gestartet wird, wird die Kontrolldomänenzeit verwendet, um die Anfangszeit der Hardware-Uhr und Systemuhr einzustellen.

Wenn Sie die Zeit auf der Hardware-Uhr ändern, wird diese Änderung beibehalten, wenn die VM neu gestartet wird.

Systemtaktverhalten hängt vom Betriebssystem der VM ab. Weitere Informationen finden Sie in der Dokumentation zu Ihrem VM-Betriebssystem.

Sie können das Verhalten der Citrix Hypervisor Zeitbehandlung für HVM Linux-VMs nicht ändern.

Installieren von HVM-VMs von Reseller Option Kit (BIOS-gesperrte) Medien

Es gibt zwei Arten von HVM-VMs: BIOS-Generic und BIOS-Customized. Um die Installation von Reseller Option Kit (BIOS-gesperrte) OEM-Versionen von Windows auf eine VM zu aktivieren, kopieren Sie die BIOS-Zeichenfolgen der VM vom Host, mit dem das Medium geliefert wurde. Alternativ können fortgeschrittene Benutzer benutzerdefinierte Werte für die BIOS-Zeichenfolgen festlegen.

BIOS-generisch

Die VM verfügt über generische Citrix Hypervisor or-BIOS-Zeichenfolgen.

> **Hinweis:**
>
> Wenn beim Start auf einer VM keine BIOS-Zeichenfolgen festgelegt sind, werden die standard-mäßigen Citrix Hypervisor or-BIOS-Zeichenfolgen eingefügt, und die VM wird zu BIOS-Generic.

BIOS-Maßgeschneidert

Für HVM-VMs können Sie das BIOS auf zwei Arten anpassen: Copy-Host-BIOS-Zeichenfolgen und be-nutzerdefinierte BIOS-Zeichenfolgen.

Kopieren-Host-BIOS-Zeichenfolgen

Die VM verfügt über eine Kopie der BIOS-Zeichenfolgen eines bestimmten Servers im Pool. Um die mit dem Host gelieferten BIOS gesperrten Medien zu installieren, befolgen Sie die unten angegebenen Schritte.

Verwenden von XenCenter:

1. Aktivieren Sie das Kontrollkästchen **Host-BIOS-Zeichenfolgen auf VM kopieren** im Assistenten für neue VM.

Verwenden der CLI:

1. Führen Sie den`vm-install copy-bios-strings-from` Befehl aus. Geben Sie den`host-uuid` als 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
```

Dieser Befehl gibt die UUID der neu erstellten VM zurück.

Zum 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
```


2. Wenn die relevanten BIOS-Strings vom Host erfolgreich in die VM kopiert wurden,`vm-is-bios-customized` bestätigt der Befehl diesen Erfolg:

```
xe vm-is-bios-customized uuid=VM uuid
```

Zum Beispiel:

```
xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
    This VM is BIOS-customized.
```

> **Hinweis:**
>
> Wenn Sie die VM starten, wird sie auf dem physischen Host gestartet, von dem Sie die BIOS-Zeichenfolgen kopiert haben.

> **Warnhinweis:**
>
> 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, benutzerdefinierte Werte in ausgewählten BIOS-Zeichenfolgen mit CLI/API festzulegen. Um die Medien in HVM-VM mit angepasstem BIOS zu installieren, befolgen Sie das unten angegebene Verfahren.

Verwenden der CLI:

1. Führen Sie den`vm-install` Befehl 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
```

Dieser Befehl gibt die UUID der neu erstellten VM zurück.

Zum Beispiel:

```
xe vm-install template="win7sp1" sr-name-label=Local\ storage  \
      new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
```

2. Um benutzerdefinierte BIOS-Zeichenfolgen 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
```

Zum 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
```

> **Hinweise:**
>
> ```
> - Sobald die benutzerdefinierten BIOS-Zeichenfolgen in einem
>   einzigen CLI/API-Aufruf festgelegt wurden, können sie nicht
>    geändert werden. - Sie können die Anzahl der Parameter
>   festlegen, die Sie angeben möchten, um die
>   benutzerdefinierten BIOS-Zeichenfolgen festzulegen.
> ```

> **Warnhinweis:**
>
> 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, funktionierende Parameter sind. Das Bereitstellen falscher Parameter kann zu einem Fehler bei der Boot-/Medieninstallation führen.

Zuweisen einer GPU zu einer Windows VM (zur Verwendung mit Citrix Virtual Desktops)

Mit Citrix Hypervisor können Sie einer Windows VM, die auf demselben Host ausgeführt wird, eine physische GPU im Citrix Hypervisor or-Server zuweisen. Diese GPU-Pass-Through-Funktion profitiert von Grafiknutzern wie CAD-Designern, die leistungsstarke Grafikfunktionen benötigen. Es wird nur für die Verwendung mit Citrix Virtual Desktops unterstützt.

Citrix Hypervisor unterstützt zwar nur eine GPU für jede VM, erkennt und gruppiert jedoch automatisch identische physische GPUs auf Hosts im selben Pool. Sobald einer Gruppe von GPUs zugewiesen wurde, 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 eine VM über bestimmte Funktionen, die nicht mehr verfügbar sind, einschließlich Livemigration, VM-Snapshots mit Arbeitsspeicher und Anhalten/Fortsetzen.

Das Zuweisen einer GPU zu einer VM in einem Pool beeinträchtigt den Betrieb anderer VMs im Pool nicht. VMs mit angeschlossenen GPUs gelten jedoch als nicht agil. Wenn VMs mit verbundenen GPUs Mitglieder eines Pools mit aktivierter Hochverfügbarkeit sind, übersehen beide Features diese VMs. Die VMs können nicht automatisch migriert werden.

GPU-Pass-Through ist nur für Windows VMs verfügbar. Sie kann mit XenCenter oder der xe CLI aktiviert werden.

Anforderungen

GPU-Pass-Through wird für bestimmte Maschinen und GPUs unterstützt. In allen Fällen muss die IOMMU-Chipsatzfunktion (VT-d für Intel-Modelle) auf dem Citrix Hypervisor or-Server verfügbar und aktiviert sein. Bevor Sie die GPU-Pass-Through-Funktion aktivieren, besuchen Sie dieHardwarekompatibilitätsliste.

Vor dem Zuweisen einer GPU zu einer VM

Bevor Sie einer VM eine GPU zuweisen, legen Sie die entsprechenden physischen GPUs in den Citrix Hypervisor or-Server ein, und starten Sie den Computer neu. Beim Neustart erkennt Citrix Hypervisor automatisch physische GPUs. Verwenden Sie den`xe pgpu-list` Befehl, um alle physischen GPUs über Hosts im Pool hinweg anzuzeigen.

Stellen Sie sicher, dass die IOMMU-Chipsatzfunktion auf dem Host aktiviert ist. Geben Sie dazu Folgendes ein:

```
1 xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=
    iommu
```

Wenn der gedruckte Wert lautet**`false`**, ist IOMMU nicht aktiviert, und GPU-Pass-Through ist über den angegebenen Citrix Hypervisor or-Server nicht verfügbar.

So weisen Sie einer Windows VM mithilfe von XenCenter eine GPU zu:

1. Fahren Sie die VM herunter, der Sie eine GPU zuweisen möchten.
2. Öffnen Sie die VM-Eigenschaften: Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Eigenschaften**aus.
3. Zuweisen einer GPU zur VM: Select 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 mithilfe der xe-CLI eine GPU zu:

1. Fahren Sie mit dem`xe vm-shutdown` Befehl die VM herunter, der Sie eine GPU-Gruppe zuweisen möchten.
2. Suchen Sie die UUID der GPU-Gruppe, indem Sie Folgendes eingeben:

   ```
   xe gpu-group-list
   ```

   Dieser Befehl druckt alle GPU-Gruppen im Pool. Beachten Sie die UUID der entsprechenden GPU-Gruppe.
3. Fügen 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
   ```

   Führen Sie den`xe vgpu-list` Befehl aus, um sicherzustellen, dass die GPU-Gruppe angefügt wurde.
4. Starten Sie die VM mit dem `xe vm-start` Befehl.
5. Sobald die VM gestartet wird, installieren Sie die Grafikkartentreiber auf der VM.

   Die Installation der Treiber ist unerlässlich, da die VM direkten Zugriff auf die Hardware auf dem Host hat. Treiber werden von Ihrem Hardwarehersteller bereitgestellt.

> **Hinweis:**
>
> Wenn Sie versuchen, eine VM mit GPU-Pass-Through auf dem Host ohne eine verfügbare GPU in der entsprechenden GPU-Gruppe zu starten, gibt Citrix Hypervisor einen Fehler aus.

So trennen Sie eine Windows VM mit XenCenter von einer GPU:

1. Fahren Sie die VM herunter.
2. Öffnen Sie die VM-Eigenschaften: Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Eigenschaften**aus.
3. GPU von der VM trennen: Select **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`xe vm-shutdown` Befehl herunter.
2. Suchen Sie die UUID der vGPU, die mit der VM verbunden ist, indem Sie Folgendes eingeben:

   ```
   xe vgpu-list vm-uuid=uuid_of_vm
   ```


3. Trennen Sie die GPU von der VM, indem Sie Folgendes eingeben:

```
xe vgpu-destroy uuid=uuid_of_vgpu
```

4. Starten Sie die VM mit dem `xe vm-start` Befehl.

Erstellen von ISO-Images

Citrix Hypervisor kann ISO-Images als Installationsmedium und Datenquellen für Windows oder Linux-VMs verwenden. In diesem Abschnitt wird beschrieben, wie ISO-Images von CD/DVD-Medien hergestellt werden.

So erstellen Sie ein ISO auf einem Linux-System:

1. Legen Sie die CD- oder DVD-ROM-Festplatte in das Laufwerk. Stellen Sie sicher, dass der Datenträger nicht bereitgestellt ist. Führen Sie zum Überprüfen den Befehl aus:

```
mount
```

   Wenn der Datenträger eingehängt ist, heben Sie die Bereitstellung des Datenträgers auf. Weitere Informationen finden Sie in der Dokumentation Ihres Betriebssystems.

2. Führen Sie als root den Befehl

```
dd if=/dev/cdrom of=/path/cdimg_filename.iso
```

   Dieser Befehl dauert einige Zeit. Wenn der Vorgang erfolgreich abgeschlossen ist, sehen Sie Folgendes:

```
1187972+0 records in
1187972+0 records out
```

   Ihre ISO-Datei ist bereit.

So erstellen Sie ein ISO auf einem Windows -System:

Windows Computer verfügen über keinen entsprechenden Betriebssystembefehl zum Erstellen eines ISO. Die meisten CD-Brennwerkzeuge verfügen über eine Möglichkeit, eine CD als ISO-Datei zu speichern.

Kopiert!
Failed!

Aktivieren von VNC für Linux-VMs

October 16, 2019

VMs sind möglicherweise nicht für die Unterstützung von Virtual Network Computing (VNC) eingerichtet, die Citrix Hypervisor 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 Sie VNC auf jeder der unterstützten Linux-Betriebssystemverteilungen so konfigurieren, dass ordnungsgemäße Interaktionen mit XenCenter möglich sind.

Verwenden Sie für CentOS-basierte VMs die Anweisungen für die Red Hat-basierten VMs unten, da sie denselben Basiscode verwenden, um grafischen VNC-Zugriff bereitzustellen. CentOS *X* basiert auf Red Hat Enterprise Linux *X* .

Aktivieren einer grafischen Konsole auf Debian-VMs

> **Hinweis:**
>
> Bevor Sie eine grafische Konsole auf Ihrer Debian-VM aktivieren, stellen Sie sicher, dass Sie den Linux-Gast-Agent installiert haben. Weitere Informationen finden Sie unter Installieren des Linux-Gast-Agents.

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-Anzeigemanager die Konsole so, dass ein Anmeldedialogfeld bereitgestellt wird.

1. Installieren Sie Ihren Debian-Gast mit den Desktop-Systempaketen oder installieren Sie GDM (den Display-Manager) mit apt (nach Standardverfahren).
2. Installieren Sie den Xvnc-Server mit`apt-get` (oder ähnlichem):

```
apt-get install vnc4server
```

> **Hinweis:**
>
> Die Debian Graphical Desktop Environment, die den Gnome Display Manager Version 3 Daemon verwendet, kann erhebliche CPU-Zeit in Anspruch nehmen. Deinstallieren Sie das Gnome Display`gdm3` Manager-Paket, und installieren Sie das`gdm` Paket wie folgt:

```
apt-get install gdm
apt-get purge gdm3
```


3. Richten Sie mithilfe desvncpasswd Befehls ein VNC-Kennwort ein (kein Kennwort ist ein ernsthaftes Sicherheitsrisiko) ein. Geben Sie einen Dateinamen ein, in den die Kennwortinformationen geschrieben werden sollen. Zum Beispiel:

```
vncpasswd /etc/vncpass
```

4. Ändern Sie Ihregdm.confDatei (/etc/gdm/gdm.conf), um einen VNC-Server für die Verwaltung der Anzeige zu konfigurieren,0indem Sie[servers]die [daemon]Abschnitte wie folgt:

```
    [servers]
    0=VNC
    [daemon]
    VTAllocation=false
    [server-VNC]
    name=VNC
    command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/
       vncpass BlacklistTimeout=0
    flexible=true
```

5. Starten Sie GDM neu, und warten Sie, bis XenCenter die grafische Konsole erkennt:

```
/etc/init.d/gdm restart
```

> **Hinweis:**
>
> Sie können überprüfen, ob der VNC-Server mit einem Befehl wie ausgeführt wirdps ax | grep vnc.

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 den Linux-Gast-Agent installiert haben. Weitere Informationen finden Sie unter Installieren des Linux-Gast-Agents.

Um VNC auf Red Hat VMs zu konfigurieren, ändern Sie die GDM-Konfiguration. Die GDM-Konfiguration wird in einer Datei gespeichert, deren Speicherort abhängig von der verwendeten Red Hat Linux-Version variiert. Bevor Sie es ändern, bestimmen Sie zuerst den Speicherort dieser Konfigurationsdatei. Diese Datei wird in mehreren nachfolgenden Verfahren in diesem Abschnitt geändert.

> **Hinweis:**

> Informationen zum Aktivieren von VNC für RHEL, CentOS oder OEL 6.x VMs finden Sie unterAktivieren von VNC für RHEL, CentOS oder OEL 6 VMs.

Bestimmen Sie den Speicherort der VNC-Konfigurationsdatei

Wenn Sie Red Hat Linux Version 5.x verwenden, lautet die GDM-Konfigurationsdatei`/etc/gdm/custom.conf`. Diese Datei ist eine geteilte Konfigurationsdatei, die nur benutzerdefinierte Werte enthält, die die Standardkonfiguration außer Kraft setzen. Dieser Dateityp wird standardmäßig in neueren Versionen von GDM verwendet. Es ist in diesen Versionen von Red Hat Linux enthalten.

Konfigurieren von GDM für die Verwendung von VNC

1. Führen Sie den Befehl als root auf der Text-CLI in der VM aus`rpm -q vnc-server gdm`. Die Paketnamen`vnc-server` und`gdm` werden mit den angegebenen Versionsnummern angezeigt.

   Die angezeigten Paketnamen zeigen die Pakete an, die bereits installiert sind. Wenn eine Meldung angezeigt wird, dass ein Paket nicht installiert ist, haben Sie die grafischen Desktop-Optionen während der Installation möglicherweise nicht ausgewählt. Installieren Sie diese Pakete, bevor Sie fortfahren können. Weitere Informationen zur Installation von mehr 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
   ```

   Mit Konfigurationsdateien unter Red Hat Linux 5.x 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 zu lesen:

     `0=VNC`

   - Wenn Sie Red Hat Linux 5.x oder höher 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 ausführen`/usr/sbin/gdm-restart`.

> **Hinweis:**
>
> Red Hat Linux verwendet Runlevel 5 für den grafischen Start. Wenn die Installation in Runlevel 3 gestartet wird, ändern Sie diese Konfiguration, damit der Display-Manager gestartet werden soll, und erhalten Sie Zugriff auf eine grafische Konsole. Weitere Informationen finden Sie unter Runlevels überprüfen.

Firewall-Einstellungen

Die Firewallkonfiguration lässt den VNC-Datenverkehr standardmäßig nicht durchlaufen. Wenn Sie über eine Firewall zwischen der VM und XenCenter verfügen, erlauben Sie Datenverkehr über den Port, den die VNC-Verbindung verwendet. Standardmäßig überwacht ein VNC-Server Verbindungen von einem VNC-Viewer am TCP-Port `5900 + n`, wobei die Anzeigenummer (normalerweise Null) `n` ist. So hört ein VNC-Server-Setup für Display-0 auf TCP-Port`5900`, Display-1 ist`TCP-5901`und so weiter. Überprüfen Sie die Firewall-Dokumentation, um sicherzustellen, dass diese Ports geöffnet sind.

Wenn Sie die IP-Verbindungsverfolgung verwenden oder die Initiierung von Verbindungen nur von einer Seite einschränken möchten, konfigurieren Sie Ihre Firewall weiter.

So konfigurieren Sie die Red HAT-Base VMS-Firewall zum Öffnen des VNC-Ports:

1. Verwenden Sie für Red Hat Linux 5.x`system-config-securitylevel-tui`.
2. Select **Anpassen** aus, und fügen`5900` Sie der Liste der anderen Ports hinzu.

Alternativ können Sie die Firewall bis zum nächsten Neustart deaktivieren`service iptables stop`, indem Sie den Befehl ausführen oder dauerhaft ausführen`chkconfig iptables off`. Diese Konfiguration kann zusätzliche Dienste für die Außenwelt bereitstellen und die allgemeine Sicherheit Ihrer VM reduzieren.

VNC-Bildschirmauflösung

Nach der Verbindung mit einer virtuellen Maschine über die grafische Konsole stimmt die Bildschirmauflösung manchmal nicht überein. Beispielsweise ist die VM-Anzeige zu groß, um bequem in den Bereich „Grafische Konsole“ zu passen. Steuern Sie dieses Verhalten, indem Sie den `geometry` VNC-Serverparameter wie folgt festlegen:

1. Öffnen Sie die GDM-Konfigurationsdatei mit Ihrem bevorzugten Texteditor. Weitere Informationen finden Sie unter Bestimmen Sie den Speicherort der VNC-Konfigurationsdatei.

2. Suchen Sie den `[server-VNC]` Abschnitt, den Sie oben hinzugefügt haben.
3. Bearbeiten Sie die zu lesende Befehlszeile, zum Beispiel:

```
1 command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
```

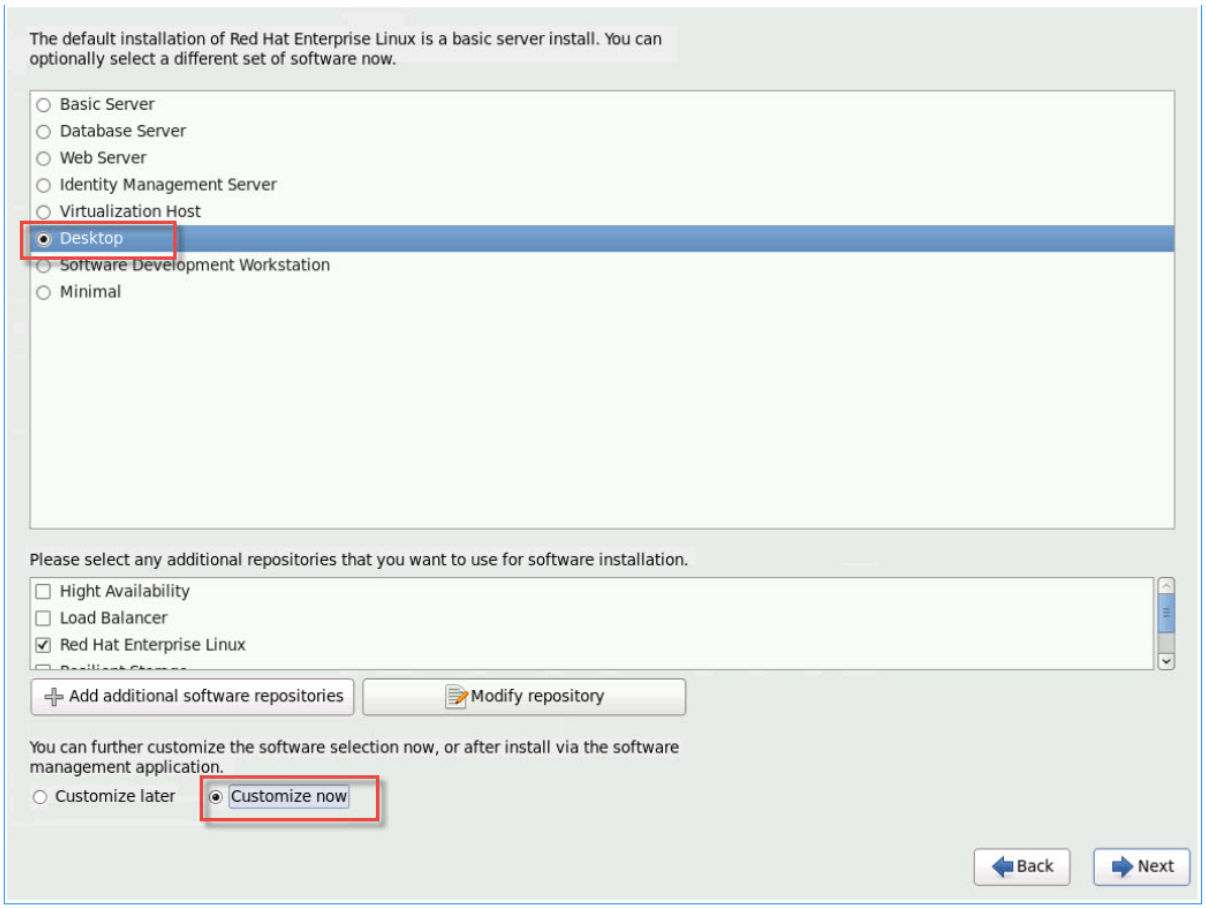
   Der Wert des `geometry` Parameters kann eine beliebige gültige Bildschirmbreite und -höhe sein.

4. Speichern und schließen Sie die Datei.

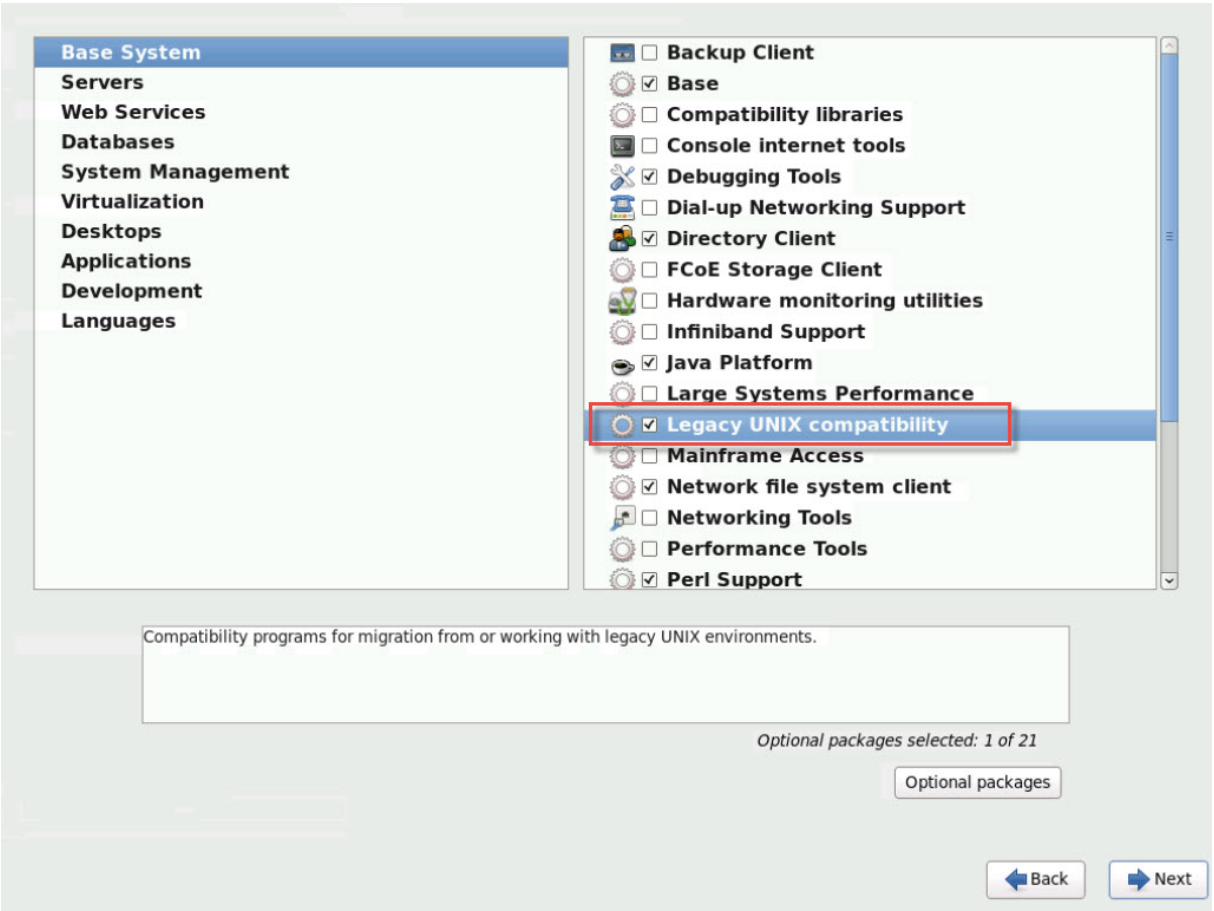
Aktivieren von VNC für RHEL, CentOS oder OEL 6 VMs

Wenn Sie Red Hat Linux Version 6.x verwenden, lautet die GDM-Konfigurationsdatei `/etc/gdm/custom.conf`. Diese Datei ist eine geteilte Konfigurationsdatei, die nur benutzerdefinierte Werte enthält, die die Standardkonfiguration außer Kraft setzen. Standardmäßig wird dieser Dateityp in neueren Versionen von GDM verwendet und ist in diesen Versionen von Red Hat Linux enthalten.

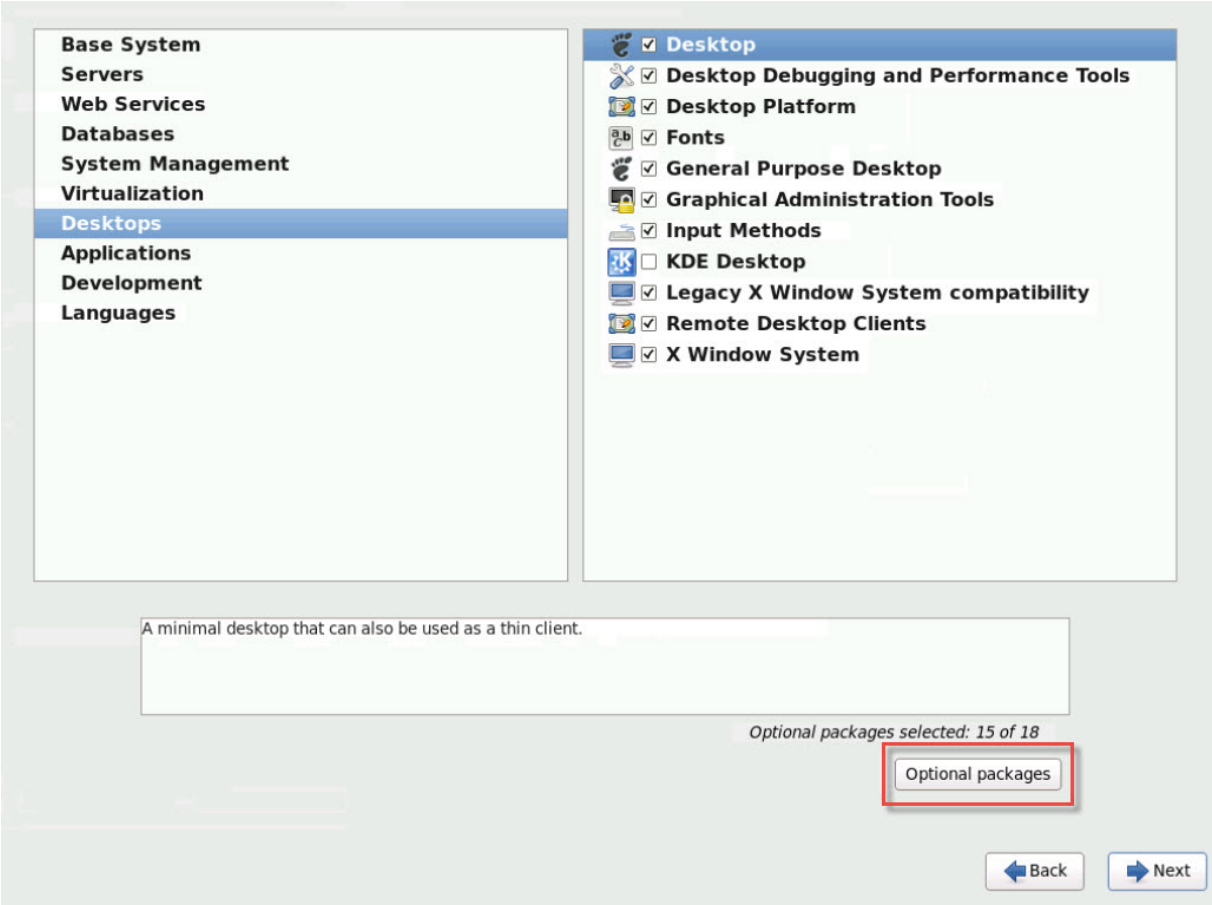
Wählen Sie während der Installation des Betriebssystems den **Desktop-Modus** aus. Wählen Sie auf dem RHEL-Installationsbildschirm **Desktop** > **Jetzt anpassen** aus, und klicken Sie dann auf **Weiter** :



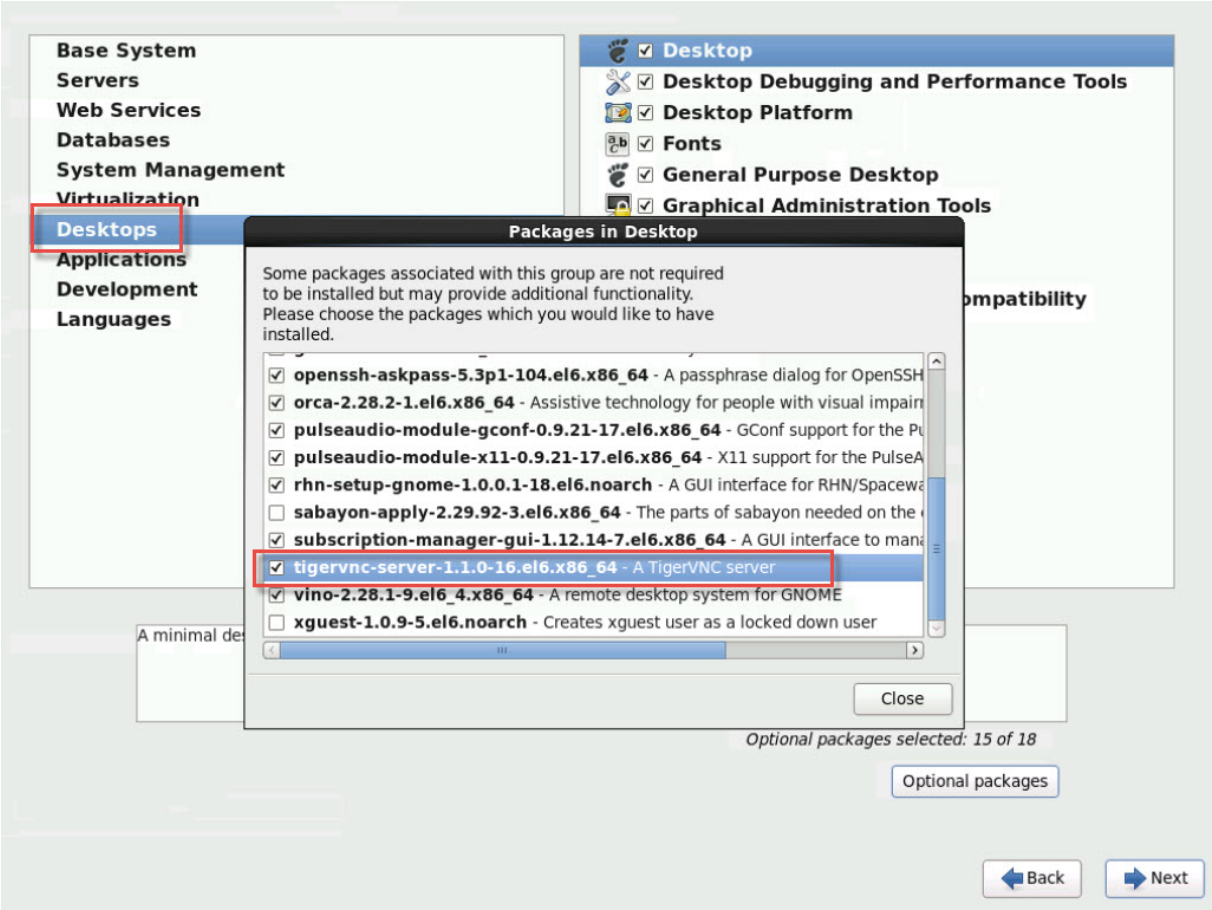
Mit dieser Aktion wird der Bildschirm Basissystem angezeigt. Stellen Sie sicher, dass die **Legacy-UNIX-Kompatibilität** ausgewählt ist:



Select **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 6.x-VMs fortzusetzen:

1. Öffnen Sie die GDM-Konfigurationsdatei mit Ihrem bevorzugten Texteditor und fügen Sie den entsprechenden Abschnitten folgende Zeilen hinzu:

```
[security]
DisallowTCP=false

[xdmcp]
Enable=true
```

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
```



```
9                 wait = no
10                user = nobody
11               group = tty
12              server = /usr/bin/Xvnc
13          server_args = -inetd -once -query localhost -
                SecurityTypes None \
14          -geometry 800x600 -depth 16
15      }
```

3. Geben Sie den folgenden Befehl ein, um den`xinetd` Dienst zu starten:

```
1 # service xinetd start
```

4. Öffnen Sie die Datei`/etc/sysconfig/iptables`. Fügen Sie die folgende Zeile über der Zeilenlesung hinzu`-A INPUT -j REJECT --reject-with icmp-host-prohibited`:

```
1 -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

5. Geben Sie den folgenden Befehl ein, um neu zu starten `iptables`:

```
1 # service iptables restart
```

6. Geben Sie den folgenden Befehl ein, um neu zu starten `gdm`:

```
1     # telinit 3
2     # telinit 5
```

> **Hinweis:**
>
> Red Hat Linux verwendet Runlevel 5 für den grafischen Start. Wenn Ihre Installation im Runlevel 3 startet, ändern Sie diese Konfiguration für den Display-Manager gestartet werden und um Zugriff auf eine grafische Konsole zu erhalten. Weitere Informationen finden Sie unter Runlevels 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 den Linux-Gast-Agent installiert haben. Weitere Informationen Installieren des Linux-Gast-Agents finden Sie unter.

SLES unterstützt die Aktivierung von „Remote Administration“ als Konfigurationsoption in`YaST`. Sie können die Remoteverwaltung zur Installationszeit aktivieren, die auf dem Bildschirm **Netzwerkdienste** des SLES-Installationsprogramms verfügbar ist. 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 ist.

Suchen Sie nach einem VNC-Server

Bevor Sie Konfigurationsänderungen vornehmen, stellen Sie sicher, dass ein VNC-Server installiert ist. SUSE liefert den`tightvnc` Server standardmäßig. Dieser Server ist ein geeigneter VNC-Server, aber Sie können auch die Standard-RealVNC-Distribution verwenden.

Sie können überprüfen, ob die`tightvnc` Software installiert ist, indem Sie den folgenden Befehl ausführen:

```
1 rpm -q tightvnc
```

Remote-Verwaltung aktivieren

Wenn die Remoteverwaltung während der Installation der SLES-Software nicht aktiviert wurde, können Sie sie wie folgt aktivieren:

1. Öffnen Sie eine Textkonsole auf der VM und führen Sie das `YaST` Dienstprogramm aus:

   ```
   1 yast
   ```

2. Verwenden Sie die Pfeiltasten, um **Netzwerkdienste** im linken Menü auszuwählen. **, und wählen Sie mithilfe der Pfeiltasten die Option **Remote Administration** aus.** Drücken Sie die **Eingabetaste**.
3. Klicken Sie im Bildschirm **Remoteverwaltungauf** den Abschnitt **Einstellungen für die Remoteverwaltung** . Verwenden Sie die Pfeiltasten, um **Remoteverwaltung zulassen** auszuwählen, und drücken **Sie die Eingabetaste** , um ein X in das Kontrollkästchen zu setzen.
4. **Klicken Sie** auf den Abschnitt **Firewall-Einstellungen** . Verwenden Sie die Pfeiltasten, um **Port in Firewall öffnen** auszuwählen, und drücken **Sie die Eingabetaste** , um ein X in das Kontrollkästchen zu setzen.
5. **Tab auf** die Schaltfläche **Fertig stellen** und drücken **Sie die Eingabetaste** .
6. Es wird ein Meldungsfeld angezeigt, in dem Sie aufgefordert werden, den Display-Manager neu zu starten, damit Ihre Einstellungen wirksam werden. Drücken **Sie die Eingabetaste** , um die Nachricht zu bestätigen.
7. Das ursprüngliche Menü der obersten Ebene von`YaST` wird angezeigt. **Tippen Sie** auf die Schaltfläche **Beenden** und drücken **Sie die Eingabetaste** .

Ändern der xinetd-Konfiguration

Ändern Sie nach dem Aktivieren der Remoteverwaltung eine Konfigurationsdatei, wenn Sie zulassen möchten, dass XenCenter eine Verbindung herstellen kann. Alternativ können Sie einen VNC-Client von Drittanbietern verwenden.

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
 }
```

3. Bearbeiten Sie die zu lesende`port` Zeile

```
port = 5900
```

4. Speichern und schließen Sie die Datei.
5. Starten Sie den Display-Manager und den `xinetd` Dienst mit den folgenden Befehlen neu:

```
/etc/init.d/xinetd restart
rcxdm restart
```

SUSE Linux verwendet Runlevel 5 für den grafischen Start. Wenn Ihr Remote-Desktop nicht angezeigt wird, stellen Sie sicher, dass Ihre VM für den Start in Runlevel 5 konfiguriert ist. Weitere Informationen finden Sie unter Runlevels überprüfen.

Firewall-Einstellungen

Standardmäßig lässt die Firewall-Konfiguration den VNC-Datenverkehr nicht durchlaufen. Wenn Sie über eine Firewall zwischen der VM und XenCenter verfügen, erlauben Sie Datenverkehr über den Port, den die VNC-Verbindung verwendet. Standardmäßig überwacht ein VNC-Server Verbindungen von einem VNC-Viewer am TCP-Port `5900 + n`, wobei die Anzeigenummer (normalerweise Null) `n` ist. So

hört ein VNC-Server-Setup für Display-0 auf TCP-Port`5900`, Display-1 ist`TCP-5901`und so weiter. Überprüfen Sie die Firewall-Dokumentation, um sicherzustellen, dass diese Ports geöffnet sind.

Wenn Sie die IP-Verbindungsverfolgung verwenden oder die Initiierung von Verbindungen nur von einer Seite einschränken 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 `YaST` Dienstprogramm aus:

   ```
   yast
   ```

2. Wählen Sie im linken Menü mit den Pfeiltasten **Sicherheit und Benutzer** aus. **Tabulatortaste** im rechten Menü und wählen Sie **Firewall** mit den Pfeiltasten aus. Drücken Sie die **Eingabetaste**.
3. Wählen Sie im **Firewall-Bildschirm** im linken Menü mit den Pfeiltasten **Benutzerdefinierte Regeln** aus, und drücken **Sie dann die EINGABETASTE**.
4. **Klicken** Sie auf die Schaltfläche **Hinzufügen** im Abschnitt **Benutzerdefinierte zulässige Regeln** , und drücken **Sie dann die EINGABETASTE** .
5. Geben Sie im Feld **Quellnetzwerk** den Wert *0/0* ein. **Tabulatortaste** in das Feld **Zielport** , und geben Sie *5900* ein.
6. **Klicken** Sie auf die Schaltfläche **Hinzufügen** , und drücken Sie dann die **Eingabetaste** .
7. **Tabulatortaste** zur Schaltfläche **Weiter** und drücken **Sie die Eingabetaste** .
8. Klicken Sie auf der **RegisterkarteZusammenfassung** auf die Schaltfläche **Fertig stellen** und drücken **Sie die Eingabetaste** .
9. **Klicken** Sie auf dem`YaST` Bildschirm auf der obersten Ebene auf die Schaltfläche **Beenden** und drücken **Sie die Eingabetaste** .
10. Starten Sie den Display-Manager und den `xinetd` Dienst mit den folgenden Befehlen neu:

    ```
    /etc/init.d/xinetd restart
    rcxdm restart
    ```

Alternativ können Sie die Firewall bis zum nächsten Neustart deaktivieren, indem Sie den Befehl **RCSUseFirewall2 stop** ausführen oder dauerhaft mithilfe von verwenden`YaST` . Diese Konfiguration kann zusätzliche Dienste für die Außenwelt bereitstellen und die allgemeine Sicherheit Ihrer VM reduzieren.

VNC-Bildschirmauflösung

Nach der Verbindung mit einer virtuellen Maschine über die grafische Konsole stimmt die Bildschirmauflösung manchmal nicht überein. Beispielsweise ist die VM-Anzeige zu groß, um bequem in den Bereich „Grafische Konsole“ zu passen. Steuern Sie dieses Verhalten, indem Sie den `geometry` VNC-Serverparameter wie folgt festlegen:

1. Öffnen Sie die`/etc/xinetd.d/vnc` Datei mit Ihrem bevorzugten Texteditor und suchen Sie den`service_vnc1` Abschnitt (entspricht`displayID` 1).
2. Bearbeiten Sie das`geometry` Argument in der`server-args` Zeile auf die gewünschte Bildschirmauflösung. Beispiel:

   ```
   server_args  = :42 -inetd -once -query localhost -geometry 800x600
       -depth 16
   ```

   Der Wert des `geometry` Parameters 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
   ```

Runlevels überprüfen

Red Hat und SUSE Linux VMs verwenden Runlevel 5 für den grafischen Start. In diesem Abschnitt wird beschrieben, wie Sie überprüfen, ob Ihre VM in Runlevel 5 gestartet wird und wie Sie diese Einstellung ändern.

1. Überprüfen`/etc/inittab` Sie, ob der Standardlauflevel auf eingestellt ist. Suchen Sie nach der Zeile, die lautet:

   ```
   id:n:initdefault:
   ```

   Wenn *n* nicht 5 ist, bearbeiten Sie die Datei so.
2. Sie können den Befehl`telinit q ; telinit 5` nach dieser Änderung ausführen, um einen Neustart zu vermeiden, um Runlevels zu wechseln.

Kopiert!
Failed!

Beheben von VM-Problemen

October 16, 2019

Citrix bietet zwei Unterstützungsformen:

- Kostenlose Selbsthilfeunterstützung auf derCitrix Website
- Paid-for Support Services, die Sie über die Support-Website erwerben können.

Mit dem technischen Support von Citrix können Sie einen Support-Fall online öffnen oder sich telefonisch an das Support-Center wenden, wenn technische Schwierigkeiten auftreten.

DieCitrix SupportWebsite beherbergt mehrere Ressourcen, die Ihnen bei ungewöhnlichem Verhalten, Abstürzen oder anderen Problemen hilfreich sein könnten. Zu den Ressourcen gehören: Support-Foren, Knowledge Base-Artikel und Produktdokumentation.

Wenn Sie ein ungewöhnliches VM-Verhalten sehen, soll dieser Abschnitt Ihnen helfen, das Problem zu lösen. In diesem Abschnitt wird beschrieben, wo sich Anwendungsprotokolle befinden und andere Informationen, die Ihrem Citrix Hypervisor Lösungsanbieter helfen können, das Problem zu verfolgen und zu beheben.

> **Wichtig:**
>
> Befolgen Sie die Informationen zur Problembehandlung in diesem Abschnitt nur unter Anleitung Ihres Citrix Hypervisor Lösungsanbieters oder des Support-Teams.
>
> Lieferantenaktualisierungen: Halten Sie Ihre VMs mit vom Hersteller bereitgestellten Updates auf dem neuesten Stand. Der Hersteller hat möglicherweise Korrekturen für VM abgestürzt und andere Fehler bereitgestellt.

VM stürzt ab

Wenn VM-Abstürze auftreten, ist es möglich, dass ein Kernel-Absturzabbild helfen kann, das Problem zu identifizieren. Reproduzieren Sie den Absturz, wenn möglich, und folgen Sie diesem Verfahren. Wenden Sie sich an Ihren Gastbetriebssystemanbieter, um weitere Untersuchungen zu diesem Problem zu erhalten.

Steuern des Verhaltens von Linux VM Crashdumps

Bei Linux-VMs kann das Crashdump-Verhalten über den`actions-after-crash` Parameter gesteuert werden. Folgende Werte sind möglich:

Wert	Beschreibung
`preserve`	Belassen Sie die VM in einem angehaltenen Zustand. (Zur Analyse)
`restart`	Kein Core-Dump, einfach VM neu starten. (Dies ist die Standardeinstellung)
`destroy`	Kein Core-Dump, lassen Sie VM angehalten.

So aktivieren Sie das Speichern von Linux-VM-Absturzabbildern:

1. Bestimmen Sie auf dem Citrix Hypervisor or-Server die UUID der gewünschten VM, indem Sie den folgenden Befehl ausführen:

```
xe vm-list name-label=name params=uuid --minimal
```

2. Ändern Sie den`actions-after-crash` Wert mit`xe vm-param-set` ; führen Sie beispielsweise den folgenden Befehl auf dom0 aus:

```
xe vm-param-set uuid=vm_uuid actions-after-crash=preserve
```

3. Absturz der VM.
   - Führen Sie für PV-Gäste den folgenden Befehl auf der VM aus:

```
echo c | sudo tee /proc/sysrq-trigger
```

4. Führen Sie den Dump Core-Befehl auf dom0 aus. Führen Sie beispielsweise Folgendes aus:

```
xl dump-core domid filename
```

Steuern des Windows VM-Absturzverhaltens

Bei Windows VMs kann der`actions-after-crash` Parameter das Kernabbildverhalten nicht steuern. Standardmäßig werden Windows Absturzabbilder`%SystemRoot%\Minidump` in der Windows-VM selbst abgelegt.

Sie können die VM-Abbildungsebene konfigurieren, indem Sie den Menüpfad **Arbeitsplatz > Eigenschaften > Erweitert > Start und Wiederherstellung**befolgen.

Beheben von Startproblemen auf Linux-VMs

In der Citrix Hypervisor`xe-edit-bootloader` or-Serversteuerungsdomäne befindet sich ein Dienstprogrammskript. Dieses Skript kann verwendet werden, um die Bootloader-Konfiguration einer Linux-VM herunterzufahren und Probleme zu beheben, die verhindern, dass die VM gestartet wird.

So verwenden Sie dieses Skript:

1. Führen Sie den folgenden Befehl aus:

   ```
   1 xe vm-list
   ```

   Dieser Befehl stellt sicher, dass die betreffende VM heruntergefahren wird (der Wert des *Power-state* wird *angehalten*).

2. Sie können die UUID wie folgt verwenden:

   ```
   1 xe-edit-bootloader -u linux_vm_uuid -p partition_number
   ```

   Oder Sie können die Namensbezeichnung wie folgt verwenden:

   ```
   1 xe-edit-bootloader -n linux_vm_name_label -p partition_number
   ```

   Die Partitionsnummer stellt die Scheibe der Festplatte dar, die das Dateisystem hat. Für die Standard-Debian-Vorlage ist die Partitionsnummer *1* , da sie die erste Partition ist.

3. Sie werden in einen Editor abgelegt, in dem die`grub.conf` Datei für die angegebene VM geladen ist. Ändern Sie die Datei, um sie zu beheben, speichern Sie die Datei, beenden Sie den Editor und starten Sie die VM.

Kopiert!
Failed!

Hohe Verfügbarkeit

October 16, 2019

Hochverfügbarkeit ist eine Reihe automatischer Funktionen, die für die Planung und Wiederherstellung von Problemen entwickelt wurden, die Citrix Hypervisor or-Server befallen oder sie nicht erreichbar machen. Beispielsweise bei physisch unterbrochenen Netzwerk- oder Host-Hardwarefehlern.

Übersicht

Hohe Verfügbarkeit stellt sicher, dass VMs, die auf diesem Host ausgeführt werden, heruntergefahren und auf einem anderen Host neu gestartet werden, wenn ein Host nicht erreichbar oder instabil wird. Beim Herunterfahren und Neustart von VMs auf einem anderen Host wird vermieden, dass die VMs (manuell oder automatisch) auf einem neuen Host gestartet werden. Irgendwann später wird der ursprüngliche Host wiederhergestellt. Dieses Szenario kann zu zwei Instanzen derselben VM führen, die auf verschiedenen Hosts ausgeführt werden, und zu einer entsprechenden hohen Wahrscheinlichkeit von VM-Datenträgerbeschädigung und Datenverlust.

Wenn der Poolmaster nicht erreichbar oder instabil wird, kann die hohe Verfügbarkeit auch die administrative Kontrolle eines Pools wiederherstellen. Hohe Verfügbarkeit stellt sicher, dass die administrative Kontrolle ohne manuellen Eingriff automatisch wiederhergestellt wird.

Optional kann Hochverfügbarkeit auch den Neustart von VMs auf Hosts automatisieren, die bekanntermaßen in einem guten Zustand sind, ohne manuelles Eingreifen. Diese VMs können für den Neustart in Gruppen geplant werden, um Zeit für das Starten von Diensten zu erhalten. Damit können Infrastruktur-VMs vor ihren abhängigen VMs gestartet werden (z. B. ein DHCP-Server vor dem abhängigen SQL-Server).

> **Warnungen:**
>
> Nutzen Sie hohe Verfügbarkeit zusammen mit Multipathed Storage und Bonded Networking. Konfigurieren Sie Multipathed Storage und Bonded Networking, bevor Sie versuchen, Hochverfügbarkeit einzurichten. Kunden, die keinen Multipathed Storage und Bonded Networking einrichten, können unerwartetes Host-Neustartverhalten (Self Fencing) sehen, wenn eine Infrastrukturinstabilität besteht.
>
> Alle Grafiklösungen (nVidia vGPU, Intel GVT-d, Intel GVT-G, AMD MxGPU und vGPU Pass-Through) können in einer Umgebung verwendet werden, die hohe Verfügbarkeit nutzt. VMs, die diese Grafiklösungen verwenden, können jedoch nicht mit hoher Verfügbarkeit geschützt werden. Diese VMs können nach bestem Aufwand neu gestartet werden, während Hosts mit den entsprechenden freien Ressourcen vorhanden sind.

Übertreibend

Ein Pool ist zu viel festgeschrieben, wenn die VMs, die derzeit ausgeführt werden, nach einer benutzerdefinierten Anzahl von Hostfehlern an anderer Stelle nicht neu gestartet werden können.

Ein Überschreiben kann auftreten, wenn im Pool nicht genügend freier Speicher vorhanden ist, um diese VMs nach einem Fehler auszuführen. Es gibt jedoch auch subtileere Änderungen, die hohe Verfügbarkeit garantiert nicht nachhaltig machen können: Änderungen an Virtual Block Devices (VBDs) und Netzwerken können sich darauf auswirken, welche VMs auf welchen Hosts neu gestartet werden

können. Citrix Hypervisor kann nicht alle potenziellen Aktionen überprüfen und feststellen, ob sie eine Verletzung der Anforderungen an hohe Verfügbarkeit verursachen. Allerdings wird eine asynchrone Benachrichtigung gesendet, wenn die hohe Verfügbarkeit nicht nachhaltig wird.

Citrix Hypervisor verwaltet dynamisch einen *Failoverplan* , der detailliert beschreibt, was zu tun ist, wenn ein Satz von Hosts in einem Pool zu einem bestimmten Zeitpunkt ausfällt. Ein wichtiges Konzept, das zu verstehen ist, dass *Hostfehler, um Wert zu tolerieren* , die als Teil der Hochverfügbarkeitskonfiguration definiert ist. Der Wert von *Hostfehlern, die toleriert* werden sollen, bestimmt die Anzahl der Fehler, die ohne Verlust des Dienstes zulässig ist. Betrachten Sie beispielsweise einen Ressourcenpool, der aus 64 Hosts besteht und die tolerierten Fehler auf 3 festgelegt ist. In diesem Fall berechnet der Pool einen Failoverplan, mit dem drei Hosts fehlschlagen und die VMs auf anderen Hosts neu starten können. Wenn ein Plan nicht gefunden werden kann, wird der Pool als *überschrieben angesehen*. Der Plan wird basierend auf VM-Lebenszyklusvorgängen und -bewegungen dynamisch neu berechnet. Wenn Änderungen, z. B. das Hinzufügen neuer VMs zum Pool, dazu führen, dass der Pool übermäßig festgeschrieben wird, werden Warnungen gesendet (entweder über XenCenter oder per E-Mail).

Warnung zu Überbindung

Wenn Versuche, eine VM zu starten oder fortzusetzen, dazu führen, dass der Pool überschrieben wird, wird eine Warnmeldung angezeigt. Diese Warnung wird in XenCenter angezeigt und ist auch als Nachrichteninstanz über die Verwaltungs-API verfügbar. Wenn Sie eine E-Mail-Adresse konfiguriert haben, wird möglicherweise auch eine Nachricht an die E-Mail-Adresse gesendet. Sie können den Vorgang dann abbrechen oder trotzdem fortfahren. Das Fortfahren bewirkt, dass der Pool überschrieben wird. Die Menge an Arbeitsspeicher, die von VMs unterschiedlicher Prioritäten verwendet werden, wird auf Pool- und Hostebene angezeigt.

Host-Fechten

Manchmal kann ein Server aufgrund des Verlusts der Netzwerkkonnektivität oder wenn ein Problem mit dem Kontrollstapel auftritt, ausfallen. In solchen Fällen stellt sich der Citrix Hypervisor or-Server selbst ein, um sicherzustellen, dass die VMs nicht gleichzeitig auf zwei Servern ausgeführt werden. Wenn eine Fencing-Aktion ausgeführt wird, startet der Server sofort und abrupt neu, sodass alle auf ihm ausgeführten VMs gestoppt werden. Die anderen Server erkennen, dass die VMs nicht mehr ausgeführt werden, und die VMs werden entsprechend den ihnen zugewiesenen Neustartprioritäten neu gestartet. Der umzäunte Server gibt eine Neustartsequenz ein, und wenn er neu gestartet wurde, versucht er erneut, dem Ressourcenpool beizutreten.

> **Hinweis:**
>
> Hosts in Cluster-Pools können sich auch selbst eingrenzen, wenn sie nicht mit mehr als der Hälfte der anderen Hosts im Ressourcenpool kommunizieren können. Weitere Informationen finden Sie unter Cluster-Pools.

Konfigurationsanforderungen

Um die Hochverfügbarkeitsfunktion nutzen zu können, benötigen Sie:

- Citrix Hypervisor Pool (diese Funktion bietet hohe Verfügbarkeit auf Serverebene innerhalb eines einzelnen Ressourcenpools).

  > **Hinweis:**
  >
  > Es wird empfohlen, Hochverfügbarkeit nur in Pools zu aktivieren, die mindestens drei Citrix Hypervisor or-Server enthalten. Weitere Informationen finden Sie unter CTX129721 - Hochverfügbarkeitsverhalten, wenn der Heartbeat in einem Pool verloren geht.

- Gemeinsamer Speicher, einschließlich mindestens einer iSCSI-, NFS- oder Fibre-Channel-LUN mit einer Größe von 356 MB oder mehr - der *Heartbeat-SR*. Der Hochverfügbarkeitsmechanismus erstellt zwei Volumes auf dem Heartbeat SR:

  4 MB Heartbeat Volume: Wird für Heartbeat verwendet.

  256 MB Metadatenvolume: Speichern von Pool-Master-Metadaten, die verwendet werden sollen, wenn ein Master-Failover vorhanden ist.

  > **Hinweise:**
  >
  > - Für maximale Zuverlässigkeit empfehlen wir, ein dediziertes NFS- oder iSCSI-Speicher-Repository als Heartbeat-Festplatte mit hoher Verfügbarkeit zu verwenden. Verwenden Sie dieses Speicher-Repository nicht für andere Zwecke.
  > - Wenn es sich bei Ihrem Pool um einen gruppierten Pool handelt, muss Ihr Heartbeat SR ein GFS2 SR sein.
  > - Speicher, der entweder mit SMB oder iSCSI verbunden ist, wenn sie mit CHAP authentifiziert wird, kann nicht als Heartbeat SR verwendet werden.
  > - Wenn Sie eine NetApp oder EqualLogic SR verwenden, stellen Sie manuell eine NFS- oder iSCSI-LUN auf dem Array bereit, die als Heartbeat-SR verwendet werden soll.

- Statische IP-Adressen für alle Hosts.

  > **Warnhinweis:**
  >
  > Wenn sich die IP-Adresse eines Servers ändert, während die hohe Verfügbarkeit aktiviert ist, geht die hohe Verfügbarkeit davon aus, dass das Netzwerk des Hosts fehlgeschla-

> gen ist. Die Änderung der IP-Adresse kann den Host umschlossen und in einem nicht startbaren Zustand belassen. Um diese Situation zu beheben, deaktivieren Sie die Hochverfügbarkeit mit dem`host-emergency-ha-disable` Befehl, setzen Sie den Poolmaster mit`pool-emergency-reset-master` zurück und aktivieren Sie dann die Hochverfügbarkeit erneut.

- Für maximale Zuverlässigkeit empfehlen wir, eine dedizierte gebundene Schnittstelle als Hochverfügbarkeits-Management-Netzwerk zu verwenden.

Damit eine VM durch hohe Verfügbarkeit geschützt wird, muss sie agil sein. Es bedeutet, dass die VM:

- Die virtuellen Laufwerke müssen sich auf gemeinsam genutztem Speicher befinden. 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 die Speicherung virtueller Festplatten verwendet werden.
- Kann Live-Migration verwenden
- Keine Verbindung zu einem lokalen DVD-Laufwerk konfiguriert
- Hat seine virtuellen Netzwerkschnittstellen in Pool-weiten Netzwerken

> **Hinweis:**
>
> Wenn die hohe Verfügbarkeit aktiviert ist, empfehlen wir dringend, eine gebundene Management-Schnittstelle auf den Servern im Pool und Multipathed Storage für den Heartbeat SR zu verwenden.

Wenn Sie VLANs und gebundene Schnittstellen von der CLI erstellen, werden sie möglicherweise nicht angeschlossen und aktiv, obwohl sie erstellt wurden. In diesem Fall kann eine VM als nicht agil erscheinen und ist nicht durch hohe Verfügbarkeit geschützt. Sie können den`pif-plug` CLI-Befehl verwenden, um die VLAN- und Bindungs-PIFs aufzurufen, damit die VM agil werden kann. Sie können auch genau bestimmen, warum eine VM nicht agil ist, indem Sie den`xe diagnostic-vm-status` CLI-Befehl verwenden. Mit diesem Befehl werden die Platzierungsbedingungen analysiert, und Sie können bei Bedarf Korrekturmaßnahmen ergreifen.

Konfigurationseinstellungen neu starten

Virtuelle Maschinen können durch hohe Verfügbarkeit als geschützt, bestmöglich oder ungeschützt angesehen werden. Der Wert von`ha-restart-priority` definiert, ob eine VM als geschützt, best-effort oder ungeschützt behandelt wird. Das Neustartverhalten für VMs in jeder dieser Kategorien ist unterschiedlich.

Geschützt

Hochverfügbarkeit garantiert einen Neustart einer geschützten VM, die offline geschaltet wird 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 Server ausfällt, versucht die Hochverfügbarkeit, die VM zu starten, wenn in einem Pool zusätzliche Kapazität vorhanden ist. Versuche, die VM zu starten, wenn zusätzliche Kapazität vorhanden ist, können nun erfolgreich sein.

`ha-restart-priority` Wert:`restart`

Best-Aufwand

Wenn der Host einer Best-Effort-VM offline geschaltet wird, versucht Hochverfügbarkeit, die Best-Effort-VM auf einem anderen Host neu zu starten. Dieser Versuch wird erst ausgeführt, nachdem alle geschützten VMs erfolgreich neu gestartet wurden. Hochverfügbarkeit macht nur einen Versuch, eine bestmögliche VM neu zu starten. Wenn dieser Versuch fehlschlägt, 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, beendet wird, versucht die Hochverfügbarkeit nicht, die VM neu zu starten.

`ha-restart-priority` Wert: Wert ist eine leere Zeichenfolge

> **Hinweis:**
>
> Hochverfügbarkeit stoppt oder migriert eine ausgeführte VM nie auf freie Ressourcen, damit eine geschützte oder bestmögliche VM neu gestartet werden kann.

Wenn der Pool Serverfehler auftritt und die Anzahl der tolerierbaren Fehler auf Null sinkt, wird der Neustart der geschützten VMs nicht garantiert. In solchen Fällen wird eine Systemwarnung generiert. Wenn ein anderer Fehler auftritt, verhalten sich alle VMs, für die eine Neustartpriorität festgelegt wurde, entsprechend dem Best-Effort-Verhalten.

Bestellung starten

Die Startreihenfolge ist die Reihenfolge, in der Citrix Hypervisor Hochverfügbarkeit 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 hoher Verfügbarkeit und auch von anderen Features verwendet, die VMs starten und herunterfahren. Für jede VM kann die`order` Eigenschaft festgelegt werden, nicht nur die VMs, die für hohe Verfügbarkeit als geschützt markiert sind. Bei hoher Verfügbarkeit wird die`order` Eigenschaft jedoch nur für geschützte VMs verwendet.

Der Wert der`order` Eigenschaft ist eine ganze Zahl. Der Standardwert ist 0, was die höchste Priorität hat. Geschützte VMs mit dem`order` Wert 0 werden zuerst durch hohe Verfügbarkeit neu gestartet. Je höher der Wert der`order` Eigenschaft ist, desto später wird die VM neu gestartet.

Sie können den Wert der`order` Eigenschaft einer VM mithilfe der Befehlszeilenschnittstelle festlegen:

```
1 xe vm-param-set uuid=VM_UUID order=int
```

Oder legen Sie in XenCenter im Bedienfeld „Startoptionen“ für eine VM die Startreihenfolge auf den erforderlichen Wert fest.

Hochverfügbarkeit in Ihrem Citrix Hypervisor Pool aktivieren

Sie können Hochverfügbarkeit in einem Pool mithilfe von XenCenter oder der Befehlszeilenschnittstelle aktivieren. In beiden Fällen geben Sie eine Reihe von Prioritäten an, die bestimmen, welche VMs die höchste Neustartpriorität erhalten, wenn ein Pool überschrieben ist.

> **Warnungen:**
>
> - Wenn Sie Hochverfügbarkeit aktivieren, werden einige Vorgänge, die den Plan für den Neustart von VMs beeinträchtigen, z. B. das Entfernen eines Servers aus einem Pool möglicherweise deaktiviert. Sie können die Hochverfügbarkeit vorübergehend deaktivieren, um solche Vorgänge auszuführen, oder alternativ VMs durch Hochverfügbarkeit ungeschützt machen.
> - Wenn die hohe Verfügbarkeit aktiviert ist, können Sie das Clustering in Ihrem Pool nicht aktivieren. Deaktivieren Sie vorübergehend Hochverfügbarkeit, um Clustering zu aktivieren. Sie können Hochverfügbarkeit in Ihrem Clusterpool aktivieren. Einige Hochverfügbarkeitsverhalten, z. B. Self-Fencing, unterscheiden sich bei Cluster-Pools. Weitere Informationen finden Sie unter Cluster-Pools

Hochverfügbarkeit mithilfe der CLI aktivieren

1. Stellen Sie sicher, dass ein kompatibles Speicher-Repository (SR) an Ihren Pool angeschlossen ist. iSCSI, NFS oder Fibre Channel-SRs sind kompatibel. Informationen zum Konfigurieren eines solchen Speicher-Repository mithilfe der CLI finden Sie unterVerwalten von Speicher-Repositories.

2. Legen Sie für jede VM, die Sie schützen möchten, eine Neustartpriorität fest und starten Sie die Reihenfolge. Sie können die Neustartpriorität wie folgt festlegen:

```
xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
```

3. Aktivieren Sie Hochverfügbarkeit im Pool und geben Sie optional ein Timeout an:

```
xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
   timeout in seconds
```

   Timeout ist der Zeitraum, in dem die Hosts in Ihrem Pool nicht auf das Netzwerk oder den Speicher zugreifen können. Wenn Sie beim Aktivieren der Hochverfügbarkeit kein Timeout angeben, verwendet Citrix Hypervisor das Standard-Timeout von 30 Sekunden. Wenn ein Citrix Hypervisor or-Server innerhalb des Timeoutzeitraums nicht auf das Netzwerk oder den Speicher zugreifen kann, kann er sich selbst einschalten und neu starten.

4. Führen Sie den Befehl aus`pool-ha-compute-max-host-failures-to-tolerate`. Dieser Befehl gibt die maximale Anzahl von Hosts zurück, die fehlschlagen können, bevor nicht genügend Ressourcen vorhanden sind, um alle geschützten VMs im Pool auszuführen.

```
xe pool-ha-compute-max-host-failures-to-tolerate
```

   Die Anzahl der zu tolerierenden Fehler bestimmt, wann eine Warnung gesendet wird. Das System berechnet einen Failoverplan neu, wenn sich der Zustand des Pools ändert. Sie verwendet diese Berechnung, um die Poolkapazität zu identifizieren und wie viele weitere Ausfälle möglich sind, ohne dass die Betriebsgarantie 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 die Anzahl der Fehler an, die Parameter toleriert werden sollen. Der Wert muss kleiner oder gleich dem berechneten Wert sein:

```
xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
```

Entfernen des Hochverfügbarkeitsschutzes von einer VM mithilfe der CLI

Um Hochverfügbarkeitsfunktionen für eine VM zu deaktivieren, legen Sie den`xe vm-param-set` Parameter mit dem`ha-restart-priority` Befehl als leere Zeichenfolge fest. Wenn Sie den`ha-restart-priority` Parameter festlegen, werden die Einstellungen für die Startreihenfolge nicht gelöscht. Sie können die Hochverfügbarkeit für eine VM erneut aktivieren, indem Sie den`ha-restart-priority` Parameter auf`restart` oder je nach`best-effort` Bedarf festlegen.

Wiederherstellen eines nicht erreichbaren Hosts

Wenn ein Host aus irgendeinem Grund nicht auf die Hochverfügbarkeitsstatusdatei zugreifen kann, ist es möglich, dass ein Host nicht erreichbar ist. Um die Citrix Hypervisor Installation wiederherzustellen, müssen Sie die Hochverfügbarkeit möglicherweise mit folgendemhost-emergency-ha-disable Befehl deaktivieren:

```
xe host-emergency-ha-disable --force
```

Wenn der Host der Poolmaster war, startet er normal mit deaktivierter Hochverfügbarkeit. Pool-Mitglieder verbinden sich erneut und deaktivieren automatisch Hochverfügbarkeit. Wenn der Host ein Pool-Mitglied war und den Master nicht kontaktieren kann, müssen Sie möglicherweise eine der folgenden Aktionen ausführen:

- Erzwingen Sie den Neustart des Hosts als Poolmaster (`xe pool-emergency-transition-to-master`)

  ```
  xe pool-emergency-transition-to-master uuid=host_uuid
  ```

- Sagen Sie dem Host, wo der neue Master ist (`xe pool-emergency-reset-master`):

  ```
  xe pool-emergency-reset-master master-address=new_master_hostname
  ```

Wenn alle Hosts erfolgreich neu gestartet wurden, aktivieren Sie die hohe Verfügbarkeit erneut:

```
xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
```

Herunterfahren eines Hosts, wenn Hochverfügbarkeit aktiviert ist

Achten Sie besonders darauf, wenn Sie einen Host herunterfahren oder neu starten, um zu verhindern, dass der Hochverfügbarkeitsmechanismus davon ausgeht, dass der Host fehlgeschlagen ist. Um einen Host bei aktivierter Hochverfügbarkeit sauber herunterzufahren,`disable` verwenden Sie`evacuate` den Host,`shutdown` den Host und schließlich den Host entweder XenCenter oder die CLI. Führen Sie die folgenden Befehle aus, um einen Host in einer Umgebung herunterzufahren, in der die hohe Verfügbarkeit aktiviert ist:

```
xe host-disable host=host_name
xe host-evacuate uuid=host_uuid
xe host-shutdown host=host_name
```


Herunterfahren einer VM, die durch hohe Verfügbarkeit geschützt ist

Wenn eine VM unter einem Hochverfügbarkeitsplan geschützt und automatisch neu gestartet wird, kann sie nicht heruntergefahren werden, während dieser Schutz aktiv ist. Um eine VM herunterzufahren, deaktivieren Sie zuerst den Hochverfügbarkeitsschutz und führen dann den CLI-Befehl aus. XenCenter bietet ein Dialogfeld, in dem Sie die Deaktivierung des Schutzes automatisieren können, 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 Hochverfügbarkeitsausfallbedingungen automatisch neu gestartet. Der automatische Neustart stellt sicher, dass ein Operatorfehler nicht dazu führt, dass eine geschützte VM versehentlich heruntergefahren wird. Wenn Sie diese VM herunterfahren möchten, deaktivieren Sie zuerst den Hochverfügbarkeitsschutz.

Kopiert!
Failed!

Disaster Recovery und Backup

October 16, 2019

Mit der Citrix Hypervisor Disaster Recovery (DR) -Funktion können Sie virtuelle Maschinen (VMs) und vApps von einem Hardwarefehler wiederherstellen, der einen ganzen Pool oder einen ganzen Standort zerstört. Informationen zum Schutz vor Ausfällen eines einzelnen Servers finden Sie unterHohe Verfügbarkeit.

> **Hinweis:**
>
> Sie müssen mit Ihrem *Root-Konto* angemeldet sein oder die Rolle des *Pool-Operator* oder höher haben, um die DR-Funktion verwenden zu können.

Grundlegendes zu Citrix Hypervisor DR

Citrix Hypervisor DR speichert alle Informationen, die für die Wiederherstellung geschäftskritischer VMs und vApps in Speicher-Repositories (SRs) erforderlich sind. Die SRs werden dann von Ihrer primären (Produktions-) Umgebung in eine Backup-Umgebung repliziert. Wenn ein geschützter Pool am primären Standort ausfällt, können Sie die VMs und vApps in diesem Pool aus dem replizierten Speicher wiederherstellen, der an einem sekundären Standort (DR) mit minimaler Anwendungs- oder Benutzerausfallzeit neu erstellt wurde.

Die **Disaster Recovery-Einstellungen** in XenCenter können verwendet werden, um den Speicher abzufragen und ausgewählte VMs und vApps während eines Disasters in einen Wiederherstellungspool zu importieren. Wenn die VMs im Wiederherstellungspool ausgeführt werden, werden auch die Metadaten des Wiederherstellungspool repliziert. Durch die Replikation der Pool-Metadaten können alle Änderungen der VM-Einstellungen wieder in den primären Pool aufgefüllt werden, wenn der primäre Pool wiederhergestellt wird. Manchmal können sich Informationen für dieselbe VM an mehreren Stellen befinden. Beispielsweise Speicher vom primären Standort, Speicher vom Disaster Recovery-Standort und auch in dem Pool, in den die Daten importiert werden sollen. Wenn XenCenter feststellt, dass die VM-Informationen an zwei oder mehr Orten vorhanden sind, wird sichergestellt, dass nur die neuesten Informationen verwendet werden.

Die Disaster Recovery-Funktion kann mit XenCenter und der xe CLI verwendet werden. Informationen zu CLI-Befehlen finden Sie unterDisaster Recovery-Befehle.

> **Tipp:**
>
> Sie können auch die Disaster Recovery-Einstellungen verwenden, um Test-Failover für unterbrechungsfreie Tests Ihres Disaster Recovery-Systems auszuführen. Bei einem Test-Failover sind alle Schritte identisch mit dem Failover. Die VMs und vApps werden jedoch nicht gestartet, nachdem sie an der Disaster Recovery-Site wiederhergestellt wurden. Nach Abschluss des Tests wird eine Bereinigung durchgeführt, um alle VMs, vApps und Speicher zu löschen, die auf der DR-Site neu erstellt wurden.

Citrix Hypervisor VMs bestehen aus zwei Komponenten:

- Virtuelle Laufwerke, die von der VM verwendet werden, die in konfigurierten Speicher-Repositories (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 Metadaten-Konfigurationsdaten werden beim Erstellen der VM geschrieben und nur aktualisiert, wenn Sie die VM-Konfiguration ändern. Bei VMs in einem Pool wird eine Kopie dieser Metadaten auf jedem Server im Pool gespeichert.

In einer Notfall-Umgebung werden VMs an einem sekundären Standort mithilfe der Pool-Metadaten und Konfigurationsinformationen zu allen VMs und vApps im Pool neu erstellt. Die Metadaten für jede VM umfassen den Namen, die Beschreibung und die Universal Unique Identifier (UUID) sowie den Arbeitsspeicher, die virtuelle CPU sowie die Netzwerk- und Speicherkonfiguration. Es umfasst auch VM-Startoptionen — Startreihenfolge, Verzögerungsintervall, hohe Verfügbarkeit und Neustartpriorität. Die VM-Startoptionen werden beim Neustart der VM in einer Umgebung mit hoher Verfügbarkeit oder Notfallwiederherstellung verwendet. Wenn Sie beispielsweise VMs während der Notfallwiederherstellung wiederherstellen, werden VMs innerhalb einer vApp in der in den VM-Metadaten angegebenen Reihenfolge neu gestartet und die angegebenen Verzögerungsintervalle verwendet.

Anforderungen an die DR-Infrastruktur

Richten Sie die entsprechende DR-Infrastruktur sowohl am primären als auch am sekundären Standort ein, um Citrix Hypervisor DR.

- Speicher, der für Pool-Metadaten verwendet wird, *und* die virtuellen Laufwerke, die von den VMs verwendet werden, müssen von der primären (Produktions-) Umgebung in eine Sicherungsumgebung repliziert werden. Die Speicherreplikation, z. B. die Verwendung der Spiegelung, variiert je nach Gerät. Wenden Sie sich daher an den Anbieter von Speicherlösungen, um die Speicherreplikation zu verarbeiten.
- Nachdem die VMs und vApps, die Sie in einem Pool auf der DR-Site wiederhergestellt haben, ausgeführt und ausgeführt wurden, müssen die SRs repliziert werden, die die Metadaten des Notfall-Pools und die virtuellen Laufwerke enthalten. Durch die Replikation können die wiederhergestellten VMs und vApps wieder am primären Standort wiederhergestellt werden *(fehlgeschlagen)* , wenn der primäre Standort wieder online ist.
- Die Hardwareinfrastruktur am DR-Standort muss nicht mit dem primären Standort übereinstimmen. Die Citrix Hypervisor Umgebung muss jedoch auf der gleichen Release- und Patch-Ebene sein. Darüber hinaus müssen ausreichende Ressourcen im Zielpool konfiguriert werden, damit alle ausgefallenen VMs neu erstellt und gestartet werden können.

> **Warnhinweis:**
>
> Die Disaster Recovery-Einstellungen steuern keine Speicher-Array-Funktionen.
>
> Benutzer der Disaster Recovery-Funktion müssen sicherstellen, dass der Metadatenspeicher in gewisser Weise zwischen den beiden Standorten repliziert wird. Einige Speicher-Arrays enthalten „Spiegelung“ -Funktionen, um die Replikation automatisch zu erreichen. Wenn Sie diese Funktionen verwenden, müssen Sie die Spiegelfunktion deaktivieren („Mirror is defekt“), bevor Sie VMs auf der Wiederherstellungs-Site neu starten.

Überlegungen zur Bereitstellung

Überprüfen Sie die folgenden Schritte, bevor Sie die Disaster Recovery aktivieren.

Schritte vor einer Katastrophe

Im folgenden Abschnitt werden die Schritte beschrieben, die vor einer Katastrophe durchgeführt werden müssen.

- Konfigurieren Sie Ihre VMs und vApps.

- Beachten Sie, wie Ihre VMs und vApps SRs und die SRs LUNs zugeordnet sind. Achten Sie besonders auf die Benennung der`name_label` Parameter`name_description` und. Das Wiederherstellen von VMs und vApps aus repliziertem Speicher ist einfacher, wenn die Namen von SRs erfassen, wie VMs und vApps SRs und LUNs zugeordnet werden.
- Ordnen Sie die Replikation der LUNs an.
- Aktivieren Sie die Pool-Metadatenreplikation auf einen oder mehrere SRs auf diesen LUNs.
- Stellen Sie sicher, dass die SRs, auf die Sie die primären Pool-Metadaten replizieren, nur einem Pool zugeordnet sind.

Schritte nach einer Katastrophe

Im folgenden Abschnitt werden die Schritte beschrieben, die nach einem Ausfall durchgeführt werden müssen.

- Unterbrechen Sie alle vorhandenen Speicherspiegelungen, sodass die Wiederherstellungs-Site Lese-/Schreibzugriff auf den freigegebenen Speicher hat.
- Stellen Sie sicher, dass die LUNs, von denen Sie VM-Daten wiederherstellen möchten, nicht mit einem anderen Pool verbunden sind, oder es kann zu einer Beschädigung kommen.
- Wenn Sie die *Wiederherstellungs-Site* vor einer Katastrophe schützen möchten, müssen Sie die Pool-Metadatenreplikation auf einen oder mehrere SRs auf der Wiederherstellungs-Site aktivieren.

Schritte nach einer Wiederherstellung

Im folgenden Abschnitt werden die Schritte beschrieben, die nach einer erfolgreichen Wiederherstellung von Daten durchgeführt werden müssen.

- Alle Speicherspiegelungen neu synchronisieren.
- Fahren Sie auf der Wiederherstellungs-Site die VMs oder vApps, die Sie wieder zum primären Standort verschieben möchten, sauber herunter.
- Befolgen Sie auf dem primären Standort das gleiche Verfahren wie für das Failover im vorherigen Abschnitt, um ausgewählte VMs oder vApps auf die primäre
- Um den primären Standort vor zukünftigen Katastrophen zu schützen, müssen Sie die Pool-Metadatenreplikation auf einen oder mehrere SRs auf den replizierten LUNs erneut aktivieren.

Kopiert!
Failed!

Disaster Recovery aktivieren

October 16, 2019

In diesem Abschnitt wird beschrieben, wie Sie Disaster Recovery in XenCenter aktivieren. Verwenden **Sie die Option DR konfigurieren** , um Speicher-Repositories zu identifizieren, in denen die Pool-Metadaten, Konfigurationsinformationen zu allen VMs und vApps im Pool gespeichert sind. Die Metadaten werden aktualisiert, wenn Sie die VM- oder vApp-Konfiguration im Pool ändern.

> **Hinweis:**
>
> Sie können Disaster Recovery nur aktivieren, wenn Sie LVM über HBA oder LVM über iSCSI verwenden. Für eine neue LUN, die die Pool-Wiederherstellungsinformationen enthält, ist ein geringer Speicherplatz auf diesem Speicher erforderlich.

Stellen Sie vor dem Start sicher, dass die für die Notfallwiederherstellung verwendeten SRs nur mit dem Pool am primären Standort verbunden sind. SRs, die für die DR verwendet werden, dürfen nicht an den Pool am sekundären Standort angeschlossen werden.

Führen Sie die folgenden Schritte aus, um die Notfallwiederherstellung 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. Select bis zu 8 SRs aus, in denen die Pool-Metadaten gespeichert werden können. Für eine neue LUN, die die Pool-Wiederherstellungsinformationen enthält, ist ein geringer Speicherplatz auf diesem Speicher erforderlich.

   > **Hinweis:**
   >
   > Informationen für alle VMs im Pool werden gespeichert, VMs müssen nicht unabhängig zum Schutz ausgewählt werden.

3. Wählen Sie **OK**aus. 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 Wizard** aus.

   Der Disaster Recovery-Assistent zeigt drei Wiederherstellungsoptionen an: **Failover, Failback**und **Test-Failover**. Zum Wiederherstellen am sekundären Standort wählen Sie **Failover** und dann **Weiter** aus.

> **Warnhinweis:**
>
> Wenn Sie gemeinsam genutzten Fibre Channel-Speicher mit LUN-Spiegelung verwenden, um Daten an den sekundären Standort zu replizieren, brechen Sie die Spiegelung ab, bevor Sie versuchen, VMs wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der sekundäre Standort über Lese-/Schreibzugriff verfügt.

2. Select die Speicher-Repositories (SRs) aus, die die Pool-Metadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

   Standardmäßig werden in der Liste auf dieser Assistentenseite alle SRs angezeigt, die derzeit im Pool angefügt sind. Um nach weiteren SRs zu **suchen, wählen Sie Speicher-Repositories** 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 aus.
   - 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 ein.

   Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

3. Select die VMs und vApps aus, die Sie wiederherstellen möchten. Select die entsprechende Option **Energiezustand nach der Wiederherstellung** aus, um anzugeben, ob der Assistent sie automatisch starten soll, wenn sie wiederhergestellt wurden. Alternativ können Sie sie manuell starten, nachdem das Failover abgeschlossen ist.

   Select **Weiter** , um zur nächsten Assistentenseite fortzufahren und Failover-Vorprüfungen zu starten.

4. Der Assistent führt vor dem Starten des Failovers mehrere Vorprüfungen durch. Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist. Wenn zu diesem Zeitpunkt ein Speicher fehlt, können Sie **SR anhängen** auf dieser Seite auswählen, um die entsprechende SR zu suchen und anzuhängen.

   Beheben Sie alle Probleme auf der Seite „Vorprüfungen“, und wählen Sie dann **Failover** aus, um den Wiederherstellungsprozess 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 Zeit für das Failover 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 an die neu erstellten VMs angehängt. Wenn angegeben, werden die VMs gestartet.

6. Wenn das Failover abgeschlossen ist, wählen Sie **Weiter** , um den Zusammenfassungsbericht anzuzeigen. Select auf der Seite des Zusammenfassungsberichts die Option **Fertig stellen**, um den Assistenten zu schließen.

Wenn der primäre Standort verfügbar ist, arbeiten Sie über den Disaster Recovery-Assistenten, und wählen Sie **Failback** aus, um zur Ausführung Ihrer VMs auf diesem Standort zurückzukehren.

Wiederherstellen von VMs und vApps nach einer Katastrophe am primären Standort (Failback)

In diesem Abschnitt wird erläutert, wie VMs und vApps aus repliziertem Speicher wiederhergestellt werden. Sie können VMs und vApps wieder in einem Pool auf Ihrem primären (Produktions-) Standort wiederherstellen, wenn der primäre Standort nach einer Katastrophe wieder aktiviert wird. Verwenden Sie den Disaster Recovery-Assistenten, um VMs und vApps auf Ihren primären Standort zu Failback.

1. Wählen Sie in XenCenter den primären Pool aus, und wählen Sie im Menü Pool die Option **Disaster Recovery** und dann **Disaster Recovery Wizard** aus.

   Der Disaster Recovery-Assistent zeigt drei Wiederherstellungsoptionen an: **Failover, Failback**und **Test-Failover**. Wenn Sie VMs und vApps auf Ihrem primären Standort wiederherstellen möchten, wählen Sie Failback und dann **Weiter**aus.

   > **Warnhinweis:**
   >
   > Wenn Sie gemeinsam genutzten Fibre Channel-Speicher mit LUN-Spiegelung verwenden, um Daten auf den primären Standort zu replizieren, brechen Sie die Spiegelung ab, bevor Sie versuchen, VMs wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der primäre Standort über Lese-/Schreibzugriff verfügt.

2. Select die Speicher-Repositories (SRs) aus, die die Pool-Metadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

   Standardmäßig werden in der Liste auf dieser Assistentenseite alle SRs angezeigt, die derzeit im Pool angefügt sind. Um nach weiteren SRs zu suchen, wählen Sie **Speicher-Repositories 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 aus.
   - 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 ein.

   Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

3. Select die VMs und vApps aus, die Sie wiederherstellen möchten. Select die entsprechende Option **Energiezustand nach der Wiederherstellung** aus, um anzugeben, ob der Assistent sie automatisch starten soll, wenn sie wiederhergestellt wurden. Alternativ können Sie sie manuell starten, nachdem das Failback abgeschlossen ist.

   Select **Weiter** , um zur nächsten Assistentenseite fortzufahren und Failbackvorprüfungen zu starten.

4. Der Assistent führt vor dem Starten des Failbacks mehrere Vorprüfungen durch. Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist. Wenn zu diesem Zeitpunkt ein Speicher fehlt, können Sie **SR anhängen auf dieser Seite** auswählen, um die entsprechende SR zu suchen und anzuhängen.

   Beheben Sie alle Probleme auf der Seite „Vorprüfungen“, und wählen Sie dann **Failback** aus, um den Wiederherstellungsprozess 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 ein Failback je nach Anzahl der wiederherstellenden VMs und vApps einige Zeit in Anspruch nehmen. Die VMs und vApps werden im primären Pool neu erstellt, und die SRs, die die virtuellen Laufwerke enthalten, werden an die neu erstellten VMs angehängt. Wenn angegeben, werden die VMs gestartet.

6. Wenn das Failback abgeschlossen ist, wählen Sie **Weiter** , um den Zusammenfassungsbericht anzuzeigen. Select auf der Seite des Zusammenfassungsberichts die Option **Fertig stellen**, um den Assistenten zu schließen.

Testen des Failovers

Failover-Tests sind eine wesentliche Komponente bei der Disaster Recovery-Planung. Sie können den Disaster Recovery-Assistenten verwenden, um unterbrechungsfreie Tests Ihres Disaster Recovery-Systems durchzuführen. Während eines Test-Failovervorgangs sind die Schritte dieselben wie für Failover. Anstatt jedoch nach der Wiederherstellung an der DR-Site gestartet zu werden, werden die VMs und vApps in einen angehaltenen Zustand versetzt. Am Ende eines Test-Failovervorgangs werden alle VMs, vApps und Speicher, die auf der DR-Site neu erstellt wurden, automatisch gelöscht. Überprüfen Sie nach der ersten DR-Konfiguration und nachdem Sie erhebliche Konfigurationsänderungen in einem DR-aktivierten Pool vorgenommen haben, ob 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. **

2. Select **Failover testen** 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 ab, bevor Sie versuchen, Daten wiederherzustellen. Die Spiegelung muss unterbrochen werden, um sicherzustellen, dass der sekundäre Standort über Lese-/Schreibzugriff verfügt.

3. Select die Speicher-Repositories (SRs) aus, die die Pool-Metadaten für die VMs und vApps enthalten, die Sie wiederherstellen möchten.

   Standardmäßig werden in der Liste auf dieser Assistentenseite alle SRs angezeigt, die derzeit im Pool angefügt sind. Um nach weiteren SRs zu **suchen, wählen Sie Speicher-Repositories** suchen und dann den Speichertyp, nach dem gesucht werden soll:

   - Um nach allen verfügbaren Hardware-HBA-SRs zu **suchen, wählen Sie Hardware-HBA-SRs**suchen aus.
   - Um nach Software-iSCSI-SRs zu **suchen, wählen Sie Software-iSCSI-SRs** suchen aus, und geben Sie dann die Zielhost-, IQN- und LUN-Details in das Feld ein.

   Wenn Sie die erforderlichen SRs im Assistenten ausgewählt haben, wählen Sie **Weiter** aus, um fortzufahren.

4. Select die VMs und vApps aus, die Sie wiederherstellen möchten, und wählen Sie **Weiter** , um zur nächsten Seite zu gelangen und Failover-Vorprüfungen zu beginnen.

5. Bevor Sie mit dem Test-Failover beginnen, führt der Assistent mehrere Vorüberprüfungen durch. Um beispielsweise sicherzustellen, dass der gesamte von den ausgewählten VMs und vApps benötigte Speicher verfügbar ist.

   - **Überprüfen Sie, ob Speicher verfügbar ist**. Wenn ein Speicher fehlt, können Sie SR anhängen auf dieser Seite auswählen, um die entsprechende SR zu suchen und anzuhängen.
   - **Überprüfen Sie, ob Hochverfügbarkeit im Ziel-DR-Pool nicht aktiviert ist**. Hochverfügbarkeit muss im sekundären Pool deaktiviert werden, um zu vermeiden, dass dieselben VMs sowohl auf dem primären als auch auf dem DR-Pool ausgeführt werden. Die hohe Verfügbarkeit muss deaktiviert werden, um sicherzustellen, dass die wiederhergestellten VMs und vApps nach der Wiederherstellung nicht automatisch gestartet werden. Um die hohe Verfügbarkeit im sekundären Pool zu deaktivieren, können Sie einfach **HA deaktivieren** auf der Seite auswählen. Wenn die hohe Verfügbarkeit zu diesem Zeitpunkt deaktiviert ist, wird sie am Ende des Test-Failoverprozesses automatisch wieder aktiviert.

   Beheben Sie alle Probleme auf der Seite Vorabprüfungen, und wählen Sie dann **Failover** aus, um das Test-Failover zu starten.

6. Auf einer Fortschrittsseite wird das Ergebnis des Wiederherstellungsprozesses für jede VM und vApp angezeigt. Der Failover-Prozess stellt Metadaten für die VMs und vApps aus dem

replizierten Speicher wieder her. Daher kann das Failover je nach Anzahl der wiederherstellen VMs und vApps einige Zeit in Anspruch nehmen. Die VMs und vApps werden im DR-Pool neu erstellt, die SRs, die die virtuellen Laufwerke enthalten, sind an die neu erstellten VMs angehängt.

Die wiederhergestellten VMs werden in einem angehaltenen Zustand versetzt: Sie werden während eines Test-Failovers nicht am sekundären Standort gestartet.

7. Nachdem Sie sich sicher sind, dass das Test-Failover erfolgreich ausgeführt wurde, wählen Sie Weiter im Assistenten aus, damit der Assistent auf der DR-Site bereinigt wird:

   - VMs und vApps, die während des Test-Failovers wiederhergestellt wurden, werden gelöscht.
   - Speicher, der während des Test-Failovers wiederhergestellt wurde, wird getrennt.
   - Wenn die hohe Verfügbarkeit im DR-Pool in der Vorprüfungsphase deaktiviert wurde, um das Test-Failover zu ermöglichen, wird es automatisch wieder aktiviert.

   Der Fortschritt des Bereinigungsvorgangs wird im Assistenten angezeigt.

8. Select **Fertig stellen** , um den Assistenten zu schließen.

Kopiert!
Failed!

vApps

October 16, 2019

Eine vApp ist eine logische Gruppe von einer oder mehreren verwandten virtuellen Maschinen (VMs). vApps können als eine einzelne Entität gestartet werden, wenn eine Katastrophe vorliegt. Wenn eine vApp gestartet wird, werden die in der vApp enthaltenen VMs in einer vom Benutzer vordefinierten Reihenfolge gestartet. Durch die Startreihenfolge können VMs, die voneinander abhängig sind, automatisch sequenziert werden. Ein Administrator muss den Start abhängiger VMs nicht mehr manuell sequenzieren, wenn ein ganzer Dienst neu gestartet werden muss. Zum Beispiel während eines Softwareupdates. Die VMs innerhalb der vApp müssen sich nicht auf einem Host befinden und werden mithilfe der normalen Regeln innerhalb eines Pools verteilt. Die vApp-Funktion ist in der Notfallwiederherstellung (Disaster Recovery, DR) nützlich. In einem DR-Szenario kann ein Administrator alle VMs auf demselben Speicher-Repository gruppieren, oder die sich auf die gleiche Service Level Agreement (SLA) beziehen.

Gehen Sie folgendermaßen vor, um VMs in einer vApp zu gruppieren:

1. Select 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. Es wird zwar empfohlen, mehrere vApps mit demselben Namen zu vermeiden, jedoch ist dies nicht erforderlich. XenCenter erzwingt keine Einschränkungen hinsichtlich eindeutiger vApp-Namen. Es ist nicht notwendig, Anführungszeichen für Namen zu verwenden, die Leerzeichen enthalten.

3. Select aus, welche VMs in die neue vApp aufgenommen werden sollen, und klicken Sie dann auf **Weiter**.

   Mit der Suchoption können Sie nur VMs mit Namen auflisten, 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 Startreihenwert von 0 (Null) werden zuerst gestartet. VMs mit dem Wert der Startreihenfolge 1 werden als Nächstes gestartet, dann die VMs mit dem Wert 2 usw.

   Versuch, die nächste VM nach zu starten: Ein Verzögerungsintervall, das angibt, wie lange nach dem Starten 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 zurückzukehren und die Einstellungen zu ändern, oder auf **Fertig stellen** , um die vApp zu erstellen.

> **Hinweis:**
>
> Eine vApp kann mehrere Server in einem einzelnen Pool umfassen, 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. Außerdem können Sie vApps starten und herunterfahren sowie vApps im ausgewählten Pool importieren und exportieren. Wenn Sie eine vApp in der Liste auswählen, werden die darin enthaltenen VMs im Detailbereich aufgeführt. Weitere Informationen finden Sie in der XenCenter Hilfe.

Kopiert!
Failed!

Sichern und Wiederherstellen von Hosts und VMs

October 16, 2019

Lassen Sie den installierten Status von Citrix Hypervisor or-Servern nach Möglichkeit unverändert. Das heißt, installieren Sie keine zusätzlichen Pakete oder starten Sie zusätzliche Dienste auf Citrix Hypervisor or-Servern und behandeln Sie sie als Appliances. Die beste Methode zum Wiederherstellen besteht dann darin, die Citrix Hypervisor or-Serversoftware vom Installationsmedium neu zu installieren. Wenn Sie über mehrere Citrix Hypervisor or-Server verfügen, ist es am besten, einen TFTP-Server und entsprechende Antwortdateien zu diesem Zweck zu konfigurieren. Weitere Informationen finden Sie unter Netzwerk-Boot-Installationen.

Wir empfehlen Ihnen, eine Sicherungslösung zu verwenden, die von einem unserer zertifizierten Partner angeboten wird. Weitere Informationen finden Sie unter Citrix Ready Marketplace.

Citrix Hypervisor Premium Edition-Kunden, die Citrix Hypervisor 7.3 oder eine neuere Version ausführen, können die Vorteile der schnelleren, geänderten Blocksicherung nutzen. Weitere Informationen finden Sie im Citrix Blog über Geänderte Blockverfolgungs-Backup-APIs.

Es wird empfohlen, dass Sie häufig so viele der folgenden Backup-Verfahren wie möglich durchführen, um nach einem möglichen Server- und Softwarefehler wiederherzustellen.

So sichern Sie Pool-Metadaten:

1. Führen Sie den Befehl aus:

```
xe pool-dump-database file-name=backup
```

2. Führen Sie den folgenden Befehl aus, um die Datenbank wiederherzustellen:

```
xe pool-restore-database file-name=backup dry-run=true
```

   Mit diesem Befehl wird überprüft, ob der Zielcomputer über eine entsprechende Anzahl von entsprechend benannten Netzwerkkarten verfügt, die für die erfolgreiche Sicherung erforderlich sind.

So sichern Sie die Hostkonfiguration und die Software:

1. Führen Sie den Befehl aus:

```
xe host-backup host=host file-name=hostbackup
```

> **Hinweise:**
>
> - Erstellen Sie die Sicherung nicht in der Steuerdomäne.

> - Der Sicherungsvorgang kann eine große Sicherungsdatei erstellen.
> - Um eine Wiederherstellung abzuschließen, müssen Sie die ursprüngliche Installations-CD neu starten.
> - Diese Daten können nur auf dem Originalcomputer wiederhergestellt werden.

So sichern Sie eine VM:

1. Stellen Sie sicher, dass die zu sichende VM offline ist.
2. Führen Sie den Befehl aus:

```
xe vm-export vm=vm_uuid filename=backup
```

> **Hinweis:**
>
> Diese Sicherung sichert auch alle VM-Daten. Beim Importieren einer VM können Sie den Speichermechanismus angeben, der für die gesicherten Daten verwendet werden soll.
>
> **Warnhinweis:**
>
> Der Sicherungsvorgang kann länger dauern, da alle VM-Daten gesichert werden.

So sichern Sie nur VM-Metadaten:

Führen Sie den Befehl aus:

```
xe vm-export vm=vm_uuid filename=backup metadata=true
```

Sichern von Metadaten virtueller Maschinen

Citrix Hypervisor or-Server verwenden auf jedem Host eine Datenbank, um Metadaten über VMs und zugehörige Ressourcen wie Speicher und Netzwerk zu speichern. In Kombination mit SRs bildet diese Datenbank die vollständige Ansicht aller VMs, die im Pool verfügbar sind. Daher ist es wichtig zu verstehen, wie Sie diese Datenbank sichern, um nach physischen Hardwarefehlern und anderen Katastrophenfällen wiederherzustellen.

In diesem Abschnitt wird zunächst beschrieben, wie Metadaten für Single-Host-Installationen und dann für komplexere Pool-Setups gesichert werden.

Sichern einzelner Host-Installationen

Verwenden Sie die CLI, um die Pooldatenbank zu sichern. Führen Sie zum Abrufen einer konsistenten Metadatensicherungsdatei`pool-dump-database` auf dem Citrix Hypervisor or-Server aus, und archivieren Sie die resultierende Datei. Die Sicherungsdatei enthält vertrauliche Authentifizierungsinformationen über den Pool. Stellen Sie daher sicher, dass sie sicher gespeichert sind.

Um die Pooldatenbank wiederherzustellen, verwenden Sie den`xe pool-restore-database` Befehl aus einer vorherigen Speicherabbilddatei. Wenn Ihr Citrix Hypervisor or-Server vollständig ausgestorben ist, müssen Sie zuerst eine Neuinstallation durchführen und dann den`pool-restore-database` Befehl auf dem neu installierten Citrix Hypervisor or-Server ausführen.

Nachdem Sie die Pooldatenbank wiederherstellen, werden einige VMs möglicherweise noch als registriert`Suspended`. Wenn das Speicher-Repository mit dem im`suspend-VDI-uuid` Feld definierten suspendierten Speicherstatus eine lokale SR ist, ist der SR möglicherweise nicht verfügbar, da der Host neu installiert wurde. Um diese VMs wieder auf den`Halted` Status zurückzusetzen, damit sie erneut gestartet werden können, verwenden Sie den`xe vm-shutdown vm=vm_name -force` Befehl oder verwenden Sie den`xe vm-reset-powerstate vm=vm_name -force` Befehl.

> **Warnhinweis:**
>
> Citrix Hypervisor behält UUIDs der Hosts bei, die mit dieser Methode wiederhergestellt wurden. Wenn Sie auf einem anderen physischen Computer wiederherstellen, während der ursprüngliche Citrix Hypervisor or-Server noch ausgeführt wird, sind möglicherweise doppelte UUIDs vorhanden. Daher verweigert XenCenter die Verbindung mit dem zweiten Citrix Hypervisor or-Server. Die Pooldatenbanksicherung ist nicht der empfohlene Mechanismus zum Klonen physischer Hosts. Verwenden Sie stattdessen die Unterstützung für die automatische Installation. Weitere Informationen finden Sie unter Installieren.

Sichern von gepoolten Installationen

In einem Poolszenario stellt der Master-Host eine autorisierende Datenbank bereit, die synchron auf alle Pool-Mitgliedshosts gespiegelt wird. Dieser Prozess bietet eine Ebene der integrierten Redundanz für einen Pool. Jedes Poolmitglied kann den Master ersetzen, da jedes Poolmitglied über eine genaue Version der Pooldatenbank verfügt. Weitere Informationen zum Übergang eines Mitglieds in ein Poolmaster finden Sie unterHosts und Ressourcenpools.

Dieses Schutzniveau reicht möglicherweise nicht aus. Wenn beispielsweise freigegebener Speicher, der die VM-Daten enthält, an mehreren Standorten gesichert wird, der lokale Serverspeicher (der die Pool-Metadaten enthält) jedoch nicht. Um einen Pool mit einem freigegebenen Speicher neu zu erstellen, müssen Sie die`pool-dump-database` Datei zunächst auf dem Master-Host sichern und diese Datei archivieren. So stellen Sie diese Sicherung später auf einem brandneuen Hosts wieder her:

1. Installieren Sie einen neuen Satz von Citrix Hypervisor or-Servern vom Installationsmedium oder ggf. vom Netzwerkstart des TFTP-Servers.
2. Verwenden Sie die`xe pool-restore-database` auf dem Host, der als neuer Master festgelegt wurde.
3. Führen Sie den`xe host-forget` Befehl auf dem neuen Master aus, um die alten Mitgliedscomputer zu entfernen.

4. Verwenden Sie den`xe pool-join` Befehl auf den Mitgliedshosts, um sie mit dem neuen Pool zu verbinden.

Sichern von Citrix Hypervisor -Servern

In diesem Abschnitt werden die Verfahren zur Sicherung und Wiederherstellung von Citrix Hypervisor or-Serversteuerungsdomänen beschrieben. Diese Prozeduren sichern *nicht* die Speicher-Repositories, in denen die VMs untergebracht sind, sondern nur die Domäne der privilegierten Kontrolle, auf der Xen und der Citrix Hypervisor Agent ausgeführt werden.

> **Hinweis:**
>
> Die privilegierte Steuerdomäne bleibt am besten wie installiert, ohne sie mit anderen Paketen anzupassen. Es wird empfohlen, eine Netzwerkstartumgebung einzurichten, um Citrix Hypervisor sauber von den Citrix Hypervisor-Medien als Wiederherstellungsstrategie zu installieren. Normalerweise müssen Sie die Steuerdomäne nicht sichern, aber wir empfehlen, die Pool-Metadaten zu speichern (sieheSichern von Metadaten virtueller Maschinen). Betrachten Sie diese Sicherungsmethode als Ergänzung zum Sichern der Pool-Metadaten.

Die Verwendung der xe-Befehle`host-backup` und`host-restore` ist ein weiterer Ansatz, den Sie ergreifen können. Der`host-backup` Befehl xe archiviert die aktive Partition in einer von Ihnen angegebenen Datei. Mit dem`host-restore` Befehl xe wird ein von xe erstelltes Archiv`host-backup` über die derzeit inaktive Festplattenpartition des Hosts extrahiert. Diese Partition kann dann aktiviert werden, indem Sie von der Installations-CD booten und die entsprechende Sicherung wiederherstellen.

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` weiter aus`/var/backup/pool-database-${ DATE }` , um die VM-Metadaten wiederherzustellen. Diese Datei wird`xe host-backup` mithilfe des`xe pool-dump-database` Befehls erstellt, bevor das laufende Dateisystem archiviert wird, um einen konsistenten Zustand der VM-Metadaten zu erstellen.

So sichern Sie Ihren Citrix Hypervisor -Server:

Führen Sie auf einem Remote-Host mit genügend Speicherplatz den folgenden Befehl aus

```
1 xe host-backup file-name=filename -h hostname -u root -pw password
```

Mit diesem Befehl wird ein komprimiertes Bild des Steuerdomänen-Dateisystems erstellt. Das Bild wird an der durch das`file-name` Argument angegebenen Position gespeichert.

So stellen Sie einen ausgeführten Citrix Hypervisor or-Server wieder her:

1. Wenn Sie den Citrix Hypervisor or-Server aus einer bestimmten Sicherung wiederherstellen möchten, führen Sie den folgenden Befehl aus, während der Citrix Hypervisor-Server hochgefahren und erreichbar ist:

   ```
   xe host-restore file-name=filename -h hostname -u root -pw
      password
   ```

   Mit diesem Befehl wird das komprimierte Image wieder auf der Festplatte des Citrix Hypervisor or-Servers wiederhergestellt, auf dem dieser Befehl ausgeführt wird (nicht auf dem Host, auf dem sich`filename` befindet). In diesem Zusammenhang kann „Wiederherstellen“ ein Missverständnis sein, da das Wort normalerweise darauf hindeutet, dass der gesicherte Zustand vollständig eingerichtet wurde. Der Befehl restore entpackt nur die komprimierte Sicherungsdatei und stellt sie in ihrer normalen Form wieder her. Es wird jedoch in eine andere Partition (`/dev/sda2`) geschrieben und überschreibt *nicht*die aktuelle Version des Dateisystems.

2. Um die wiederhergestellte Version des Stammdateisystems zu verwenden, starten Sie den Citrix Hypervisor or-Server mit der Citrix Hypervisor-Installations-CD neu, und wählen Sie die Option **Aus Sicherung wiederherstellen** .

   Nachdem die Wiederherstellung aus der Sicherung abgeschlossen ist, starten Sie den Citrix Hypervisor or-Server neu, und er wird vom wiederhergestellten Image gestartet.

3. Stellen Sie schließlich 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
   ```

> **Hinweis:**
>
> Das Wiederherstellen von einer Sicherung, wie in diesem Abschnitt beschrieben, zerstört die Sicherungspartition nicht.

So starten Sie einen abgestürzten Citrix Hypervisor or-Server neu:

Wenn Ihr Citrix Hypervisor or-Server abgestürzt ist und nicht erreichbar ist, verwenden Sie die Citrix Hypervisor Installations-CD, um eine Upgrade-Installation durchzuführen. Wenn die Aktualisierung abgeschlossen ist, starten Sie den Computer neu, und stellen Sie sicher, dass Ihr Host mit XenCenter oder Remote-CLI erreichbar ist.

Fahren Sie dann wie in diesem Abschnitt beschrieben mit der Sicherung von Citrix Hypervisor or-Servern fort.

Sichern von VMs

Wir empfehlen Ihnen, eine Sicherungslösung zu verwenden, die von einem unserer zertifizierten Partner angeboten wird. Weitere Informationen finden Sie unter Citrix Ready Marketplace.

Citrix Hypervisor Premium Edition-Kunden, die Citrix Hypervisor 7.3 oder eine neuere Version ausführen, können die Vorteile der schnelleren, geänderten Blocksicherung nutzen. Weitere Informationen finden Sie im Citrix Blog über Geänderte Blockverfolgungs-Backup-APIs.

Kopiert!
Failed!

VM-Snapshots

October 16, 2019

Citrix Hypervisor bietet einen praktischen Mechanismus, mit dem ein Snapshot eines VM-Speichers und Metadaten zu einem bestimmten Zeitpunkt erstellt werden kann. Falls erforderlich, werden die E/A-Vorgänge vorübergehend angehalten, während der Snapshot erstellt wird, um sicherzustellen, dass ein selbstkonsistentes Festplattenimage 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 angeschlossener VIFs, sodass sie zu Sicherungszwecken exportiert und wiederhergestellt werden können. Snapshots werden von allen Speichertypen unterstützt. Für die LVM-basierten Speichertypen müssen jedoch folgende Anforderungen erfüllt sein:

- Wenn das Speicher-Repository auf einer früheren Version von Citrix Hypervisor erstellt wurde, muss es aktualisiert worden sein
- Das Volume muss im Standardformat sein (Sie können keinen Snapshot von `type=raw` Volumes erstellen)

Der Snapshot-Vorgang ist ein zweistufiger Prozess:

- Erfassen von Metadaten als Vorlage.
- Erstellen eines VDI-Snapshots der Festplatten.

Es werden drei Arten von VM-Snapshots unterstützt: regulär, stillgelegt und Snapshot mit Arbeitsspeicher

Regelmäßige Schnappschüsse

Regelmäßige Snapshots sind absturzkonsistent und können auf allen VM-Typen, einschließlich Linux-VMs, ausgeführt werden.

Stillgestellte Snapshots

Stillgelegte Snapshots nutzen den Windows Volume Shadow Copy Service (VSS), um anwendungskonsistente Point-in-Time-Snapshots zu generieren. Das VSS-Framework hilft VSS-fähigen Anwendungen (z. B. Microsoft SQL Server), Daten auf den Datenträger zu leeren und den Snapshot vorzubereiten, bevor er erstellt wird.

Stillgelaufene Snapshots können daher sicherer wiederhergestellt werden, können jedoch während der Ausführung eine größere Leistungsauswirkung auf ein System haben. Sie können auch unter Last fehlschlagen, so dass mehr als ein Versuch erforderlich ist, den Snapshot zu erstellen.

Citrix Hypervisor unterstützt stillschweigte Snapshots auf:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32/64-bit)

Windows 10, Windows 8.1 und Windows 7 werden für stillschweigte Snapshots nicht unterstützt. Weitere Informationen zu stillgestellten Snapshots finden Sie unterErweiterte Hinweise für stillschweigte Snapshots.

Snapshots mit Speicher

Neben dem Speichern des VMS-Speichers (Speicher) und der Metadaten speichern Snapshots mit Speicher auch den VMS-Status (RAM). Diese Funktion kann nützlich sein, wenn Sie Software aktualisieren oder patchen, aber Sie möchten auch die Option, den VM-Status (Pre-Change VM Status, RAM) wiederherzustellen. Das Wiederherstellen eines Snapshots mit Arbeitsspeicher erfordert keinen Neustart der VM.

Sie können über die Management-API, die xe CLI oder XenCenter einen Snapshot mit Speicher einer laufenden oder angehaltenen VM erstellen.

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
- Vorbereiten des Klonvorbereitung einer Linux-VM

Stellen Sie zunächst sicher, dass die VM ausgeführt oder angehalten wird, damit der Speicherstatus erfasst werden kann. Die einfachste Möglichkeit, die VM auszuwählen, auf der der Vorgang ausgeführt werden soll, ist die Angabe des Argumentsvm=name odervm=vm uuid .

Führen Sie dievm-snapshot Befehlevm-snapshot-with-quiesce und aus, um einen Snapshot einer VM zu erstellen.

```
xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
xe vm-snapshot-with-quiesce vm=vm uuid new-name-label=vm_snapshot_name
```

Erstellen eines Snapshots mit Speicher

Führen Sie denvm-checkpoint Befehl aus und geben Sie einen beschreibenden Namen für den Snapshot mit Speicher an, damit Sie ihn später identifizieren können:

```
xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
```

Wenn Citrix Hypervisor das Erstellen des Snapshots mit Speicher abgeschlossen hat, wird dessen uuid angezeigt.

Zum Beispiel:

```
xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \
new-name-label=example_checkpoint_1
b3c0f369-59a1-dd16-ecd4-a1211df29886
```

Ein Snapshot mit Arbeitsspeicher benötigt mindestens 4 MB Festplattenspeicher pro Festplatte plus die Größe des Arbeitsspeichers plus etwa 20% Overhead. Ein Checkpoint mit 256 MB RAM würde also ungefähr 300 MB Speicher erfordern.

> **Hinweis:**
>
> Während der Prüfpunkterstellung wird die VM für einen kurzen Zeitraum angehalten und kann während dieses Zeitraums nicht verwendet werden.

So listen Sie alle Snapshots im Citrix Hypervisor Pool auf

Führen Sie densnapshot-list Befehl aus:

```
xe snapshot-list
```

Dieser Befehl listet alle Snapshots im Citrix Hypervisor Pool auf.

So listen Sie die Snapshots auf einer bestimmten VM auf

Ruft die uuid der jeweiligen VM ab, indem Sie den`vm-list` Befehl ausführen.

```
xe vm-list
```

Dieser Befehl zeigt eine Liste aller VMs und ihrer UUIDs an. Zum Beispiel:

```
xe vm-list
uuid ( RO): 116dd310-a0ef-a830-37c8-df41521ff72d
name-label ( RW): Windows Server 2012 (1)
power-state ( RO): halted

uuid ( RO): 96fde888-2a18-c042-491a-014e22b07839
name-label ( RW): Windows 2008 R2 (1)
power-state ( RO): running

uuid ( RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
name-label ( RW): Control domain on host
power-state ( RO): running
```

VMs können auch durch Filtern der vollständigen Liste der VMs nach den Werten von Feldern angegeben werden.

Beispielsweise werden alle VMs`power-state=halted` ausgewählt, deren Power-State-Feld gleich ‘angehalten’ ist. Wenn mehrere VMs übereinstimmen,`--multiple` muss die Option angegeben werden, um den Vorgang auszuführen. 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 Folgendes ein:

```
xe snapshot-list snapshot-of=vm uuid
```

Zum Beispiel:

```
xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
```

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
```



```
8       name-label ( RW): Snapshot with memory
9       name-description ( RW):
10      snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
11      snapshot_time ( RO): 20090914T15:39:45Z
```

Wiederherstellen einer VM in ihren vorherigen Status

Stellen Sie sicher, dass Sie die uuid des Snapshots haben, zu dem Sie zurückkehren möchten, und führen Sie dann densnapshot-revert folgenden Befehl aus:

1. Führen Sie den snapshot-list Befehl aus, um die UUID des Snapshots oder Checkpoints zu finden, zu dem Sie zurückkehren möchten:

   ```
   1 xe snapshot-list
   ```

2. Notieren Sie sich die uuid des Snapshots, und führen Sie dann den folgenden Befehl zum Wiederherstellen aus:

   ```
   1 xe snapshot-revert snapshot-uuid=snapshot uuid
   ```

   Zum Beispiel:

   ```
   1 xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
       a1211df29886
   ```

   Nachdem eine VM auf einen Prüfpunkt zurückgesetzt wurde, wird die VM angehalten.

> **Hinweise:**
>
> - Wenn nicht genügend Speicherplatz für die Bereitstellung des Snapshots verfügbar ist, 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 einem beliebigen Snapshot zurückzukehren. Vorhandene Snapshots und Checkpoints werden beim Wiederherstellen nicht gelöscht.

Löschen eines Snapshots

Stellen Sie sicher, dass Sie über die UUID des zu entfernenden Prüfpunkts oder Snapshots verfügen, und führen Sie dann den folgenden Befehl aus:

1. Führen Sie den snapshot-list Befehl aus, um die UUID des Snapshots oder Checkpoints zu finden, zu dem Sie zurückkehren möchten:


```
xe snapshot-list
```

2. Notieren Sie sich die UUID des Snapshots, und führen Sie dann den`snapshot-uninstall` Befehl aus, um ihn zu entfernen:

```
xe snapshot-uninstall snapshot-uuid=snapshot-uuid
```

3. Dieser Befehl weist Sie auf die gelöschten VM und VDIs hin. Geben Sie`yes` zur Bestätigung ein.

Zum 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
```

Wenn Sie nur die Metadaten eines Checkpoints oder Snapshots entfernen möchten, führen Sie den folgenden Befehl aus:

```
xe snapshot-destroy snapshot-uuid=snapshot-uuid
```

Zum Beispiel:

```
xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
```

Snapshot-Vorlagen

Erstellen einer Vorlage aus einem Snapshot

Sie können eine VM-Vorlage aus einem Snapshot erstellen. Der Speicherstatus wird jedoch entfernt.

1. Verwenden Sie den Befehl`snapshot-copy` und geben Sie eine`new-name-label` für die Vorlage an:

```
xe snapshot-copy new-name-label=vm-template-name \
      snapshot-uuid=uuid of the snapshot
```

   Zum Beispiel:


```
xe snapshot-copy new-name-label=example_template_1
      snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
```

> **Hinweis:**
>
> Mit diesem Befehl wird ein Vorlagenobjekt im SAME-Pool erstellt. Diese Vorlage ist nur für den aktuellen Pool in der Citrix Hypervisor Datenbank vorhanden.

2. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Vorlage erstellt wurde`template-list`:

```
xe template-list
```

Dieser Befehl listet alle Vorlagen auf dem Citrix Hypervisor or-Server auf.

Exportieren eines Snapshots 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
```

Zum Beispiel:

```
xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16-
   ecd4-a1211df29886 \
      filename=example_template_export
```

Die VM-Export/Importfunktion kann auf verschiedene Arten verwendet werden:

- Als praktische Backup-Einrichtung für Ihre VMs. Eine exportierte VM-Datei kann verwendet werden, um eine ganze VM in einem Katastrophenfall wiederherzustellen.
- Als eine Möglichkeit, eine VM schnell zu kopieren, beispielsweise eine spezielle Serverkonfiguration, die Sie oft verwenden. Sie konfigurieren die VM einfach nach Ihren Wünschen, exportieren sie und importieren sie dann, um Kopien Ihrer ursprünglichen VM zu erstellen.
- Als einfache Methode zum Verschieben einer VM auf einen anderen Server.

Weitere Informationen zur Verwendung von Vorlagen finden Sie unterVMs erstellenund auch im Abschnitt Verwalten von VMs in der XenCenter Hilfe.

Erweiterte Notizen für stillschweigte Snapshots

> **Hinweis:**
>
> Vergessen Sie nicht, den Xen VSS-Anbieter im Windows Gast zu installieren, um VSS zu unterstützen. Diese Installation wird mit dem `install- XenProvider.cmd` Skript durchgeführt, das mit den Citrix VM-Tools bereitgestellt wird. Weitere Informationen finden Sie unter Windows VMs.

Im Allgemeinen kann eine VM nur über die VSS-Schnittstelle auf VDI-Snapshots (keine VDI-Klone) zugreifen. Ein Citrix Hypervisor Administrator kann der VM ein Attribut von`snapmanager=true` hinzufügen,`other-config` damit diese VM Snapshots von VDIs von anderen VMs importieren kann.

> **Warnhinweis:**
>
> Diese Konfiguration öffnet eine Sicherheitslücke. Verwenden Sie es mit Vorsicht. Damit kann ein Administrator VSS-Snapshots mithilfe einer transportierbaren Snapshot-ID, die von der VSS-Schicht generiert wird, an eine andere VM zum Zwecke der Sicherung anhängen.

VSS-Ruhezeitüberschreitung: Die Microsoft VSS-Ruhezeit wird auf einen nicht konfigurierbaren Wert von 10 Sekunden festgelegt. Es ist wahrscheinlich, dass ein Snapshot nicht rechtzeitig abgeschlossen werden kann. Wenn der XAPI-Daemon beispielsweise zusätzliche Blockierungsaufgaben wie einen SR-Scan in die Warteschlange gestellt hat, kann der VSS-Snapshot ein Timeout aufweisen und fehlschlagen. Wenn diese Zeitüberschreitung auftritt, wiederholen Sie den Vorgang.

> **Hinweis:**
>
> Je mehr VBDs an eine VM angeschlossen sind, desto wahrscheinlicher ist es, dass dieses Timeout erreicht wird. Wir empfehlen, nicht mehr als 2 VBDs an eine VM anzuhängen, um das Timeout zu vermeiden. Es gibt jedoch eine Problemumgehung für dieses Problem. Die Wahrscheinlichkeit, einen erfolgreichen VSS-basierten Snapshot einer VM mit mehr als 2 VBDs zu erstellen, kann erhöht werden, wenn sich alle VDIs für die VM auf unterschiedlichen SRs befinden.

*VSS-Snapshot aller Festplatten, die an eine VM angeschlossen*sind: zum Speichern aller Daten, die zum Zeitpunkt eines VSS-Snapshots verfügbar sind. Der XAPI-Manager erstellt einen Snapshot aller Festplatten und der VM-Metadaten, die einer VM zugeordnet sind, für die Sie mithilfe der Citrix Hypervisor or-Speicher-Manager-API einen Snapshot erstellen können. Wenn der VSS-Layer nur einen Snapshot einer Teilmenge der Festplatten anfordert, wird kein vollständiger VM-Snapshot erstellt.

`vm-snapshot-with-quiesce`: Erstellt startfähige Snapshot-VM-Images: Der Citrix Hypervisor VSS-Hardwareanbieter macht Snapshot-Volumes beschreibbar, einschließlich des Snapshots des Boot-Volumes.

*VSS-Snap-Volumes, die auf dynamischen Datenträgern im Windows Gast gehostet*werden: Die`vm-snapshot-with-quiesce`CLI und der Citrix Hypervisor VSS-Hardwareanbieter unterstützen keine Snapshots von Volumes, die auf dynamischen Datenträgern auf der Windows-VM gehostet werden.

> **Hinweis:**
>
> Vergessen Sie nicht, den Xen VSS-Anbieter im Windows Gast zu installieren, um VSS zu unterstützen. Diese Installation wird mit dem `install-XenProvider.cmd` Skript durchgeführt, das mit den Citrix VM-Tools bereitgestellt wird. Weitere Informationen finden Sie unter Windows VMs.

Geplante Snapshots

Die Funktion „Geplante Snapshots“ bietet ein einfaches Sicherungs- und Wiederherstellungsprogramm für kritische Service-VMs. Regelmäßige geplante Snapshots werden automatisch erstellt und können zum Wiederherstellen einzelner VMs verwendet werden. Geplante Snapshots funktionieren mit pool-weiten Snapshot-Zeitplänen für ausgewählte VMs im Pool. Wenn ein Snapshot-Zeitplan aktiviert ist, werden Snapshots der angegebenen VM zu der geplanten Zeit jede Stunde, Tag oder Woche erstellt. Mehrere geplante Snapshots können in einem Pool 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, mit denen Sie diese Funktion verwenden können:

- Verwenden Sie den Assistenten für **Neuer Snapshot, um einen geplanten Snapshot** zu definieren.
- Verwenden Sie das Dialogfeld „ **VM-Snapshots“ -Zeitpläne** , um geplante Snapshots für einen Pool zu aktivieren, zu deaktivieren, zu bearbeiten und zu löschen.
- Um einen Snapshot-Zeitplan zu bearbeiten, öffnen Sie das Dialogfeld **Eigenschaften** 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 zu geplanten Snapshots finden Sie in der *XenCenter Hilfe*.

Kopiert!
Failed!

Bewältigen Sie Maschinenausfälle

October 16, 2019

Dieser Abschnitt enthält Details zum Wiederherstellen von verschiedenen Ausfallszenarien. Alle Fehlerwiederherstellungsszenarien erfordern die Verwendung eines oder mehrerer der in aufgeführten SicherungstypenBackup.

Mitgliederfehler

In Ermangelung von HA erkennen Master-Knoten die Fehler von Mitgliedern, indem sie regelmäßige Heartbeat-Nachrichten empfangen. Wenn 600 Sekunden lang kein Heartbeat empfangen wurde, geht der Master davon aus, dass das Mitglied tot ist. Es gibt zwei Möglichkeiten, dieses Problem zu beheben:

- Reparieren Sie den toten Host (z.B. durch physischen Neustart). Wenn die Verbindung zum Mitglied wiederhergestellt wird, markiert der Master das Mitglied erneut als lebendig.
- Fahren Sie den Host herunter und weisen Sie den Master an, den Mitgliedsknoten mithilfe des`xe host-forget` CLI-Befehls zu vergessen. Sobald das Mitglied vergessen wurde, werden alle dort ausgeführten VMs als offline markiert und können auf anderen Citrix Hypervisor or-Servern neu gestartet werden. Beachten Sie, dass es *sehr* wichtig ist, sicherzustellen, dass der Citrix Hypervisor or-Server tatsächlich offline ist, da sonst VM-Daten beschädigt werden können. Achten Sie darauf, Ihren Pool nicht in mehrere Pools eines einzelnen Hosts zu teilen`xe host-forget`, da dies dazu führen kann, dass alle denselben gemeinsam genutzten Speicher zuordnen und VM-Daten beschädigt werden.

> **Warnhinweis:**
>
> - Wenn Sie den vergessenen Host erneut als aktiven Host verwenden möchten, führen Sie eine Neuinstallation der Citrix Hypervisor or-Software durch.
> - Verwenden Sie keinen`xe host-forget` Befehl, wenn HA im Pool aktiviert ist. Deaktivieren Sie zuerst HA, dann vergessen Sie den Host, und aktivieren Sie dann HA wieder.

Wenn ein Citrix Hypervisor or-Server eines Mitglieds ausfällt, sind möglicherweise noch VMs im Status „*Ausführen* “ registriert. Wenn Sie sicher sind, dass der Citrix Hypervisor or-Server des Mitglieds definitiv ausgefallen ist, verwenden Sie den`xe vm-reset-powerstate` CLI-Befehl, um den Energiezustand der VMs auf festzulegen`halted` . Weitere Informationen finden Sie unter vm-reset-powerstate.

> **Warnhinweis:**
>
> Eine falsche Verwendung dieses Befehls kann zu Datenbeschädigung führen. Verwenden Sie diesen Befehl nur, wenn dies unbedingt erforderlich ist.

Bevor Sie VMs auf einem anderen Citrix Hypervisor or-Server starten können, müssen Sie die Sperren für den VM-Speicher freigeben. Jeder Datenträger in einem SR kann jeweils nur von einem Host verwendet werden. Daher ist es wichtig, dass der Datenträger für andere Citrix Hypervisor or-Server zugänglich gemacht werden kann, sobald ein Host ausgefallen ist. Führen Sie dazu das folgende

Skript auf dem Poolmaster für jeden SR aus, der Datenträger 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-Master - Poolmaster Citrix Hypervisor or-Server mit lokalem Speicher - war.

> **Warnhinweis:**
>
> Stellen Sie sicher, dass der Host ausgefallen ist, bevor Sie diesen Befehl ausführen. Eine falsche Verwendung dieses Befehls kann zu Datenbeschädigung führen.

Wenn Sie versuchen, eine VM auf einem anderen Citrix Hypervisor or-Server zu starten, bevor Sie das obige Skript ausführen, wird die folgende Fehlermeldung angezeigt:VDI <UUID> already attached RW“

Master-Fehler

Jedes Mitglied eines Ressourcenpools enthält alle Informationen, die erforderlich sind, um die Rolle des Masters zu übernehmen, falls erforderlich. Wenn ein Master-Knoten fehlschlägt, tritt die folgende Reihenfolge von Ereignissen auf:

1. Wenn HA aktiviert ist, wird automatisch ein anderer Master gewählt.
2. Wenn HA nicht aktiviert ist, wartet jedes Mitglied auf die Rückkehr des Masters.

Wenn der Master an diesem Punkt wieder auftaucht, stellt er die Kommunikation mit seinen Mitgliedern wieder her, und der Vorgang wird wieder normal.

Wenn der Master wirklich tot ist, wählen Sie eines der Mitglieder und führen Sie den Befehl`xe pool-emergency-transition-to-master` darauf aus. Sobald es zum Master geworden ist, führen Sie den Befehl aus`xe pool-recover-slaves` und die Mitglieder zeigen nun auf den neuen Master.

Wenn Sie den Server reparieren oder ersetzen, der der ursprüngliche Master war, können Sie ihn einfach starten, die Citrix Hypervisor or-Serversoftware installieren und dem Pool hinzufügen. Da die Citrix Hypervisor or-Server im Pool als homogen erzwungen werden, ist es nicht notwendig, den ersetzten Server zum Master zu machen.

Wenn ein Mitglied Citrix Hypervisor or-Server auf einen Master umgestellt wird, sollten Sie auch überprüfen, ob das Standard-Poolspeicher-Repository auf einen entsprechenden Wert festgelegt ist. Dies kann mit dem`xe pool-param-list` Befehl geschehen und überprüft werden, ob der`default-SR` Parameter auf ein gültiges Speicher-Repository verweist.

Pool-Fehler

Im bedauerlichen Fall, dass Ihr gesamter Ressourcenpool fehlschlägt, müssen Sie die Pooldatenbank von Grund auf neu erstellen. Stellen Sie sicher, dass Sie Ihre Pool-Metadaten regelmäßig mit dem`xe`

`pool-dump-database` CLI-Befehl sichern (siehePool-Dump-Datenbank).

So stellen Sie einen vollständig fehlgeschlagenen Pool wieder her:

1. Installieren Sie einen neuen Satz von Hosts. Becken Sie sie in diesem Stadium nicht auf.
2. Stellen Sie für den Host, der als Master nominiert wurde, die Pooldatenbank mithilfe des`xe pool-restore-database` Befehls aus Ihrer Sicherung wieder her (siehePool-Restore-Datenbank).
3. Stellen Sie mithilfe von XenCenter eine Verbindung zum Master-Host her, und stellen Sie sicher, dass alle freigegebenen Speicher und VMs wieder verfügbar sind.
4. Führen Sie einen Pool-Join-Vorgang auf den verbleibenden neu installierten Mitgliedshosts aus, und starten Sie Ihre VMs auf den entsprechenden Hosts.

Bewältigung von Fehlern aufgrund von Konfigurationsfehlern

Wenn der physische Hostcomputer betriebsbereit ist, aber die Software- oder Hostkonfiguration beschädigt ist:

1. Führen Sie den folgenden Befehl aus, um die Hostsoftware und -konfiguration wiederherzustellen:

```
1 xe host-restore host=host file-name=hostbackup
```

2. Starten Sie die Host-Installations-CD neu, und wählen Sie **Aus Sicherung wiederherstellen**.

Physischer Maschinenausfall

Wenn der physische Hostcomputer fehlgeschlagen ist, verwenden Sie die unten aufgelistete Vorgehensweise zum Wiederherstellen.

> **Warnung:**
>
> Alle VMs, die auf einem früheren Mitglied (oder dem vorherigen Host) ausgeführt werden, die fehlgeschlagen sind, werden weiterhin als`Running`in der Datenbank markiert. Dies dient der Sicherheit. Das gleichzeitige Starten einer VM auf zwei verschiedenen Hosts würde zu schwerwiegenden Datenträgerbeschädigungen führen. Wenn Sie sicher sind, dass die Maschinen (und VMs) offline sind, können Sie den Energiezustand der`Halted`VM auf zurücksetzen
>
> **`xe vm-reset-powerstate vm=vm_uuid --force`** VMs können dann mit XenCenter oder der CLI neu gestartet werden.

So ersetzen Sie einen fehlgeschlagenen Master durch ein noch laufendes Mitglied:

1. Führen Sie die folgenden Befehle aus:


```
xe pool-emergency-transition-to-master
xe pool-recover-slaves
```

2. Wenn die Befehle erfolgreich sind, starten Sie die VMs neu.

Fehler beim Wiederherstellen eines Pools mit allen Hosts:

1. Führen Sie den Befehl aus:

```
xe pool-restore-database file-name=backup
```

> **Warnhinweis:**
>
> Dieser Befehl ist nur erfolgreich, wenn der Zielcomputer über eine entsprechende Anzahl von entsprechend benannten Netzwerkkarten verfügt.

2. Wenn der Zielcomputer eine andere Ansicht des Speichers hat (z. B. eine Blockspiegelung mit einer anderen IP-Adresse) als der ursprüngliche Computer, ändern Sie die Speicherkonfiguration mit dem`pbd-destroy` Befehl und dann mit dem`pbd-create` Befehl , um Speicherkonfigurationen neu zu erstellen. Dokumentation`pbd-Befehle`zu diesen Befehlen finden Sie unter.
3. Wenn Sie eine neue Speicherkonfiguration erstellt haben, verwenden Sie`pbd-plug` oder Speicher> Speicher-Repository reparieren in XenCenter, um die neue Konfiguration zu verwenden.
4. Starten Sie alle VMs neu.

So stellen Sie eine VM wieder her, wenn der VM-Speicher nicht verfügbar ist:

1. Führen Sie den folgenden Befehl aus:

```
xe vm-import filename=backup metadata=true
```

2. Wenn der Metadatenimport fehlschlägt, führen Sie den folgenden Befehl aus:

```
xe vm-import filename=backup metadata=true --force
```

   Dieser Befehl versucht, die VM-Metadaten auf einer „besten“ Basis wiederherzustellen.

3. Starten Sie alle VMs neu.

Kopiert!
Failed!

Problembehandlung

October 16, 2019

Unterstützung

Citrix bietet zwei Arten von Support: kostenloser Selbsthilfe-Support auf derCitrix SupportWebsite und kostenpflichtige Support-Services, die Sie über die Support-Website erwerben können. Mit dem technischen Support von Citrix können Sie einen Support-Fall online öffnen oder sich telefonisch an das Support-Center wenden, wenn technische Schwierigkeiten auftreten.

DieCitrix WissenszentrumHosts mehrere Ressourcen, die Ihnen bei ungeraden Verhaltensweisen, Abstürzen oder anderen Problemen hilfreich sein könnten. Zu den Ressourcen gehören: Foren, Knowledge Base-Artikel, Whitepaper, Produktdokumentation, Hotfixes und andere Updates.

Wenn Sie technische Schwierigkeiten mit dem Citrix Hypervisor or-Server haben, soll dieser Abschnitt Ihnen helfen, das Problem möglichst zu lösen. Wenn dies nicht möglich ist, verwenden Sie die Informationen in diesem Abschnitt, um die Anwendungsprotokolle und andere Daten zu sammeln, die Ihrem Lösungsanbieter helfen können, das Problem zu verfolgen und zu beheben.

Informationen zur Behandlung von Citrix Hypervisor Installationsproblemen finden Sie unterProblembehandlung bei der Installation. Informationen zur Behebung von Problemen mit virtuellen Maschinen finden Sie unterBeheben von VM-Problemen.

> **Wichtig:**
>
> Wir empfehlen Ihnen, die Informationen zur Fehlerbehebung in diesem Abschnitt ausschließlich unter Anleitung Ihres Lösungsanbieters oder des Support-Teams zu befolgen.

In einigen Supportfällen ist der Zugriff auf die serielle Konsole für Debug-Zwecke erforderlich. Daher wird empfohlen, beim Einrichten der Citrix Hypervisor Konfiguration den Zugriff auf die serielle Konsole zu konfigurieren. Prüfen Sie bei Hosts, die keinen physischen seriellen Anschluss haben (z. B. einen Blade-Server) oder wenn keine geeignete physische Infrastruktur verfügbar ist, ob ein eingebettetes Verwaltungsgerät wie Dell DRAC oder HP iLO konfiguriert werden kann.

Hinweise zum Einrichten des seriellen Konsolenzugriffs finden Sie unterCTX121442.

Gesundheitsprüfung

Verwenden Sie die Integritätsprüfung, um den Serverstatusbericht zu generieren und in Citrix Insight Services (CIS) hochzuladen und CIS-Analyseberichte in XenCenter zu empfangen.

Wenn Sie einen berechtigten Pool mit XenCenter verbinden, werden Sie aufgefordert, die Integritätsprüfung für den Pool zu aktivieren. Während des Registrierungsprozesses können Sie die folgenden Aktionen ausführen:

- Geben Sie den Zeitplan an, der für das automatische Hochladen des Serverstatusberichts in CIS verwendet werden soll.

- Geben Sie Citrix Hypervisor Anmeldeinformationen ein, die zum Herstellen einer Verbindung mit dem Pool verwendet werden
- Authentifizieren Sie Ihre Uploads mit CIS

Nachdem der Pool erfolgreich bei der Integritätsprüfung registriert wurde, erhalten Sie in XenCenter Benachrichtigungen über den Zustand des Pools. Mit dieser Funktion können Sie die Integrität der Citrix Hypervisor or-Systeme basierend auf dem Bericht, den CIS generiert, proaktiv überwachen.

Anforderungen

So verwenden Sie die Integritätsprüfung:

- Auf allen Hosts im Pool muss Citrix Hypervisor 8.0 ausgeführt werden.
- Herstellen einer Verbindung mit dem Citrix Hypervisor-Pool mithilfe von XenCenter im Lieferumfang von Citrix Hypervisor 8.0
- XenCenter muss Zugang zum Internet haben
- Der Integritätsprüfung Dienst muss auf dem XenCenter Computer installiert und ausgeführt werden.
- Wenn Sie Active Directory (AD) verwenden, benötigen Sie einen Pooloperator oder eine höhere Rolle

Ausführliche Informationen zur Integritätsprüfung und Schritt-für-Schritt-Anleitungen zum Einschalten eines Pools für die Integritätsprüfung finden Sie in der XenCenter Hilfe.

Citrix Hypervisor-Serverprotokolle

XenCenter kann zum Sammeln von Citrix Hypervisor-Serverinformationen verwendet werden.

Klicken Sie im Menü **Extras** auf **Serverstatusbericht** , um den Task **Serverstatusbericht** zu öffnen. Sie können aus einer Liste verschiedener Arten von Informationen 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 Hilfe.

Darüber hinaus verfügt der Citrix Hypervisor or-Server über mehrere CLI-Befehle, die die Ausgabe von Protokollen und verschiedenen anderen Bits von Systeminformationen mithilfe des Dienstprogramms zusammenstellen`xen-bugtool`. Verwenden Sie den Befehl xe`host-bugreport-upload` , um die entsprechenden Protokolldateien und Systeminformationen zu sammeln und sie auf die Support-FTP-Site hochzuladen. Eine vollständige Beschreibung dieses Befehls und seiner optionalen Parameter finden Sie unter [`host-bugreport-upload`] (/de-de/citrix-hypervisor/command-line-interface.html #host -bugreport-upload). Wenn Sie aufgefordert werden, ein crashdump an das

Support-Team zu senden, verwenden Sie den Befehl xe`host-crashdump-upload`. Eine vollständige Beschreibung dieses Befehls und seiner optionalen Parameter finden Sie unter [`host-crashdump-upload`] (/de-de/citrix-hypervisor/command-line-interface.html #host -crashdump-upload).

> **Wichtig:**
>
> Citrix Hypervisor or-Serverprotokolle können vertrauliche Informationen enthalten.

Senden von Hostprotokollmeldungen an einen zentralen Server

Anstatt Protokolle in das Dateisystem der Steuerdomäne geschrieben zu haben, können Sie den Citrix Hypervisor or-Server so konfigurieren, dass er sie auf einen Remoteserver schreibt. Auf dem Remoteserver muss der`syslogd` Daemon ausgeführt werden, um die Protokolle zu empfangen und korrekt zu aggregieren. Der`syslogd` Daemon ist ein Standardteil aller Varianten von Linux und Unix, und Drittanbieter-Versionen sind für Windows und andere Betriebssysteme verfügbar.

Setzen Sie den Parameter syslog_destination auf den Hostnamen oder die IP-Adresse des Remoteservers, auf den die Protokolle geschrieben werden sollen:

```
xe host-param-set uuid=BRAND_SERVER_host_uuid logging:
   syslog_destination=hostname
```

Führen Sie den Befehl aus:

```
xe host-syslog-reconfigure uuid= BRAND_SERVER_host_uuid
```

Um die Änderung zu erzwingen. (Sie können diesen Befehl auch remote ausführen, indem Sie den`host` Parameter angeben.)

XenCenter Protokolle

XenCenter verfügt auch über ein clientseitiges Protokoll. Diese Datei enthält eine vollständige Beschreibung aller Vorgänge und Fehler, die bei der Verwendung von XenCenter auftreten. Es enthält auch Informationsprotokollierung von Ereignissen, die Ihnen einen Audit-Trail mit verschiedenen aufgetretenen Aktionen zur Verfügung stellen. Die XenCenter Protokolldatei wird im Profilordner gespeichert. Wenn XenCenter unter Windows 2008 installiert ist, lautet der Pfad

`%userprofile%\AppData\Citrix\XenCenter\logs\XenCenter.log`

Wenn XenCenter unter Windows 8.1 installiert ist, lautet der Pfad

`%userprofile%\AppData\Citrix\Roaming\XenCenter\logs\XenCenter.log`

Um die XenCenter Protokolldateien zu suchen, z. B. wenn Sie die Protokolldatei öffnen oder per E-Mail versenden möchten, klicken Sie im XenCenter-Hilfemenü auf Anwendungsprotokolldateien anzeigen.

Problembehandlung bei Verbindungen zwischen XenCenter und dem Citrix Hypervisor or-Server

Wenn Sie Probleme beim Herstellen einer Verbindung mit dem Citrix Hypervisor or-Server mit XenCenter haben, überprüfen Sie Folgendes:

- Ist Ihr XenCenter eine ältere Version als der Citrix Hypervisor or-Server, mit dem Sie eine Verbindung herstellen möchten?

  Die XenCenter-Anwendung ist abwärtskompatibel und kann ordnungsgemäß mit älteren Citrix Hypervisor or-Servern kommunizieren. Ein älteres XenCenter kann jedoch nicht ordnungsgemäß mit neueren Citrix Hypervisor-Servern kommunizieren.

  Um dieses Problem zu beheben, installieren Sie die XenCenter Version, die mit der Version des Citrix Hypervisor or-Servers identisch ist.

- Ist Ihr Führerschein aktuell?

  Das Ablaufdatum für den Lizenzzugriffscode finden Sie auf der Registerkarte „ **Allgemein“ des Citrix Hypervisor or-Servers „Allgemein** “ im Abschnitt „ **Lizenzdetails** “ in XenCenter.

  Weitere Informationen zum Lizenzieren eines Hosts finden Sie unterLizenzierung.

- Der Citrix Hypervisor or-Server spricht mit XenCenter über die folgenden Ports über HTTPS:
  - Port 443 (eine bidirektionale Verbindung für Befehle und Antworten mithilfe der Management-API)
  - Port 5900 für grafische VNC-Verbindungen mit paravirtualisierten Linux-VMs.

  Wenn zwischen dem Citrix Hypervisor or-Server und dem Computer, auf dem die Clientsoftware ausgeführt wird, eine Firewall aktiviert ist, stellen Sie sicher, dass Datenverkehr von diesen Ports zugelassen wird.

Kopiert!
Failed!

Ergänzungspaket für gemessene Stiefel

October 16, 2019

Mit dem Citrix Hypervisor Measured Boot Supplemental Pack können Kunden wichtige Komponenten ihrer Citrix Hypervisor Hosts beim Booten messen. Es bietet auch APIs, mit denen Remote-Bescheinigungslösungen diese Messungen sicher erfassen können. Dieses Ergänzungspaket ist kompatibel mit Intel-Computersystemen, die *Trusted Execution Technology* (TXT) unterstützen.

Dieses Ergänzungspaket kann von derCitrix Hypervisor 8.0 Premium EditionSeite heruntergeladen werden.

> **Hinweis:**
>
> Measured Boot Supplemental Pack ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.

Hintergrund

Nach der Installation dieses Supplemental Packs, wenn ein Citrix Hypervisor or-Server als nächstes gestartet wird, nimmt Intels TXT Messungen von Systemkomponenten niedriger Stufe (wie Firmware, BIOS, Xen Hypervisor, dom0 Kernel und dom0 initrd) vor und speichert sie an einem sicheren Ort auf dem als *vertrauenswürdigen Host bekannten Trusted Plattformmodul* (TPM). Eine neue Schnittstelle für Kunden, wie z. B. eine Remote-Bescheinigungslösung, wird zur sicheren Erfassung dieser Messungen bereitgestellt.

Remote-Bescheinigung

Remote-Bescheinigungslösungen funktionieren, indem eine Verbindung zu einem Citrix Hypervisor or-Server hergestellt wird, der sich in einem sauberen Zustand befindet. Es kann remote und sicher das TPM des Citrix Hypervisor or-Servers abfragen, um eine Liste der niedrigen Systemmessungen zu erhalten. Sie speichert diese Messungen in einer „White-List“ oder „Bekanntes Gut“ -Messliste.

An dieser Stelle sammelt die Remote-Bescheinigungssoftware regelmäßig wichtige Systemmessungen und vergleicht sie mit ihrer Liste „Bekanntes Gut“.

Ein Host gilt in folgenden Fällen als „nicht vertrauenswürdig“:

- Wenn die Remote-Bescheinigungssoftware die Messungen nicht erfassen kann
- Wenn sich die Messungen ändern
- Wenn die kryptografischen Schlüssel ungültig sind

In diesem Fall wird der Kunde benachrichtigt. Eine höhere Orchestrierungssoftware wie CloudStack, OpenStack oder Workload-Balancing-Software kann intelligente Sicherheitsvorgänge auf den betroffenen Hosts ausführen.

Vorbereiten des Citrix Hypervisor -Servers

Damit dieses Supplemental Pack ordnungsgemäß funktioniert, bearbeiten Sie vor dem Versuch, Daten zu sammeln, die folgenden Einstellungen im BIOS ihres Hosts:

1. Richten Sie den Citrix Hypervisor or-Server so ein, dass er im Legacy-Modus gestartet wird.

> **Hinweis:**
>
> Der UEFI-Boot-Modus wird beim gemessenen Start nicht unterstützt.

2. Aktivieren Sie **Intel AES-NI**.
3. Schalten Sie **TPM Security** oder **On mit Messungen vor dem Start** ein.
4. Reinigen Sie das TPM.

   Mit dieser Aktion werden alle vorherigen Einstellungen und Kennwörter gelöscht, die mit dem TPM verknüpft sind, damit das Citrix Hypervisor Measured Boot Supplemental Pack die Kontrolle über das TPM übernehmen kann.

   > **Hinweis:**
   >
   > Nach diesem Schritt ist ein Neustart erforderlich.

5. Aktivieren Sie **TPM**.
6. Aktivieren Sie **Intel TXT**.

> **Hinweis:**
>
> - Nach Schritt 5 und Schritt 6 ist ein Neustart erforderlich.
> - Die BIOS-Einstellungen variieren je nach Hardwarehersteller. Lesen Sie in der Hardwaredokumentation, wie Sie TPM und TXT für ihre spezifische Umgebung aktivieren.

Installieren Sie das Supplemental Pack

Verwenden Sie die Citrix Hypervisor CLI, um dieses Supplemental Pack zu installieren. Wie bei jedem Softwareupdate empfehlen wir Ihnen, Ihre Daten zu sichern, bevor Sie dieses Ergänzungspaket anwenden.

Supplemental Packs können innerhalb einer *ZIP-Datei* übertragen werden. Wenn das Supplemental Pack-ISO in einer ZIP-Datei enthalten ist, entpacken Sie diese ZIP-Datei (um das Disk-ISO-Image zu erzeugen), bevor Sie die folgenden Schritte ausführen.

Installation auf einem laufenden Citrix Hypervisor -System

1. Laden Sie das Supplemental Pack direkt auf den zu aktualisierenden Citrix Hypervisor Host herunter.

   Wir empfehlen, es im `/tmp/` Verzeichnis zu speichern.

   Alternativ können Sie die Datei auf einen mit dem Internet verbundenen Computer herunterladen und das ISO-Image auf eine CD brennen.

2. Verwenden Sie XenCenter, um auf die Konsole des Citrix Hypervisor Hosts zuzugreifen, oder verwenden Sie Secure Shell (SSH), um sich direkt anzumelden.

3. Die einfachste Methode besteht darin, direkt aus der ISO-Datei zu installieren. Geben Sie Folgendes ein:

   ```
   xe-install-supplemental-pack /tmp/Citrix Hypervisor-8.0-measured-boot.iso
   ```

   Wenn Sie das ISO auf eine CD brennen möchten, müssen Sie den Datenträger mounten. Geben Sie beispielsweise für eine CD-ROM Folgendes ein:

   ```
   mkdir -p /mnt/tmp
   mount /dev/<path to cd-rom> /mnt/tmp
   cd /mnt/tmp/
   ./install.sh
   cd /
   umount /mnt/tmp
   ```

4. Damit die Änderungen wirksam werden, starten Sie Ihren Host neu.

Neuinstallation

Wenn Sie dieses Supplemental Pack auf einer früheren Version installieren, bestätigen Sie das Überschreiben der vorherigen Installation. Geben Sie ein`Y` , wenn Sie während der`xe-install-supplemental-pack` Installation aufgefordert werden.

Standardkennwort aktualisieren

In früheren Versionen des Zusatzpakets wurde das Standardkennwort`xenroot` mit einem nachfolgenden Zeilenumbruch auf gesetzt. Dieser nachfolgende Zeilenumbruch wurde für das Standardkennwort in dieser Version des Zusatzpakets entfernt, wobei das neue Standardkennwort lautet`xenroot`.

Ein benutzerdefiniertes Passwort kann in gesetzt werden`/opt/xensource/tpm/config` und muss ein sha1 Hash eines Nur-Text-Passworts sein, das mit generiert werden kann`echo -n <password | sha1sum` . Wenn in dieser Befehlszeile weggelassen`-n` wird, ist ein nachgestellter Zeilenumbruch im Kennwort enthalten.

Asset-Tags festlegen

Asset-Tags können mit der`/opt/xensource/tpm/xentpm` Binärdatei mit den`--tpm_set_asset_tag` Methoden`--tpm_clear_asset_tag` und festgelegt werden, oder auch mit dem`tpm` Management-

API-Plug-In mit dentpm_set_asset_tag (ein 'tag' Argument nehmen) undtpm_clear_asset_tag Funktionen:

```
/opt/xensource/tpm/xentpm --tpm_set_asset_tag <tag_sha1>
/opt/xensource/tpm/xentpm --tpm_clear_asset_tag
xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
   tpm_set_asset_tag args:tag=<tag_sha1>
xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
   tpm_clear_asset_tag
```

> **Hinweis:**
>
> Nach diesem Schritt ist ein Neustart erforderlich.

Weitere Informationen

Informationen zum Herunterladen des Supplemental Packs für Meßboote finden SieCitrix Hypervisor 8.0 Premium Editionauf der Seite.

Wenn Sie Schwierigkeiten bei der Installation dieses Supplemental Packs haben, wenden Sie sich anTechnischer Support von Citrix.

Die Dokumentation zu Citrix Hypervisor 8.0 finden SieCitrix Produktdokumentationauf der Website.

Kopiert!
Failed!

Arbeitslastausgleich

October 16, 2019

Workload Balancing ist eine Citrix Hypervisor Komponente, die als virtuelle Appliance verpackt ist, die:

- Erstellung von Berichten zur VM-Leistung in Ihrer Citrix Hypervisor Umgebung
- Bewertet die Ressourcenauslastung und sucht virtuelle Maschinen auf den bestmöglichen Hosts im Pool nach den Anforderungen ihrer Arbeitslast.

> **Hinweise:**
>
> - Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben.
> - Workload Balancing 8.0 ist mit allen unterstützten Versionen von Citrix Hypervisor und

> XenServer kompatibel.

Selbst wenn Sie den Workload-Balancing nicht zum Ausgleich Ihrer VMs verwenden möchten, sollten Sie ihn trotzdem für die Workload-Berichterstellungsfunktion ausführen. Bei der Bereitstellung zur Verwaltung von Arbeitslasten virtueller Maschinen kann der Workload Balancing folgende Aufgaben ausführen:

- Ausgleich von VM-Arbeitslasten über Hosts in einem Citrix Hypervisor Ressourcenpool
- Ermitteln des besten Hosts, auf dem eine virtuelle Maschine gestartet werden soll
- Bestimmen Sie den besten Host, auf dem eine virtuelle Maschine fortgesetzt werden soll, die Sie ausgeschaltet haben
- Bestimmen Sie den besten Host, auf den eine virtuelle Maschine verschoben werden soll, wenn ein Host ausfällt
- Bestimmen Sie den optimalen Server für jede virtuelle Maschine des Hosts, wenn Sie einen Host in den Wartungsmodus versetzen oder einen Host aus dem Wartungsmodus ziehen.

Abhängig von Ihrer Präferenz 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 (z. B. um Strom in der Nacht zu sparen).

Workload-Balancing-Funktionen durch Auswertung der Verwendung von VMs in einem Pool. Wenn ein Host einen Leistungsschwellenwert überschreitet, verlagert der Workload Balancing die VM auf einen weniger besteuerten Host im Pool. Zum Neuausgleich von Arbeitslasten verschiebt der Workload Balancing VMs, um die Ressourcenverwendung auf Hosts auszugleichen.

Um sicherzustellen, dass die Empfehlungen zum Neuausgleich und zur Platzierung den Anforderungen Ihrer Umgebung entsprechen, können Sie den Workload-Balancing so konfigurieren, dass die Workloads entweder für die Ressourcenleistung optimiert werden oder die Anzahl der virtuellen Maschinen maximiert werden, die auf Hosts passen. Diese Optimierungsmodi können so konfiguriert werden, dass sie sich automatisch zu vordefinierten Zeiten ändern oder immer gleich bleiben. Optimieren Sie die Gewichtung einzelner Ressourcenmetriken (CPU, Netzwerk, Festplatte und Speicher) für zusätzliche Granularität.

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.

Berichte zu Arbeitslasten

Da der Workload Balancing Performance-Daten erfasst, können Sie diese Komponente auch zum Generieren von Berichten (Workload Reports) über Ihre virtualisierte Umgebung verwenden.

Workload-Berichte stellen Daten für den Zustand eines Pools oder Hosts, für die Überwachung, Optimierung und den Platzierungsverlauf (oder Bewegungsverlauf) bereit. Außerdem können Sie einen Ausgleichsbericht ausführen, der die Nutzung virtueller Maschinen anzeigt und Ihnen dabei helfen kann, Kosten zu messen und zuzuordnen.

Zum Ausführen von Berichten müssen Sie nicht für den Workload Balancing konfigurieren, um Platzierungsempfehlungen abzugeben oder virtuelle Maschinen zu verschieben. Sie müssen jedoch die Komponente „Workload Balancing“ konfigurieren. Idealerweise müssen Sie kritische Schwellenwerte auf Werte festlegen, die den Punkt widerspiegeln, an dem sich die Leistung der Hosts in Ihrem Pool verschlechtert.

Weitere Informationen finden Sie unter Generieren von Workload-Berichten.

Workload Balancing Grundkonzepte

Wenn virtuelle Maschinen ausgeführt werden, verbrauchen sie *Rechenressourcen* auf dem physischen Host, z. B. CPU, Arbeitsspeicher, Netzwerklesevorgänge, Netzwerkschreibvorgänge, Datenträgerlesungen und Festplattenschreibvorgänge. Beispielsweise können einige virtuelle Maschinen, abhängig von ihrer *Arbeitslast*, mehr CPU-Ressourcen verbrauchen als andere virtuelle Maschinen auf demselben Host. Die Arbeitslast wird durch die auf einer virtuellen Maschine ausgeführten Anwendungen und deren Benutzertransaktionen definiert. Natürlich reduziert der kombinierte Ressourcenverbrauch aller virtuellen Maschinen auf einem Host die verfügbaren Ressourcen auf dem Host.

Workload Balancing erfasst Daten zur Ressourcenleistung auf virtuellen Maschinen und physischen Hosts und speichert sie in einer Datenbank. Workload Balancing verwendet diese Daten zusammen mit den von Ihnen festgelegten Einstellungen, um Optimierungs- und Platzierungsempfehlungen bereitzustellen.

Optimierungen sind eine Art und Weise, wie Hosts „verbessert“ werden, um Ihren Zielen anzupassen: Workload Balancing gibt Empfehlungen für die Umverteilung der virtuellen Maschinen auf Hosts im Pool aus, um die Leistung oder Dichte zu erhöhen. Wenn Workload Balancing Empfehlungen ausgibt, werden sie im Hinblick auf ihr Ziel gesetzt: Gleichgewicht oder Harmonie über die Hosts im Pool hinweg zu schaffen. Wenn der Workload Balancing auf diese Empfehlungen reagiert, wird die Aktion als Optimierung bezeichnet.

In einem Workload-Balancing-Kontext:

- **Leistung** ist die Verwendung physischer Ressourcen auf einem Host (z. B. CPU, Arbeitsspeicher, Netzwerk und Festplattenauslastung auf einem Host). Wenn Sie den Workload Balancing so einstellen, dass die Leistung maximiert wird, empfiehlt es sich, virtuelle Maschinen zu platzieren, um sicherzustellen, dass die maximale Menge an Ressourcen für jede virtuelle Maschine verfügbar ist.

- **Dichte** ist die Anzahl der VMs auf einem Host. Wenn Sie den Workload Balancing so einstellen, dass die Dichte maximiert wird, empfiehlt es sich, VMs zu platzieren, damit Sie die Anzahl der in einem Pool eingeschalteten Hosts reduzieren können. Es stellt sicher, dass die VMs über eine ausreichende Rechenleistung verfügen.

Der Arbeitslastausgleich steht nicht in Konflikt mit den Einstellungen, die Sie bereits für Hochverfügbarkeit festgelegt haben: Diese Funktionen sind kompatibel.

Anforderungen an den Pool

Um einen Pool mit dem Workload-Balancing auszugleichen, müssen die Hosts im Pool die Anforderungen für die Live-Migration erfüllen, einschließlich:

- Gemeinsamer Remotespeicher
- Ähnliche Prozessorkonfigurationen
- Gigabit Ethernet

Wenn die Hosts diese Anforderungen nicht erfüllen, kann der Workload-Balancing die virtuellen Maschinen im Pool nicht migrieren.

> **Hinweis**
>
> Der Workload-Balancing wird für einen Pool, der VGPU-fähige VMs enthält, nicht unterstützt. Der Workload-Balancing kann keine Kapazitätsplanung für VMs, die eine vGPU angeschlossen haben.

Kopiert!
Failed!

Erste Schritte mit Workload Balancing

October 16, 2019

Sie können die virtuelle Workload-Balancing-Appliance in wenigen einfachen Schritten konfigurieren:

1. Laden Sie die virtuelle Workload Balancing-Appliance herunterhttp://www.citrix.com/downloadsund importieren Sie sie in XenCenter.
2. Konfigurieren Sie die Workload Balancing Appliance über die Konsole der virtuellen Appliance.
3. Verbinden Sie Ihren Pool mit der virtuellen Appliance „Workload Balancing“.

Um einen Pool mit dem Workload-Balancing auszugleichen, müssen die Hosts des Pools die Anforderungen für die Live-Migration erfüllen, wie unter beschriebenVerwalten.

Importieren der virtuellen Workload-Balancing-Appliance

Die virtuelle Workload Balancing-Appliance ist eine einzelne vorinstallierte virtuelle Maschine, die auf einem Citrix Hypervisor or-Server ausgeführt werden kann. Überprüfen Sie vor dem Importieren die erforderlichen Informationen und Überlegungen.

Voraussetzungen

Diese Appliance wurde für Citrix Hypervisor 7.1 und höher entwickelt. Er kann Pools überwachen, auf denen Citrix Hypervisor 5.5-Hosts und höher ausgeführt werden. Es wird empfohlen, die virtuelle Appliance mit der XenCenter Verwaltungskonsole zu importieren. Die virtuelle Workload Balancing-Appliance benötigt mindestens 2 GB RAM und 20 GB Festplattenspeicher.

Vor dem Importieren der virtuellen Appliance zu berücksichtigende Informationen

Beachten Sie vor dem Importieren der virtuellen Appliance die folgenden Informationen und nehmen Sie gegebenenfalls die entsprechenden Änderungen an Ihrer Umgebung vor. Überprüfen Sie außerdem die Versionshinweise für den Workload Balancing, um späte, versionsspezifische Anforderungen zu erhalten.

- **Kommunikationsport**. Bevor Sie den Assistenten für die Konfiguration des Arbeitslastausgleichs starten, bestimmen Sie den Port, über den die virtuelle Appliance „Workload Balancing“ kommunizieren soll. Sie werden während der Konfiguration des Arbeitslastausgleichs zur Eingabe dieses Ports aufgefordert. Standardmäßig verwendet der Workload Balancing Server 8012.

  > **Hinweis:**
  >
  > Legen Sie den Workload Balancing-Port nicht auf Port 443 fest. Die virtuelle Workload Balancing-Appliance kann keine Verbindungen über Port 443 (Standard-SSL/HTTPS-Port) akzeptieren.

- **Konto für den Arbeitslastausgleich**. Für den Workload Balancing Configuration Wizard müssen Sie einen Benutzernamen und ein Kennwort für das Workload Balancing-Konto und das Datenbankkonto auswählen und eingeben. Sie müssen diese Konten nicht erstellen, bevor Sie den Konfigurations-Assistenten ausführen. Der Konfigurationsassistent erstellt diese Konten für Sie.
- **Überwachung über Pools hinweg**. Sie können die virtuelle Workload-Balancing-Appliance in einem Pool platzieren und einen anderen Pool damit überwachen. (Die virtuelle Appliance „Workload Balancing“ befindet sich beispielsweise in Pool A, Sie verwenden sie jedoch zur Überwachung von Pool B).

> **Hinweis:**
>
> Die virtuelle Appliance für den Workload Balancing erfordert, dass die Zeit auf dem physischen Computer, auf dem die virtuelle Appliance gehostet wird, der vom überwachten Pool verwendet wird. Es gibt keine Möglichkeit, die Zeit auf der virtuellen Appliance „Workload Balancing“ zu ändern. Es wird empfohlen, sowohl den physischen Computer, auf dem der Workload Balancing gehostet wird, als auch die Hosts im Pool, den er überwacht, auf denselben NTP-Server (Network Time, Network Time) zu verweisen.

- **Citrix Hypervisor und Workload Balancing kommunizieren über HTTPS**. Daher erstellt der Workload Balancing während der Konfiguration des Workload Balancing automatisch ein selbstsigniertes Zertifikat in Ihrem Namen. Sie können dieses Zertifikat von einer Zertifizierungsstelle in eines ändern oder Citrix Hypervisor so konfigurieren, dass das Zertifikat oder beides überprüft wird. Weitere Informationen finden Sie im Workload Balancing Administrator's Guide.
- **Speichern von historischen Daten und Datenträgergröße**. Die Menge der historischen Daten, die Sie speichern können, basiert auf den folgenden:
  - Die Größe des virtuellen Laufwerks, das dem Workload-Balancing zugewiesen ist (standardmäßig 20 GB)
  - Der minimale Speicherplatz, der standardmäßig 2.048 MB beträgt und durch den`GroomingRequiredM` Parameter in der Datei wlb.conf gesteuert wird.

  Wenn Sie viele historische Daten speichern möchten, können Sie eine der folgenden Aktionen ausführen:

  - Archivieren Sie die Daten wie unterVerwalten
  - Vergrößern Sie die virtuelle Datenträgergröße, die der virtuellen Appliance „Workload Balancing“ zugewiesen ist.

  Wenn Sie beispielsweise das Feature WLB Pool Audit Trail verwenden und die Berichtgranularität auf Medium oder höher konfigurieren möchten.

  Um die Datenträgergröße zu erhöhen, importieren Sie die virtuelle Appliance und erhöhen Sie dann die Größe des virtuellen Laufwerks, indem Sie die im Workload Balancing Administrator's Guide beschriebenen Schritte befolgen.
- **Lastenausgleich Arbeitslastausgleich**. Wenn Sie Ihre virtuelle Workload Balancing-Appliance zur Verwaltung selbst verwenden möchten, geben Sie beim Importieren der virtuellen Appliance gemeinsam genutzten Remotespeicher an.

> **Hinweis:**
>
> Workload Balancing kann die Empfehlung „Start On Placement“ für die virtuelle Appliance „Workload Balancing“ nicht ausführen, wenn Sie den Workload Balancing verwenden, um

> sich selbst zu verwalten. Der Grund, warum Workload Balancing bei der Verwaltung selbst keine Platzierungsempfehlungen abgeben kann, liegt darin, dass die virtuelle Appliance ausgeführt werden muss, um diese Funktion auszuführen. Sie kann jedoch die virtuelle Workload-Balancing-Appliance so ausgleichen, wie sie jede andere VM, die sie verwaltet, ausgleichen würde.

Planen der Ressourcenpoolgröße

Für den Workload Balancing sind bestimmte Konfigurationen erforderlich, um in großen Pools erfolgreich ausgeführt zu werden.

Laden Sie die virtuelle Appliance herunter

Die virtuelle Workload Balancing-Appliance ist in einem `.xva` Format verpackt. Sie können die virtuelle Appliance von der Citrix Downloadseite herunterladenhttp://www.citrix.com/downloads. Speichern Sie die Datei beim Herunterladen in einem Ordner auf der lokalen Festplatte (normalerweise auf dem Computer, auf dem XenCenter installiert ist). Wenn der `.xva` Download abgeschlossen ist, können Sie ihn in XenCenter importieren.

Importieren der virtuellen Appliance in XenCenter

Verwenden Sie XenCenter, um die virtuelle Workload Balancing-Appliance in einen Pool zu importieren.

So importieren Sie die virtuelle Appliance in Citrix Hypervisor:

1. Öffnen Sie XenCenter.
2. Klicken Sie mit der rechten Maustaste auf den Pool (oder den Host), in den Sie das Paket der virtuellen Appliance importieren möchten, und wählen Sie **Importieren**aus.
3. Navigieren Sie zum`vpx-wlb.xva` Paket.
4. Select den Pool oder den Home-Server aus, auf dem die virtuelle Workload-Balancing-Appliance ausgeführt werden soll.

   Wenn Sie den Pool auswählen, startet die VM automatisch auf dem am besten geeigneten Host in diesem Pool.

   Wenn Sie die virtuelle Appliance „Workload Balancing“ nicht mit dem Workload Balancing verwalten, können Sie auch einen Home-Server für die virtuelle Appliance „Workload Balancing“ festlegen. Diese Einstellung stellt sicher, dass die virtuelle Appliance immer auf demselben Host gestartet wird.

5. Wählen Sie ein Speicher-Repository aus, in dem das virtuelle Laufwerk für die virtuelle Appliance „Workload Balancing“ gespeichert werden soll. Dieses Repository muss mindestens 20 GB freien Speicherplatz haben.

   Sie können entweder lokalen Speicher oder Remotespeicher auswählen. Wenn Sie jedoch lokalen Speicher auswählen, können Sie die virtuelle Appliance nicht mit dem Workload Balancing verwalten.

6. Definieren Sie die virtuellen Schnittstellen für die virtuelle Appliance „Workload Balancing“. In dieser Version ist der Workload Balancing so konzipiert, dass er über eine einzige virtuelle Schnittstelle kommuniziert.

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 **Fertig stellen** , um die virtuelle Appliance zu importieren.

9. Nachdem Sie den Import der `.xva` Datei „Workload Balancing“ abgeschlossen haben, wird die virtuelle Maschine „Workload Balancing“ im Bereich „ **Ressource** “ in XenCenter angezeigt.

Konfigurieren der virtuellen Workload-Balancing-Appliance

Nachdem Sie den Import der virtuellen Appliance „Workload Balancing“ abgeschlossen haben, müssen Sie sie konfigurieren, bevor Sie sie zum Verwalten Ihres Pools verwenden können. Um Sie durch die Konfiguration zu führen, stellt Ihnen die virtuelle Appliance „Workload Balancing“ einen Konfigurationsassistenten in XenCenter zur Verfügung. Wählen Sie die virtuelle Appliance im Ressourcenbereich 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 Appliance „Workload Balancing“ auf die Registerkarte „ **Konsole** “.

2. Geben Sie ein`yes` , um die Bedingungen der Lizenzvereinbarung zu akzeptieren. Geben Sie ein, um die Endbenutzer-Lizenzvereinbarung abzulehnen`no`.

   > **Hinweis:**
   >
   > Die virtuelle Workload Balancing-Appliance unterliegt außerdem den Lizenzen, die im `/opt/vpx/wlb` Verzeichnis der virtuellen Appliance für den Workload Balancing enthalten sind.

3. Geben Sie ein neues Stammkennwort für die virtuelle Maschine „Workload Balancing“ ein, und bestätigen Sie es. Citrix empfiehlt, ein sicheres Kennwort auszuwählen.

> **Hinweis:**
>
> Wenn Sie das Kennwort eingeben, werden in der Konsole keine Platzhalter wie Sternchen für die Zeichen angezeigt.

4. Geben Sie den Computernamen ein, den Sie der virtuellen Appliance „Workload Balancing“ zuweisen möchten.
5. Geben Sie das Domänensuffix für die virtuelle Appliance ein.

   Wenn z. B. der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) für die virtuelle Appliance lautet`wlb-vpx-pos-pool.domain4.bedford4.ctx`, geben Sie ein`domain4.bedford4.ctx`.

   > **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 zum Herstellen einer Verbindung mit dem Workload Balancing verwenden soll, müssen Sie den FQDN Ihrem DNS-Server hinzufügen.

6. Geben Sie ein`y` , um DHCP zu verwenden, um die IP-Adresse für die virtuelle Maschine „Workload Balancing“ automatisch abzurufen. Andernfalls geben Sie eine statische IP-Adresse, eine Subnetzmaske`n` und ein Gateway für die virtuelle Maschine ein, und geben Sie sie ein.

   > **Hinweis:**
   >
   > Die Verwendung von DHCP ist akzeptabel, 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, um in die Workload Balancing-Datenbank zu lesen/zu schreiben. Notieren Sie sich den Benutzernamen und das Kennwort. Sie können sie benötigen, wenn Sie jemals direkt in die Workload Balancing PostgreSQL Datenbank verwalten möchten (z. B. wenn Sie Daten exportieren möchten).

8. Geben Sie ein Kennwort für die Workload Balancing-Datenbank ein. Nach dem Drücken der **Eingabetaste**werden Meldungen angezeigt, die besagt, dass der Konfigurations-Assistent Datenbankobjekte lädt.
9. Geben Sie einen Benutzernamen und ein Kennwort für den Workload Balancing Server ein.

Mit dieser Aktion wird das Konto erstellt, das Citrix Hypervisor für die Verbindung mit dem Workload Balancing verwendet. Der Standardbenutzername ist **wlbuser**.

10. Geben Sie den Port für den Workload Balancing Server ein. Der Workload Balancing Server kommuniziert über diesen Port.

    Standardmäßig verwendet der Workload-Balancing-Server 8012. Die Portnummer kann nicht auf 443 festgelegt werden, was die Standard-SSL-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 Dialogfeld Mit **WLB-Server verbinden** angeben.

    Stellen Sie sicher, dass der Port, den Sie für den Workload Balancing angeben, in allen Firewalls geöffnet ist.

    Nachdem Sie die **Eingabetaste**gedrückt haben, wird der Workload Balancing mit der Konfiguration der virtuellen Appliance fortgesetzt, einschließlich der Erstellung selbstsignierter Zertifikate.

11. Jetzt können Sie sich auch bei der virtuellen Appliance anmelden, indem Sie den VM-Benutzernamen (normalerweise`root`) und das Root-Kennwort eingeben, das Sie zuvor erstellt haben. Die Anmeldung ist jedoch nur erforderlich, wenn Sie Workload Balancing-Befehle ausführen oder die Workload Balancing-Konfigurationsdatei bearbeiten möchten.

Nachdem Sie den Workload Balancing konfiguriert haben, verbinden Sie Ihren Pool mit der virtuellen Workload Balancing-Appliance, wie unter beschriebenHerstellen einer Verbindung mit der virtuellen Appliance „Workload Balancing“.

Bei Bedarf finden Sie die Konfigurationsdatei für den Workload Balancing unter folgendem Speicherort: /opt/vpx/wlb/wlb.conf. Die Protokolldatei für den Workload Balancing befindet sich an folgendem Speicherort: /var/log/wlb/logfile.log. Weitere Informationen zu diesen Dateien und ihrem Zweck finden Sie im Workload Balancing Administrator’s Guide.

Herstellen einer Verbindung mit der virtuellen Appliance „Workload Balancing“

> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

Nachdem Sie den Workload Balancing konfiguriert haben, verbinden Sie den Pool, den Sie verwalten möchten, mit der virtuellen WLB-Appliance mithilfe der CLI oder XenCenter.

Um das folgende XenCenter Verfahren abzuschließen, benötigen Sie Folgendes:

- IP-Adresse oder FQDN der virtuellen Appliance „Workload Balancing“ und deren Portnummer
- Anmeldeinformationen für den Ressourcenpool (d. h. den Poolmaster), den der Workload Balancing überwachen soll.
- Anmeldeinformationen für das Konto „Workload Balancing“, das Sie während der Konfiguration des Workload Balancing erstellt haben. Citrix Hypervisor verwendet dieses Konto, um mit dem Workload Balancing zu kommunizieren.

Um den Workload-Balancing-FQDN anzugeben, wenn Sie eine Verbindung zum Workload-Balancing-Server herstellen, fügen Sie zuerst den Hostnamen und die IP-Adresse dem DNS-Server hinzu.

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.

Herstellen einer Verbindung mit Workload-Balancing und Zertifikaten

Wenn Sie ein anderes (vertrauenswürdiges) Zertifikat hochladen oder die Zertifikatüberprüfung konfigurieren möchten, beachten Sie Folgendes, bevor Sie Ihren Pool mit dem Workload Balancing verbinden:

- Wenn Citrix Hypervisor das selbstsignierte Workload Balancing-Zertifikat verifizieren soll, müssen Sie die IP-Adresse des Workload Balancing-Netzwerklastenausgleichs verwenden, um eine Verbindung mit dem Workload Balancing herzustellen. Das selbstsignierte Zertifikat wird basierend auf seiner IP-Adresse an den Workload Balancing ausgegeben.
- Wenn Sie ein Zertifikat von einer Zertifizierungsstelle verwenden möchten, ist es einfacher, den FQDN anzugeben, wenn Sie eine Verbindung mit dem Workload Balancing herstellen. Sie können jedoch im Dialogfeld Mit **WLB-Server verbinden** eine statische IP-Adresse angeben. Verwenden Sie diese IP-Adresse als alternativer Subject Name (SAN) im Zertifikat.

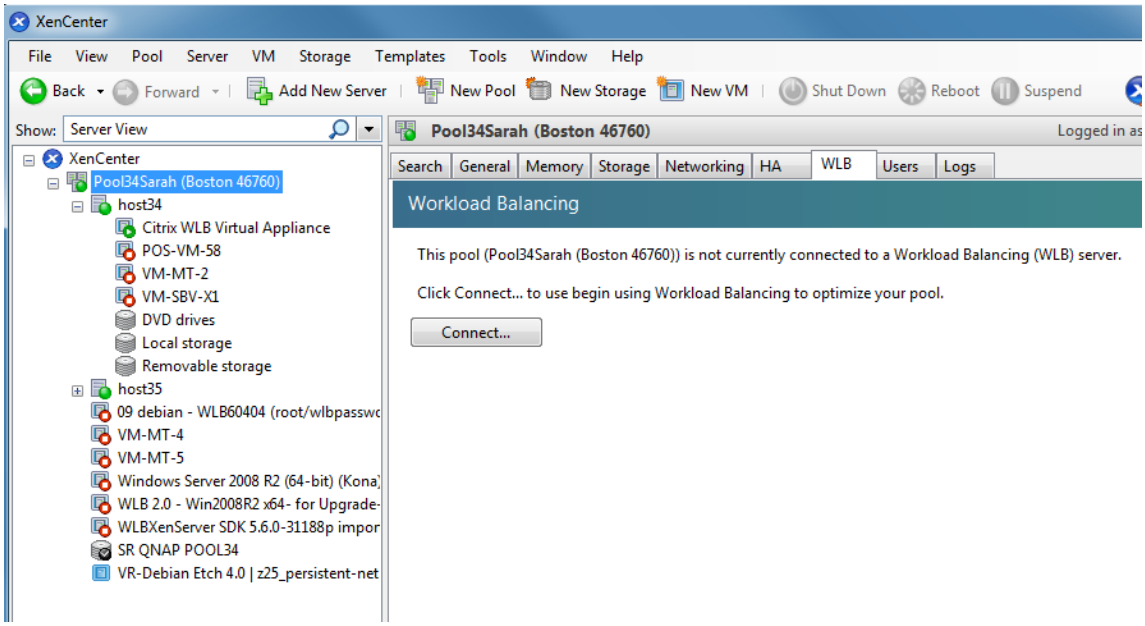
Weitere Informationen zum Konfigurieren von Zertifikaten finden Sie im Workload Balancing Administrator’s Guide.

So verbinden Sie Ihren Pool mit der virtuellen Workload-Balancing-Appliance

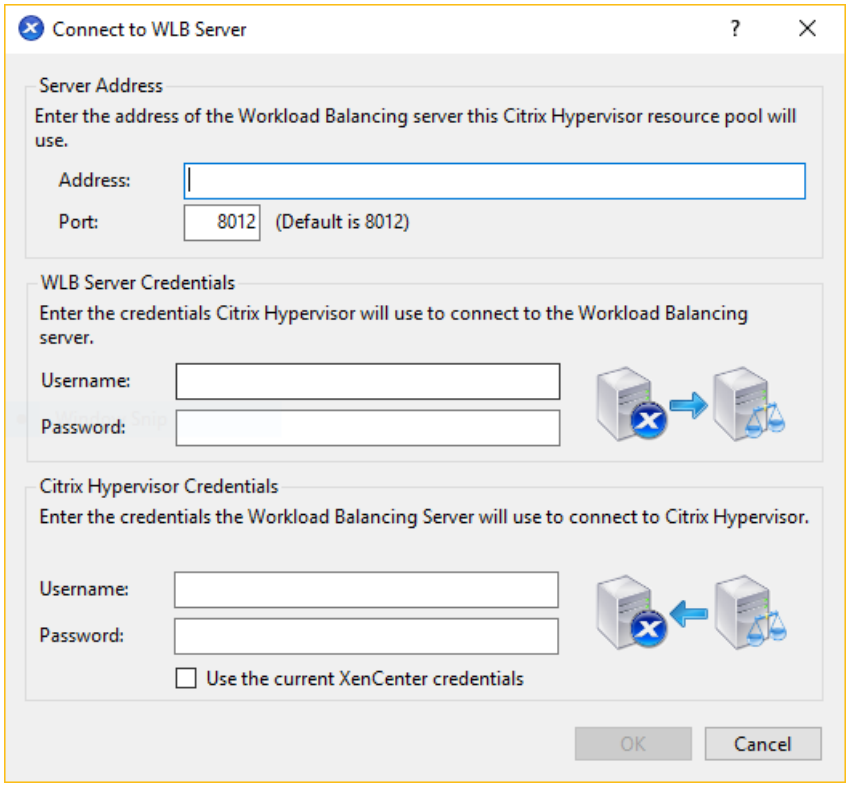
> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

1. Wählen Sie im Infrastrukturbereich von XenCenter XenCenter > `your-resource-pool`.
2. Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

   Auf der Registerkarte WLB wird die Schaltfläche Verbinden angezeigt.



3. Klicken Sie auf der Registerkarte WLB auf Verbinden. Das Dialogfeld Verbindung mit WLB-Server herstellen wird angezeigt.



4. Geben Sie im Abschnitt Serveradresse Folgendes ein:

   a) Geben Sie im Feld Adresse die IP-Adresse oder den FQDN der virtuellen Appliance „Workload Balancing“ ein. Zum Beispiel Ihre`WLB-appliance-computername.yourdomain.net`.

   > **Tipp:**
   >
   > Weitere Informationen finden Sie unter So erhalten Sie die IP-Adresse für die virtuelle WLB-Appliance.

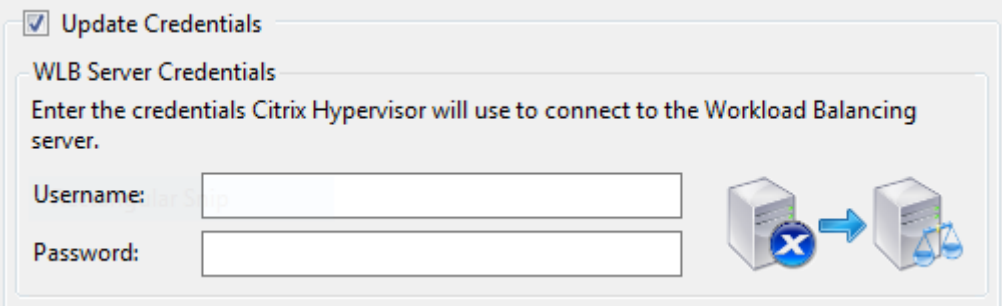
   b) (Optional) Wenn Sie den Workload Balancing-Port während der Konfiguration des Workload Balancing geändert haben, geben Sie die Portnummer in das Feld Port ein. Citrix Hypervisor verwendet diesen Port für die Kommunikation mit dem Workload Balancing.

   Standardmäßig stellt Citrix Hypervisor eine Verbindung zum Workload Balancing auf Port 8012 her.

   > **Hinweis:**
   >
   > Bearbeiten Sie die Portnummer nur, wenn Sie sie während der Konfiguration des Arbeitslastausgleichs geändert haben. Die bei der Konfiguration des Arbeitslastausgleichs, in allen Firewallregeln und im Dialogfeld Verbindung mit WLB-Server herstellen angegebene Portnummer muss übereinstimmen.

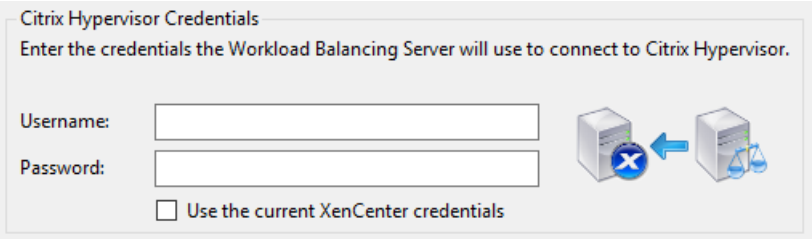
5. Geben Sie im Abschnitt Anmeldeinformationen des WLB-Servers den Benutzernamen und das

Kennwort ein, das der Citrix Hypervisor Pool (Master) für die Verbindung mit der virtuellen Workload-Balancing-Appliance verwendet.



Diese Anmeldeinformationen müssen das Konto sein, das Sie während der Konfiguration des Arbeitslastausgleichs erstellt haben. Standardmäßig ist der Benutzername für dieses Konto **wlbuser**.

6. Geben Sie im Abschnitt Citrix Hypervisor Anmeldeinformationen den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren (normalerweise das Kennwort für den Poolmaster). Der Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung mit den Hosts im Pool herzustellen.



Aktivieren Sie das Kontrollkästchen Aktuelle XenCenter Anmeldeinformationen verwenden, um die Anmeldeinformationen zu verwenden, mit denen Sie aktuell bei Citrix Hypervisor angemeldet sind. Wenn Sie diesem Konto mithilfe der RBAC-Funktion eine Rolle zugewiesen haben, stellen Sie sicher, dass die Rolle über ausreichende Berechtigungen zum Konfigurieren des Arbeitslastausgleichs verfügt. Weitere Informationen finden Sie im Abschnitt RBAC im Workload Balancing Administrator's Guide.

7. 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 für bestimmte Ressourcen zu ändern, warten Sie mindestens 60 Sekunden, bevor Sie fortfahren. Oder warten Sie, bis das XenCenter Protokoll anzeigt, dass die Erkennung abgeschlossen ist.

> **Wichtig:**
>
> Wenn Sie keine optimalen Empfehlungen erhalten, sollten Sie die Leistungsgrenzwerte wie unter beschrieben bewerten, nachdem der Workload Balancing für einen bestimmten Zeitraum aus-

> geführt wirdVerwalten. Es ist wichtig, den Workload-Balancing auf die richtigen Schwellenwerte für Ihre Umgebung festzulegen, da die Empfehlungen möglicherweise nicht angemessen sind.

So erhalten Sie die IP-Adresse für die virtuelle WLB-Appliance

1. Select im Ressourcenbereich in XenCenter die virtuelle Appliance „Workload Balancing“ aus, und wählen Sie die Registerkarte „Konsole“.
2. Melden Sie sich bei der Appliance an. Geben Sie den VM-Benutzernamen (normalerweise „root“) und das Root-Kennwort ein, das Sie beim Importieren der Appliance erstellt haben.
3. Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
1 ifconfig
```

Kopiert!
Failed!

Verwalten der virtuellen Appliance „Workload Balancing“

October 16, 2019

Dieser Artikel enthält Informationen zu den folgenden Themen:

- Verwenden von Workload Balancing zum Starten von VMs auf dem bestmöglichen Host
- Annehmen der Empfehlungen Workload-Balancing-Probleme zum Verschieben von VMs auf verschiedene Hosts

> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

Einführung in grundlegende Aufgaben

Der Workload Balancing ist eine leistungsstarke Citrix Hypervisor Komponente, die viele Funktionen zur Optimierung der Workloads in Ihrer Umgebung enthält. Zu diesen Merkmalen gehören:

- Host-Energieverwaltung
- Planen von Änderungen im Optimierungsmodus

- Berichte werden ausgeführt.

Darüber hinaus können Sie die Kriterien, die Workload Balancing verwendet, um Optimierungsempfehlungen abzugeben.

Wenn Sie jedoch zum ersten Mal mit dem Workload Balancing beginnen, gibt es zwei Hauptaufgaben, für die Sie den Workload Balancing täglich (oder regelmäßig) verwenden:

- Ermitteln des besten Hosts, auf dem eine VM ausgeführt werden soll
- Empfehlungen zur Optimierung des Arbeitslastausgleichs akzeptieren

Das Ausführen von Berichten über die Arbeitslasten in Ihrer Umgebung, wie in beschriebenGenerieren von Workload-Berichten, ist eine weitere häufig verwendete Aufgabe.

Ermitteln des besten Hosts, auf dem eine VM ausgeführt werden soll

Mit der VM-Platzierung können Sie den Host bestimmen, auf dem eine VM gestartet und ausgeführt werden soll. Diese Funktion ist nützlich, wenn Sie eine ausgeschalteten VM neu starten und eine VM auf einen anderen Host migrieren möchten. Platzierungsempfehlungen können auch in Citrix Virtual Desktops Umgebungen nützlich sein.

Empfehlungen für den Workload Balancing akzeptieren

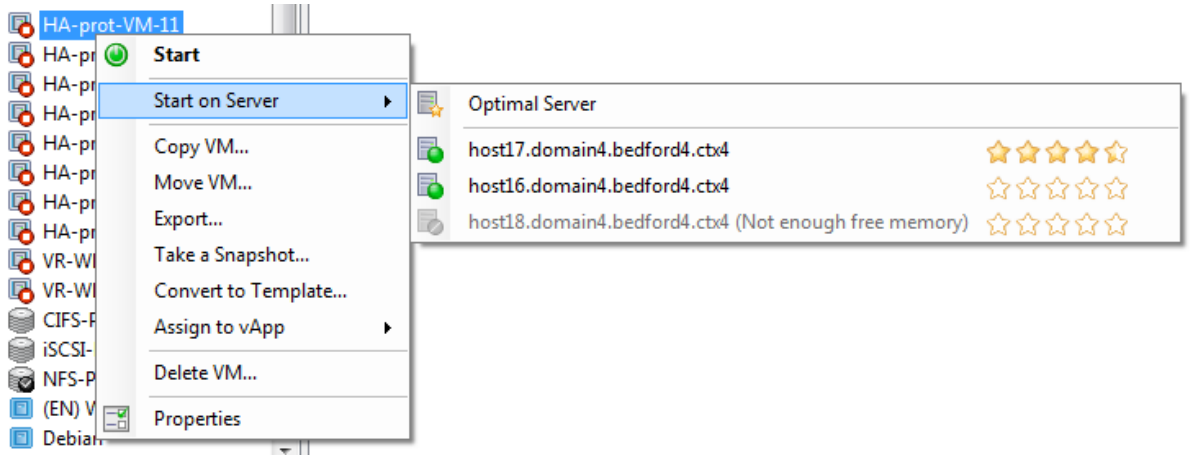
Nachdem der Workload Balancing für eine Weile ausgeführt wird, werden Empfehlungen zu Möglichkeiten zur Verbesserung der Umgebung abgegeben. Wenn Ihr Ziel beispielsweise darin besteht, die VM-Dichte auf Hosts zu verbessern, empfiehlt der Workload Balancing möglicherweise, VMs auf einem Host zu konsolidieren. Wenn Sie nicht im automatisierten Modus ausgeführt werden, können Sie diese Empfehlung akzeptieren und anwenden oder sie ignorieren.

Beide Aufgaben und deren Ausführung in XenCenter werden in den folgenden Abschnitten ausführlicher erläutert.

> **Wichtig:**
>
> Wenn Sie keine optimalen Platzierungsempfehlungen erhalten, sollten Sie die Leistungsschwellenwerte bewerten, nachdem der Workload Balancing für einen bestimmten Zeitraum ausgeführt wurde. Diese Auswertung wird unter beschriebenVerstehen, wann Workload Balancing Empfehlungen ausgibt. Es ist wichtig, den Workload-Balancing auf die richtigen Schwellenwerte für Ihre Umgebung festzulegen, da die Empfehlungen möglicherweise nicht angemessen sind.

Wählen Sie den besten Host für eine VM

Wenn Sie den Workload-Balancing aktiviert haben und eine Offline-VM neu starten, empfiehlt XenCenter die optimalen Pool-Mitglieder zum Starten der VM. Die Empfehlungen werden auch als Sternebewertungen bezeichnet, da Sterne verwendet werden, um den besten Gastgeber anzugeben.



Der Begriff *optimal* gibt den physischen Server an, der am besten geeignet ist, um Ihre Arbeitslast zu hosten. Es gibt mehrere Faktoren, die Workload Balancing verwendet, um zu bestimmen, welcher Host für eine 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 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 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 Workload Balancing VMs auf Hosts, auf denen bereits VMs ausgeführt werden. Dieser Ansatz stellt sicher, dass VMs auf so wenigen Hosts wie möglich ausgeführt werden.
- **Die Menge und Art der Ressourcen, die die VM benötigt**. Nachdem WLB eine VM für eine Weile überwacht hat, verwendet es die VM-Metriken, um Platzierungsempfehlungen entsprechend der Art der Ressourcen abzugeben, die die VM benötigt. Beispielsweise kann der Workload-Balancing einen Host mit weniger verfügbarer CPU, aber mehr verfügbaren Arbeitsspeicher auswählen, wenn dies der VM entspricht.

Wenn der Workload Balancing aktiviert ist, bietet XenCenter Bewertungen, um die optimalen Hosts für den Start einer VM anzuzeigen. Diese Bewertungen werden auch angeboten:

- Wenn Sie die VM starten möchten, wenn sie ausgeschaltet ist

- Wenn Sie die VM starten möchten, wenn sie angehalten wird
- Wenn Sie die VM auf einen anderen Host migrieren möchten (Migrations- 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 geben den niedrigsten (am wenigsten optimalen) Server an. Wenn Sie eine VM nicht auf einen Host starten oder migrieren können, wird der Hostname im Menübefehl für eine Platzierungsfunktion ausgegraut. Der Grund, warum die VM nicht akzeptiert werden kann, wird daneben angezeigt.

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 eine der Platzierungsfunktionen, um den Host mit den meisten Sternen daneben auszuwählen.

So starten Sie eine virtuelle Maschine auf dem optimalen Server

1. Wählen Sie im Ressourcenbereich von XenCenter die VM aus, die Sie starten möchten.
2. Wählen Sie im Menü VM die Option Start on Server aus, und wählen Sie dann eine der folgenden Optionen aus:
    - **Optimaler Server**. Der optimale Server ist der physische Host, der am besten für die Ressourcenanforderungen der VM geeignet ist, die Sie starten. Der Workload-Balancing bestimmt den optimalen Server basierend auf den historischen Datensätzen der Performance-Metriken und Ihrer Platzierungsstrategie. Der optimale Server ist der Server mit den meisten Sternen.
    - **Einer der Server mit Sternbewertungen**, die unter dem Befehl Optimal Server aufgeführt sind. Fünf Sterne geben den am meisten empfohlenen (optimalen) Server an und fünf leere Sterne geben den am wenigsten empfohlenen Server an.

> **Tipp:**
>
> Sie können auch auf Server starten auswählen, indem Sie im Ressourcenbereich mit der rechten Maustaste auf die VM klicken, die Sie starten möchten.

So setzen Sie eine virtuelle Maschine auf dem optimalen Server fort

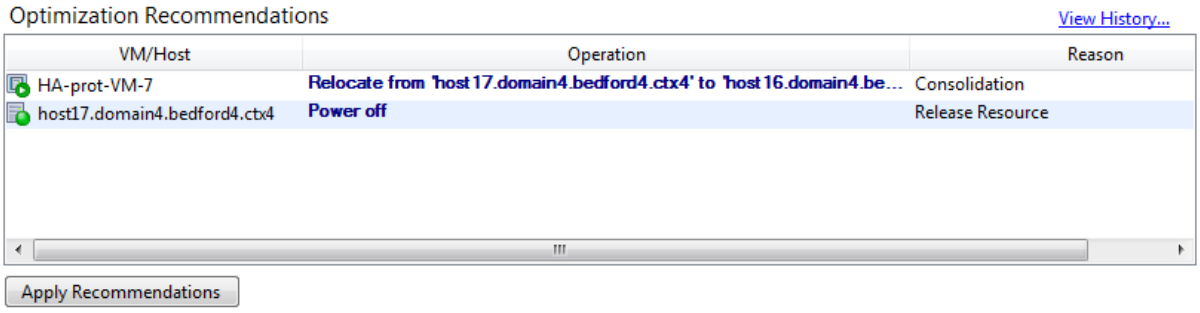
1. Wählen Sie im Bereich Ressourcen von XenCenter die angehaltene VM aus, die Sie fortsetzen möchten.
2. Wählen Sie im Menü „VM“ die Option „Auf Server fortsetzen“, und wählen Sie dann eine der folgenden Optionen aus:

- **Optimaler Server**. Der optimale Server ist der physische Host, der am besten für die Ressourcenanforderungen der VM geeignet ist, die Sie starten. Der Workload-Balancing bestimmt den optimalen Server basierend auf den historischen Datensätzen der Performance-Metriken und Ihrer Platzierungsstrategie. Der optimale Server ist der Server mit den meisten Sternen.
- **Einer der Server mit Sternbewertungen**, die unter dem Befehl Optimal Server aufgeführt sind. Fünf Sterne geben den am meisten empfohlenen (optimalen) Server an und fünf leere Sterne geben den am wenigsten empfohlenen Server an.

> **Tipp:**
>
> Sie können auch auf Server fortsetzen auswählen, indem Sie im Ressourcenbereich mit der rechten Maustaste auf die angehaltene VM klicken.

Optimierungsempfehlungen akzeptieren

Workload Balancing enthält Empfehlungen zur Migration von VMs zur Optimierung Ihrer Umgebung. Optimierungsempfehlungen werden auf der Registerkarte „WLB-Optimierung“ in XenCenter angezeigt.



Optimierungsempfehlungen basieren auf:

- Die von Ihnen gewählte Platzierungsstrategie (d. h. der Optimierungsmodus).
- Leistungsmetriken für Ressourcen wie CPU, Arbeitsspeicher, Netzwerk und Festplattenauslastung eines physischen Hosts.
- Die Rolle des Hosts im Ressourcenpool. Bei Platzierungsempfehlungen berücksichtigt der Workload Balancing den Poolmaster für die VM-Platzierung nur, wenn kein anderer Host die Arbeitslast akzeptieren kann. Wenn ein Pool im Modus „Maximale Dichte“ arbeitet, berücksichtigt der Workload Balancing den Pool-Master als zuletzt, wenn er die Reihenfolge zum Füllen von Hosts mit VMs bestimmt.

Optimierungsempfehlungen zeigen die folgenden Informationen an:

- Der Name der VM, die Workload Balancing empfiehlt, das Verlagern von

- Der Host, auf dem sich die VM derzeit befindet
- Der Host-Workload-Balancing empfiehlt als neuen Speicherort.

In den Optimierungsempfehlungen wird auch der Grund angezeigt, warum Workload Balancing das Verschieben der VM empfiehlt. In der Empfehlung wird beispielsweise „CPU“ angezeigt, um die CPU-Auslastung zu verbessern. Wenn die Energieverwaltung „Workload Balancing“ aktiviert ist, zeigt Workload Balancing auch Optimierungsempfehlungen für Hosts an, die das Ein- oder Ausschalten empfiehlt. Insbesondere sind diese Empfehlungen für Konsolidierungen.

Nachdem Sie auf Empfehlungen anwenden geklickt haben, führt Citrix Hypervisor alle Vorgänge aus, die in der Liste Optimierungsempfehlungen aufgeführt sind.

> **Tipp:**
>
> Finden Sie den Optimierungsmodus für einen Pool mithilfe von XenCenter zum Auswählen des Pools heraus. Suchen Sie im Abschnitt Konfiguration der Registerkarte WLB nach den Informationen.

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 für VMs im ausgewählten Ressourcenpool empfohlene Optimierungen vorhanden sind, werden diese im Abschnitt Optimierungsempfehlungen der Registerkarte WLB angezeigt.
3. Um die Empfehlungen zu akzeptieren, klicken Sie auf Empfehlungen anwenden. Citrix Hypervisor beginnt mit der Ausführung aller Vorgänge, die in der Spalte „Vorgänge“ 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 anzeigen können.

Verstehen von WLB-Empfehlungen unter hoher Verfügbarkeit

Wenn Workload Balancing und Citrix Hypervisor High Availability im selben Pool aktiviert sind, ist es hilfreich zu verstehen, wie die beiden Features interagieren. Der Workload-Balancing ist so konzipiert, dass die hohe Verfügbarkeit nicht beeinträchtigt wird. Wenn ein Konflikt zwischen einer Arbeitslastausgleichsempfehlung und einer Einstellung für hohe Verfügbarkeit besteht, hat die Einstellung Hochverfügbarkeit immer Vorrang. In der Praxis bedeutet diese Priorität, dass:

- 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 Anzahl hinausgehen, die im Dialogfeld „ **HA konfigurieren** “ im Feld „Fehler zulässig“ angegeben ist.
  - Der Workload-Balancing gibt jedoch immer noch Empfehlungen, um mehr Hosts auszuschalten als die Anzahl der zu tolerierenden Hostfehler. (Der Workload-Balancing empfiehlt beispielsweise weiterhin, zwei Hosts auszuschalten, wenn Hochverfügbarkeit nur so konfiguriert ist, dass ein Hostfehler toleriert wird.) Wenn Sie jedoch versuchen, die Empfehlung anzuwenden, zeigt XenCenter möglicherweise eine Fehlermeldung an, die besagt, dass die hohe Verfügbarkeit nicht mehr gewährleistet ist.
  - Wenn der Workload Balancing im automatisierten Modus ausgeführt wird und die Energieverwaltung aktiviert ist, werden Empfehlungen ignoriert, die die Anzahl tolerierter Hostfehler überschreiten. In diesem Fall zeigt das Arbeitslastausgleichsprotokoll eine Meldung an, dass die Energieverwaltungsempfehlung nicht angewendet wurde, da Hochverfügbarkeit aktiviert ist.

Generieren von Workload-Berichten

Dieser Abschnitt enthält Informationen zur Verwendung der Komponente „Workload Balancing“ zum Generieren von Berichten über Ihre Umgebung, einschließlich Berichten über Hosts und VMs. Insbesondere enthält dieser Abschnitt Informationen zu den folgenden Themen:

- So erstellen Sie Berichte
- Welche Workload-Berichte sind verfügbar

> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie imLizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

Übersicht über Workload-Berichte

Die Workload-Balancing-Berichte können Sie bei der Kapazitätsplanung, bei der Ermittlung des Zustands des virtuellen Servers und bei der Bewertung der Wirksamkeit der konfigurierten Schwellenwerte unterstützen.

Mit dem Workload Balancing können Sie Berichte über drei Objekttypen erstellen: physische Hosts, Ressourcenpools und VMs. Auf hoher Ebene bietet der Workload Balancing zwei Arten von Berichten:

- Historische Berichte, die Informationen nach Datum anzeigen
- „Roll up“ -Style-Berichte, die einen zusammenfassenden Überblick über einen Bereich bieten

Der Workload-Balancing stellt einige Berichte für Überwachungszwecke bereit, sodass Sie beispielsweise bestimmen können, wie oft eine VM verschoben wurde.

Sie können den Pool-Integritätsbericht verwenden, um zu bewerten, wie effektiv Ihre Optimierungsschwellenwerte sind. Während der Workload Balancing Standardschwelleneinstellungen enthält, müssen Sie diese Standardwerte möglicherweise anpassen, damit sie einen Wert in Ihrer Umgebung bereitstellen. Wenn die Optimierungsschwellenwerte nicht auf die richtige Ebene für Ihre Umgebung angepasst sind, sind die Empfehlungen für den Arbeitslastausgleich möglicherweise nicht für Ihre Umgebung geeignet.

Um einen Workload Balancing-Bericht zu generieren, muss der Pool den Workload Balancing ausführen. Idealerweise führt der Pool den Workload-Balancing für einige Stunden oder lang genug aus, um die Daten zu generieren, die in den Berichten angezeigt werden sollen.

Generieren eines Workload Balancing-Berichts

1. Wählen Sie in XenCenter im Menü Pool die Option Workload-Berichte anzeigen aus.

   > **Tipp:**
   >
   > Sie können den Bildschirm „Workload-Berichte“ auch auf der Registerkarte „WLB“ anzeigen, indem Sie auf die Schaltfläche „Berichte“ klicken.

2. Wählen Sie im Fenster „Workload-Berichte“ einen Bericht aus dem Bereich „Berichte“ aus.
3. Select das Startdatum und das Enddatum für die Auswertungsperiode. Abhängig vom ausgewählten Bericht müssen Sie möglicherweise einen Host im Listenfeld Host angeben.
4. Klicken Sie auf Bericht ausführen. Der Bericht wird im Berichtsfenster angezeigt. Hinweise zur Bedeutung der Berichte finden Sie unterGlossar „Workload Balancing“.

Navigieren in einem Workload-Balancing-Bericht

Nach dem Generieren eines Berichts können Sie mithilfe der Symbolleistenschaltflächen im Bericht navigieren und bestimmte Aufgaben ausführen. Um den Namen einer Symbolleistenschaltfläche anzuzeigen, halten Sie den Mauszeiger über das Symbolleistensymbol an.

Symbolleistenschaltflächen	Beschreibung
	Mit**der Dokumentzuordnung** können Sie eine Dokumentzuordnung anzeigen, mit der Sie durch lange Berichte navigieren können.

Symbolleistenschaltflächen	Beschreibung
	Mit**Seite Vorwärts/Zurück** können Sie im Bericht eine Seite vorwärts oder zurück verschieben.
	**Zurück zum übergeordneten Bericht** ermöglicht es Ihnen, beim Arbeiten mit Drill-Through-Berichten zum übergeordneten Bericht zurückzukehren. **Hinweis:** Diese Schaltfläche ist nur in Drill-Through-Berichten verfügbar, z. B. im Pool-Integritätsbericht.
	**Rendering beenden** bricht die Berichtsgenerierung ab.
	**Drucken** ermöglicht es Ihnen, einen Bericht zu drucken und allgemeine Druckoptionen festzulegen. Zu diesen Optionen gehören: der Drucker, die Anzahl der Seiten und die Anzahl der Kopien.
	Mit dem**Drucklayout** können Sie eine Vorschau des Berichts anzeigen, bevor Sie ihn drucken. Um das Drucklayout zu beenden, klicken Sie erneut auf die Schaltfläche Drucklayout.
	Mit der**Seite einrichten** können Sie Druckoptionen wie Papierformat, Seitenausrichtung und Seitenränder festlegen.
	Mit**Export** können Sie den Bericht als Acrobat-Datei (.PDF) oder als Excel-Datei mit der Erweiterung.XLS exportieren.
	**Suchen** ermöglicht es Ihnen, in einem Bericht nach einem Wort zu suchen, z. B. dem Namen einer VM.

Drucken eines Arbeitslastausgleichsberichts

Bevor Sie einen Bericht drucken können, müssen Sie ihn zuerst generieren.

1. (Optional) Zeigen Sie eine Vorschau des gedruckten Dokuments an, indem Sie auf die folgende Schaltfläche „Drucklayout“ klicken:
2. (Optional) Ändern Sie das Papierformat und die Quelle, die Seitenausrichtung oder die Seitenränder, indem Sie auf die folgende Schaltfläche „Seite einrichten“ klicken:
3. Klicken Sie auf die folgende Schaltfläche Drucken:

Exportieren eines Arbeitslastausgleichsberichts

Sie können einen Bericht in Microsoft Excel oder Adobe Acrobat (PDF) Format exportieren.

1. Klicken Sie nach dem Generieren des Berichts auf die folgende Schaltfläche „Exportieren“:
2. Select eines der folgenden Elemente aus dem Menü „Exportieren“:
   - Excel
   - Acrobat-Datei (PDF)

> **Hinweis:**
>
> Die Daten, die zwischen Berichtsexportformaten angezeigt werden, sind möglicherweise inkonsistent, abhängig vom ausgewählten Exportformat. In Excel exportierte Berichte enthalten alle für Berichte verfügbaren Daten, einschließlich „Drilldown“ -Daten. Berichte, die als PDF exportiert und in XenCenter angezeigt werden, enthalten nur die Daten, die Sie beim Erstellen des Berichts ausgewählt haben.

Glossar „Workload Balancing“

Dieser Abschnitt enthält Informationen zu den folgenden Workload Balancing-Berichten:

Analyse der Auslastungsauslastung

Mit der Auswertung „Analyse der Ausgleichsbelastung“ („Rückbelastungsbericht“) können Sie bestimmen, wie viel Ressource eine bestimmte Abteilung in Ihrer Organisation verwendet hat. Insbesondere enthält der Bericht Informationen zu allen VMs in Ihrem Pool, einschließlich ihrer Verfügbarkeit und Ressourcenauslastung. Da dieser Bericht die Betriebszeit der virtuellen Maschine anzeigt, kann er Ihnen dabei helfen, die Einhaltung und Verfügbarkeit von Service Level Agreements zu demonstrieren.

Der Rückbelastungsbericht kann Ihnen dabei helfen, eine einfache Rückbelastungslösung zu implementieren und die Abrechnung zu erleichtern. Um Kunden für eine bestimmte Ressource in Rechnung zu stellen, erstellen Sie den Bericht, speichern Sie ihn als Excel, und bearbeiten Sie die Tabelle so, dass der Preis pro Einheit berücksichtigt wird. Alternativ können Sie die Excel-Daten in Ihr Abrechnungssystem importieren.

Wenn Sie interne oder externe Kunden für die VM-Nutzung in Rechnung stellen möchten, sollten Sie Abteilungs- oder Kundennamen in Ihre VM-Namenskonventionen integrieren. Diese Vorgehensweise erleichtert das Lesen von Rückbuchungsberichten.

Die Ressourcenberichterstattung im Rückbelastungsbericht basiert manchmal auf der Zuordnung physischer Ressourcen zu einzelnen VMs.

Die durchschnittlichen Speicherdaten in diesem Bericht basieren auf der aktuell der VM zugewiesenen Speichermenge. Mit Citrix Hypervisor können Sie über eine feste Speicherzuweisung oder eine automatisch anpassende Speicherzuweisung verfügen (Dynamic Memory Control).

Der Rückbelastungsbericht enthält die folgenden Datenspalten:

- **VM-Name**. Der Name der VM, auf die die Daten in den Spalten in dieser Zeile angewendet werden.
- **VM-Betriebszeit**. Die Anzahl der Minuten, in denen die VM eingeschaltet wurde (oder, genauer gesagt, mit einem grünen Symbol in XenCenter angezeigt wird).
- **vCPU-Zuweisung**. Die Anzahl der virtuellen CPUs, die auf der VM konfiguriert sind. Jede virtuelle CPU erhält einen gleichen Anteil an den physischen CPUs auf dem Host. Betrachten Sie beispielsweise den Fall, in dem Sie acht virtuelle CPUs auf einem Host konfiguriert haben, der zwei physische CPUs enthält. Wenn die **vCPU-Zuordnungsspalte** „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 Arbeitslast dar, die virtuelle CPU verarbeitet hat. Wenn Sie beispielsweise einer VM eine vCPU zuweisen und die PCPU auf dem Host 2,4 GHz beträgt, wird der VM 0,3 GHz zugewiesen. Wenn die **minimale CPU-Auslastung** für die VM 20% betrug, betrug die niedrigste Auslastung der CPU des physischen Hosts während des Berichtszeitraums 60 MHz.
- **Maximale CPU-Auslastung (%)**. Der höchste Prozentsatz der virtuellen CPU-Kapazität der virtuellen VM, den die VM während des Berichtszeitraums belegt 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 der gemeldeten Zeit 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 (%)**. Der durchschnittliche Betrag (ausgedrückt als Prozentsatz) der virtuellen CPU-Kapazität der virtuellen Maschine, die während des Berichtszeitraums 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 zurzeit der VM zum Zeitpunkt der Ausführung des Berichts zugewiesen ist. Dieser Festplattenspeicher ist häufig, sofern Sie ihn nicht geändert haben, der Speicherplatz, den Sie der VM bei der Erstellung zugewiesen haben.
- **Zuweisung virtueller Netzwerkkarten**. Die Anzahl der virtuellen Schnittstellen (VIFs), die der VM zugewiesen sind.
- **Aktueller minimaler dynamischer Arbeitsspeicher (MB)**.
  - **Feste Speicherzuweisung**. Wenn Sie einer VM eine feste Menge an Arbeitsspeicher zugewiesen haben (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).
  - **Dynamische Speicherzuweisung**. Wenn Sie Citrix Hypervisor 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 maximaler Speicher aufweist, wird in der Spalte **Aktueller minimaler dynamischer Speicher (MB)** 1.024 MB angezeigt.
- **Aktueller maximaler dynamischer Speicher (MB)**.
  - **Dynamische Speicherzuweisung**. Wenn Citrix Hypervisor den Arbeitsspeicher einer virtuellen Maschine automatisch basierend auf einem Bereich anpasst, wird die im 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 **Aktueller maximaler dynamischer Speicher (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 an, wie viel Speicher Citrix Hypervisor 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 virtuellen Maschine 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 Citrix Hypervisor der VM im Berichtszeitraum zugewiesen ist.
  - **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 virtuellen Maschine 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 des Zeitraums wider.

- **Durchschnittliche Netzwerklesevorgänge (BPS)**. Die durchschnittliche Datenmenge (in Bits pro Sekunde), die die VM während des Berichtszeitraums empfangen hat.
- **Durchschnittliche Netzwerkschreibvorgänge (BPS)**. Die durchschnittliche Datenmenge (in Bits pro Sekunde), die die VM während des Berichtszeitraums gesendet hat.
- **Durchschnittliche Netzwerkauslastung (BPS)**. Die kombinierte Summe (in Bits pro Sekunde) der durchschnittlichen Netzwerklesevorgänge und des durchschnittlichen Netzwerkschreibens. Wenn eine VM im Durchschnitt 1.027 Bit/s sendet und im Berichtszeitraum

durchschnittlich 23.831 Bit/s empfängt, entspricht die durchschnittliche Netzwerkauslastung der Gesamtsumme dieser Werte: 24.858 Bit/s.

- **Gesamte Netzwerkauslastung (BPS)**. Die Summe aller Lese- und Schreibtransaktionen im Netzwerk in Bits pro Sekunde im Berichtszeitraum.

Host-Integritätsverlauf

Dieser Bericht zeigt die Leistung von Ressourcen (CPU, Arbeitsspeicher, Netzwerk-Lesevorgänge und Netzwerk-Schreibvorgänge) auf einem bestimmten Host in Bezug auf Schwellenwerte an.

Die farbigen Linien (rot, grün, gelb) stellen Ihre Schwellenwerte dar. Sie können diesen Bericht zusammen mit dem Pool-Integritätsbericht für einen Host verwenden, um zu bestimmen, wie sich die Leistung des Hosts auf den Gesamtzustand des Pools auswirken kann. Wenn Sie die Performance-Schwellenwerte bearbeiten, können Sie diesen Bericht verwenden, um Einblicke in die Host-Performance zu erhalten.

Sie können die Ressourcenauslastung als Tages- oder Stundendurchschnitt anzeigen. Im Stundendurchschnitt können Sie die geschäftigsten Stunden des Tages, gemittelt, für den Zeitraum anzeigen.

Um Berichtsdaten anzuzeigen, die nach Stunden gruppiert sind, erweitern **Sie unter **Host-Integritätsverlauf** Klicken Sie auf, 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 Auslastungsdurchschnitt für diese Stunde für alle Tage im Zeitraum. In einem Bericht für den 1. Mai 2009 bis zum 15. Mai 2009 stellt der Datenpunkt Durchschnittliche CPU-Auslastung die Ressourcenauslastung aller 15 Tage bei 12:00 Stunden dar. Diese Informationen werden als Durchschnitt kombiniert. Wenn die CPU-Auslastung am 1. Mai 82% um 12.00 Uhr, am 2. Mai 88% um 12.00 Uhr und an allen anderen Tagen 75% betrug, beträgt der angezeigte Durchschnitt für 12.00 Uhr 76.3%.

> **Hinweis:**
>
> Der Workload Balancing glättet Spikes und Peaks, sodass die Daten nicht künstlich hoch erscheinen.

Performance-Historie der Pooloptimierung

Der Optimierungsleistungsbericht zeigt Optimierungsereignisse für die durchschnittliche Ressourcenauslastung dieses Pools an. Bei diesen Ereignissen handelt es sich um Instanzen, wenn Sie einen Ressourcenpool optimiert haben. Insbesondere wird die Ressourcenauslastung für CPU, Arbeitsspeicher, Netzwerk-Lesevorgänge und Netzwerkschreibvorgänge angezeigt.

Die gestrichelte Linie stellt die durchschnittliche Nutzung im Pool über den ausgewählten Zeitraum von Tagen dar. Ein blauer Balken zeigt den Tag an, an dem Sie den Pool optimiert haben.

Dieser Bericht kann Ihnen helfen zu ermitteln, 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 Ressourcenverwendung vor der empfohlenen Optimierung von Workload Balancing).

Dieser Bericht zeigt den durchschnittlichen Ressourcenverbrauch für den Tag an. Die Spitzenauslastung wird nicht angezeigt, z. B. wenn das System gestresst ist. Sie können diesen Bericht auch verwenden, um zu sehen, wie ein Ressourcenpool funktioniert, wenn der Workload Balancing keine Optimierungsempfehlungen abgibt.

Im Allgemeinen sinkt die Ressourcennutzung nach einem Optimierungsereignis 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 während des angegebenen Zeitraums neue VMs hinzugefügt oder entfernt haben.

Pool-Audit-Trail

Dieser Bericht zeigt den Inhalt des Citrix Hypervisor Überwachungsprotokolls an. Das Überwachungsprotokoll ist eine Citrix Hypervisor Funktion, mit der Versuche protokolliert werden, nicht autorisierte Aktionen auszuführen und autorisierte Aktionen auszuwählen. Zu diesen Aktionen gehören:

- Import und Export
- Host- und Pool-Backups
- Zugriff auf die Gast- und Hostkonsole.

Der Bericht enthält aussagekräftigere Informationen, wenn Sie Citrix Hypervisor Administratoren über die RBAC-Funktion eigene Benutzerkonten mit unterschiedlichen Rollen bereitstellen.

> **Wichtig:**
>
> Um den Überwachungsprotokollbericht auszuführen, müssen Sie die Überwachungsprotokollierung aktivieren. Standardmäßig ist das Überwachungsprotokoll in der virtuellen Appliance „Workload Balancing“ immer aktiviert.

Mit der erweiterten Pool-Audit-Trail-Funktion können Sie die Granularität des Überwachungsprotokollberichts festlegen. Sie können die Audit-Trail-Protokolle auch nach bestimmten Benutzern, Objekten und nach Zeit durchsuchen und filtern. Die Pool-Audit-Trail-Granularität ist standardmäßig auf Minimum festgelegt. Diese Option erfasst eine begrenzte Datenmenge für bestimmte Benutzer und Objekttypen. Sie können die Einstellung jederzeit auf der Grundlage der Detailgenauigkeit ändern, die Sie in Ihrem Bericht benötigen. Legen Sie beispielsweise die Granularität auf Mittel für einen benutzerfreundlichen Bericht des Überwachungsprotokolls fest. Wenn Sie einen detaillierten Bericht benötigen, setzen Sie die Option auf Maximum.

Inhalt des Berichts

Der Bericht Pool-Audit-Trail enthält Folgendes:

- Zeit. Der Zeitpunkt, zu dem Citrix Hypervisor die Aktion des Benutzers aufgezeichnet hat.
- Benutzername. Der Name der Person, die die Sitzung erstellt hat, in der die Aktion ausgeführt wurde. Manchmal kann dieser Wert die Benutzer-ID sein
- Ereignisobjekt. Das Objekt, das Gegenstand der Aktion war (z. B. eine VM).
- Ereignisaktion. Die Aktion, die aufgetreten ist. Definitionen dieser Aktionen finden Sie unter Überwachungsprotokoll-Ereignisnamen.
- Zugang. Gibt an, ob der Benutzer die Berechtigung zum Ausführen der Aktion hatte.
- 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 oder nicht).

Ereignisnamen des Überwachungsprotokolls

Der Überwachungsprotokollbericht protokolliert Citrix Hypervisor Ereignisse, Ereignisobjekte und Aktionen, einschließlich Import/Export, Host- und Pool-Backups sowie Zugriff auf die Gast- und Hostkonsole. In der folgenden Tabelle werden einige der typischen Ereignisse beschrieben, die häufig im Citrix Hypervisor Audit-Log und Pool-Audit-Trail-Bericht angezeigt werden. Die Tabelle gibt auch die Granularität dieser Ereignisse an.

Im Pool-Audit-Trail-Bericht gelten die in der`Event Action` Spalte aufgeführten Ereignisse für einen Pool, eine VM oder einen Host. Informationen zum Bestimmen, für welche Ereignisse gelten, finden Sie in den`Event Object` Spalten`Object Name` und im Bericht. Weitere Ereignisdefinitionen finden Sie im Abschnitt Ereignisse der Citrix Hypervisor Management-API.

Pool-Audit-Trail Granularität	Ereignisaktion	Benutzeraktion
Minimum	`pool.join`	Der Host wird angewiesen, einem neuen Pool beizutreten
Minimum	`pool.join_force`	Der Host wird angewiesen (gezwungen), einem Pool beizutreten
Mittel	`SR.destroy`	Speicher-Repository zerstört
Mittel	`SR.create`	Speicher-Repository erstellt

Pool-Audit-Trail Granularität	Ereignisaktion	Benutzeraktion
Mittel	VDI.snapshot	Erstellte einen schreibgeschützten Snapshot des VDI und gab einen Verweis auf den Snapshot zurück
Mittel	VDI.clone	Nah eine exakte Kopie des VDI und gab einen Verweis auf die neue Festplatte zurück
Mittel	VIF.plug	Hot-Plug-fähige angegebene VIF, dynamische Anbindung an die laufende VM
Mittel	VIF.unplug	Hot-Unplugged des angegebenen VIF, dynamisches Trennen von der ausgeführten VM
Maximal	auth.get_subject_identifier	Der externe Verzeichnisdienst wurde abgefragt, um den Betreff-Bezeichner als Zeichenfolge aus dem für Menschen lesbaren Betreffnamen zu erhalten.
Maximal	task.cancel	Anforderung, dass eine Aufgabe abgebrochen wird
Maximal	VBD.insert	Neue Medien in das Gerät eingefügt
Maximal	VIF.get_by_uuid	Einen Verweis auf die VIF-Instanz mit der angegebenen UUID erhalten
Maximal	VDI.get_sharable	Ermittelt das gemeinsam nutzbare Feld des angegebenen VDI
Maximal	SR.get_all	Gibt eine Liste aller dem System bekannten SRs zurück

Pool-Audit-Trail Granularität	Ereignisaktion	Benutzeraktion
Maximal	`pool.create_new_blob`	Erstellt einen Platzhalter für eine benannte Binärdatei, die diesem Pool zugeordnet ist
Maximal	`host.send_debug_keys`	Die angegebene Zeichenfolge als Debugging-Schlüssel in Xen injiziert
Maximal	`VM.get_boot_record`	Es wurde ein Datensatz zurückgegeben, der den dynamischen Status der VMs beschreibt, initialisiert, wenn die VM gestartet wird, und aktualisiert, um Änderungen der Laufzeitkonfiguration wiederzugeben, z. B. CPU-Hotplug

Pool Gesundheit

Der Pool-Integritätsbericht zeigt den Prozentsatz der Zeit an, die ein Ressourcenpool und seine Hosts in vier verschiedenen Schwellenbereichen verbracht hat: Kritisch, Hoch, Mittel und Niedrig. Sie können den Pool-Integritätsbericht 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 gibt der blaue Abschnitt im Kreisdiagramm 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 Ressourcenauslastung grün ist, passt WLB möglicherweise nicht an die maximale Anzahl von VMs, die auf diesem Host oder Pool möglich ist. Wenn ja, passen Sie die Leistungsschwellenwerte an, bis der größte Teil der Ressourcenauslastung in den Schwellenbereich Durchschnittlich (blau) fällt.
- Die Ressourcenauslastung im Durchschnitt kritischer Schwellenwert in Prozent (rot) gibt an, wie lange die durchschnittliche Ressourcenauslastung den kritischen Schwellenwert erreicht oder

überschritten hat.

Wenn Sie für die Ressourcenverwendung eines Hosts auf ein Kreisdiagramm doppelklicken, zeigt XenCenter den Hostintegritätsbericht für diese Ressource auf diesem Host an. Wenn Sie auf der Symbolleiste auf **Zurück zu übergeordnetem Bericht** klicken, gelangen Sie zum Bericht über den Pool-Integritätsverlauf.

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 Standardschwelleneinstellungen bereitstellt, sind diese Standardwerte 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 Arbeitslastausgleichs möglicherweise nicht geeignet. Weitere Informationen finden Sie unter *Ändern der kritischen Schwellenwerte*.

Pool-Gesundheitsverlauf

Dieser Bericht stellt ein Liniendiagramm zur Ressourcenauslastung auf allen physischen Hosts in einem Pool im Laufe der Zeit bereit. Sie können den Trend der Ressourcenauslastung erkennen, wenn sie im Verhältnis zu Ihren Schwellenwerten (kritisch, hoch, mittel und niedrig) tendenziell zunimmt. Sie können die Effektivität Ihrer Performance-Schwellenwerte bewerten, indem Sie Trends der Datenpunkte in diesem Bericht überwachen.

Der Workload-Balancing extrapoliert die Schwellenwerte von den Werten, die Sie für die kritischen Schwellenwerte festgelegt haben, wenn Sie den Pool mit dem Workload-Balancing verbunden haben. Obwohl der Bericht „Poolintegrität“ ähnlich ist, zeigt der Bericht „Poolintegritätsverlauf“ die durchschnittliche Auslastung für eine Ressource an einem bestimmten Datum an. Anstelle der gesamten Zeit, die die Ressource in einem Schwellenwert ausgegeben wird.

Mit Ausnahme des Graphen „Durchschnittlicher freier Speicher“ durchschnittlich die Datenpunkte niemals über der kritischen Schwellenlinie (rot) liegen. Für das Diagramm Durchschnittlicher freier Speicher werden die Datenpunkte niemals *unter* der kritischen Schwellenlinie (die sich am unteren Rand des Diagramms befindet) Durchschnitt. Da in diesem Diagramm *freien* Speicher angezeigt wird, ist der kritische Schwellenwert im Gegensatz zu den anderen Ressourcen ein geringer Wert.

Einige Punkte zur Interpretation dieses Berichts:

- Wenn sich die Zeile Durchschnittliche Nutzung im Diagramm der mittleren (blauen) Linie nähert, zeigt sie 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, dass:

  - Ihre Platzierungsstrategie ist die maximale Dichte
  - In den meisten Tagen befindet sich die Zeile „Durchschnittliche Nutzung“ unter oder unter der grünen Linie „
    Workload Balancing“ 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 Durchschnittliche Nutzung mit dem durchschnittlichen kritischen Schwellenwert in Prozent (rot) schneidet, gibt dies die Tage an, an denen die durchschnittliche Ressourcenauslastung den kritischen Schwellenwert für diese Ressource erreicht oder überschritten hat.

Wenn sich Datenpunkte in Ihren Diagrammen nicht im Bereich Durchschnittlicher mittlerer Schwellenwert befinden, Sie aber mit der Leistung zufrieden sind, können Sie den kritischen Schwellenwert für diesen Pool anpassen. Weitere Informationen finden Sie unter Ändern der kritischen Schwellenwerte.

Pool Optimierungsverlauf

Der Bericht „Pool-Optimierungsverlauf“ bietet chronologische Einblicke in die Optimierung der Workload-Balancing-Aktivitäten.

Optimierungsaktivität wird grafisch und in einer Tabelle zusammengefasst. Das Drilling in ein Datumsfeld innerhalb der Tabelle zeigt detaillierte Informationen für jede Pooloptimierung an, die für diesen Tag durchgeführt wurde.

In diesem Bericht werden die folgenden Informationen angezeigt:

- VM-Name. Der Name der VM, die Workload-Balancing optimiert hat.
- Vernunft. Der Grund für die Optimierung.
- Methode. Ob die Optimierung erfolgreich war.
- Vom Host. Der physische Server, auf dem die VM ursprünglich gehostet wurde.
- Zum Host. Der physische Server, auf dem die VM migriert wurde.
- Zeit. Der Zeitpunkt, zu dem die Optimierung stattgefunden hat.

> **Tipp:**
>
> Sie können einen Bericht über die Pooloptimierungsverlauf auch über die Registerkarte WLB generieren, indem Sie auf den Link Historie anzeigen klicken.

Bewegungshistorie der virtuellen Maschine

Dieses Liniendiagramm zeigt an, wie oft VMs in einem Ressourcenpool über einen Zeitraum migriert wurden. Es gibt an, ob eine Migration aus einer Optimierungsempfehlung resultierte 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 auf der Anzahl der VMs in einem Ressourcenpool.
- Sie können Details der Migrationen zu einem bestimmten Datum anzeigen, indem Sie das + -Zeichen im Abschnitt Datum des Berichts erweitern.

Historie der virtuellen Maschine

Dieser Bericht zeigt Performance-Daten für jede VM auf einem bestimmten Host für einen angegebenen Zeitraum an. Der Workload-Balancing basiert auf den Leistungsdaten der Menge der virtuellen Ressourcen, die für die VM zugewiesen wurden. Wenn beispielsweise die durchschnittliche CPU-Auslastung für Ihre VM 67% beträgt, verwendet Ihre VM im Durchschnitt 67% ihrer vCPU für den angegebenen Zeitraum.

In der ersten Ansicht des Berichts wird ein Durchschnittswert für die Ressourcenauslastung in der angegebenen Periode angezeigt.

Durch das Erweitern des + -Zeichens werden Liniendiagramme für einzelne Ressourcen angezeigt. Sie können diese Diagramme verwenden, um Trends bei der Ressourcenauslastung im Laufe der Zeit anzuzeigen.

Dieser Bericht zeigt Daten für die CPU-Auslastung, freien Arbeitsspeicher, Netzwerk-Lese-/Schreibzugriff und Plattenlese/-Schreibvorgänge an.

Verwalten von Workload Balancing-Funktionen und -Einstellungen

Dieser Abschnitt enthält Informationen zum Ausführen optionaler Änderungen an den Einstellungen für den Workload Balancing, einschließlich der folgenden Schritte:

- Optimierungsmodus anpassen
- Automatische Optimierung und Verwaltung der Stromversorgung
- Ändern der kritischen Schwellenwerte
- Metrische Gewichtungen abstimmen
- Hosts von Empfehlungen ausschließen
- Konfigurieren von erweiterten Automatisierungseinstellungen und Datenspeicherung

- Anpassen der Granularitätseinstellungen für den Pool Audit Trail

In diesem Abschnitt wird davon ausgegangen, dass Sie Ihren Pool bereits mit einer virtuellen Workload Balancing-Appliance verbunden haben. Informationen zum Herunterladen, Importieren und Konfigurieren einer virtuellen Workload Balancing-Appliance finden Sie unterErste Schritte. Informationen zum Herstellen einer Verbindung mit der virtuellen Appliance finden Sie unterHerstellen einer Verbindung mit der virtuellen Workload-Balancing-Appliance.

Ändern der Einstellungen für den Workload Balancing

Nachdem Sie eine Verbindung mit der virtuellen Appliance „Workload Balancing“ hergestellt haben, können Sie bei Bedarf die Einstellungen bearbeiten, die der Workload Balancing zur Berechnung der Platzierung und Empfehlungen verwendet.

Zu den Einstellungen für die Platzierung und Optimierung, die Sie ändern können, gehören die folgenden:

- Ändern der Platzierungsstrategie
- Konfigurieren von automatischen Optimierungen und Energieverwaltung
- Bearbeiten von Leistungsschwellenwerten und Metrikgewichtungen
- Ausschließen von Hosts.

Die Einstellungen für den Workload Balancing gelten gemeinsam für alle VMs und Hosts im Pool.

Vorausgesetzt, die Netzwerk- und Festplattenschwellenwerte 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, die Leistungsschwellenwerte zu bewerten und zu bestimmen, ob sie bearbeitet werden sollen. Überlegen Sie beispielsweise, ob Sie Folgendes sind:

- Empfehlungen erhalten, wenn sie noch nicht benötigt werden. Wenn ja, versuchen Sie, die Schwellenwerte anzupassen, bis der Workload Balancing mit geeigneten Empfehlungen beginnt.
- Sie erhalten keine Empfehlungen, wenn Sie erwarten, sie zu erhalten. Wenn Ihr Netzwerk beispielsweise über unzureichende Bandbreite verfügt und Sie keine Empfehlungen erhalten, müssen Sie möglicherweise Ihre Einstellungen anpassen. Wenn ja, versuchen Sie, die netzwerkkritischen Schwellenwerte zu senken, bis der Workload Balancing mit Empfehlungen beginnt.

Bevor Sie die Schwellenwerte bearbeiten, können Sie für jeden physischen Host im Pool einen Pool-Integritätsbericht und den Pool-Integritätsverlauf erstellen.

Sie können die Konfigurationseigenschaften des Arbeitslastausgleichs in XenCenter verwenden, um die Konfigurationseinstellungen zu ändern.

Informationen zum Aktualisieren der Anmeldeinformationen, die Citrix Hypervisor und des Workload Balancing-Servers zur Kommunikation verwenden, finden Sie unterBearbeiten der Konfigurationsdatei für den Workload Balancing.

Wählen Sie im Infrastrukturbereich von XenCenter XenCenter > `your-pool`.

Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

Klicken Sie auf der Registerkarte WLB auf Einstellungen.

Optimierungsmodus anpassen

Der Workload-Balancing gibt Empfehlungen zum Neubalancieren oder Optimieren der VM-Arbeitslast in Ihrer Umgebung basierend auf einer von Ihnen gewählten Strategie für die Platzierung aus. Die Platzierungsstrategie wird als Optimierungsmodus bezeichnet.

Mit dem Workload Balancing können Sie zwischen zwei Optimierungsmodi wählen:

- Maximieren Sie die Leistung. (Standard.) Der Workload Balancing versucht, die Arbeitslast gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, CPU, Arbeitsspeicher und Netzwerkdruck für alle Hosts zu minimieren. Wenn die Maximierung der Leistung Ihre Platzierungsstrategie ist, empfiehlt der Workload Balancing eine Optimierung, wenn ein Host den Schwellenwert „Hoch“ erreicht.
- Dichte maximieren. Der Workload-Balancing versucht, die Anzahl der physischen Hosts zu minimieren, die online sein müssen, indem die aktiven VMs konsolidiert werden.

  Wenn Sie die Option „Dichte maximieren“ als Platzierungsstrategie auswählen, können Sie Parameter angeben, die denen in „Leistung maximieren“ ähnlich sind. Der Workload Balancing verwendet jedoch diese Parameter, um zu bestimmen, wie VMs auf einem Host verpackt werden können. Wenn die Maximize Density Ihre Platzierungsstrategie ist, empfiehlt Workload Balancing Konsolidierungsoptimierungen, wenn eine VM den Niedrigen Schwellenwert erreicht.

Mit Workload Balancing können Sie diese Optimierungsmodi auch die ganze Zeit anwenden, Fixed, oder zwischen den Modi für bestimmte Zeiträume wechseln, Geplant:

- Feste Optimierungsmodi setzen den Workload Balancing so ein, dass er immer ein bestimmtes Optimierungsverhalten hat. Dieses Verhalten kann entweder versuchen, die beste Leistung zu erstellen oder die höchste Dichte zu erstellen.
- Mit den Geplanten Optimierungsmodi können Sie festlegen, dass der Workload Balancing je nach Tageszeit unterschiedliche Optimierungsmodi anwenden kann. Beispielsweise können Sie den Workload Balancing so konfigurieren, dass die Leistung während des Tages optimiert

wird, an dem Benutzer verbunden sind. Um Energie zu sparen, können Sie dann für Workload Balancing festlegen, um die maximale Dichte in der Nacht zu optimieren.

Wenn Sie Zeitgesteuerte Optimierungsmodi konfigurieren, wechselt der Workload Balancing automatisch zu Beginn des angegebenen Zeitraums in den Optimierungsmodus. Sie können jeden Tag, Wochentage, Wochenenden oder einzelne Tage konfigurieren. Für die Stunde wählen Sie eine Tageszeit aus.

Wählen Sie im Ressourcenbereich von XenCenter XenCenter > `your-pool`.

Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

Klicken Sie auf der Registerkarte WLB auf Einstellungen.

Klicken Sie im linken Bereich auf Optimierungsmodus.

Wählen Sie im Abschnitt Fest der Seite Optimierungsmodus einen der folgenden Optimierungsmodi aus:

- Maximieren Sie die Leistung. (Standard.) Versucht, die Arbeitslast gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, 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. (Der Workload-Balancing berücksichtigt die Leistung konsolidierter VMs und gibt eine Empfehlung zur Verbesserung der Leistung aus, wenn eine Ressource auf einem Host einen kritischen Schwellenwert erreicht.)

Wählen Sie im Infrastrukturbereich von XenCenter XenCenter > `your-pool`.

Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

Klicken Sie auf der Registerkarte WLB auf Einstellungen.

Klicken Sie im linken Bereich auf Optimierungsmodus

Wählen Sie im Bereich Optimierungsmodus die Option Geplant aus. Der Abschnitt „Geplant“ wird verfügbar.

Klicken Sie auf Neu hinzufügen.

Wählen Sie im Feld Ändern in einen der folgenden Modi aus:

- Maximieren Sie die Leistung. Versucht, die Arbeitslast gleichmäßig auf alle physischen Hosts in einem Ressourcenpool zu verteilen. Ziel ist es, 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.

Select den Wochentag und die Uhrzeit aus, zu der der Arbeitslastausgleich in diesem Modus gestartet werden soll.

Erstellen Sie weitere geplante Änderungen im Modus (d. h. „Aufgaben“), bis Sie die benötigte Nummer haben. Wenn Sie nur einen Task planen, wechselt der Workload Balancing wie geplant in diesen Modus, wechselt aber nie wieder zurück.

Klicken Sie auf OK.

Zeigen Sie das Dialogfeld Optimierungsmodus an, indem Sie die Schritte 1 bis 4 im vorherigen Verfahren ausführen.

Select die Task aus, die Sie löschen oder deaktivieren möchten, aus der Liste Geplante Modusänderungen.

Führen Sie einen der folgenden Schritte aus:

- **Löschen Sie die Aufgabe endgültig**. Klicken Sie auf die Schaltfläche Löschen.
- **Beenden Sie die Ausführung des Tasks 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 den Task auswählen, auf Bearbeiten klicken und im Dialogfeld Optimierungsmodusplaner das Kontrollkästchen Task aktivieren aktivieren aktivieren aktivieren.
  > – Um eine Aufgabe erneut zu aktivieren, klicken Sie in der Liste Geplante Modusänderungen mit der rechten Maustaste auf die Aufgabe, und klicken Sie auf Aktivieren.

Führen Sie einen der folgenden Schritte aus:

- Doppelklicken Sie auf die Aufgabe, die Sie bearbeiten möchten.
- Select die Aufgabe aus, die Sie bearbeiten möchten, und klicken Sie auf Bearbeiten.

Wählen Sie im Feld Ändern in einen anderen Modus aus, oder nehmen Sie andere Änderungen wie gewünscht vor.

> **Hinweis:**
>
> Wenn Sie auf Abbrechen klicken, werden vor dem Klicken auf OK alle Änderungen rückgängig gemacht, die Sie auf der Registerkarte Optimierung vorgenommen haben, einschließlich des Löschens einer Aufgabe.

Automatische Optimierung und Verwaltung der Stromversorgung

Sie können den Workload Balancing so konfigurieren, dass Empfehlungen automatisch angewendet werden (Automation) und Hosts automatisch aktiviert oder deaktiviert werden. Um Hosts automa-

tisch herunterzufahren (z. B. während Zeiten mit 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 konfigurieren, dass Empfehlungen in Ihrem Namen angewendet und die empfohlenen Optimierungsaktionen automatisch ausgeführt werden. Sie können diese Funktion, die als Automatische Optimierung Akzeptanz bezeichnet wird, verwenden, um Empfehlungen automatisch anzuwenden, einschließlich Empfehlungen zur Verbesserung der Leistung oder zum Herunterfahren von Hosts. Um jedoch Hosts herunterzufahren, müssen Sie Automatisierung, Energieverwaltung und Maximum Density Modus konfigurieren.

Standardmäßig wendet Workload Balancing Empfehlungen nicht automatisch an. Wenn Workload Balancing Empfehlungen automatisch anwenden soll, aktivieren Sie Automatisierung. Andernfalls müssen Sie Empfehlungen manuell anwenden, indem Sie auf Empfehlungen anwenden klicken.

Der Workload-Balancing wendet Empfehlungen nicht automatisch auf Hosts oder VMs an, wenn die Empfehlungen mit den Einstellungen für hohe Verfügbarkeit in Konflikt stehen. Wenn ein Pool durch Anwendung der Optimierungsempfehlungen für den Workload Balancing überschrieben wird, werden Sie von XenCenter aufgefordert, ob Sie die Empfehlung weiterhin anwenden möchten. Wenn Automatisierung aktiviert ist, wendet Workload Balancing keine Empfehlungen zur Energieverwaltung an, die die Anzahl der im Hochverfügbarkeitsplan zu tolerierenden Hostfehler überschreiten.

Wenn der Workload Balancing mit aktivierter Automatisierungsfunktion ausgeführt wird, wird dieses Verhalten manchmal als im automatisierten Modus ausgeführt bezeichnet.

Es ist möglich, die Art und Weise zu optimieren, wie Workload Balancing Empfehlungen im automatisierten Modus anwendet. Weitere Informationen finden Sie unter Einstellen konservativer oder aggressiver automatisierter Empfehlungen.

Energieverwaltung für den Workload Balancing aktivieren

Der Begriff Energieverwaltung bezeichnet die Möglichkeit, das Ein- oder Ausschalten für physische Hosts ein- oder ausschalten zu können. In einem Workload Balancing-Kontext bedeutet dieser Begriff, dass Hosts in einem Pool basierend auf der Gesamtarbeitslast 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 Remote-Ein-/Ausschaltfunktionen
- Die Host-Einschaltfunktion ist für den Host konfiguriert

- Der Host wurde explizit als Host für die Teilnahme an der Energieverwaltung (Workload Balancing) ausgewählt.

Wenn Sie möchten, dass der Workload Balancing Hosts automatisch ausschaltet, konfigurieren Sie den Workload Balancing so, dass folgende Aktionen ausgeführt werden:

- Empfehlungen automatisch anwenden
- Automatisches Anwenden von Energieverwaltungsempfehlungen

Wenn WLB nicht verwendete Ressourcen in einem Pool im Modus „Maximale Dichte“ erkennt, empfiehlt es sich, Hosts auszuschalten, bis die überschüssige Kapazität beseitigt wird. Wenn im Pool nicht genügend Hostkapazität vorhanden ist, um Hosts herunterzufahren, empfiehlt WLB, die Hosts eingeschaltet zu lassen, bis die Poolarbeitslast ausreicht. Wenn Sie den Workload Balancing so konfigurieren, dass zusätzliche Hosts automatisch ausgeschaltet werden, wendet er diese Empfehlungen automatisch an und verhält sich daher genauso.

Wenn ein Host für die Teilnahme an der Energieverwaltung festgelegt ist, gibt Workload Balancing bei Bedarf Empfehlungen zum Einschalten und Ausschalten aus.
Wenn Sie im Modus Maximale Leistung ausführen:

- Wenn Sie WLB so konfigurieren, dass Hosts automatisch eingeschaltet werden, aktiviert WLB Hosts, wenn die Ressourcenauslastung auf einem Host den Schwellenwert „Hoch“ überschreitet.
- Der Workload-Balancing schaltet Hosts nie aus, nachdem er sie eingeschaltet hat.

Wenn Sie die Option zum automatischen Anwenden von Energieverwaltungsempfehlungen aktivieren, tun Sie dies auf Poolebene. Sie können jedoch angeben, welche Hosts aus dem Pool an der Energieverwaltung teilnehmen möchten.

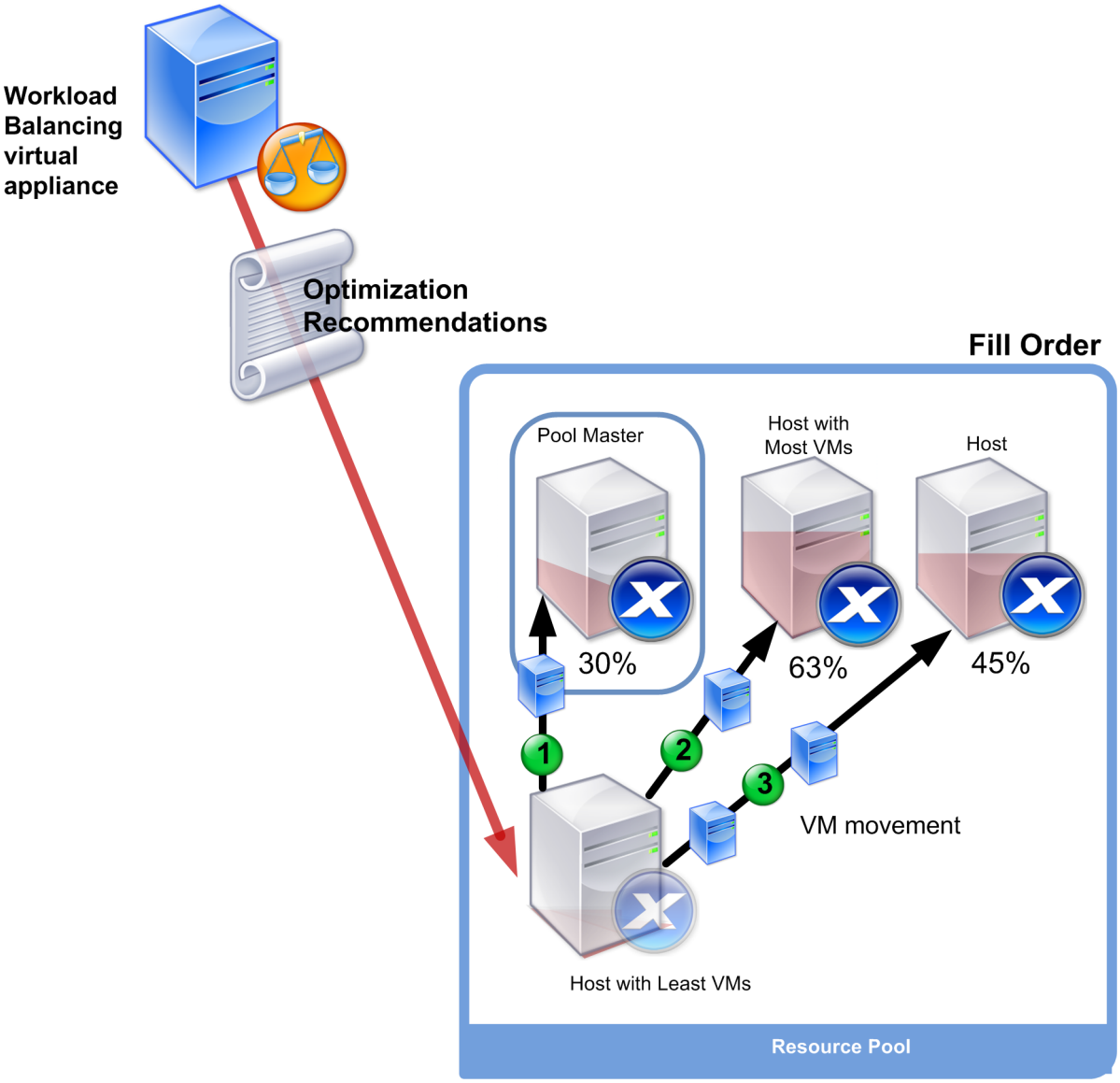
Verstehen des Energieverwaltungsverhaltens

Bevor der Workload Balancing empfiehlt, Hosts ein- oder auszuschalten, werden die Hosts ausgewählt, auf die VMs übertragen werden sollen (d. h. „füllen“). Es tut dies in der folgenden Reihenfolge:

1. Füllen des Poolmasters, da es sich um den Host handelt, der nicht ausgeschaltet werden kann.
2. Füllen des Hosts mit den meisten VMs.
3. Füllen nachfolgender Hosts, nach denen Hosts die meisten VMs laufen.

Wenn der Workload Balancing den Poolmaster füllt, nimmt er dies künstlich niedrige (interne) Schwellenwerte für den Master an. Der Workload-Balancing verwendet diese niedrigen Schwellenwerte als Puffer, um zu verhindern, dass der Poolmaster überlastet wird.

Workload Balancing füllt Hosts in dieser Reihenfolge, um die Dichte zu fördern.



Wenn WLB ein Leistungsproblem erkennt, während sich der Pool im Modus „Maximale Dichte“ befindet, empfiehlt es sich, Arbeitslasten zwischen den eingeschalteten Hosts zu migrieren. Wenn der Workload Balancing das Problem mit dieser Methode nicht beheben kann, versucht er, einen Host einzuschalten. (Der Workload-Balancing bestimmt, welche Hosts eingeschaltet werden sollen, indem dieselben Kriterien angewendet werden, wie wenn der Optimierungsmodus auf Maximale Leistung eingestellt wäre.)

Wenn WLB im Modus „Maximale Leistung“ ausgeführt wird, empfiehlt WLB, Hosts einzuschalten, bis die Ressourcenauslastung für alle Pool-Mitglieder unter den Schwellenwert „Hoch“ fällt.

Wenn Workload Balancing während der Migration von VMs feststellt, dass die Erhöhung der Kapazität die Gesamtleistung des Pools zugute kommt, werden Hosts automatisch eingeschaltet oder empfiehlt dies.

> **Wichtig:**
>
> Der Workload-Balancing empfiehlt nur, einen Host einzuschalten, den der Workload-Balancing ausgeschaltet hat.

Entwurfsumgebungen für Energieverwaltung und VM-Konsolidierung

Wenn Sie eine Citrix Hypervisor Implementierung planen und die automatische VM-Konsolidierung und Energieverwaltung konfigurieren möchten, sollten Sie Ihren Workload-Entwurf berücksichtigen. Sie können beispielsweise Folgendes tun:

- **Platzieren Sie verschiedene Arten von Arbeitslasten in separate Pools**. Wenn Sie über eine Umgebung mit unterschiedlichen Arten von Arbeitslasten verfügen, sollten Sie prüfen, ob die VMs, die diese Arbeitslasten hostet, in verschiedenen Pools gefunden werden sollen. Erwägen Sie auch, VMs zu teilen, die Typen von Anwendungen hosten, die mit bestimmten Hardwaretypen besser funktionieren, in verschiedene Pools zu teilen.

  Da Energieverwaltung und VM-Konsolidierung auf Pool-Ebene verwaltet werden, entwerfen Sie Pools so, dass sie Arbeitslasten enthalten, die konsolidiert werden sollen. Stellen Sie sicher, dass Sie Überlegungen wie in berücksichtigenAutomatisierte Empfehlungen steuern.

- **Hosts vom Arbeitslastausgleich ausschließen**. Einige Hosts müssen möglicherweise immer eingeschaltet sein. Weitere Informationen finden Sie unter Hosts von Empfehlungen ausschließen.

So wenden Sie Optimierungsempfehlungen automatisch an

1. Wählen Sie im Infrastrukturbereich von XenCenter XenCenter > `your-pool`.
2. Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.
3. Klicken Sie auf der Registerkarte WLB auf Einstellungen.
4. Klicken Sie im linken Bereich auf Automation.
5. Select eines oder mehrere der folgenden Kontrollkästchen:
   - Optimierungsempfehlungen automatisch anwenden. Wenn Sie diese Option auswählen, müssen Sie Optimierungsempfehlungen nicht manuell akzeptieren. Workload Balancing akzeptiert automatisch Optimierungs- und Platzierungsempfehlungen.
   - Automatisches Anwenden der Energieverwaltungsempfehlungen. Das Verhalten dieser Option variiert je nach Optimierungsmodus des Pools:
     - Maximaler Leistungsmodus. Wenn die Energieverwaltungsempfehlungen automatisch anwenden aktiviert sind, wird der Workload-Balancing automatisch Hosts aktiviert, wenn dies geschieht, die Hostleistung verbessert.

- Maximaler Density-Modus. Wenn die Energieverwaltungsempfehlungen automatisch anwenden aktiviert sind, schaltet der Workload-Balancing automatisch Hosts aus, wenn die Ressourcenauslastung unter den Schwellenwert niedrig fällt. Das heißt, der Workload-Balancing schaltet Hosts während niedriger Nutzungszeiten automatisch aus.

6. (Optional.) Optimierungsempfehlungen optimieren, indem Sie im linken Bereich des Dialogfelds Einstellungen auf Erweitert klicken und eine oder mehrere der folgenden Aktionen ausführen:

   - Geben Sie an, wie oft Workload Balancing eine Optimierungsempfehlung abgeben muss, bevor die Empfehlung automatisch angewendet wird. Der Standardwert ist dreimal, was bedeutet, dass die Empfehlung beim dritten Mal angewendet wird.
   - Wählen Sie die niedrigste Optimierungsebene aus, die Workload-Balancing automatisch angewendet werden soll. Der Standardwert ist Hoch.
   - Ändern der Aggressivität, mit der Workload Balancing seine Optimierungsempfehlungen anwendet.

     Sie können auch angeben, wie viele Minuten der Workload Balancing warten muss, bevor eine Optimierungsempfehlung auf eine kürzlich verschobene VM angewendet wird.

     Alle diese Einstellungen werden ausführlicher in erläutertEinstellen konservativer oder aggressiver automatisierter Empfehlungen.

7. Führen Sie einen der folgenden Schritte aus:

   - Wenn Sie die Energieverwaltung konfigurieren möchten, klicken Sie auf Automatisierung/Energieverwaltung, und fahren Sie mit der fortSo wählen Sie Hosts für die Energieverwaltung aus.
   - Wenn Sie die Energieverwaltung nicht konfigurieren möchten und die Automatisierung konfiguriert haben, klicken Sie auf OK.

So wählen Sie Hosts für die Energieverwaltung aus

1. Wählen Sie im Abschnitt Energieverwaltung die Hosts aus, für die der Arbeitslastausgleich das Ein- und Ausschalten empfohlen werden soll.

   > **Hinweis:**
   >
   > Wenn Sie Hosts für Energieverwaltungsempfehlungen auswählen, ohne die Option **Energieverwaltungsempfehlungen automatisch anwenden** auszuwählen, schlägt WLB Empfehlungen zur Energieverwaltung vor, wendet sie jedoch nicht automatisch für Sie an.

2. Klicken Sie auf OK. Wenn keiner der Hosts im Ressourcenpool die Remote-Energieverwaltung unterstützt, zeigt der Workload-Balancing die Meldung „Keine Hosts unterstützen Energieverwaltung. „

Verstehen, wann Workload Balancing Empfehlungen ausgibt

Der Workload-Balancing wertet kontinuierlich die Ressourcenmetriken von physischen Hosts und VMs in den Pools aus, die er verwaltet, gegen Schwellenwerte aus. Schwellenwerte sind voreingestellte Werte, die wie Grenzen funktionieren, die ein Host überschreiten muss, bevor der Workload Balancing eine Optimierungsempfehlung abgeben kann. Auf einem sehr hohen Niveau. Der Workload-Balancing-Prozess ist wie folgt:

1. Der Workload-Balancing erkennt, dass der Schwellenwert für eine Ressource verletzt wurde.
2. Der Workload Balancing wird ausgewertet, ob er eine Optimierungsempfehlung ausgibt.
3. Der Workload Balancing legt fest, welche Hosts empfohlen werden, als Zielhosts zu fungieren. Ein Zielhost ist der Host, auf dem Workload Balancing empfiehlt, eine oder mehrere VMs zu verlegen.
4. Der Workload-Balancing gibt die Empfehlung aus.

Nachdem WLB ermittelt hat, dass ein Host von der Optimierung profitieren kann, bevor er die Empfehlung ausgibt, wertet er andere Hosts im Pool aus, um Folgendes zu entscheiden:

1. Die Reihenfolge, um die Optimierung durchzuführen (welche Hosts, welche VMs)
2. Wo sollte man empfehlen, eine VM zu platzieren, wenn sie eine Empfehlung ausgibt?

Um diese beiden Aufgaben auszuführen, verwendet der Workload Balancing Schwellenwerte und Gewichtungen wie folgt:

- **Schwellenwerte** sind die Grenzwerte, mit denen Workload Balancing die Ressourcenmetriken Ihres Pools verglichen. Die Schwellenwerte werden verwendet, um zu bestimmen, ob eine Empfehlung abgegeben werden soll und welche Hosts ein geeigneter Kandidat für das Hosten von umgeleiteten VMs sind.
- **Gewichtungen** sind eine Möglichkeit, Ressourcen entsprechend, wie viel Sie möchten, dass sie berücksichtigt werden, werden verwendet, um die Verarbeitungsreihenfolge zu bestimmen. Nachdem der Workload-Balancing beschlossen hat, eine Empfehlung abzugeben, verwendet er Ihre Spezifikationen, welche Ressourcen wichtig sind, um Folgendes zu bestimmen:
  - Welche Host-Leistung zuerst angesprochen werden soll
  - Welche VMs sollten zuerst migriert werden

Für jede Ressource Workload-Balancing-Monitore verfügt sie über vier Schwellenwerte (Kritisch, Hoch, Mittel und Niedrig), die in den folgenden Abschnitten erläutert werden. Beim Workload-

Balancing wird ausgewertet, ob eine Empfehlung abgegeben werden soll, wenn eine Ressourcenmetrik auf einem Host:

- Überschreitet den Schwellenwert „Hoch“, wenn der Pool im Modus „Maximale Leistung“ ausgeführt wird (Leistung verbessern)
- Unterschreitet den Schwellenwert niedrig, wenn der Pool im Modus Maximale Dichte ausgeführt wird (Konsolidierung von VMs auf Hosts)
- Überschreitet den kritischen Schwellenwert, wenn der Pool im Modus „Maximale Dichte“ ausgeführt wird (Leistung verbessern)

Wenn der Schwellenwert für einen Pool, der im Modus Maximale Leistung ausgeführt wird, 80% beträgt und die CPU-Auslastung auf einem Host 80,1% erreicht, bewertet WLB, ob eine Empfehlung abgegeben werden soll.

Wenn eine Ressource ihren Schwellenwert verletzt, wertet WLB die Metrik der Ressource anhand der historischen Performance aus, um zu verhindern, dass eine Optimierungsempfehlung basierend auf einem temporären Spike erstellt wird. Dazu erstellt der Workload Balancing eine historisch gemittelte Auslastungsmetrik, indem die Daten für die Ressourcenauslastung ausgewertet werden, die zu folgenden Zeiten erfasst wurden:

Erfasste Daten	Gewicht
Sofort wurde zum Zeitpunkt der Schwelle überschritten (dh Echtzeitdaten)	70%
30 Minuten vor Überschreitung der Schwelle	25%
24 Stunden vor Überschreitung der Schwelle	5%

Wenn die CPU-Auslastung auf dem Host um 12:02 Uhr den Schwellenwert überschreitet, überprüft WLB die Auslastung an diesem Tag um 11:32 Uhr und am Vortag um 12:02 Uhr. Wenn beispielsweise die CPU-Auslastung den folgenden Werten entspricht, gibt WLB keine Empfehlung ab:

- 80.1% at 12:02 an diesem Tag
- 50% um 11:32 Uhr an diesem Tag
- 78% um 12:32 Uhr am Vortag

Dieses Verhalten liegt daran, dass die historisch gemittelte Auslastung 72,47% beträgt, so dass Workload Balancing davon ausgeht, dass die Auslastung eine temporäre Spitze ist. Wenn die CPU-Auslastung jedoch um 11:32 Uhr 78% betrug, empfiehlt der Workload-Balancing, da die historisch gemittelte Auslastung 80,1% beträgt.

Optimierungs- und Konsolidierungsprozess

Der Workload-Balancing-Prozess zur Bestimmung potenzieller Optimierungen variiert je nach Optimierungsmodus (Maximale Leistung oder Maximale Dichte). Unabhängig vom Optimierungsmodus werden jedoch Optimierungs- und Platzierungsempfehlungen in einem zweistufigen Prozess abgegeben:

1. Bestimmen Sie potenzielle Optimierungen. (Das heißt, welche VMs von Hosts zu migrieren.)
2. Bestimmen Sie die Platzierungsempfehlungen. (Das heißt, welche Hosts wären geeignete Kandidaten für neue Hosts.)

> **Hinweis:**
>
> Workload Balancing empfiehlt nur die Migration von VMs, die die Citrix Hypervisor Kriterien für die Live-Migration erfüllen, einschließlich des Zielhosts muss über den Speicher verfügen, den die VM benötigt. Der Zielhost muss außerdem über ausreichende Ressourcen verfügen, um die VM hinzuzufügen, ohne die Schwellenwerte des im Pool konfigurierten Optimierungsmodus zu überschreiten. Beispielsweise der Schwellenwert „Hoch“ im Modus „Maximale Leistung“ und der kritische Schwellenwert für den Modus „Maximale Dichte“.

Wenn der Workload Balancing im automatisierten Modus ausgeführt wird, können Sie die Art und Weise einstellen, wie Empfehlungen angewendet werden. Weitere Informationen finden Sie unter Einstellen konservativer oder aggressiver automatisierter Empfehlungen.

Optimierungsempfehlungsprozess im Modus „Maximale Leistung“

Wenn der Workload Balancing im Modus Maximale Leistung ausgeführt wird, wird der folgende Prozess verwendet, um potenzielle Optimierungen zu ermitteln:

1. Alle zwei Minuten wertet Workload Balancing die Ressourcenauslastung für jeden Host im Pool aus. Dies geschieht, indem auf jedem Host überwacht wird und festgestellt wird, ob die Auslastung der einzelnen Ressourcen den Schwellenwert für hohe Werte überschreitet. Weitere InformationenÄndern des kritischen Schwellenwertszum Hohen Schwellenwert finden Sie unter.

   Wenn die Auslastung einer Ressource im Modus „Maximale Leistung“ den Schwellenwert „Hoch“ überschreitet, startet WLB den Prozess, um zu bestimmen, ob eine Optimierungsempfehlung abgegeben werden soll. Der Workload-Balancing legt fest, ob eine Optimierungsempfehlung abgegeben werden soll, basierend darauf, ob dadurch Performance-Einschränkungen erleichtert werden können, z. B.

   Betrachten Sie beispielsweise den Fall, in dem Workload-Balancing erkennt, dass unzureichende CPU-Ressourcen die Leistung der VMs auf Host A negativ beeinflussen. Wenn Workload-Balancing einen anderen Host mit weniger CPU-Auslastung finden kann, empfiehlt es sich, einen oder mehrere VMs auf einen anderen Host zu verschieben.

2. Wenn die Auslastung einer Ressource auf einem Host den relevanten Schwellenwert überschreitet, kombiniert der Workload Balancing die folgenden Daten zur historisch gemittelten Auslas-

tung:

- Aktuelle Auslastung der Ressource
- Historische Daten von vor 30 Minuten
- Historische Daten von vor 24 Stunden
  Wenn die historisch gemittelte Auslastung den Schwellenwert der Ressource überschreitet, legt der Workload Balancing fest, dass er eine Optimierungsempfehlung ausgibt.

3. Workload Balancing verwendet Metrik-Gewichtungen, um zu bestimmen, welche Hosts zuerst optimiert werden sollen. Die Ressource, der Sie die größte Gewichtung zugewiesen haben, ist die Ressource, die Workload Balancing zuerst adressieren möchte. Metrische Gewichtungen abstimmen#tune-metric-weightings[()]Weitere Informationen zu Metrikgewichtungen finden Sie unter.

4. Der Workload-Balancing legt fest, welche Hosts die VMs unterstützen können, die von Hosts migriert werden sollen.

   Der Workload-Balancing ermittelt diese Bestimmung, indem der projizierte Effekt der Platzierung verschiedener Kombinationen von VMs auf Hosts auf die Ressourcenauslastung berechnet wird. (Workload Balancing verwendet eine Methode zur Durchführung dieser Berechnungen, die in der Mathematik als Permutation bezeichnet wird.)

   Dazu erstellt der Workload Balancing eine einzelne Metrik oder Bewertung, um die Auswirkungen der Migration einer VM auf den Host zu prognostizieren. Die Bewertung zeigt die Eignung eines Hosts als Heimanwender für weitere VMs an.

   Um die Leistung des Hosts zu bewerten, kombiniert der Workload Balancing die folgenden Metriken:

   - Aktuelle Metriken des Hosts
   - Die Metriken des Hosts der letzten 30 Minuten
   - Die Metriken des Gastgebers von vor 24 Stunden
   - Die Metriken der VM.

5. Nach der Bewertung von Hosts und VMs versucht WLB, virtuelle Modelle mit unterschiedlichen Kombinationen von VMs zu erstellen, wie die Hosts aussehen. WLB verwendet diese Modelle, um den besten Host für die Platzierung der VM zu ermitteln.

   Im Modus „Maximale Leistung“ verwendet der Workload Balancing Metrik-Gewichtungen, um zu bestimmen, welche Hosts zuerst optimiert werden sollen und welche VMs auf diesen Hosts zuerst migriert werden sollen. Der Workload Balancing basiert auf den metrischen Gewichtungen. Wenn beispielsweise die CPU-Auslastung die höchste Bedeutung zugewiesen wird, sortiert Workload Balancing Hosts und VMs zur Optimierung nach den folgenden Kriterien:

   - Erstens, was die CPU-Auslastung des Hosts am stärksten beeinflusst (d. h., sie laufen am nächsten am oberen Schwellenwert für die CPU-Auslastung)

- Welche VMs haben die höchste CPU-Auslastung (oder laufen am nächsten an ihrem hohen Schwellenwert).

6. Workload Balancing setzt die Berechnung der Optimierungen fort. Es betrachtet Hosts als Kandidaten für die Optimierung und VMs als Kandidaten für die Migration, bis die prognostizierte Ressourcenauslastung auf dem Host der VM unter den Schwellenwert für Hoch fällt. Die prognostizierte Ressourcenauslastung ist die Ressourcenauslastung, die der Workload-Balancing von einem Host prognostiziert, nachdem der Workload-Balancing eine VM vom Host hinzugefügt oder entfernt hat.

Konsolidierungsprozess im Modus „Maximale Dichte“

WLB legt fest, ob eine Empfehlung abgegeben werden soll, basierend darauf, ob sie eine VM auf einen Host migrieren und diesen Host weiterhin unterhalb des kritischen Schwellenwerts ausführen kann.

1. Wenn die Auslastung einer Ressource unter den niedrigen Schwellenwert fällt, beginnt der Workload-Balancing mit der Berechnung potenzieller Konsolidierungsszenarien.
2. Wenn WLB eine Möglichkeit entdeckt, VMs auf einem Host zu konsolidieren, wird ausgewertet, ob der Zielhost ein geeignetes Zuhause für die VM ist.
3. Wie im Modus „Maximale Leistung“ bewertet der Workload Balancing den Host, um die Eignung eines Hosts als Home für neue VMs zu bestimmen.

   Bevor WLB Empfehlungen zur Konsolidierung von VMs auf weniger Hosts ausgibt, wird überprüft, ob die Ressourcenauslastung auf diesen Hosts nach dem Umzug von VMs auf sie unter kritischen Schwellenwerten liegt.

   > **Hinweis:**
   >
   > Der Workload-Balancing berücksichtigt keine Metrikgewichtungen, wenn er eine Konsolidierungsempfehlung ausgibt. Es berücksichtigt nur Metrikgewichtungen, um die Leistung auf Hosts zu gewährleisten.

4. Nach der Bewertung von Hosts und VMs versucht WLB, virtuelle Modelle mit unterschiedlichen Kombinationen von VMs zu erstellen, wie die Hosts aussehen. Es verwendet diese Modelle, um den besten Host für die Platzierung der VM zu ermitteln.
5. WLB berechnet den Effekt, dass VMs zu einem Host hinzugefügt werden, bis prognostiziert wird, dass das Hinzufügen einer anderen VM dazu führt, dass eine Hostressource den kritischen Schwellenwert überschreitet.
6. Arbeitslastausgleichsempfehlungen schlagen immer vor, den Poolmaster zuerst zu füllen, da der Host nicht ausgeschaltet werden kann. Der Workload Balancing wendet jedoch einen Puffer auf den Poolmaster an, sodass er nicht überlastet werden kann.

7. WLB empfiehlt weiterhin, VMs auf Hosts zu migrieren, bis keine Hosts übrig bleiben, die einen kritischen Schwellenwert nicht überschreiten, wenn eine VM zu ihnen migriert wird.

Ändern der kritischen Schwellenwerte

Sie können kritische Schwellenwerte ändern, um zu steuern, wenn Optimierungsempfehlungen ausgelöst werden. In diesem Abschnitt finden Sie Hinweise zu:

- Ändern der standardmäßigen kritischen Schwellenwerte auf Hosts im Pool
- Wie Werte für den kritischen Schwellenwert „Hoch“, „Mittel“ und „Niedrig“ geändert werden.

Der Workload-Balancing legt fest, ob Empfehlungen erstellt werden sollen, basierend darauf, ob die durchschnittliche historische Auslastung für eine Ressource auf einem Host gegen ihren Schwellenwert verstößt. Arbeitslastausgleichsempfehlungen werden ausgelöst, wenn der Schwellenwert „Hoch“ im Modus „Maximale Leistung“ oder „Niedrig“ und „Kritisch“ für den Modus „Maximale Dichte“ verletzt wird. 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. (Zur Vereinfachung der Benutzeroberfläche ist der Schwellenwert Kritisch der einzige Schwellenwert, den Sie über XenCenter ändern können.)

Die folgende Tabelle zeigt die Standardwerte für die Schwellenwerte für den Arbeitslastausgleich:

Metrik	Kritisch	Hoch	Mittel	Niedrig
CPU-Auslastung	90%	76.5%	45%	22.5%
Freier Speicher	51 MB	63,75 MB	510 MB	1020 MB
Netzwerk-Lesevorgänge	25 MB/s	21,25 MB/s	12,5 MB/s	6,25 MB/s
Netzwerkschreibvorgänge	25 MB/s	21,25 MB/s	12,5 MB/s	6,25 MB/s
Datenträgerlesevo	25 MB/s	21,25 MB/s	12,5 MB/s	6,25 MB/s
Festplattenschreibvorgänge	25 MB/s	21,25 MB/s	12,5 MB/s	6,25 MB/s

Um die Werte für alle Metriken außer Speicher zu berechnen, multipliziert Workload Balancing den neuen Wert für den kritischen Schwellenwert mit den folgenden Faktoren:

- **Hoher Schwellenwert**: 0,85
- **Mittlerer Schwellenwert**: 0,50
- **Niedriger Schwellenwert**: 0,25

Wenn Sie beispielsweise den kritischen Schwellenwert für die CPU-Auslastung auf 95% erhöhen, setzt WLB die Schwellenwerte Hoch, Mittel und Niedrig auf 80,75%, 47,5% und 23,75% zurück.

Um die Schwellenwerte für freien Speicher zu berechnen, multipliziert Workload Balancing den kritischen Schwellenwert mit den folgenden Faktoren:

- **Hoher Schwellenwert**: 1,25
- **Mittlerer Schwellenwert**: 10,0
- **Niedriger Schwellenwert**: 20,0

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:

Hoher, mittlerer oder niedriger Schwellenwert = kritischer Schwellenwert * Schwellenwert Faktor

Wenn Sie beispielsweise den kritischen Schwellenwert für Netzwerklesevorgänge auf 40 MB/s ändern, multiplizieren Sie 40 mit 0,25, was 10 MB/s entspricht. Um den Schwellenwert Mittel zu erhalten, multiplen Sie 40 mal 0,50 usw.

Während der kritische Schwellenwert viele Optimierungsempfehlungen auslöst, können andere Schwellenwerte auch Optimierungsempfehlungen auslösen, wie folgt:

- **Hohe Schwelle**.
  - **Maximale Leistung**. Das Überschreiten des Schwellenwerts „Hoch“ löst Optimierungsempfehlungen aus, um eine VM auf einen Host mit geringerer Ressourcenauslastung zu verlagern.
  - **Maximale Dichte**. Der Workload-Balancing empfiehlt nicht, eine VM auf dem Host zu platzieren, wenn diese VM auf den Host verschoben wird, bewirkt, dass die Hostressourcenauslastung einen Hohen Schwellenwert überschreitet.
- **Niedrige Schwelle**.
  - **Maximale Leistung**. Der Workload-Balancing löst keine Empfehlungen aus dem Schwellenwert „Niedrig“ aus.
  - **Maximale Dichte**. Wenn ein Metrikwert unter den Schwellenwert „Niedrig“ fällt, ermittelt WLB, dass Hosts nicht ausgelastet sind, und empfiehlt eine Optimierungsempfehlung, 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 den Schwellenwert „Hoch“ erreicht haben.

Nachdem eine VM verlagert wurde, kann die Auslastung einer Ressource auf dem neuen Host der VM jedoch einen kritischen Schwellenwert überschreiten. In diesem Fall verwendet WLB vorübergehend einen Algorithmus, der dem Lastausgleichsalgorithmus für maximale Leistung entspricht, 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 im Infrastrukturbereich von XenCenter XenCenter > `your-resource-pool`.
2. Klicken Sie im Bereich Eigenschaften 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 VM-Platzierung und Pool-Optimierungsempfehlungen abgegeben werden. Der Workload-Balancing ist bestrebt, die Ressourcenauslastung auf einem Host unter den festgelegten kritischen Werten zu halten.

Metrische Gewichtungen abstimmen

Wie Workload Balancing Metrik-Gewichtungen verwendet, um zu bestimmen, welche Hosts und VMs zuerst verarbeitet werden sollen, variiert je nach Optimierungsmodus: Maximale Dichte oder Maximale Leistung.

Wenn Workload Balancing Optimierungsempfehlungen verarbeitet, wird eine Optimierungsreihenfolge erstellt. Um dies zu bestimmen, ordnet Workload Balancing die Hosts als erste Adresse an, nach denen Hosts die höchsten Metrikwerte für jede Ressource haben, die auf der Metrikgewichtungsseite als wichtigste eingestuft wird.

Im Allgemeinen werden Metrikgewichtungen verwendet, wenn sich ein Pool im Modus „Maximale Leistung“ befindet. Wenn sich der Workload-Balancing jedoch im Modus „Maximale Dichte“ befindet, werden Metrikgewichtungen verwendet, wenn eine Ressource ihren kritischen Schwellenwert überschreitet.

Maximaler Leistungsmodus

Im Modus „Maximale Leistung“ verwendet der Workload Balancing Metrik-Gewichtungen, um (a) zu bestimmen, welche Host-Leistung zuerst adressieren soll, und (b) welche VMs zuerst die Migration empfehlen sollen.

Wenn beispielsweise Netzwerkschreibvorgänge die wichtigste Ressource für WLB ist, gibt WLB zunächst Optimierungsempfehlungen für den Host mit der höchsten Anzahl von Netzwerkschreibvorgängen pro Sekunde aus. Damit Network Writes die wichtigste Ressource ist, bewegen Sie den Schieberegler **Metrikgewichtung** nach rechts und alle anderen Schieberegler in die Mitte.

Wenn Sie alle Ressourcen so konfigurieren, dass sie gleich wichtig sind, befasst sich der Workload Balancing zuerst mit der CPU-Auslastung und zweitem Arbeitsspeicher, da diese Ressourcen normalerweise am stärksten eingeschränkt sind. Damit alle Ressourcen gleich wichtig sind, legen Sie fest, dass sich der Schieberegler **Metrikgewichtung** für alle Ressourcen an derselben Stelle befindet.

Modus „Maximale Dichte“

Im Modus „Maximale Dichte“ verwendet der Workload-Balancing nur Metrik-Gewichtungen, wenn ein Host den kritischen Schwellenwert erreicht. Zu diesem Zeitpunkt wendet Workload Balancing einen Algorithmus an, der dem für Maximale Leistung ähnelt, bis keine Hosts die kritischen Schwellenwerte überschreiten. Bei Verwendung dieses Algorithmus verwendet der Workload Balancing Metrik-Gewichtungen, um die Optimierungsreihenfolge auf die gleiche Weise zu bestimmen wie im Modus Maximale Leistung.

Wenn zwei oder mehr Hosts über Ressourcen verfügen, die ihre kritischen Schwellenwerte überschreiten, überprüft der Workload-Balancing die Bedeutung, die Sie für jede Ressource festlegen. Diese Wichtigkeit wird verwendet, um zu bestimmen, welcher Host zuerst optimiert werden soll und welche VMs auf diesem Host zuerst verlagert werden sollen.

Beispielsweise enthält Ihr Pool Host A und Host B, die sich im folgenden Zustand befinden:

- Die CPU-Auslastung auf Host A überschreitet den kritischen Schwellenwert, und die Metrik-Gewichtung für die CPU-Auslastung wird ganz rechts gesetzt: **Mehr Wichtig**.
- Die Speicherauslastung auf Host B überschreitet den kritischen Schwellenwert, und die Metrikgewichtung für die Speicherauslastung wird ganz links gesetzt: **Weniger wichtig**.

Workload Balancing empfiehlt, Host A zunächst zu optimieren, da die Ressource, die den kritischen Schwellenwert erreicht hat, die höchste Gewichtung zugewiesen ist. Nachdem der Workload-Balancing feststellt, dass er die Leistung auf Host A erfüllen muss, beginnt der Workload-Balancing mit der Empfehlung von Platzierungen für VMs auf diesem Host. Es beginnt mit der VM, die die höchste CPU-Auslastung hat, da diese CPU-Auslastung die Ressource mit dem höchsten Gewicht ist.

Nachdem der Workload Balancing die Optimierung von Host A empfohlen hat, gibt er Optimierungsempfehlungen für Host B aus. Wenn er Platzierungen für die VMs auf Host B empfiehlt,

wird dies zuerst durch die CPU-Auslastung adressieren, da die CPU-Auslastung das höchste Gewicht zugewiesen wurde.

Wenn mehr Hosts optimiert werden müssen, richtet sich der Workload Balancing an die Leistung auf diesen Hosts, je nachdem, welcher Host die dritthöchste CPU-Auslastung hat.

Standardmäßig sind alle Metrikgewichtungen auf den am weitesten entfernten Punkt auf dem Schieberegler (Wichtiger) festgelegt.

> **Hinweis:**
>
> Die Gewichtung von Metriken ist relativ. Wenn alle Metriken auf dieselbe Ebene festgelegt sind, selbst wenn diese Stufe weniger wichtig ist, werden sie alle gleich gewichtet. Die Beziehung der Metriken zueinander ist wichtiger als das tatsächliche Gewicht, mit dem Sie jede Metrik festlegen.

So bearbeiten Sie Metrikgewichtungsfaktoren

1. Anhalten
2. Wählen Sie im Infrastrukturbereich von XenCenter XenCenter > `your-resource-pool`.
3. Klicken Sie auf die Registerkarte WLB, und klicken Sie dann auf Einstellungen.
4. Wählen Sie im linken Bereich die Option Metrik-Gewichtung aus.
5. Passen Sie auf der Seite Metrikgewichtung nach Bedarf die Schieberegler neben den einzelnen Ressourcen an.

   Bewegen Sie den Schieberegler in Richtung Weniger wichtig, um anzugeben, dass VMs immer über die höchste verfügbare Menge dieser Ressource verfügen, für diesen Pool nicht so wichtig ist.

Hosts von Empfehlungen ausschließen

Bei der Konfiguration von Workload Balancing können Sie angeben, dass bestimmte physische Hosts von der Optimierung des Arbeitslastausgleichs und der Platzierungsempfehlungen ausgeschlossen werden, einschließlich der Empfehlungen für die Platzierung „Start On On“.

Situationen, in denen Sie Hosts von Empfehlungen ausschließen möchten, sind:

- 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-Arbeitslasten, die immer auf demselben Host ausgeführt werden müssen. Zum Beispiel, wenn die VMs komplementäre Anwendungen oder Arbeitslasten haben.
- Sie haben Arbeitslasten, die nicht verschoben werden sollen (z. B. einen Domänencontroller oder einen Datenbankserver).

- Sie möchten Wartungsarbeiten auf einem Host durchführen, und Sie möchten nicht, dass VMs auf dem Host platziert werden.
- Die Leistung der Arbeitslast ist so kritisch, dass die Kosten für dedizierte Hardware irrelevant sind.
- Bestimmte Hosts führen Workloads (VMs) mit hoher Priorität aus, und Sie möchten diese VMs nicht mit der Funktion Hochverfügbarkeit priorisieren.
- Die Hardware im Host ist nicht optimal für die anderen Workloads im Pool.

Unabhängig davon, ob Sie einen festen oder geplanten Optimierungsmodus angeben, bleiben ausgeschlossene Hosts auch dann ausgeschlossen, 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 nicht aktivieren (oder deaktivieren). Weitere Informationen finden Sie unter Automatische Optimierung und Verwaltung der Stromversorgung.

Wenn Sie einen Host von Empfehlungen ausschließen, geben Sie an, dass der Workload Balancing diesen Host überhaupt nicht verwaltet. Diese Konfiguration bedeutet, dass Workload Balancing keine Optimierungsempfehlungen für einen ausgeschlossenen Host ausgibt. Wenn Sie hingegen keinen Host für die Teilnahme an der Energieverwaltung auswählen, verwaltet WLB den Host weiterhin, gibt jedoch keine Energieverwaltungsempfehlungen für ihn aus.

So schließen Sie Hosts aus dem Workload-Balancing aus

Gehen Sie folgendermaßen vor, um einen Host in einem Pool, den Workload Balancing verwaltet, von den Empfehlungen für Energieverwaltung, Hostevakuierung, Platzierung und Optimierung auszuschließen.

1. Wählen Sie im Ressourcenbereich von XenCenter XenCenter > `your-resource-pool`.
2. Klicken Sie im Bereich Eigenschaften 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 WLB alternative Platzierungen und Optimierungen nicht empfehlen soll.

Automatisierte Empfehlungen steuern

Workload Balancing enthält einige erweiterte Einstellungen, mit denen Sie steuern können, wie Workload Balancing automatisierte Empfehlungen anwendet. Diese Einstellungen werden im Dialogfeld „Workload Balancing Configuration“ auf der Seite „Erweitert“ angezeigt.

Wählen Sie im Ressourcenbereich von XenCenter XenCenter > `your-resource-pool`.

Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

Klicken Sie auf der Registerkarte WLB auf Einstellungen.

Wählen Sie im linken Bereich Erweitert aus.

Einstellen konservativer oder aggressiver automatisierter Empfehlungen

Bei der Ausführung im automatisierten Modus sind die Häufigkeit der Optimierungs- und Konsolidierungsempfehlungen und die automatische Anwendung mehrerer Faktoren, darunter:

- Wie lange Sie den Workload Balancing angeben, wartet nach dem Verschieben einer VM, bevor Sie eine weitere Empfehlung abgeben
- Die Anzahl der Empfehlungen, die Workload-Balancing vorgeben muss, bevor eine Empfehlung automatisch angewendet wird
- Der Schweregrad, den eine Empfehlung erreichen muss, bevor die Optimierung automatisch angewendet wird
- Der Grad der Konsistenz in Empfehlungen (empfohlene VMs zum Verschieben, Zielhosts) Der Workload-Balancing erfordert, bevor Empfehlungen automatisch angewendet werden.

> **Wichtig:**
>
> Passen Sie im Allgemeinen nur die Einstellungen für Faktoren in den folgenden Fällen an:
>
> - Sie haben Anleitungen vom technischen Support von Citrix
> - Sie haben das Verhalten Ihres Pools mit aktiviertem Workload-Balancing signifikant beobachtet und getestet.

Eine falsche Konfiguration dieser Einstellungen kann dazu führen, dass Workload Balancing keine Empfehlungen ausgibt.

VM-Migrationsintervall

Sie können angeben, wie viele Minuten WLB wartet, nachdem eine VM das letzte Mal verschoben wurde, bevor WLB eine weitere Empfehlung für diese VM aussprechen kann.

Das Empfehlungsintervall soll verhindern, dass der Workload-Balancing Empfehlungen aus künstlichen Gründen generiert (z. B. wenn eine vorübergehende Auslastung vorlag).

Bei der Konfiguration der Automatisierung ist es besonders wichtig, beim Ändern des Empfehlungsintervalls vorsichtig zu sein. Wenn ein Problem auftritt, das zu kontinuierlichen, wiederkehrenden Spitzen führt, kann das Erhöhen der Häufigkeit (d. h. das Einstellen einer niedrigeren Zahl) viele Empfehlungen und daher Umzüge generieren.

> **Hinweis:**
>
> Das Festlegen eines Empfehlungsintervalls wirkt sich nicht darauf aus, wie lange der Workload Balancing wartet, um kürzlich neu ausbalancierte Hosts in Empfehlungen für Start-On Placement, Wiederaufnahme und Wartungsmodus zu berücksichtigen.

Anzahl der Empfehlungen

Alle zwei Minuten überprüft der Workload Balancing, ob er Empfehlungen für den überwachten Pool generieren kann. Wenn Sie Automatisierung aktivieren, können Sie angeben, wie oft eine konsistente Empfehlung durchgeführt werden muss, bevor der Workload Balancing die Empfehlung automatisch anwendet. Dazu konfigurieren Sie eine Einstellung, die als Recommendation Count bezeichnet wird. Mit der Einstellung „Anzahl der Empfehlungen“ und „Optimierungsaggressivität“ können Sie die automatisierte Anwendung von Empfehlungen in Ihrer Umgebung optimieren.

Wie im Abschnitt Aggressivität beschrieben, verwendet Workload Balancing die Ähnlichkeit der Empfehlungen, um folgende Prüfungen durchzuführen:

1. Ob die Empfehlung wirklich benötigt wird
2. Gibt an, ob der Zielhost über einen längeren Zeitraum stabil genug Leistung hat, um eine umgeleiteten VM zu akzeptieren (ohne ihn in Kürze wieder vom Host verschieben zu müssen)

Workload Balancing verwendet den Wert „Recommendation Count“, um zu bestimmen, dass 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 Anzahl der Empfehlungen. Wenn die Empfehlung die Konsistenzanforderungen nicht erfüllt, kann der Workload Balancing die Anzahl der Empfehlungen auf Null zurücksetzen, abhängig von den in beschriebenen FaktorenOptimierung Aggressivität.
2. Wenn WLB genügend konsistente Empfehlungen generiert, um den Wert für die Empfehlungsanzahl zu erfüllen, wie im Textfeld Empfehlungen angegeben, wird die Empfehlung automatisch angewendet.

Wenn Sie diese Einstellung ändern, variiert der festzulegenden Wert je nach Umgebung. Betrachten Sie diese Szenarien:

- Wenn Host-Lasten und 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 die Empfehlung nach sechs Minuten automatisch an.

- Wenn die Host-Lasten und die Aktivität in Ihrer Umgebung schrittweise zunehmen, sollten Sie den Wert für die Anzahl der Empfehlungen verringern.

Das Akzeptieren von Empfehlungen verwendet Systemressourcen und wirkt sich auf die Leistung aus, wenn der Workload Balancing die VMs verlagert. Wenn Sie die Anzahl der Empfehlungen erhöhen, erhöht sich die Anzahl der übereinstimmenden Empfehlungen, die auftreten müssen, bevor der Workload Balancing die Empfehlung anwendet. Diese Einstellung ermutigt den Workload-Balancing, konservativere, stabilere Empfehlungen anzuwenden und das Potenzial für unvorsichtige VM-Verschiebungen zu verringern. Die Anzahl der Empfehlungen ist standardmäßig auf einen konservativen Wert festgelegt.

Aufgrund der potenziellen Auswirkungen, die die Anpassung dieser Einstellung auf Ihre Umgebung haben kann, ändern Sie sie nur mit äußerster Vorsicht. Nehmen Sie diese Anpassungen vorzugsweise vor, indem Sie den Wert testen und iterativ ändern oder unter Anleitung des technischen Supports von Citrix durchführen.

Schweregrad der Empfehlung

Alle Optimierungsempfehlungen enthalten einen Schweregrad (Kritisch, Hoch, Mittel, Niedrig), der die Bedeutung der Empfehlung angibt. Der Workload-Balancing basiert auf einer Kombination von Faktoren, einschließlich der folgenden:

- Konfigurationsoptionen, die Sie festlegen, wie Schwellenwerte und Metrik-Tunings
- Ressourcen, die für die Arbeitslast verfügbar sind
- Ressourcennutzungshistorie.

Der Schweregrad für eine Empfehlung wird im Bereich Optimierungsempfehlungen auf der Registerkarte WLB angezeigt.

Wenn Sie WLB so konfigurieren, dass Empfehlungen automatisch angewendet werden, können Sie den Mindestschweregrad festlegen, der einer Empfehlung zugeordnet werden soll, bevor der Workload Balancing diese automatisch anwendet.

Optimierung Aggressivität

Um zusätzliche Sicherheit bei der Ausführung im automatisierten Modus zu bieten, verfügt der Workload Balancing über Konsistenzkriterien für die automatische Annahme von Optimierungen. Dies kann dazu beitragen, das Verschieben von VMs aufgrund von Spikes und Anomalien zu verhindern. Im automatisierten Modus akzeptiert der Workload Balancing nicht die erste Empfehlung, die er erstellt. Stattdessen wartet der Workload Balancing darauf, eine Empfehlung automatisch anzuwenden, bis ein Host oder eine VM im Laufe der Zeit konsistentes Verhalten aufweist. Das konsistente Verhalten im Laufe der Zeit umfasst Faktoren wie z. B., 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 der Abgabe derselben Empfehlung festgelegt wird. Sie können konfigurieren, wie streng der Workload Balancing die Konsistenzkriterien anwenden soll, indem Sie die Einstellung Optimierungsaggressivität verwenden.

Wir haben in erster Linie die Einstellung Optimierung Aggressivität für Demonstrationszwecke konzipiert. Sie können diese Einstellung jedoch verwenden, um die gewünschte Stabilität in Ihrer Umgebung zu steuern, bevor der Workload Balancing eine Optimierungsempfehlung anwendet. Die stabilste Einstellung (Niedrige Aggressivität) ist standardmäßig konfiguriert. In diesem Zusammenhang bedeutet der Begriff stable die Ähnlichkeit der empfohlenen Änderungen im Laufe der Zeit, wie in diesem Abschnitt erläutert. Aggressivität ist in den meisten Umgebungen nicht wünschenswert. 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, variiert je nach Ebene, die Sie in der Einstellung Optimierungsaggressivität festgelegt haben. Je niedriger die Stufe (z. B. niedrig oder mittel), desto weniger aggressiv nimmt der Workload-Balancing eine Empfehlung an. Mit anderen Worten: Workload Balancing ist strenger, wenn die Aggressivität auf Niedrig eingestellt ist, Kriterien zu erfüllen (oder weniger kavalierender oder aggressiver).

Wenn die Aggressivitätsstufe beispielsweise auf Niedrig festgelegt ist, muss jedes Kriterium für Niedrig die Anzahl der durch den Empfehlungszähler angegebenen Male erreicht werden, bevor die Empfehlung automatisch angewendet wird.

Wenn Sie die Anzahl der Empfehlungen auf **3**festlegen, wartet der Arbeitslastausgleich, bis alle für Niedrig aufgeführten Kriterien erfüllt und in drei aufeinander folgenden Empfehlungen wiederholt werden. Diese Einstellung stellt sicher, dass die VM tatsächlich verschoben werden muss und dass der empfohlene Zielhost über einen längeren Zeitraum eine stabile Ressourcenauslastung hat. Dadurch wird das Potenzial reduziert, dass eine kürzlich verschobene VM aufgrund von Änderungen an der Hostleistung nach dem Verschieben von einem Host verschoben wird. Standardmäßig ist diese Einstellung auf eine konservative Einstellung (Niedrig) eingestellt, um die Stabilität zu fördern.

Wir empfehlen nicht, 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 Pool-Integritätsbericht.

Die Konsistenzkriterien, die mit den verschiedenen Ebenen der Aggressivität verbunden sind, sind die folgenden:

Niedrig:

- Alle VMs in nachfolgenden Empfehlungen müssen identisch sein (wie durch übereinstimmende UUIDs in jeder Empfehlung gezeigt).
- Alle Zielhosts müssen in nachfolgenden Empfehlungen identisch sein

- Die Empfehlung, die unmittelbar auf die erste Empfehlung folgt, muss übereinstimmen, andernfalls wird die Anzahl der Empfehlungen auf 1 zurückgesetzt.

Mittel:

- Alle VMs in nachfolgenden Empfehlungen müssen von demselben Host stammen, jedoch können sie sich von den VMs in der ersten Empfehlung unterscheiden.
- Alle Zielhosts müssen in nachfolgenden Empfehlungen 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 vom selben Host stammen. Die Empfehlungen müssen sich jedoch nicht sofort befolgen.
- Der Host, von dem der Workload-Balancing empfohlen hat, die VM zu verschieben, muss in jeder Empfehlung identisch sein
- Die Anzahl der Empfehlungen wird nicht auf 1 zurückgesetzt, wenn die beiden Empfehlungen, die der ersten Empfehlung folgen, nicht übereinstimmen

Beispiel

Im folgenden Beispiel wird veranschaulicht, wie Workload Balancing die Einstellung Optimierungsaggressivität und die Anzahl der Empfehlungen verwendet, um zu bestimmen, ob eine Empfehlung automatisch akzeptiert werden soll.

Die erste Spalte stellt die Empfehlungsnummer dar. Die zweite Spalte „Platzierungsempfehlungen“ stellt die Platzierungsempfehlungen dar, die beim Workload-Balancing die Optimierungsempfehlung abgegeben hat: Jede Empfehlung schlägt drei VM-Platzierungen vor. Die dritte, vierte und fünfte Spalte stellen die Auswirkungen der Einstellung Optimierungsaggressivität auf eine Gruppe von Platzierungsempfehlungen dar. Die Zeile bezeichnet die Gruppe, zum Beispiel **Empfehlung #1**. Die Zahl in den Aggressivitätsspalten ist die Anzahl der aufeinanderfolgenden Empfehlungen bei dieser Einstellung für die Optimierung Aggressivität. Beispiel: 1 in der Spalte Medium für Empfehlung #2 gibt an, dass die Empfehlung bei dieser Einstellung Optimierungsaggressivität nicht konsistent genug war. Der Zähler wurde auf 1 zurückgesetzt.

In den folgenden Beispielen wird die Anzahl der Empfehlungen nach Empfehlung #1, #2 und #3 weiter erhöht, wenn die Einstellung Optimierungsaggressivität auf Hoch festgelegt ist. Diese Erhöhung geschieht, obwohl die gleichen VMs nicht für neue Platzierungen in jeder Empfehlung empfohlen werden. Workload-Balancing wendet die Platzierungsempfehlung mit Empfehlung #3 an, da dieser Host für drei aufeinander folgende Empfehlungen dasselbe Verhalten hat.

Im Gegensatz dazu erhöht sich bei niedriger Aggressivität die Anzahl der aufeinander folgenden Empfehlungen nicht für die ersten vier Empfehlungen. Die Anzahl der Empfehlungen wird mit jeder Empfehlung auf 1 zurückgesetzt, da dieselben VMs für Platzierungen nicht empfohlen wurden. Die Anzahl der Empfehlungen beginnt erst zu erhöhen, wenn die gleiche Empfehlung in Empfehlung #5 abgegeben wurde. Schließlich wendet Workload Balancing automatisch die Empfehlung in Recommendation #6 an, nachdem es zum dritten Mal die gleichen Platzierungsempfehlungen ausgibt.

Empfehlung #1:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host B
- Verschieben von VM5 von Host A auf Host C

Hohe Aggressivität Empfehlung Anzahl: 1

Mittlere Aggressivität Empfehlung Anzahl: 1

Niedrige Aggressivität Empfehlung Anzahl: 1

Empfehlung #2:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host C
- Verschieben von VM7 von Host A auf Host C

Hohe Aggressivität Empfehlung Anzahl: 2

Mittlere Aggressivität Empfehlung Anzahl: 1

Niedrige Aggressivität Empfehlung Anzahl: 1

Empfehlung #3:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host C
- Verschieben von VM5 von Host A auf Host C

Hohe Aggressivität Empfehlung Anzahl: 3 (Bewerben)

Mittlere Aggressivität Empfehlung Anzahl: 1

Niedrige Aggressivität Empfehlung Anzahl: 1

Empfehlung #4:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host B
- Verschieben von VM5 von Host A auf Host C

Mittlere Aggressivität Empfehlung Anzahl: 2

Niedrige Aggressivität Empfehlung Anzahl: 1

Empfehlung #5:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host B
- Verschieben von VM5 von Host A auf Host C

Mittlere Aggressivität Empfehlung Anzahl: 3 (Bewerben)

Niedrige Aggressivität Empfehlung Anzahl: 2

Empfehlung #6:

- Verschieben von VM1 von Host A auf Host B
- Verschieben von VM3 von Host A auf Host B
- Verschieben von VM5 von Host A auf Host C

Niedrige Aggressivität Empfehlung Anzahl: 3 (Bewerben)

So konfigurieren Sie VM-Empfehlungsintervalle

1. Wählen Sie im Ressourcenbereich von XenCenter XenCenter >`your-pool`.
2. Klicken Sie im Bereich Eigenschaften 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, in denen Workload Balancing wartet, bevor eine weitere Optimierungsempfehlung auf einem neu ausbalancierten Host abgegeben wird.
    - Geben Sie im Feld Empfehlungen einen Wert für die Anzahl der Empfehlungen ein, die Workload-Balancing vorgeben soll, bevor eine Empfehlung automatisch angewendet wird.
    - Select einen Mindestschweregrad aus, bevor Optimierungen automatisch angewendet werden.
    - Ändern Sie, wie aggressiv Workload Balancing Optimierungsempfehlungen anwendet, wenn es im automatisierten Modus ausgeführt wird. Die Erhöhung des Aggressivitätsniveaus reduziert Beschränkungen für die Konsistenz von Empfehlungen, bevor sie automatisch angewendet werden. Die Einstellung „Optimierungsaggressivität“ ergänzt direkt die Einstellung „Anzahl der Empfehlungen“ (d. h. das Feld „Empfehlungen“).

> **Hinweis:**
>
> Wenn Sie „1" für den Wert in der Einstellung Empfehlungen eingeben, ist die Einstellung Optimierungsaggressivität nicht relevant.

So ändern Sie die Granularitätseinstellungen für den Pool Audit Trail

Gehen Sie folgendermaßen vor, um die Granularitätseinstellungen zu ändern:

1. Select den Pool in der Infrastrukturansicht aus, klicken Sie auf die Registerkarte WLB, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im linken Bereich auf Erweitert.
3. Klicken Sie auf der Seite „Erweitert" auf die Liste „ **Pool-Audit-Trail-Berichtgranularität** ", und wählen Sie eine Option aus der Liste aus.

   > **Wichtig:**
   >
   > Select die Granularität basierend auf Ihren Prüfprotokollanforderungen aus. Wenn Sie beispielsweise die Granularität des Überwachungsprotokollberichts auf Minimum festlegen, erfasst der Bericht nur eine begrenzte Datenmenge für bestimmte Benutzer und Objekttypen. Wenn Sie die Granularität auf Mittel festlegen, stellt der Bericht einen benutzerfreundlichen Bericht des Überwachungsprotokolls bereit. Wenn Sie die Granularität auf Maximum festlegen, enthält der Bericht detaillierte Informationen zum Überwachungsprotokollbericht. Das Festlegen des Überwachungsprotokollberichts auf Maximum kann dazu führen, dass der Workload Balancing-Server mehr Speicherplatz und Arbeitsspeicher benötigt.

4. Klicken Sie auf OK, um Ihre Änderungen zu bestätigen.

So zeigen Sie Pool-Audit-Trail-Berichte basierend auf Objekten in XenCenter an

Gehen Sie folgendermaßen vor, um Berichte von Pool Audit Trail basierend auf dem ausgewählten Objekt auszuführen und anzuzeigen:

1. Nachdem Sie die Einstellung „Pool-Audit-Trailgranularität" festgelegt haben, klicken Sie auf Berichte. Die Seite „Workload-Berichte" wird angezeigt.
2. Select im linken Bereich die Option Pool-Audit-Trail aus.
3. Sie können Berichte basierend auf einem bestimmten Objekt ausführen und anzeigen, indem Sie es in der Liste **Objekt** auswählen. Wählen Sie beispielsweise **Host** aus der Liste, um die Berichte allein auf Host basierenden.

Workload-Balancing verwalten

Dieser Abschnitt enthält Informationen zu den folgenden Themen:

- So konfigurieren Sie einen Pool für die Verwendung einer anderen virtuellen Workload Balancing-Appliance neu
- Trennen eines Pools von Workload Balancing oder vorübergehend Beenden von Workload Balancing
- Datenbankpflege
- Ändern der Konfigurationsoptionen

> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder für Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

Verwalten und Pflegen des Arbeitslastausgleichs

Nachdem der Workload Balancing für eine Weile ausgeführt wurde, müssen Sie möglicherweise Routineaufgaben ausführen, damit der Workload Balancing optimal ausgeführt werden kann. Diese Aufgaben können entweder durch Änderungen an Ihrer Umgebung (z. B. unterschiedliche IP-Adressen oder Anmeldeinformationen), Hardware-Upgrades oder routinemäßige Wartung entstehen.

Einige administrative Aufgaben, die Sie für den Workload Balancing ausführen möchten, sind:

- Verbinden oder erneutes Verbinden eines Pools mit einer virtuellen Workload-Balancing-Appliance
- Neukonfigurieren eines Pools für die Verwendung einer anderen virtuellen Workload Balancing-Appliance
- Umbenennen des Benutzerkontos „Workload Balancing“
- Trennen der virtuellen Workload-Balancing-Appliance von einem Pool
- Entfernen der virtuellen Appliance „Workload Balancing“
- Grundlegendes zu den rollenbasierten Zugriffssteuerungsberechtigungen Workload Balancing erfordert

Mit dem Workload Balancing können Sie einige Aspekte seines Verhaltens mithilfe einer Konfigurationsdatei, die als Datei wlb.conf bekannt ist, optimieren.

In diesem Abschnitt werden auch einige Aufgaben der Datenbankverwaltung für Benutzer erläutert, die an zusätzlichen Möglichkeiten zur Verwaltung der Datenbank „Workload Balancing“ interessiert sind.

Herstellen einer Verbindung mit der virtuellen Workload-Balancing-Appliance

Verbinden Sie nach der Konfiguration des Workload Balancing den Pool, den Sie verwalten möchten, mit der virtuellen Workload Balancing-Appliance über die CLI oder XenCenter. Ebenso müssen Sie möglicherweise irgendwann wieder eine Verbindung zur gleichen virtuellen Appliance herstellen.

Um das folgende XenCenter Verfahren abzuschließen, benötigen Sie Folgendes:

- Hostname (oder IP-Adresse) und Port der virtuellen Workload Balancing-Appliance.
- Anmeldeinformationen für den Ressourcenpool, den Workload Balancing überwachen soll.
- Anmeldeinformationen für das Konto, das Sie auf der virtuellen Appliance „Workload Balancing“ erstellt haben. Dieses Konto wird oft als Arbeitslastausgleich-Benutzerkonto bezeichnet. Citrix Hypervisor kommuniziert mit diesem Konto mit dem Workload Balancing. Sie haben dieses Konto auf der virtuellen Appliance „Workload Balancing“ während der Konfiguration des Workload Balancing erstellt.

Um den Hostnamen der virtuellen Appliance für den Workload Balancing anzugeben, der beim Herstellen einer Verbindung mit der virtuellen Appliance „Workload Balancing“ verwendet wird, fügen Sie zuerst den Hostnamen und die IP-Adresse dem DNS-Server hinzu.

Wenn Sie Zertifikate von einer Zertifizierungsstelle konfigurieren möchten, empfehlen wir, einen FQDN oder eine nicht ablaufende IP-Adresse anzugeben.

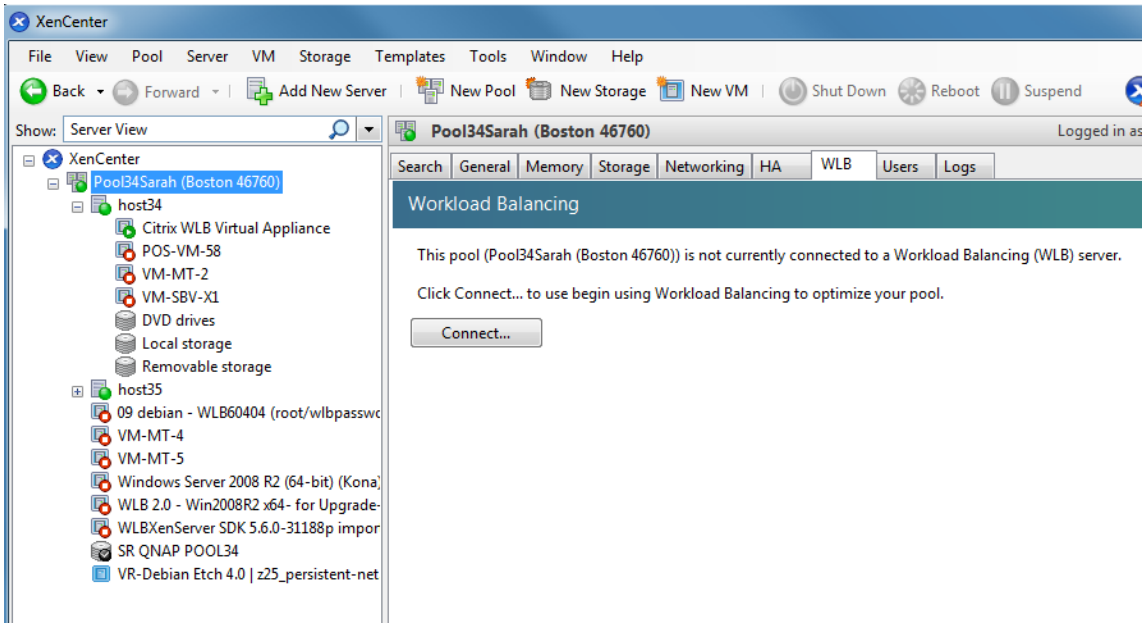
Wenn Sie zum ersten Mal eine Verbindung mit dem Workload Balancing herstellen, werden die Standardschwellenwerte und -einstellungen für den Ausgleich von Arbeitslasten verwendet. Automatische Funktionen wie automatisierter Optimierungsmodus, Energieverwaltung und Automatisierung sind standardmäßig deaktiviert.

> **Hinweis:**
>
> Der Workload Balancing ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die Citrix Website.

So verbinden Sie Ihren Pool mit der virtuellen Workload-Balancing-Appliance

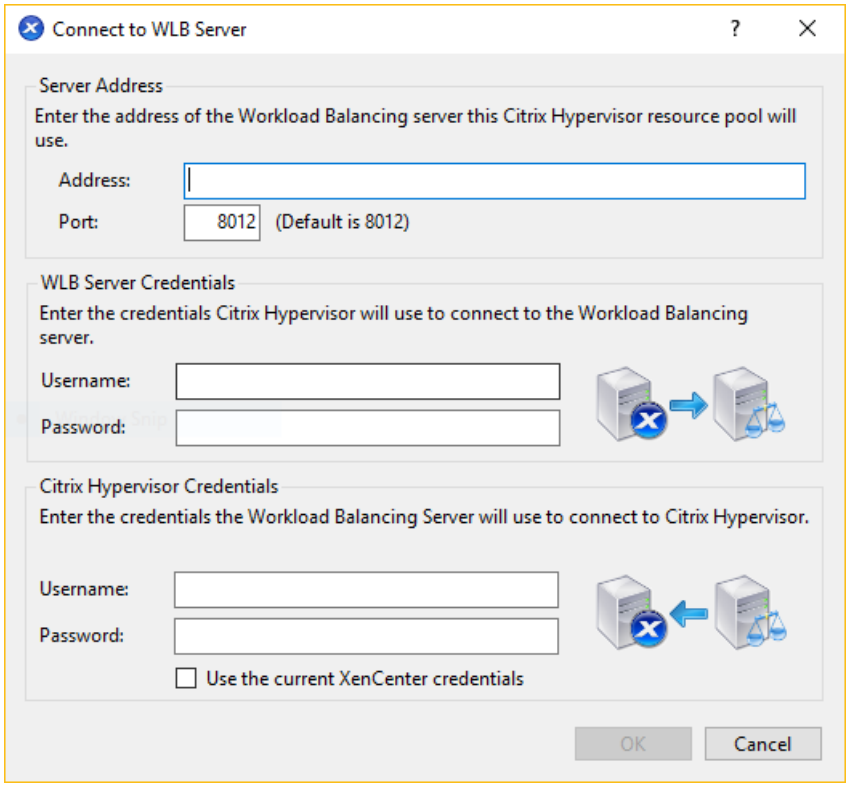
1. Wählen Sie im Ressourcenbereich von XenCenter XenCenter > `your-resource-pool`.
2. Klicken Sie im Bereich Eigenschaften auf die Registerkarte WLB.

   Auf der Registerkarte WLB wird die Schaltfläche Verbinden angezeigt.



3. Klicken Sie auf der Registerkarte WLB auf Verbinden.

   Das Dialogfeld Verbindung mit WLB-Server herstellen wird angezeigt.



4. Geben Sie im Abschnitt Serveradresse Folgendes ein:

   a) Geben Sie im Feld Adresse die IP-Adresse oder den FQDN der virtuellen Appliance „Workload Balancing“ ein (z. B.`your-WLB-appliance-computername.yourdomain.net`).

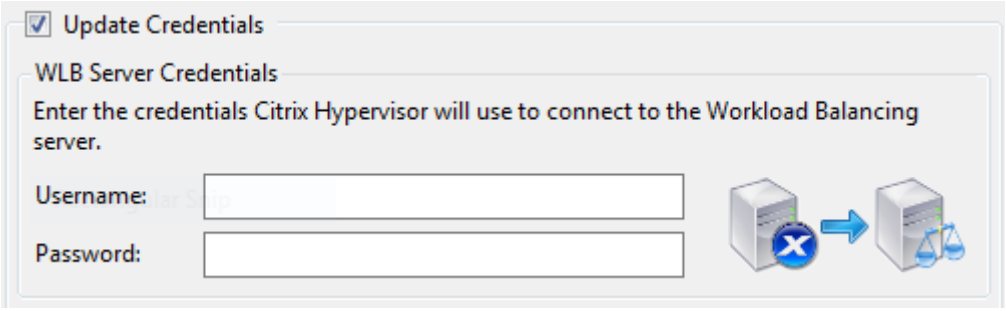
   > **Tipp:**
   >
   > Weitere Informationen finden Sie unter So erhalten Sie die IP-Adresse für die virtuelle WLB-Appliance.

   b) Geben Sie die Portnummer in das Feld Port ein. Citrix Hypervisor verwendet diesen Port für die Kommunikation mit dem Workload Balancing.

   Standardmäßig stellt Citrix Hypervisor eine Verbindung mit Workload Balancing (insbesondere dem Webdiensthostdienst) auf Port 8012 her. Wenn Sie die Portnummer während der Konfiguration des Arbeitslastausgleichs geändert haben, müssen Sie diese Portnummer hier eingeben.

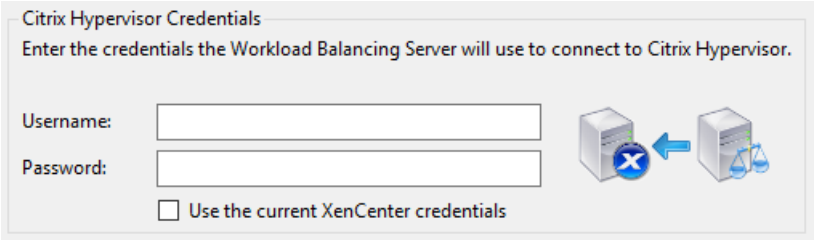
   > **Hinweis:**
   >
   > Verwenden Sie die Standardportnummer, es sei denn, Sie haben sie während der Konfiguration des Arbeitslastausgleichs geändert. Die bei der Konfiguration des Arbeitslastausgleichs, in allen Firewallregeln und im Dialogfeld Verbindung mit WLB-Server herstellen angegebene Portnummer muss übereinstimmen.

5. Geben Sie im Abschnitt WLB-Server-Anmeldeinformationen den Benutzernamen (z. B.`wlbuser`) und das Kennwort ein, mit dem der Pool eine Verbindung mit der virtuellen Workload Balancing-Appliance hergestellt wird.



   Diese Anmeldeinformationen müssen für das Konto sein, das Sie während der Konfiguration des Arbeitslastausgleichs erstellt haben. Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`.

6. Geben Sie im Abschnitt Citrix Hypervisor Anmeldeinformationen den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren. Der Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung mit den Citrix Hypervisor or-Servern in diesem Pool herzustellen.



   Aktivieren Sie das Kontrollkästchen Aktuelle XenCenter Anmeldeinformationen verwenden, um die Anmeldeinformationen zu verwenden, mit denen Sie aktuell bei Citrix Hypervisor angemeldet sind. Wenn Sie diesem Konto mithilfe der Zugriffssteuerungsfunktion (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 Workload Balancing.

7. 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 Protokoll anzeigt, dass die Erkennung abgeschlossen ist, bevor Sie fortfahren. Weitere Informationen finden Sie unter Ändern der Arbeitslastausgleichseinstellungen.

So erhalten Sie die IP-Adresse für die virtuelle WLB-Appliance

1. Select die virtuelle WLB-Appliance im Ressourcenbereich in XenCenter aus, und wählen Sie die Registerkarte Konsole aus.
2. Melden Sie sich bei der Appliance an. Geben Sie den VM-Benutzernamen (normalerweise „root“) und das Root-Kennwort ein, das Sie beim Importieren der Appliance erstellt haben.
3. Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
ifconfig
```

Zugriffssteuerungsberechtigungen für Workload Balancing

Wenn Role Based Access Control (Role Based Access Control, RBAC) in Ihrer Umgebung implementiert ist, können alle Benutzerrollen die Registerkarte WLB anzeigen. Allerdings können nicht alle Rollen alle Operationen ausführen. In der folgenden Tabelle sind die *Mindestrollen* aufgeführt, die Administratoren für die Verwendung von Workload Balancing-Features benötigen:

Aufgabe	Erforderliche Mindestrolle
Konfigurieren, Initialisieren, Aktivieren, Deaktivieren von WLB	Poolbetreiber
WLB-Optimierungsempfehlungen anwenden (auf der Registerkarte WLB)	Poolbetreiber
WLB-Berichtsabonnements ändern	Poolbetreiber
WLB-Platzierungsempfehlungen akzeptieren („Stern“ -Empfehlungen)	VM Power Admin
Erstellen von WLB-Berichten, einschließlich des Pool-Audit-Trail-Berichts	Schreibgeschützt
WLB-Konfiguration anzeigen	Schreibgeschützt

Definition von Berechtigungen

Die folgende Tabelle enthält weitere Details zu Berechtigungen.

Erlaubnis	Zugewiesene an
Konfigurieren, Initialisieren, Aktivieren, Deaktivieren von WLB	WLB konfigurieren
	WLB initialisieren und WLB-Server ändern
	WLB aktivieren

Erlaubnis	Zugewiesene an
	WLB deaktivieren
WLB-Optimierungsempfehlungen anwenden (auf der Registerkarte WLB)	Anwenden von Optimierungsempfehlungen, die auf der Registerkarte WLB angezeigt werden
WLB-Berichtsabonnements ändern	Ändern des erzeugten WLB-Berichts oder seines Empfängers
WLB-Platzierungsempfehlungen akzeptieren („Stern“ -Empfehlungen)	Select einen der Server aus, die Workload Balancing für die Platzierung empfiehlt („Stern“ Empfehlungen)
Erstellen von WLB-Berichten, einschließlich des Pool-Audit-Trail-Berichts	Anzeigen und Ausführen von WLB-Berichten, einschließlich des Pool-Audit-Trail-Berichts
WLB-Konfiguration anzeigen	WLB-Einstellungen für einen Pool anzeigen, wie auf der Registerkarte WLB dargestellt

Wenn ein Benutzer versucht, den Workload Balancing zu verwenden und dieser Benutzer nicht über ausreichende Berechtigungen verfügt, wird ein Dialogfeld für Rollenhöhen angezeigt. Weitere Hinweise zu RBAC finden Sie unterRollenbasierte Zugriffssteuerung.

Ermitteln des Status der virtuellen Workload-Balancing-Appliance

Führen Sie den`service workloadbalancing status` Befehl aus, wie in beschriebenWorkload-Balancing-Befehle .

Neukonfigurieren eines Pools für die Verwendung einer anderen WLB-Appliance

Sie können einen Ressourcenpool neu konfigurieren, um eine andere virtuelle Workload Balancing-Appliance zu verwenden.

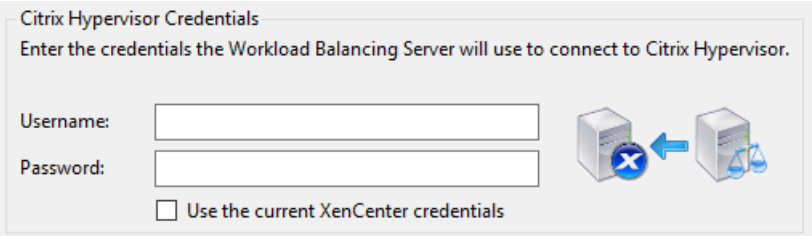
Um jedoch zu verhindern, dass die alte virtuelle Workload-Balancing-Appliance für einen Pool ausgeführt wird, stellen Sie sicher, dass Sie zuerst den Pool von der alten virtuellen Workload-Balancing-Appliance trennen.

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. Führen Sie die Schritte im folgenden Verfahren für den Pool aus, den Sie eine Verbindung mit einer anderen virtuellen Workload Balancing-Appliance herstellen möchten.

So verwenden Sie eine andere virtuelle Workload Balancing-Appliance:

1. Wählen Sie im Menü Pool die Option Workload Balancing Server trennen aus, und klicken Sie auf Trennen, wenn Sie dazu aufgefordert werden.
2. Klicken Sie auf der Registerkarte WLB auf Verbinden. Das Dialogfeld Verbindung mit WLB-Server herstellen wird angezeigt.
3. Geben Sie im Feld Adresse die IP-Adresse oder den FQDN des neuen Workload Balancing-Servers ein.
4. Geben Sie im Abschnitt WLB-Server-Anmeldeinformationen den Benutzernamen und das Kennwort ein, mit dem der Citrix Hypervisor Pool eine Verbindung mit der virtuellen Workload Balancing-Appliance hergestellt wird.

   Diese Anmeldeinformationen müssen für das Konto gelten, das Sie während der Konfiguration des Arbeitslastausgleichs für die neue virtuelle Appliance erstellt haben. Standardmäßig lautet der Benutzername für dieses Konto `wlbuser`.
5. Geben Sie im Abschnitt Citrix Hypervisor Anmeldeinformationen den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren (normalerweise das Kennwort für den Poolmaster). Der Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung mit den Hosts im Pool herzustellen.

   Aktivieren Sie das Kontrollkästchen Aktuelle XenCenter Anmeldeinformationen verwenden, um die Anmeldeinformationen zu verwenden, mit denen Sie aktuell bei Citrix Hypervisor angemeldet sind. Wenn Sie diesem Konto mithilfe der Zugriffssteuerungsfunktion (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 Workload Balancing.

Aktualisieren von Anmeldeinformationen für den Arbeitslastausgleich

Wenn Sie nach der Erstkonfiguration die Anmeldeinformationen von Citrix Hypervisor und der Workload Balancing-Appliance aktualisieren möchten, die für die Kommunikation verwendet werden, gehen Sie folgendermaßen vor:

1. Pausieren Sie den Arbeitslastausgleich, indem Sie auf der Registerkarte WLB auf Pause klicken.
2. Ändern Sie die WLB-Anmeldeinformationen, indem Sie den`wlbconfig` Befehl ausführen. Weitere Informationen finden Sie unter Arbeitslastausgleichsbefehle.

3. Aktivieren Sie den Workload Balancing erneut, und geben Sie die neuen Anmeldeinformationen an.
4. Klicken Sie nach Abschluss des Fortschrittsbalkens auf Verbinden.

   Das Dialogfeld Verbindung mit WLB-Server herstellen wird angezeigt.
5. Klicken Sie auf Anmeldeinformationen aktualisieren.
6. Ändern Sie im Abschnitt Serveradresse die folgenden Optionen wie gewünscht:
   - Geben Sie im Feld Adresse die IP-Adresse oder den FQDN der Workload Balancing-Appliance ein.
   - (Optional.) 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 Konfiguration des Arbeitslastausgleichs angeben, ist die Portnummer, die Citrix Hypervisor für die Verbindung mit dem Workload Balancing verwendet.

   Standardmäßig stellt Citrix Hypervisor eine Verbindung zum Workload Balancing auf Port 8012 her.

   > **Hinweis:**
   >
   > Bearbeiten Sie diese Portnummer nur, wenn Sie sie beim Ausführen des Assistenten für die Konfiguration des Arbeitslastausgleichs geändert haben. Der Wert der Portnummer, der beim Ausführen des Assistenten für die Konfiguration des Arbeitslastausgleichs und des Dialogfelds Verbindung mit WLB-Server angegeben wurde, muss übereinstimmen.
7. Geben Sie im Abschnitt WLB-Server-Anmeldeinformationen den Benutzernamen (z. B.`wlbuser`) und das Kennwort ein, mit dem die Computer, auf denen Citrix Hypervisor ausgeführt wird, um eine Verbindung mit dem Workload Balancing-Server herzustellen.
8. Geben Sie im Abschnitt Citrix Hypervisor Anmeldeinformationen den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren (normalerweise das Kennwort für den Poolmaster). Der Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung mit den Computern herzustellen, auf denen Citrix Hypervisor in diesem Pool ausgeführt wird.
9. Geben Sie im Abschnitt Citrix Hypervisor Anmeldeinformationen den Benutzernamen und das Kennwort für den Pool ein, den Sie konfigurieren. Der Workload Balancing verwendet diese Anmeldeinformationen, um eine Verbindung mit den Computern herzustellen, auf denen Citrix Hypervisor in diesem Pool ausgeführt wird.

Aktivieren Sie das Kontrollkästchen Aktuelle XenCenter Anmeldeinformationen verwenden, um die Anmeldeinformationen zu verwenden, mit denen Sie aktuell bei Citrix Hypervisor angemeldet sind.

Ändern der IP-Adresse des Arbeitslastausgleichs

Situationen, in denen Sie die

Gehen Sie folgendermaßen vor, um die IP-Adresse des Arbeitslastausgleichs zu ändern:

1. Beenden Sie die Workload-Balancing-Dienste, indem Sie den`service workloadbalancing stop` Befehl auf der virtuellen Appliance ausführen.
2. Ändern Sie die IP-Adresse des Arbeitslastausgleichs, indem Sie den`ifconfig` Befehl auf der virtuellen Appliance ausführen.
3. Aktivieren Sie den Workload Balancing erneut, und geben Sie die neue IP-Adresse an.
4. Starten Sie die Workload-Balancing-Dienste, indem Sie den`service workloadbalancing start` Befehl auf der virtuellen Appliance ausführen.

Arbeitslastausgleich stoppen

Da der Workload-Balancing auf Pool-Ebene konfiguriert ist, müssen Sie einen der folgenden Schritte ausführen, wenn die Verwaltung eines Pools beendet werden soll:

- **Arbeitslastausgleich anhalten**. Durch das Anhalten des Arbeitslastenausgleichs wird verhindert, dass XenCenter Empfehlungen für den angegebenen Ressourcenpool angezeigt und den Pool verwaltet. Das Pausieren ist für einen kurzen Zeitraum konzipiert und ermöglicht es Ihnen, die Überwachung fortzusetzen, ohne neu konfigurieren zu müssen. Wenn Sie den Arbeitslastausgleich anhalten, stoppt die Datensammlung für diesen Ressourcenpool, bis Sie den Arbeitslastausgleich erneut aktivieren.
- **Trennen Sie den Pool vom Arbeitslastausgleich**. Das Trennen der Verbindung zur virtuellen Appliance „Workload Balancing“ unterbricht die Verbindung zwischen dem Pool und löscht die Pooldaten nach Möglichkeit aus der Datenbank „Workload Balancing“. Wenn Sie die Verbindung zum Workload Balancing trennen, stoppt der Workload Balancing das Sammeln von Daten im Pool.

1. Wählen Sie im Ressourcenbereich von XenCenter den Ressourcenpool aus, für den Sie den Arbeitslastausgleich 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 wird.

   > **Tipp:**
   >
   > Um die Überwachung fortzusetzen, klicken Sie auf der Registerkarte WLB auf die Schaltfläche Fortsetzen.

3. Wählen Sie im Bereich Infrastruktur von XenCenter den Ressourcenpool aus, in dem Sie den Arbeitslastausgleich beenden möchten.
4. Wählen Sie im Menü Infrastruktur die Option *Workload Balancing Server trennen*aus. Das Dialogfeld „ *Workload Balancing Server trennen* “ wird angezeigt.

5. Klicken Sie auf Trennen, um die Überwachung des Pools durch den Workload Balancing zu beenden.

> **Tipp:**
>
> Wenn Sie den Pool von der virtuellen Workload Balancing-Appliance getrennt haben, müssen Sie erneut eine Verbindung mit einer Workload Balancing-Appliance herstellen, um den Workload Balancing in diesem Pool wieder zu aktivieren. Weitere Informationen finden Sie imHerstellen einer Verbindung mit der virtuellen Workload-Balancing-Appliance.

In den Wartungsmodus mit aktiviertem Arbeitslastausgleich wechseln

Wenn Sie einen Host in den Wartungsmodus versetzen, migriert Citrix Hypervisor die auf diesem Host ausgeführten VMs auf die optimalen Hosts, sofern verfügbar. Citrix Hypervisor migriert sie basierend auf Empfehlungen zum Workload Balancing (Performance-Daten, Ihre Platzierungsstrategie und Performance-Schwellenwerte).

Wenn kein optimaler Host verfügbar ist, werden die Wörter Klicken Sie hier, um die VM anzuhalten, im Dialogfeld Wartungsmodus eingeben angezeigt. Da in diesem Fall kein Host mit ausreichenden Ressourcen zum Ausführen der VM vorhanden ist, empfiehlt der Workload Balancing keine Platzierung. 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 eingeben“ erneut aufrufen, kann der Workload Balancing möglicherweise einen Host auflisten, der für die Migration geeignet ist.

> **Hinweis:**
>
> Wenn Sie einen Host für die Wartung offline schalten und den Arbeitslastausgleich aktiviert ist, werden im Assistenten zum Eingeben des Wartungsmodus die Wörter „Arbeitslastausgleich“ angezeigt.

So wechseln Sie mit aktiviertem Workload-Balancing in den Wartungsmodus:

1. Wählen Sie im Bereich Ressourcen von XenCenter den physischen Host aus, den Sie offline nehmen möchten. Wählen Sie im Menü Server die Option Wartungsmodus eingeben.
2. Klicken Sie im Dialogfeld Wartungsmodus eingeben auf Wartungsmodus eingeben. Die VMs, die auf dem Host ausgeführt werden, werden automatisch auf den optimalen Host migriert, basierend auf den Performance-Daten des Workload Balancing, Ihrer Platzierungsstrategie und Performance-Schwellenwerten.

Um den Wartungsmodus zu beenden, klicken Sie mit der rechten Maustaste auf den Host, und wählen Sie Wartungsmodus beenden. Wenn Sie einen Host aus dem Wartungsmodus entfernen, stellt Citrix Hypervisor die ursprünglichen VMs dieses Hosts automatisch auf diesem Host wieder her.

Vergrößern der Datenträgergröße des Arbeitslastausgleichs

In diesem Verfahren wird erläutert, wie Sie die Größe des virtuellen Laufwerks der virtuellen Appliance „Workload Balancing“ ändern. Fahren Sie die virtuelle Appliance herunter, bevor Sie diese Schritte ausführen. Der Arbeitslastausgleich ist ungefähr fünf Minuten lang nicht verfügbar.

> **Warnhinweis:**
>
> Wir empfehlen, einen Schnappschuss Ihrer Daten zu erstellen, bevor Sie dieses Verfahren ausführen. Falsches Ausführen dieser Schritte kann dazu führen, dass die virtuelle Workload Balancing-Appliance beschädigt wird.

1. Fahren Sie die virtuelle Appliance „Workload Balancing“ herunter.

   Wählen Sie im XenCenter Ressourcenbereich die virtuelle Appliance „Workload Balancing“ aus.
2. Klicken Sie auf die Registerkarte Speicher.
3. Select die Diskette „vdi_xvda“ und klicken Sie auf die Schaltfläche Eigenschaften.
4. Wählen Sie im Dialogfeld „vdi_xvda“ Eigenschaften die Option Größe und Speicherort aus.
5. Erhöhen Sie die Datenträgergröße nach Bedarf, und klicken Sie auf OK.
6. Starten Sie die virtuelle Appliance „Workload Balancing“, und melden Sie sich bei ihr an.
7. Führen Sie den folgenden Befehl auf der virtuellen Appliance „Workload Balancing“ aus:

   ```
   resize2fs /dev/xvda
   ```

   > **Hinweis:**
   >
   > Wenn das`resize2fs` Tool nicht installiert ist, stellen Sie sicher, dass Sie mit dem Internet verbunden sind, und installieren Sie es mit dem folgenden Befehl:
   >
   > `yum install -y --enablerepo=base,updates --disablerepo=citrix-* e2fsprogs`

Wenn es keinen Internetzugang gibt:

1. Laden Sie die folgenden von herunterhttp://mirror.centos.org/centos-7/7.2.1511/os/x86_64/Packages/.
   - `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 WLB VM hoch.
3. Führen Sie den folgenden Befehl von WLB-VM aus:

   ```
   rpm -ivh libss-\*.rpm e2fsprogs-\*.rpm
   ```


Das Tool`resize2fs` ist jetzt installiert.

4. Führen Sie den`df -h` Befehl aus, um die neue Datenträgergröße zu bestätigen.

Entfernen der virtuellen Appliance für den Arbeitslastausgleich

Es wird empfohlen, die virtuelle Workload Balancing-Appliance mithilfe der Standardprozedur zu entfernen, um VMs aus XenCenter zu löschen.

Wenn Sie die virtuelle Appliance „Workload Balancing“ 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 Appliance „Workload Balancing“ 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 Web 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 ist der PostgreSQL Benutzername postgres. Sie legen das Kennwort für dieses Konto während der Konfiguration des Arbeitslastausgleichs fest.

Die Menge an historischen Daten, die Sie speichern können, basiert auf der Größe des virtuellen Laufwerks, das WLB zugewiesen ist, und dem minimal erforderlichen Speicherplatz. Standardmäßig beträgt die Größe des virtuellen Laufwerks, das WLB zugewiesen ist, 20 GB. Weitere Informationen finden Sie unter Datenbankpflege Parameter.

Um viele historische Daten zu speichern, z. B. wenn Sie den Pool-Audit-Trail-Bericht aktivieren möchten, können Sie einen der folgenden Schritte ausführen:

- Vergrößern Sie die virtuelle Datenträgergröße, die der virtuellen Appliance „Workload Balancing“ zugewiesen ist. Importieren Sie dazu die virtuelle Appliance, und erhöhen Sie die Größe des virtuellen Laufwerks, indem Sie die Schritte unter ausführenVergrößern der Datenträgergröße des Arbeitslastausgleichs.
- Erstellen Sie periodische doppelte Sicherungskopien der Daten, indem Sie den Remote-Clientzugriff auf die Datenbank aktivieren und ein Datenbankverwaltungstool eines Drittanbieters verwenden.

Im Hinblick auf die Verwaltung der Datenbank können Sie den Speicherplatz steuern, den Datenbankdaten belegen, indem Sie die Datenbankpflege konfigurieren.

Zugriff auf die Datenbank

Für die virtuelle Appliance „Workload Balancing“ ist eine Firewall konfiguriert. Bevor Sie auf die Datenbank zugreifen können, müssen Sie den Postgresql-Serverport zu den iptables hinzufügen.

Führen Sie in der Konsole des virtuellen Arbeitslastausgleichs den folgenden Befehl aus:

```
1 iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
2 state --state NEW,ESTABLISHED -j ACCEPT
```

(Optional.) Führen Sie den folgenden Befehl aus, um diese Konfiguration nach dem Neustart der virtuellen Appliance zu erhalten:

```
1 iptables-save > /etc/sysconfig/potables
```

Datenbankpflege steuern

Die Workload Balancing-Datenbank löscht automatisch die ältesten Daten, wenn der VPX den minimalen Speicherplatz erreicht, der Workload Balancing benötigt. Standardmäßig ist der erforderliche Speicherplatz auf 1.024 MB festgelegt.

Die Datenbankbereinigungsoptionen für den Workload Balancing werden über die Datei wlb.conf gesteuert.

Wenn auf der virtuellen Appliance „Workload Balancing“ nicht genügend Speicherplatz vorhanden ist, beginnt der Workload Balancing automatisch die Pflege historischer Daten. Der Prozess ist wie folgt:

1. In einem vordefinierten Bereinigungsintervall prüft der Datensammler „Workload Balancing“, ob die Pflege erforderlich ist. Die Bereinigung ist erforderlich, wenn die Datenbankdaten bis zu dem Punkt gewachsen sind, an dem der einzige Speicherplatz, der nicht belegt bleibt, der minimal erforderliche Speicherplatz ist. Verwenden Sie`GroomingRequiredMinimumDiskSizeInMB` diese Option, um den minimalen 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 die Pflege erforderlich ist, beginnt der Workload Balancing mit der Pflege der Daten ab dem ältesten Tag. Der Workload-Balancing prüft dann, ob nun genügend Speicherplatz vorhanden ist, um die Mindestplatzanforderungen zu erfüllen.

3. Wenn bei der ersten Pflege nicht genügend Speicherplatz zur Verfügung steht, wiederholt der Workload Balancing die Pflege bis zu`GroomingRetryCounter` Zeiten, ohne`GroomingIntervalInHour` eine Stunde zu warten.

4. Wenn die erste oder wiederholte Pflege genügend Speicherplatz freigegeben hat, wartet der Workload Balancing`GroomingIntervalInHour` eine Stunde und kehrt zu Schritt 1 zurück.

5. Wenn die vom initiierte PflegeGroomingRetryCounter nicht genügend Speicherplatz frei hat, wartet der Workload-Balancing fürGroomingIntervalInHour eine Stunde und kehrt zu Schritt 1 zurück.

Datenbankpflege Parameter

Es gibt fünf Parameter in derwlb.conf Datei, die verschiedene Aspekte der Datenbankpflege steuern. Sie sind wie folgt:

- GroomingIntervalInHour. Steuert, wie viele Stunden vergehen, bevor die nächste Pflegeprüfung durchgeführt wird. Wenn Sie beispielsweise **1**eingeben, prüft Workload Balancing den Speicherplatz stündlich. Wenn Sie **2**eingeben, überprüft der Workload Balancing den Speicherplatz alle zwei Stunden, um festzustellen, ob die Pflege erfolgen muss.
- GroomingRetryCounter. Steuert, wie oft der Workload-Balancing versucht, die Bereinigung Datenbankabfrage erneut auszuführen.
- GroomingDBDataTrimDays. Steuert die Anzahl der Tage der Daten, die Workload Balancing bei jedem Versuch, Daten zu pflegen, aus der Datenbank gelöscht wird. Der Standardwert ist ein Tag.
- GroomingDBTimeoutInMinute. Steuert die Anzahl der Minuten, die die Datenbankpflege dauert, bevor das Timeout und abgebrochen wird. Wenn die Bereinigungsabfrage länger dauert als erwartet und nicht innerhalb des Zeitüberschreitungszeitraums ausgeführt wird, wird der Bereinigungstask abgebrochen. Der Standardwert ist 0 Minuten, was bedeutet, dass die Datenbankpflege niemals ein Timeout hat.
- GroomingRequiredMinimumDiskSizeInMB. Steuert die minimale Menge an freiem Speicherplatz auf dem virtuellen Laufwerk, das der virtuellen Appliance „Workload Balancing“ zugewiesen ist. Wenn die Daten auf dem virtuellen Laufwerk so lange wachsen, bis nur die minimale Festplattengröße auf dem virtuellen Laufwerk übrig bleibt, löst der Workload Balancing die Datenbankpflege aus. Der Standardwert ist 2.048 MB.

Informationen zum Bearbeiten dieser Werte finden Sie unterBearbeiten der Konfigurationsdatei für den Workload Balancing.

Ändern des Datenbankkennworts

Obwohl es möglich ist, das Datenbankkennwort mithilfe derwlb.conf Datei zu ändern, empfehlen wir, stattdessen denwlbconfig Befehl auszuführen. Weitere Informationen finden Sie unter Ändern der Konfigurationsoptionen für den Workload Balancing.

Datenbankdaten archivieren

Um zu vermeiden, dass ältere historische Daten gelöscht werden, können Sie optional Daten aus der Datenbank zur Archivierung kopieren. Dazu müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Clientauthentifizierung für die Datenbank.
2. Richten Sie die Archivierung mit dem PostgreSQL Datenbankverwaltungstool Ihrer Wahl ein.

Clientauthentifizierung für die Datenbank aktivieren

Sie können zwar direkt über die Workload Balancing-Konsole eine Verbindung zur Datenbank herstellen, aber Sie können auch ein PostgreSQL Datenbankverwaltungstool verwenden. Nachdem Sie ein Datenbankmanagement-Tool heruntergeladen haben, installieren Sie es auf dem System, von dem aus Sie eine Verbindung mit der Datenbank herstellen möchten. Sie können das Tool beispielsweise auf demselben Laptop installieren, auf dem XenCenter ausgeführt wird.

Bevor Sie die Remoteclientauthentifizierung für die Datenbank aktivieren können, müssen Sie:

1. Ändern Sie die Datenbankkonfigurationsdateien, einschließlich der Datei pg_hba.conf und der postgresql.conf, um Verbindungen zuzulassen.
2. Beenden Sie die Workload-Balancing-Dienste, starten Sie die Datenbank neu, und starten Sie die Workload-Balancing-Dienste neu.
3. Konfigurieren Sie im Datenbank-Management-Tool die IP-Adresse der Datenbank (d. h. die IP-Adresse des Workload Balancing VPX) und das Datenbankkennwort.

Ändern der Datenbankkonfigurationsdateien

Um die Clientauthentifizierung in der Datenbank zu aktivieren, müssen Sie zwei Dateien auf der virtuellen Appliance „Workload Balancing“ ändern: die Datei „pg_hba.conf“ und die Datei „postgresql.conf“.

So bearbeiten Sie die Datei pg_hba.conf:

1. Ändern Sie die Datei pg_hba.conf. Öffnen Sie in der Konsole der virtuellen Appliance Workload Balancing die Datei pg_hba.conf mit einem Editor, z. B. VI. Zum Beispiel:

   ```
   vi /var/lib/pgsql/9.0/data/pg_hba.conf
   ```

2. Wenn Ihr Netzwerk IPv4 verwendet, fügen Sie die IP-Adresse des angeschlossenen Computers zu dieser Datei hinzu. Zum Beispiel:

   Geben Sie im Abschnitt Konfiguration Folgendes ein`##IPv4 local connections`:

   - **TYP:** Host
   - **DATABASE:** alle
   - **BENUTZER:** alle

- **CIDR-ADRESSE:** 0.0.0.0/0
- **METHODE:** Vertrauen

3. Geben Sie Ihre IP-Adresse in das`CIDR-ADDRESS` Feld 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 nachfolgende „24" nach dem/definiert die Subnetzmaske und erlaubt nur Verbindungen von IP-Adressen innerhalb dieser Subnetzmaske.

   Wenn Sie`trust` für das`Method` Feld eingeben, kann sich die Verbindung authentifizieren, ohne dass ein Kennwort erforderlich ist. Wenn Sie`password` für das`Method` Feld eingeben, müssen Sie bei der Verbindung mit der Datenbank ein Kennwort angeben.

4. Wenn Ihr Netzwerk IPv6 verwendet, fügen Sie der Datei die IP-Adresse des verbindenden Computers hinzu. Zum Beispiel:

   Geben Sie unter`##IPv6 local connections`:

   - **TYP:** Host
   - **DATABASE:** alle
   - **BENUTZER:** alle
   - **CIDR-ADRESSE:::0/0"**
   - **METHODE:** Vertrauen

   Geben Sie die IPv6-Adressen in das`CIDR-ADDRESS` Feld ein. In diesem Beispiel`::0/0` wird die Datenbank für Verbindungen von beliebigen IPv6-Adressen geöffnet.

5. Speichern Sie die Datei und beenden Sie den Editor.

6. Nachdem Sie alle Datenbankkonfigurationen geändert haben, müssen Sie die Datenbank neu starten, um die Änderungen anzuwenden. Führen Sie den folgenden Befehl aus:

```
1 service postgresql-9.0 restart
```

So bearbeiten Sie die Datei postgresql.conf:

1. Ändern Sie die Datei postgresql.conf. Öffnen Sie in der Konsole der virtuellen Appliance Workload Balancing die Datei postgresql.conf mit einem Editor, z. B. VI. Zum Beispiel:

```
1 vi /var/lib/pgsql/9.0/data/postgresql.conf
```

2. Bearbeiten Sie die Datei so, dass sie auf jedem Port und nicht nur auf dem lokalen Host wartet. Zum Beispiel:

   a) Suchen Sie die folgende Zeile:

```
1 # listen_addresses='localhost'
```


b) Entfernen Sie das Kommentarsymbol (##) und bearbeiten Sie die Zeile folgendermaßen:

```
listen_addresses='*'
```

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Nachdem Sie alle Datenbankkonfigurationen geändert haben, müssen Sie die Datenbank neu starten, um die Änderungen anzuwenden. Führen Sie den folgenden Befehl aus:

```
service postgresql-9.0 restart
```

Ändern des Datenbankwartungsfensters

Der Workload-Balancing führt standardmäßig täglich um 12:05 Uhr GMT (00:05) eine routinemäßige Datenbankwartung durch. Während dieses Wartungsfensters erfolgt die Datenerfassung, aber die Aufzeichnung von Daten kann verzögert werden. In diesem Zeitraum sind jedoch die Steuerelemente der Benutzeroberfläche „Workload Balancing“ verfügbar, und der Workload Balancing gibt weiterhin Optimierungsempfehlungen aus.

> **Hinweis:**
>
> So vermeiden Sie einen Verlust des Arbeitslastausgleichs:
>
> - Während des Wartungsfensters wird der Arbeitslastausgleichsserver neu gestartet. Stellen Sie sicher, dass Sie Ihre VMs nicht gleichzeitig neu starten.
> - Wenn Sie alle VMs in Ihrem Pool neu starten, starten Sie den Workload Balancing-Server nicht neu.

Die Datenbankwartung umfasst die Freigabe von zugewiesenem nicht genutztem Speicherplatz und die Neuindizierung der Datenbank. Die Wartung dauert ca. 6 bis 8 Minuten. In größeren Pools kann die Wartung länger dauern, je nachdem, wie lange der Workload Balancing für die Erkennung dauert.

Abhängig von Ihrer Zeitzone können Sie die Zeit ändern, zu der die Wartung erfolgt. In der Zeitzone „Japan Standard Time (JST)“ erfolgt beispielsweise die Wartung des Arbeitslastausgleichs um 9:05 Uhr (09:05), was mit der Spitzenauslastung in einigen Organisationen in Konflikt steht. Wenn Sie eine saisonale Zeitänderung angeben möchten, z. B. Sommerzeit oder Sommerzeit, müssen Sie die Änderung in den eingegebenen Wert aufbauen.

So ändern Sie die Wartungszeit:

1. Führen Sie in der Workload Balancing-Konsole den folgenden Befehl aus einem beliebigen Verzeichnis aus:

```
crontab -e
```

Workload Balancing zeigt Folgendes an:


```
05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
```

Der Wert`05 0` stellt die Standardzeit dar, in der Workload Balancing Wartungsarbeiten in Minuten (05) und dann Stunden (0) durchführen soll. (Die Sternchen stellen den Tag, den Monat und das Jahr dar, in dem der Job ausgeführt wird: Bearbeiten Sie diese Felder nicht.) Der Eintrag`05 0` zeigt an, dass die Datenbankwartung um 12:05 Uhr oder 00:05 Uhr Greenwich Mean Time (GMT) jede Nacht stattfindet. Diese Einstellung bedeutet, dass die Wartung, wenn Sie in New York leben, um 19:05 Uhr (19:05) während der Wintermonate und 20:05 Uhr in den Sommermonaten durchgeführt wird.

> **Wichtig:**
>
> Bearbeiten Sie nicht den Tag, den Monat und das Jahr, in dem der Job ausgeführt wird (wie durch Sternchen dargestellt). Die Datenbankwartung muss täglich ausgeführt werden.

2. Geben Sie den Zeitpunkt ein, zu dem die Wartung in GMT erfolgen soll. Angenommen, die Wartung soll um Mitternacht ausgeführt werden:

Wenn Ihre Zeitzone…	UTC-Offset	Wert für Wartungsarbeiten um 12:05 Uhr Ortszeit	Wert in Sommerzeit
Pacific Zeitzone (PST) in den Vereinigten Staaten (z. B.	UTC-08	05 8	05 7
Japanische Standardzeit (JST)	UTC+09	05 15	Nicht zutreffend
Chinesische Standardzeit	UTC +08	04 15	Nicht zutreffend

1. Speichern Sie die Datei und beenden Sie den Editor.

Arbeitslastausgleich anpassen

Workload Balancing bietet verschiedene Anpassungsmethoden:

- **Befehlszeilen für Skripterstellung**. Siehe die Befehle unterWorkload-Balancing-Befehle.
- **Unterstützung für Host Power On Skripterstellung**. Sie können den Arbeitslastausgleich (indirekt) auch über das Host Power On Scripting anpassen.

Arbeitslastausgleich aktualisieren

Das Online-Upgrade von Workload Balancing wurde aus Sicherheitsgründen nicht mehr empfohlen. Kunden können kein Upgrade mehr mit dem yum Repo durchführen. Kunden können WLB auf die neueste Version aktualisieren, indem sie die neueste WLB VPX importieren, die unter heruntergeladen werden kannhttps://www.citrix.com/downloads/citrix-hypervisor/product-software/.

Problembehandlung beim Workload-Balancing

Während der Workload Balancing in der Regel reibungslos ausgeführt wird, bietet diese Reihe von Abschnitten Anleitungen für den Fall, dass Probleme auftreten.

Allgemeine Tipps zur Fehlerbehebung

- Starten Sie die Problembehandlung, indem Sie die Protokolldateien für den Workload Balancing (Logfile.log und wlb_install_log.log) überprüfen. Diese Protokolle finden Sie in der virtuellen Appliance „Workload Balancing“ an diesem Speicherort (standardmäßig):
  - /var/log/wlb
- Weitere (unterschiedliche) Informationen finden Sie in den Protokollen auf der Registerkarte XenCenter Protokolle.
- Um die Buildnummer der virtuellen Appliance Workload Balancing zu überprüfen, führen Sie den folgenden Befehl auf einem Hosts in einem Pool aus, den der VPX überwacht:

  ```
  1  xe pool-retrieve-wlb-diagnostics | more
  ```

  Die Versionsnummer des Workload Balancing wird oben in der Ausgabe angezeigt.

Fehlermeldungen

Workload Balancing zeigt Fehler auf dem Bildschirm als Dialogfelder und als Fehlermeldungen auf der Registerkarte Protokolle in XenCenter an.

Wenn eine Fehlermeldung angezeigt wird, lesen Sie das XenCenter Ereignisprotokoll nach weiteren Informationen. Informationen zum Speicherort dieses Protokolls finden Sie in der XenCenter Hilfe.

Probleme beim Eingeben von Anmeldeinformationen für den Workload Balancing

Wenn Sie das Benutzerkonto und das Kennwort der virtuellen Appliance nicht erfolgreich eingeben können, während Sie das Dialogfeld Verbindung mit WLB-Server herstellen konfigurieren, versuchen Sie Folgendes:

- Stellen Sie sicher, dass die virtuelle Appliance „Workload Balancing“ importiert und ordnungsgemäß konfiguriert wurde und alle zugehörigen Dienste ausgeführt werden. Weitere Informationen finden Sie unter [wlb-start] (#wlb -start).
- Stellen Sie sicher, dass Sie die richtigen Anmeldeinformationen eingeben. Die Standardanmeldeinformationen werden im Schnellstart des Arbeitslastausgleichs angezeigt.
- Sie können einen Hostnamen in das Feld Adresse eingeben, muss jedoch der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) der virtuellen Workload Balancing-Appliance sein. Geben Sie nicht den Hostnamen des physischen Servers ein, der die Appliance hostet. Beispiel: `yourcomputername`. 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 Citrix Hypervisor or-Server den Workload Balancing-Server über seinen FQDN kontaktieren kann. Führen Sie dazu einen Ping der Workload Balancing-Appliance mithilfe des FQDN vom Citrix Hypervisor or-Server aus. Geben Sie beispielsweise Folgendes in die Citrix Hypervisor-Serverkonsole ein:

```
1  ping wlb-vpx-1.mydomain.net
```

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: „Es ist ein Fehler beim Herstellen der Verbindung mit dem Workload-Balancing-Server aufgetreten: <pool name> Klicken Sie auf WLB initialisieren, um die Verbindungseinstellungen neu initialisieren. „ Dieser Fehler kann auch auftreten, wenn die Workload Balancing-Appliance ansonsten nicht erreichbar ist.

Auflösung:

Wenn sich die virtuelle Workload Balancing-Appliance hinter einer Firewall befindet, öffnen Sie Port 8012.

Ebenso muss der Port, der Citrix Hypervisor verwendet, um den Workload Balancing zu kontaktieren (standardmäßig 8012), mit der beim Ausführen des Assistenten für die Konfiguration des Workload Balancing angegebenen Portnummer übereinstimmen.

Verbindung zum Workload-Balancing verlieren

Wenn nach dem Konfigurieren und Herstellen einer Verbindung mit dem Workload Balancing ein Verbindungsfehler angezeigt wird, sind die Anmeldeinformationen möglicherweise nicht mehr gültig. Versuchen Sie, um dieses Problem zu isolieren:

- Überprüfen Sie, ob die Anmeldeinformationen, die Sie im Dialogfeld Mit WLB-Server verbinden eingegeben haben, mit den Anmeldeinformationen übereinstimmen:
  - Sie haben während der Konfiguration des Arbeitslastausgleichs erstellt
  - Auf Citrix Hypervisor (d. h. die Poolmasteranmeldeinformationen)
- Überprüfen der IP-Adresse oder des FQDN für die virtuelle Workload-Balancing-Appliance, die Sie im Dialogfeld Mit WLB-Server verbinden eingegeben haben, korrekt ist.
- Überprüfen Sie, ob der Benutzername, den Sie während der Konfiguration des Arbeitslastausgleichs erstellt haben, mit den Anmeldeinformationen übereinstimmt, die Sie im Dialogfeld Mit WLB-Server verbinden eingegeben haben.

Verbindungsfehler beim Workload Balancing

Wenn in der Zeile Workload Balancing Status auf der Registerkarte WLB ein Verbindungsfehler angezeigt wird, müssen Sie den Workload Balancing möglicherweise in diesem Pool neu konfigurieren.

Klicken Sie auf der Registerkarte WLB auf die Schaltfläche Verbinden, und geben Sie die Anmeldeinformationen des Servers erneut ein.

Workload Balancing funktioniert nicht mehr

Wenn der Workload Balancing nicht funktioniert (z. B. können Sie Änderungen an den Einstellungen nicht speichern), überprüfen Sie die Protokolldatei für den Workload Balancing auf die folgende Fehlermeldung:

```
1 dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
```

Ursache:

Dieser Fehler tritt normalerweise in Pools auf, die eine oder mehrere problematische VMs haben. Wenn VMs problematisch sind, wird möglicherweise das folgende Verhalten angezeigt:

- **Windows**. Die Windows VM stürzt aufgrund eines Stop-Fehlers („blauer Bildschirm“) ab.
- **Linux**. Die Linux-VM reagiert in der Konsole möglicherweise nicht und wird normalerweise nicht heruntergefahren.

Problemumgehung:

1. Erzwingen Sie das Herunterfahren der virtuellen Maschine. Dazu können Sie auf dem Host mit der problematischen VM eine der folgenden Aktionen ausführen:
   - Wählen Sie in XenCenter die VM aus, und klicken Sie dann im Menü VM auf Herunterfahren erzwingen.

- Führen Sie den Befehl`vm-shutdown` xe mit dem force Parameter true aus, wie im Citrix Hypervisor Administratorhandbuch beschrieben. Zum Beispiel:

  ```
  xe vm-shutdown force=true uuid=vm_uuid
  ```

  Sie finden die Host-UUID auf der Registerkarte Allgemein für diesen Host (in XenCenter) oder durch Ausführen des Befehls`host-list` xe. Sie finden die VM UUID auf der Registerkarte Allgemein für die VM oder durch Ausführen des Befehls`vm-list` xe. Weitere Informationen finden Sie unter Befehlszeilenschnittstelle.

2. Migrieren Sie in der xsconsole des Citrix Hypervisor, der die abgestürzte VM oder in XenCenter ausgeführt wird, alle VMs auf einen anderen Host, und führen Sie den`xe-toolstack-restart` Befehl aus.

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, Datensammlung und Webdienst.

> **Hinweis:**
>
> Verwenden Sie den Befehl`pool-deconfigure-wlb` xe nicht, um einen Pool von der virtuellen Workload Balancing-Appliance zu trennen, oder verwenden Sie den Befehl`pool-initialize-wlb` xe, um eine andere Appliance anzugeben.

Workload-Balancing-Befehle

Dieser Abschnitt enthält eine Referenz für die Befehle „Workload Balancing“. Sie können diese Befehle über den Citrix Hypervisor-Server oder die Citrix Hypervisorkonsole ausführen, um den Workload Balancing zu steuern oder Workload Balancing-Einstellungen auf dem Citrix Hypervisor-Server zu konfigurieren. Dieser Anhang enthält xe-Befehle und Dienstbefehle.

Führen Sie die folgenden Dienstbefehle auf der Workload Balancing-Appliance aus. Dazu müssen Sie sich bei der virtuellen Appliance „Workload Balancing“ anmelden.

Melden Sie sich bei der virtuellen Appliance für den Workload Balancing an

Bevor Sie Dienstbefehle ausführen oder die Datei wlb.conf bearbeiten können, müssen Sie sich bei der virtuellen Appliance „Workload Balancing“ anmelden. Dazu müssen Sie einen Benutzernamen und ein Kennwort eingeben. Melden Sie sich mit dem Stammbenutzerkonto an, sofern Sie keine zusätzlichen Benutzerkonten auf der virtuellen Appliance erstellt haben. Sie haben dieses Konto beim Ausführen des Assistenten für die Konfiguration des Arbeitslastausgleichs angegeben (bevor Sie Ihren Pool mit dem Workload Balancing verbunden haben). Sie können optional die Registerkarte Konsole in XenCenter verwenden, um sich bei der Appliance anzumelden.

So melden Sie sich bei der virtuellen Appliance „Workload Balancing“ an:

1. Geben Sie an der Anmeldeaufforderung „ *Name-of-your-WLB-VPX* “ den Benutzernamen des Kontos ein. Beispiel: Wo`wlb-vpx-pos-pool` ist der Name Ihrer Workload Balancing-Appliance:

   ```
   1 wlb-vpx-pos-pool login: root
   ```

2. Geben Sie an der Eingabeaufforderung Kennwort das Kennwort für das Konto ein:

   ```
   1 wlb-vpx-pos-pool login: root
   ```

   > **Hinweis:**
   >
   > Um sich von der virtuellen Appliance „Workload Balancing“ abzumelden, geben Sie einfach`logout` an der Eingabeaufforderung ein.

`wlb restart`

Führen Sie den`wlb restart` Befehl von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Workload Balancing Data Collection, Web Service und Data Analysis Services zu beenden und neu zu starten.

`wlb start`

Führen Sie den`wlb start` Befehl von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Workload Balancing Data Collection, Web Service und Data Analysis Services zu starten.

`wlb stop`

Führen Sie den`wlb stop` Befehl von einer beliebigen Stelle in der Workload Balancing-Appliance aus, um die Workload Balancing Data Collection, Web Service und Data Analysis Services zu stoppen.

`wlb status`

Führen Sie den`wlb status` Befehl 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 (Web Service, Data Collection Service und Data Analysis Service) angezeigt.

Ändern der Konfigurationsoptionen für den Workload Balancing

Viele Workload Balancing-Konfigurationen, wie die Datenbank- und Web-Service-Konfigurationsoptionen, werden in der Datei wlb.conf gespeichert. Die Datei wlb.conf ist eine Konfigurationsdatei auf der virtuellen Appliance „Workload Balancing“.

Um das Ändern der am häufigsten verwendeten Optionen zu erleichtern, stellt Citrix einen Befehl bereit`wlb config`. Wenn Sie den`wlb config` Befehl auf der virtuellen Appliance „Workload Balancing“ ausführen, können Sie das Benutzerkonto „Workload Balancing“ umbenennen, das Kennwort ändern oder das PostgreSQL Kennwort ändern. Nachdem Sie diesen Befehl ausgeführt haben, werden die Workload Balancing-Dienste neu gestartet.

So führen Sie den Befehl wlb config aus:

1. Führen Sie an der Eingabeaufforderung Folgendes aus:

```
1 wlb config
```

Auf dem Bildschirm werden eine Reihe von Fragen angezeigt, die Sie durch die Änderung des Benutzernamens und des Kennworts für den Workload Balancing und des PostgreSQL Kennworts führen. Befolgen Sie die Fragen auf dem Bildschirm, um diese Elemente zu ändern.

> **Wichtig:**
>
> Überprüfen Sie alle Werte, die Sie in der Datei wlb.conf eingeben: 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 kein Fehlerprotokoll.

Bearbeiten der Konfigurationsdatei für den Workload Balancing

Sie können die Konfigurationsoptionen für den Workload Balancing ändern, indem Sie die Datei wlb.conf bearbeiten, die im Verzeichnis /opt/vpx/wlb auf der virtuellen Appliance Workload Balancing gespeichert ist. Ändern Sie im Allgemeinen nur die Einstellungen in dieser Datei unter Anleitung von Citrix. Es gibt jedoch drei Kategorien von Einstellungen, die Sie bei Bedarf ändern können:

- **Kontoname und Kennwort des Arbeitslastausgleichs**. Es ist einfacher, diese Anmeldeinformationen zu ändern, indem Sie den`wlb config` Befehl ausführen.
- **Datenbankkennwort**. Dieser Wert kann mit der Datei wlb.conf geändert werden. Citrix empfiehlt jedoch, sie über den`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 Datei wlb.conf ändern möchten, müssen Sie eine Abfrage ausführen, um die Datenbank mit dem neuen Kennwort zu aktualisieren.
- **Datenbank-Grooming-Parameter**. Mithilfe dieser Datei können Sie Datenbankpflegeparameter ändern, z. B. das Datenbankpflegeintervall, indem Sie die Anweisungen im Abschnitt Datenbankverwaltung befolgen. In diesem Fall empfiehlt Citrix jedoch Vorsicht.

Für alle anderen Einstellungen in der Datei wlb.conf empfiehlt Citrix zurzeit, sie standardmäßig zu belassen, es sei denn, Citrix hat Sie angewiesen, sie zu ändern.

So bearbeiten Sie die Datei wlb.conf:

1. Führen Sie Folgendes an der Eingabeaufforderung auf der virtuellen Appliance „Workload Balancing“ aus (Beispiel VI):

   ```
   1 vi /opt/vpx/wlb/wlb.conf
   ```

   Auf dem Bildschirm werden verschiedene Abschnitte der Konfigurationsoptionen angezeigt.

2. Ändern Sie die Konfigurationsoptionen, und beenden Sie den Editor.

Nach dem Bearbeiten der Datei wlb.conf müssen Sie die Workload Balancing Services nicht neu starten. Die Änderungen treten unmittelbar nach dem Beenden des Editors in Kraft.

> **Wichtig:**
>
> Überprüfen Sie alle Werte, die Sie in der Datei wlb.conf eingeben: 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 kein Fehlerprotokoll.

Vergrößern der Details im Arbeitslastausgleichsprotokoll

Das Workload-Balancing-Protokoll enthält eine Liste der Ereignisse auf der virtuellen Workload-Balancing-Appliance, einschließlich Aktionen für das Analysemodul, die Datenbank und das Überwachungsprotokoll. Diese Protokolldatei befindet sich an folgendem Speicherort: /var/log/wlb/logfile.log.

Sie können, falls gewünscht, die Detailgenauigkeit des Workload Balancing-Protokolls erhöhen. Ändern Sie dazu den Abschnitt Ablaufverfolgungsflags der Konfigurationsdatei „Workload Balancing“ (wlb.conf), der sich an folgendem Speicherort befindet: /opt/vpx/wlb/wlb.conf. Geben Sie 1 oder true

ein, um die Protokollierung für eine bestimmte Ablaufverfolgung zu aktivieren, und 0 oder false, um die Protokollierung zu deaktivieren. Geben Sie beispielsweise Folgendes ein, um die Protokollierung für die Analysis Engine-Ablaufverfolgung zu aktivieren:

```
1 AnalEngTrace=1
```

Möglicherweise möchten Sie die Protokollierungsdetails erhöhen, bevor Sie ein Problem an den technischen Support von Citrix melden oder bei der Fehlerbehebung melden.

Protokollierungsoption	Ablaufverfolgungskennzeichen	Nutzen oder Zweck
Analyse-Engine-Ablaufverfolgung	`AnalEngTrace`	Protokolliert Details der Berechnungen der Analyse-Engine. Zeigt Details zu den Entscheidungen, die die Analyse-Engine trifft, und erhält möglicherweise Einblick in die Gründe, warum Workload Balancing keine Empfehlungen ausgibt.
Datenbank-Trace	`DatabaseTrace`	Protokolliert Details zu Datenbank-Lese-/Schreibvorgängen. Wenn Sie diese Ablaufverfolgung jedoch belassen, erhöht sich die Größe der Protokolldatei schnell.
Datenerfassungsverfolgung	`DataCollectionTrace`	Protokolliert die Aktionen zum Abrufen von Metriken. Mit diesem Wert können Sie die Metriken anzeigen, die Workload Balancing abruft und in den Workload Balancing-Datenspeicher eingefügt wird. Wenn Sie diese Ablaufverfolgung jedoch belassen, erhöht sich die Größe der Protokolldatei schnell.

Protokollierungsoption	Ablaufverfolgungskennzeichen	Nutzen oder Zweck
Verfolgung der Datenkomprimierung	`DataCompactionTrace`	Protokolliert Details darüber, wie viele Millisekunden es gedauert hat, um die Metrikdaten zu komprimieren.
Datenereignisverfolgung	`DataEventTrace`	Diese Ablaufverfolgung enthält Details zu Ereignissen, die Workload Balancing von XenServer abfangen.
Datenpflege Ablaufverfolgung	`DataGroomingTrace`	Diese Ablaufverfolgung enthält Details zur Datenbankpflege.
Datenmetrikverfolgung	`DataMetricsTrace`	Protokolliert Details zum Analysieren von Metrikdaten. Wenn diese Ablaufverfolgung eingeschaltet wird, erhöht sich die Größe der Protokolldatei schnell.
Warteschlangenverwaltung Ablaufverfolgung	`QueueManagementTrace`	Protokolliert Details zur Datenerfassungswarteschlangenverwaltung. (Diese Option ist für den internen Gebrauch geeignet.)
Datenspeicher-Ablaufverfolgung	`DataSaveTrace`	Protokolliert Details zum Pool, der in der Datenbank gespeichert wird.

Protokollierungsoption	Ablaufverfolgungskennzeichen	Nutzen oder Zweck
Host-Trace bewerten	`ScoreHostTrace`	Protokolliert Details darüber, wie der Workload Balancing zu einem Score für einen Host kommt. Diese Ablaufverfolgung zeigt die detaillierten Ergebnisse, die durch den Workload Balancing generiert werden, wenn die Sternbewertungen für die Auswahl der optimalen Server für die VM-Platzierung berechnet werden.
Überwachungsprotokollablauf\	`AuditLogTrace`	Zeigt die Aktion der Überwachungsprotokoll-daten an, die erfasst und geschrieben werden. (Diese Option ist nur für die interne Verwendung bestimmt und enthält keine Informationen, die im Überwachungsprotokoll erfasst werden.) Wenn Sie diese Ablaufverfolgung jedoch belassen, erhöht sich die Größe der Protokolldatei schnell.
Zeitgesteuerte Task-Ablaufverfolgung	`ScheduledTaskTrace`	Protokolliert Details zu geplanten Tasks. Wenn beispielsweise Änderungen im geplanten Modus nicht funktionieren, können Sie diese Ablaufverfolgung aktivieren, um die Ursache zu untersuchen.

Protokollierungsoption	Ablaufverfolgungskennzeichen	Nutzen oder Zweck
Webdienstablaufverfolgung	`WlbWebServiceTrace`	Protokolliert Details über die Kommunikation mit der Web-Service-Schnittstelle.

Kopiert!
Failed!

Zertifikate für den Workload-Balancing

October 16, 2019

Dieser Abschnitt enthält Informationen zu zwei optionalen Aufgaben zum Sichern von Zertifikaten:

- Konfigurieren von Citrix Hypervisor zum Überprüfen eines Zertifikats von einer vertrauenswürdigen Behörde
- Konfigurieren von Citrix Hypervisor zum Überprüfen des selbstsignierten Citrix WLB-Standardzertifikats

Übersicht

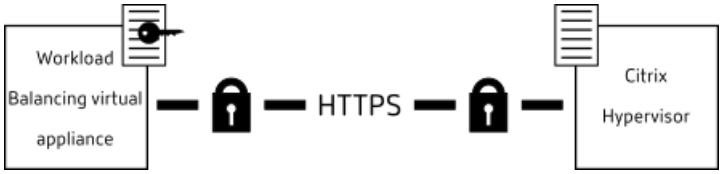
Citrix Hypervisor und Workload Balancing kommunizieren über HTTPS. Folglich erstellt der Assistent während der Konfiguration des Workload Balancing automatisch ein selbstsigniertes Testzertifikat. Mit diesem selbstsignierten Testzertifikat kann Workload Balancing eine SSL-Verbindung mit Citrix Hypervisor hergestellt werden.

> **Hinweis:**
>
> Das selbstsignierte Zertifikat ist ein Platzhalter zur Erleichterung der HTTPS-Kommunikation und stammt nicht von einer vertrauenswürdigen Zertifizierungsstelle. Für zusätzliche Sicherheit empfehlen wir die Verwendung eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Standardmäßig erstellt Workload Balancing diese SSL-Verbindung mit Citrix Hypervisor automatisch. Sie müssen während oder nach der Konfiguration keine Zertifikatkonfigurationen durchführen, damit der Workload Balancing diese SSL-Verbindung erstellt werden kann.

Wenn Sie jedoch ein Zertifikat einer anderen Zertifizierungsstelle verwenden möchten, z. B. ein signiertes Zertifikat einer kommerziellen Behörde, müssen Sie den Workload Balancing und Citrix Hypervisor so konfigurieren, dass es verwendet wird.

Unabhängig davon, welches Zertifikat Workload Balancing verwendet, überprüft Citrix Hypervisor die Identität des Zertifikats standardmäßig nicht, bevor eine Verbindung zum Workload Balancing hergestellt wird. Um Citrix Hypervisor für die Überprüfung nach einem bestimmten Zertifikat zu konfigurieren, müssen Sie das Stammzertifikat exportieren, das zum Signieren des Zertifikats verwendet wurde, in Citrix Hypervisor kopieren und Citrix Hypervisor so konfigurieren, dass es überprüft wird, wenn eine Verbindung zum Workload Balancing hergestellt wird. In diesem Szenario fungiert Citrix Hypervisor als Client und Workload Balancing fungiert als Server.



Abhängig von Ihren Sicherheitszielen können Sie entweder:

- Konfigurieren Sie Citrix Hypervisor, um das selbstsignierte Testzertifikat zu überprüfen. Siehe Konfigurieren von Citrix Hypervisorzum Überprüfen des selbstsignierten Zertifikats.
- Konfigurieren Sie Citrix Hypervisor, um ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu überprüfen. Siehe Konfigurieren von Citrix Hypervisorzum Überprüfen eines Zertifikatzertifikats.

Konfigurieren von Citrix Hypervisor zum Überprüfen des selbstsignierten Zertifikats

Sie können Citrix Hypervisor so konfigurieren, dass das selbstsignierte Citrix WLB-Zertifikat authentisch ist, bevor Citrix Hypervisor Workload Balancing eine Verbindung zulässt.

> **Wichtig:**
>
> Um das selbstsignierte Citrix WLB-Zertifikat zu überprüfen, müssen Sie mithilfe des Hostnamens eine Verbindung zum Workload Balancing herstellen. Führen Sie den`hostname` Befehl auf der virtuellen Appliance aus, um den Hostnamen des Arbeitslastausgleichs zu suchen.

Wenn Sie den Workload Balancing so konfigurieren möchten, dass das selbstsignierte Citrix WLB-Zertifikat überprüft wird, führen Sie die Schritte im folgenden Verfahren aus.

So konfigurieren Sie Citrix HypervisorSo überprüfen Sie das selbstsignierte Zertifikat:

1. Kopieren Sie das selbstsignierte Zertifikat von der virtuellen Workload Balancing-Appliance in den Poolmaster. Das selbstsignierte Citrix WLB-Zertifikat wird unter /etc/ssl/certs/server.pemgespeichert. Führen Sie Folgendes auf dem Poolmaster aus, um das Zertifikat zu kopieren:

```
scp root@wlb-ip:/etc/ssl/certs/server.pem .
```


2. Wenn Sie eine Meldung erhalten, dass die Authentizität von`wlb-ip` nicht hergestellt werden kann, geben Sie ein,`yes` um fortzufahren.
3. Geben Sie das Stammkennwort für die virtuelle Appliance Workload Balancing ein, wenn Sie dazu aufgefordert werden. Das Zertifikat wird in das aktuelle Verzeichnis kopiert.
4. Installieren Sie das Zertifikat. Führen Sie den`pool-certificate-install` Befehl aus dem Verzeichnis aus, in das Sie das Zertifikat kopiert haben. Zum Beispiel:

```
1 xe pool-certificate-install filename=server.pem
```

5. Überprüfen Sie, ob das Zertifikat ordnungsgemäß installiert wurde, indem Sie den`pool-certificate-list` Befehl auf dem Poolmaster ausführen:

```
1 xe pool-certificate-list
```

   Wenn Sie das Zertifikat ordnungsgemäß installiert haben, enthält die Ausgabe dieses Befehls das exportierte Stammzertifikat (z. B. server.pem). Wenn Sie diesen Befehl ausführen, werden alle installierten SSL-Zertifikate aufgelistet, einschließlich des soeben installierten Zertifikats.

6. Synchronisieren Sie das Zertifikat vom Master mit allen Hosts im Pool, indem Sie den`pool-certificate-sync` Befehl auf dem Poolmaster ausführen:

```
1 xe pool-certificate-sync
```

   Wenn`pool-certificate-sync` Sie den Befehl auf dem Master ausführen, werden die Zertifikat- und Zertifikatsperrlisten auf allen Poolservern mit dem Master synchronisiert. Dadurch wird sichergestellt, dass alle Hosts im Pool dieselben Zertifikate verwenden.

   Es gibt keine Ausgabe von diesem Befehl. Der nächste Schritt funktioniert jedoch nicht, wenn dieser nicht erfolgreich funktioniert hat.

7. Weisen Sie Citrix Hypervisor an, das Zertifikat zu überprüfen, bevor Sie eine Verbindung mit der virtuellen Workload Balancing-Appliance herstellen. Führen Sie den folgenden Befehl auf dem Poolmaster aus:

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

   > **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) Führen Sie den`pool-certificate-list` Befehl auf diesen Hosts aus, um zu testen, ob das Zertifikat mit den anderen Hosts im Pool synchronisiert wurde.

b) Um zu testen, ob Citrix Hypervisor zum Überprüfen des Zertifikats festgelegt wurde, führen Sie den`pool-param-get` Befehl mit dem Parameter`param-name` =wlb-verify-cert aus. Zum Beispiel:

```
xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
```

Konfigurieren von Citrix Hypervisor zum Überprüfen eines Zertifikatzertifikats

Sie können Citrix Hypervisor so konfigurieren, dass ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat überprüft wird.

Für vertrauenswürdige Autoritätszertifikate benötigt Citrix Hypervisor ein exportiertes Zertifikat oder eine Zertifikatkette (das Zwischen- und Stammzertifikat) im PEM-Format, das den öffentlichen Schlüssel enthält.

Wenn der Workload Balancing ein Zertifikat der vertrauenswürdigen Autorität verwenden soll, gehen Sie folgendermaßen vor:

1. Beziehen Sie ein signiertes Zertifikat von der Zertifizierungsstelle. Siehe Aufgabe 1: Beschaffung eines Zertifikatszertifikats.
2. Befolgen Sie die Anweisungen unterAufgabe 2: Angeben des neuen Zertifikats, um das neue Zertifikat anzugeben und anzuwenden.
3. Installieren Sie die erhaltenen Zertifikate und aktivieren Sie die Zertifikatüberprüfung auf dem Poolmaster. Siehe Aufgabe 3: Importieren der Zertifikatkette in den Pool.

Bevor Sie mit diesen Tasks beginnen, stellen Sie sicher:

- Sie kennen die IP-Adresse für den Citrix Hypervisor Poolmaster.
- Citrix Hypervisor kann den Hostnamen des Workload Balancing auflösen. (Sie können beispielsweise versuchen, den FQDN „Workload Balancing“ über die Citrix Hypervisor Konsole für den Poolmaster zu pingen.)

> **Wichtig:**
>
> Wenn Sie eine IP-Adresse zum Herstellen einer Verbindung mit dem Workload Balancing verwenden möchten, müssen Sie diese IP-Adresse als alternativen Antragstellernamen (Subject Alternative Name, SAN) angeben, wenn Sie das Zertifikat erstellen.

Aufgabe 1: Beschaffung eines Zertifikatszertifikats

Um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, müssen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren. Das Generieren einer CSR für die virtuelle

Appliance „Workload Balancing“ ist ein zweistufiger Prozess. Sie müssen (1) einen privaten Schlüssel erstellen und (2) diesen privaten Schlüssel verwenden, um die CSR zu generieren. Beide Verfahren müssen auf der virtuellen Appliance „Workload Balancing“ ausgeführt werden.

Richtlinien für die Angabe des allgemeinen Namens

Der Common Name (CN), den Sie beim Erstellen einer CSR angeben, muss genau mit dem FQDN Ihrer virtuellen Workload Balancing-Appliance und dem FQDN oder der IP-Adresse übereinstimmen, die Sie im Dialogfeld Mit WLB-Server verbinden im Feld Adresse angegeben haben.

Um sicherzustellen, dass der Name übereinstimmt, geben Sie den allgemeinen Namen mit einer der folgenden Richtlinien an:

- Geben Sie dieselben Informationen für den allgemeinen Namen des Zertifikats an, wie Sie im Dialogfeld Mit WLB-Server verbinden angegeben haben. Wenn Ihre virtuelle Workload-Balancing-Appliance beispielsweise benannt ist`wlb-vpx.yourdomain`, geben Sie`wlb-vpx.yourdomain`im Bereich Verbindung mit WLB-Server an und geben`wlb-vpx.yourdomain`Sie beim Erstellen der CSR den allgemeinen Namen an.
- Wenn Sie Ihren Pool über eine IP-Adresse mit dem Workload Balancing verbunden haben, verwenden Sie den FQDN als Common Name, und geben Sie die IP-Adresse als Subject Alternative Name (SAN) an. Dies funktioniert jedoch möglicherweise nicht in allen Situationen.

> **Hinweis:**
>
> Die Zertifikatüberprüfung ist eine Sicherheitsmaßnahme, um unerwünschte Verbindungen zu verhindern. Daher müssen Workload Balancing-Zertifikate strenge Anforderungen erfüllen, da sonst die Zertifikatüberprüfung nicht erfolgreich ist und Citrix Hypervisor die Verbindung nicht zulässt. Ebenso müssen Sie die Zertifikate an den bestimmten Speicherorten speichern, an denen Citrix Hypervisor erwartet, dass die Zertifikate gefunden werden.

So erstellen Sie eine private Schlüsseldatei:

1. Erstellen Sie eine private Schlüsseldatei:

```
openssl genrsa -des3 -out privatekey.pem 2048
```

2. Entfernen Sie das Kennwort:

```
openssl rsa -in privatekey.pem -out privatekey.nop.pem
```

> **Hinweis:**
>
> Wenn Sie das Kennwort falsch oder inkonsistent eingeben, erhalten Sie möglicherweise einige Meldungen, die darauf hinweisen, dass ein Benutzerschnittstellenfehler vorliegt. Sie können die Nachricht ignorieren und den Befehl einfach erneut ausführen, um die private Schlüsseldatei zu

> erstellen.

So generieren Sie die CSR:

1. Erstellen Sie die CSR:

   a) Erstellen Sie die CSR mit dem privaten Schlüssel:

   ```
   openssl req -new -key privatekey.nop.pem -out csr
   ```

   b) Folgen Sie den Anweisungen, um die Informationen bereitzustellen, die für die Erstellung der CSR erforderlich sind:

   Name des Landes. Geben Sie die Ländercodes des SSL-Zertifikats für Ihr Land ein. Beispiel: CA für Kanada oder JM für Jamaika. Eine Liste der Ländercodes des SSL-Zertifikats finden Sie im Internet.

   Name des Bundesstaates oder der Provinz (vollständiger Name). Geben Sie den Bundesstaat oder die Provinz ein, in der sich der Pool befindet. Zum Beispiel Massachusetts oder Alberta.

   Name des Ortes. Der Name der Stadt, in der sich der Pool befindet.

   Organisationsname. Der Name Ihres Unternehmens oder Ihrer Organisation.

   Name der Organisationseinheit. Geben Sie den Abteilungsnamen ein. Dieses Feld ist optional.

   Gemeinsamer Name. Geben Sie den FQDN Ihres Workload-Balancing-Servers ein. Dies muss mit dem Namen übereinstimmen, den der Pool für die Verbindung mit dem Workload Balancing verwendet.

   E-Mail-Adresse. Diese E-Mail-Adresse ist im Zertifikat enthalten, wenn Sie es generieren.

   c) Geben Sie optionale Attribute an, oder klicken Sie auf Eingabetaste, um die Bereitstellung dieser Informationen zu überspringen.

   Die CSR-Anforderung wird im aktuellen Verzeichnis gespeichert und trägt den Namen`csr`.

2. Zeigen Sie die CSR im Konsolenfenster an, indem Sie die folgenden Befehle in der Workload Balancing-Appliance-Konsole ausführen:

   ```
   cat csr
   ```

3. Kopieren Sie die gesamte Zertifikatsanforderung, und verwenden Sie die CSR, um das Zertifikat von der Zertifizierungsstelle anzufordern.

Aufgabe 2: Festlegen des neuen Zertifikats

Gehen Sie wie folgt vor, um anzugeben, dass der Workload Balancing ein Zertifikat von einer Zertifizierungsstelle verwendet. Diese Prozedur installiert die Stamm- und (falls verfügbar) Zwischenzertifikate.

So geben Sie ein neues Zertifikat an:

1. Laden Sie das signierte Zertifikat, das Stammzertifikat und, falls die Zertifizierungsstelle eines besitzt, das Zwischenzertifikat von der Zertifizierungsstelle herunter.
2. Wenn Sie die Zertifikate nicht auf die virtuelle Workload Balancing-Appliance heruntergeladen haben. Führen Sie einen der folgenden Schritte aus:

   a) Wenn Sie die Zertifikate von einem Windows Computer auf die Workload Balancing-Appliance kopieren, verwenden Sie WinSCP oder ein anderes Kopierdienstprogramm, um die Dateien zu kopieren.

   Für den Hostnamen können Sie die IP-Adresse eingeben und den Port standardmäßig belassen. Der Benutzername und das Kennwort sind in der Regel root und das Kennwort, das Sie während der Konfiguration festlegen.

   a) Wenn Sie die Zertifikate von einem Linux-Computer auf die Workload Balancing-Appliance kopieren, verwenden Sie SCP oder ein anderes Kopierdienstprogramm, um die Dateien in das Verzeichnis Ihrer Wahl auf der Workload Balancing-Appliance zu kopieren. Zum Beispiel:

   ```
   1 scp root_ca.pem root@wlb-ip:/path_on_your_WLB
   ```

3. Verbinden Sie auf der virtuellen Appliance „Workload Balancing“ den Inhalt aller Zertifikate (Stammzertifikat, Zwischenzertifikat (falls vorhanden) und signiertes Zertifikat) in einer Datei. Zum Beispiel:

   ```
   1 cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
   ```

4. Benennen Sie das vorhandene Zertifikat und den Schlüssel mit dem Befehl move um:

   ```
   1 mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
   2 mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
   ```

5. Kopieren Sie das zusammengeführte Zertifikat:

   ```
   1 mv server.pem /etc/ssl/certs/server.pem
   ```

6. Kopieren Sie den zuvor erstellten privaten Schlüssel:


```
mv privatekey.nop.pem /etc/ssl/certs/server.key
```

7. Machen Sie den privaten Schlüssel nur durch root lesbar. Verwenden Siechmod den Befehl, um Berechtigungen zu beheben.

```
chmod 600 /etc/ssl/certs/server.key
```

8. Neustartstunnel:

```
killall stunnel
stunnel
```

Aufgabe 3: Importieren der Zertifikatkette in den Pool

Nach dem Abrufen von Zertifikaten müssen Sie die Zertifikate auf den Citrix Hypervisor Poolmaster importieren (installieren) und die Hosts im Pool synchronisieren, um diese Zertifikate zu verwenden. Anschließend können Sie Citrix Hypervisor so konfigurieren, dass die Identität und Gültigkeit des Zertifikats jedes Mal überprüft wird, wenn der Workload Balancing eine Verbindung mit einem Host herstellt.

1. Kopieren Sie das signierte Zertifikat, das Stammzertifikat und, falls die Zertifizierungsstelle eines besitzt, das Zwischenzertifikat von der Zertifizierungsstelle auf den Citrix Hypervisor Poolmaster.
2. Installieren Sie das Stammzertifikat auf dem Poolmaster:

```
xe pool-certificate-install filename=root_ca.pem
```

3. Installieren Sie ggf. das Zwischenzertifikat auf dem Poolmaster:

```
xe pool-certificate-install filename=intermediate_ca.pem
```

4. Überprüfen Sie sowohl die Zertifikate ordnungsgemäß installiert, indem Sie diesen Befehl auf dem Poolmaster ausführen:

```
xe pool-certificate-list
```

   Wenn Sie diesen Befehl ausführen, werden alle installierten SSL-Zertifikate aufgelistet. Wenn die Zertifikate erfolgreich installiert wurden, werden sie in dieser Liste angezeigt.

5. Synchronisieren Sie das Zertifikat auf dem Poolmaster mit allen Hosts im Pool:

```
xe pool-certificate-sync
```


Wenn`pool-certificate-sync` Sie den Befehl auf dem Master ausführen, werden die Zertifikate und Zertifikatsperrlisten auf allen Poolservern mit dem Poolmaster synchronisiert. Dadurch wird sichergestellt, dass alle Hosts im Pool dieselben Zertifikate verwenden.

6. Weisen Sie Citrix Hypervisor an, ein Zertifikat zu überprüfen, bevor Sie eine Verbindung mit der virtuellen Workload Balancing-Appliance herstellen. Führen Sie den folgenden Befehl auf dem Poolmaster aus:

```
xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

> **Tipp:**
>
> Durch Drücken der Tabulatortaste wird automatisch die UUID des Pools aufgefüllt.

7. Wenn Sie vor der Aktivierung der Zertifikatüberprüfung im Dialogfeld Mit WLB verbinden eine IP-Adresse angegeben haben, werden Sie möglicherweise aufgefordert, den Pool erneut mit dem Workload Balancing zu verbinden.

   Geben Sie in diesem Fall den **FQDN** für die Workload Balancing-Appliance im Feld Adresse im Dialogfeld Mit WLB verbinden *genau so an, wie er im Common Name (CN) des Zertifikats angezeigt wird* . (Sie müssen den FQDN eingeben, da der allgemeine Name und der Name, den Citrix Hypervisor für die Verbindung verwendet, übereinstimmen müssen.)

Tipps zur Fehlerbehebung

- Wenn der Pool nach der Konfiguration der Zertifikatüberprüfung keine Verbindung mit dem Workload Balancing herstellen kann, überprüfen Sie, ob der Pool eine Verbindung herstellen kann, wenn Sie die Zertifikatüberprüfung deaktivieren (durch Ausführen`xe pool-param-set wlb-verify-cert=false uuid=uuid_of_pool`). Wenn es eine Verbindung mit der Überprüfung aus herstellen kann, liegt das Problem in der Zertifikatkonfiguration. Wenn es keine Verbindung herstellen kann, liegt das Problem entweder in den Anmeldeinformationen für den Workload Balancing oder in der Netzwerkverbindung.
- Einige kommerzielle Zertifizierungsstellen stellen stellen Tools zur Verfügung, um das ordnungsgemäß installierte Zertifikat zu überprüfen. Erwägen Sie, diese Tools auszuführen, wenn diese Prozeduren das Problem nicht isolieren können. Wenn für diese Tools ein SSL-Port angegeben werden muss, geben Sie Port 8012 oder einen beliebigen Port an, den Sie während der Konfiguration des Arbeitslastausgleichs festlegen.
- Wenn nach diesen Verfahren eine Fehlermeldung auf der Registerkarte WLB angezeigt wird, die besagt: „Es ist ein Fehler beim Herstellen der Verbindung mit dem WLB-Server aufgetreten“, kann es zu einem Konflikt zwischen dem allgemeinen Namen im Zertifikat und dem Namen der virtuellen Workload-Balancing-Appliance kommen. Der Name der virtuellen Appliance Workload Balancing und der allgemeine Name des Zertifikats müssen genau übereinstimmen.

Kopiert!
Failed!

Konvertierungs-Manager

October 16, 2019

Mit Citrix Hypervisor Conversion Manager können Sie Workloads von VMware zu Citrix Hypervisor migrieren, indem Stapel virtueller VMware-Maschinen in Ihre Citrix Hypervisor-Umgebung verschoben werden.

Citrix Hypervisor Conversion Manager vereinfacht die Migration und ermöglicht mehr als nur die Konvertierung virtueller Maschinen. Citrix Hypervisor Conversion Manager unterstützt Sie bei der Vorbereitung der virtuellen Maschinen auf Netzwerk- und Speicherkonnektivität. Nach der Konvertierung sind die virtuellen Maschinen fast betriebsbereit.

Konvertieren von VMware zu Citrix Hypervisor

Mit Citrix Hypervisor Conversion Manager können Sie:

- Konvertieren mehrerer VMs mit einem einfachen Assistenten
- Ordnen Sie Netzwerkeinstellungen zwischen VMware und Citrix Hypervisor zu, damit Ihre konvertierten VMs mit den richtigen Netzwerkeinstellungen ausgeführt werden können
- Select einen Speicherort aus, an dem Ihre neuen Citrix Hypervisor VMs ausgeführt werden sollen.

> **Hinweise:**
>
> - Citrix Hypervisor Conversion Manager entfernt oder ändert Ihre vorhandene VMware Umgebung nicht. VMs werden in Ihrer Citrix Hypervisor Umgebung dupliziert und nicht aus VMware entfernt.
> - Citrix Hypervisor Conversion Manager ist für Citrix Hypervisor Premium Edition-Kunden oder Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor 8.0 Lizenz zu erwerben, besuchen Sie dieCitrix Website.

Grundlegendes zu Citrix Hypervisor

Bevor Sie Ihre Umgebung konvertieren können, sollten Sie sich mit den Citrix Hypervisor Konzepten vertraut machen. Weitere Informationen finden Sie unter Technische Übersicht.

Führen Sie die folgenden Aufgaben aus, um Citrix Hypervisor Conversion Manager erfolgreich zu verwenden:

- Einrichten einer grundlegenden Citrix Hypervisor-Umgebung, einschließlich der Installation von Citrix Hypervisor. Weitere Informationen finden Sie unter. Schnellstart] (/de-de/citrix-hypervisor/quick-start.html) undInstallieren.
- Erstellen eines Netzwerks in Citrix Hypervisor und Zuweisen einer IP-Adresse zu einer Netzwerkkarte. Weitere Informationen finden Sie unter Schnellstart.
- Anschluss an den Speicher. Weitere Informationen finden Sie unter Schnellstart.

> **Hinweis:**Die Dokumentation zu
>
> Citrix Hypervisor ist über docs.citrix.com verfügbar, Knowledge Center-Artikel und Whitepaper sind verfügbar im Citrix Knowledge Center.

Vergleichen der VMware und Citrix Hypervisor -Terminologie

In der folgenden Tabelle sind die ungefähren Citrix Hypervisor Äquivalent für allgemeine VMware Features, Konzepte und Komponenten aufgeführt:

VMware Begriff	Citrix Hypervisor Äquivalent
VMware vSphere Client	XenCenter (die Verwaltungskonsole für Citrix Hypervisor)
Cluster/Ressourcenpool	Ressourcenpool
Datenspeicher	Speicher-Repository
vMotion	Live-Migration
Verteilte Ressourcenplanung (DRS)	Arbeitslastausgleich
Hochverfügbarkeit (HA)	Hochverfügbarkeit (HA)
vCenter Konverter	Citrix Hypervisor Konvertierungs-Manager
Rollenbasierte Zugriffssteuerung (RBAC)	Rollenbasierte Zugriffssteuerung (RBAC)

Konvertierungsübersicht

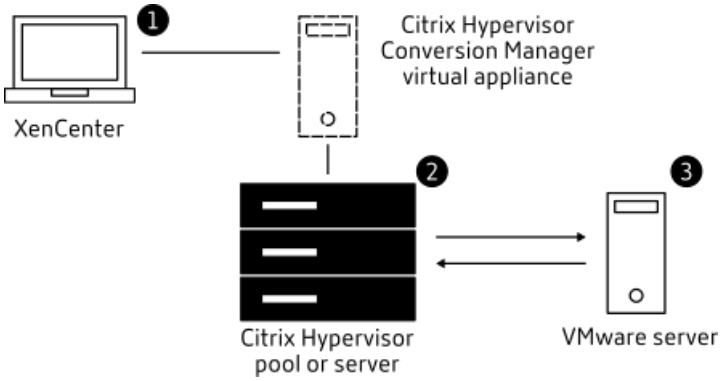
Citrix Hypervisor Conversion Manager erstellt eine Kopie jeder Ziel-VM. Nachdem die Ziel-VM in eine Citrix Hypervisor VM mit vergleichbarer Netzwerk- und Speicherkonnektivität konvertiert wurde, importiert sie die VM in Ihren Citrix Hypervisor-Pool oder -Host. Mit Citrix Hypervisor Conversion Manager können Sie nur ein oder zwei VMs konvertieren oder Batchkonvertierungen einer gesamten Umgebung durchführen.

> **Hinweis:**
>
> Bevor Sie die VMs von vSphere konvertieren, müssen Sie die VMs (für die Konvertierung vorgesehen) auf vSphere herunterfahren. Die aktuelle Version von Citrix Hypervisor Conversion Manager unterstützt die Konvertierung einer ausgeführten VM mit Speicher, der von vSphere in Citrix Hypervisor kopiert wurde.

Der Conversion-Manager-Konvertierungsprozess von Citrix Hypervisor erfordert vier Elemente:

- **Citrix Hypervisor Conversion Manager-Konsole** - die Benutzeroberfläche, auf der Sie Konvertierungsoptionen und Steuerkonvertierung festlegen. Sie können die Konsole auf Ihrem Windows oder einem lokalen Linux-Desktop installieren. Citrix Hypervisor Conversion Manager erfordert eine Verbindung mit Citrix Hypervisor und der Citrix Hypervisor Conversion Manager Virtual Appliance.
- **Citrix Hypervisor Conversion Manager Virtual Appliance** - eine vorkonfigurierte VM, die Sie in den Citrix Hypervisor-Host oder -Pool importieren, auf dem Sie die konvertierten VMs ausführen möchten. Die virtuelle Appliance konvertiert die Kopien der VMware VMs in das virtuelle Citrix Hypervisor Computerformat. Nach der Konvertierung werden diese Kopien in den Citrix Hypervisor-Pool oder -Host importiert.
- **Standalone-Host oder -Pool von Citrix Hypervisor** — die Citrix Hypervisor Umgebung, in der die konvertierten VMs ausgeführt werden sollen.
- **VMware Server**. Citrix Hypervisor Conversion Manager erfordert 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 erfolgen. Die VMs werden nicht vom VMware Server entfernt. Stattdessen erstellt die Citrix Hypervisor Conversion Manager Virtual Appliance eine Kopie dieser VMs und konvertiert sie in Citrix Hypervisor Virtual-Machine-Format.

Die folgende Abbildung zeigt die Beziehungen zwischen diesen Komponenten:



> Diese Abbildung zeigt:
>
> 1. Kommunikation von Citrix Hypervisor Conversion Manager mit Citrix Hypervisor Conversion Manager Virtual Appliance
> 2. Wie sich die Citrix Hypervisor Conversion Manager Virtual Appliance beim VMware Server authentifiziert.
> 3. Wie der VMware Server während der Konvertierung auf die virtuelle Citrix Hypervisor Conversion Manager-Appliance reagiert.

Der VMware Server kommuniziert nur dann mit der Citrix Hypervisor Conversion Manager Virtual Appliance, wenn die Appliance den VMware Server während der Konvertierung nach Umgebungsinformationen und Datenträgerdaten abfragt.

Zusammenfassung der Konvertierung von VMs

Sie können den Citrix Hypervisor Conversion Manager konfigurieren und mit der Konvertierung von VMs beginnen:

1. Laden Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance und die Citrix Hypervisor Conversion Manager-Konsole vom herunter[Seite Citrix Hypervisor 8.0 Premium Edition].
2. Importieren Sie die virtuelle Citrix Hypervisor Conversion Manager Appliance mit XenCenter in den Citrix Hypervisor.
3. Konfigurieren Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance mit XenCenter.
4. Installieren Sie die Citrix Hypervisor Conversion Manager-Konsole.
5. Starten Sie in der Citrix Hypervisor Conversion Manager-Konsole den Konvertierungsassistenten, und beginnen Sie mit der Konvertierung von VMs.

In den folgenden Abschnitten werden diese Schritte im Detail erläutert. Informationen sind auch in der Citrix Hypervisor Conversion Manager-Hilfe verfügbar, die in der Citrix Hypervisor Conversion Manager-Konsole angezeigt wird.

Bereiten Sie Ihre Umgebung vor

Bevor Sie Ihre VMware Umgebung konvertieren, müssen Sie den eigenständigen Citrix Hypervisor-Host oder -Umgebung für die Ausführung der konvertierten VMware s erstellen und vorbereiten. Die Vorbereitung Ihrer Umgebung umfasst die folgenden Aktivitäten:

1. Definieren Sie eine Strategie für die Konvertierung Ihrer VMware Umgebung. Möchten Sie nur 1 oder 2 VMs konvertieren? Möchten Sie Ihre gesamte Umgebung umwandeln? Möchten Sie zuerst ein Pilotprojekt erstellen, um sicherzustellen, dass Ihre Konfiguration korrekt ist? Führen Sie beide Umgebungen parallel aus? Möchten Sie Ihren vorhandenen Cluster-Entwurf beibehalten, wenn Sie in Citrix Hypervisor konvertieren?
2. Planen der Netzwerkkonfiguration. Möchten Sie eine Verbindung zu denselben physischen Netzwerken herstellen? Möchten Sie Ihre Netzwerkkonfiguration vereinfachen oder ändern?
3. Installieren von Citrix Hypervisor auf den Hosts, die im Pool verwendet werden sollen. Idealerweise sollten Sie die Netzwerkkarten auf den Hosts an ihre physischen Netzwerke anschließen, bevor Sie mit der Installation beginnen.
4. Erstellen eines Pools und Ausführen einer grundlegenden Netzwerkkonfiguration. Gehen Sie beispielsweise folgendermaßen vor:
   - Konfigurieren Sie ein Netzwerk für die Verbindung mit dem VMware Cluster auf dem Citrix Hypervisor Host (wenn sich der Cluster nicht im selben Netzwerk wie der Citrix Hypervisor-Host befindet).
   - Konfigurieren Sie ein Netzwerk für die Verbindung mit dem Speicher-Array. Wenn Sie also IP-basierten Speicher verwenden, erstellen Sie ein Citrix Hypervisor Netzwerk, das eine Verbindung mit dem physischen Netzwerk des Speicher-Arrays herstellt.
   - Erstellen Sie einen Pool und fügen Sie Hosts zu diesem Pool hinzu.
5. (Für gemeinsam genutzten Speicher und Citrix Hypervisor Pools.) Vorbereiten des gemeinsam genutzten Speichers, in dem Sie die virtuellen Laufwerke speichern, und Erstellen einer Verbindung mit dem Speicher, das als Speicher-Repository (SR) im Pool bezeichnet wird.
6. (Optional.) Obwohl keine Konvertierung erforderlich ist, sollten Sie die Administratorkonten im Citrix Hypervisor Pool so konfigurieren, dass sie diesen Konten auf dem VMware Server entsprechen. Informationen zum Konfigurieren der rollenbasierten Zugriffssteuerung für Active Directory Konten finden Sie in der XenCenter Hilfe oderSchnellstart.

Installieren von Citrix Hypervisor und Erstellen eines Pools

Bevor Sie VMware VMs konvertieren können, stellen Sie sicher, dass Sie einen Citrix Hypervisor-Pool oder Host erstellen, auf dem die konvertierten VMs ausgeführt werden sollen. Für diesen Pool muss

ein Netzwerk konfiguriert sein, damit eine Verbindung mit dem VMware Server hergestellt werden kann. Sie können auch die gleichen physischen Netzwerke im Citrix Hypervisor Pool konfigurieren, die Sie im VMware Cluster haben, oder die Netzwerkkonfiguration vereinfachen. Wenn Sie die konvertierten VMs in einem Pool ausführen möchten, erstellen Sie vor der Konvertierung ein Speicher-Repository, und fügen Sie den freigegebenen Speicher dem Pool hinzu.

Wenn Sie mit Citrix Hypervisor noch nicht vertraut sind, können Sie die Grundlagen von Citrix Hypervisor, einschließlich der grundlegenden Installation und Konfiguration, lesenSchnellstart.

Überlegungen zur Citrix Hypervisor Umgebung

Berücksichtigen Sie vor der Installation von Citrix Hypervisor und dem Importieren der virtuellen Appliance die folgenden Faktoren, die Ihre Konvertierungsstrategie möglicherweise ändern:

Wählen Sie den Host aus, auf dem die Citrix Hypervisor Conversion Manager Virtual Appliance ausgeführt werden soll. Importieren Sie die virtuelle Appliance in den eigenständigen Host oder in einen Host im Pool, auf dem Sie die konvertierten VMs ausführen.

Bei Pools können Sie die virtuelle Appliance auf jedem Host im Pool ausführen, vorausgesetzt, der Speicher erfüllt die Speicheranforderungen.

Der für den Pool oder den Host konfigurierte Speicher, auf dem die konvertierten VMs ausgeführt werden sollen, muss bestimmte Anforderungen erfüllen. Wenn Sie die neu konvertierten VMs in einem Pool ausführen möchten, müssen die virtuellen Laufwerke im freigegebenen Speicher gespeichert werden. Wenn die konvertierten VMs jedoch auf einem einzelnen eigenständigen Host (kein Pool) ausgeführt werden, können ihre virtuellen Laufwerke lokalen Speicher verwenden.

Wenn Sie die konvertierten VMs in einem Pool ausführen möchten, stellen Sie sicher, dass Sie den gemeinsam genutzten Speicher zum Pool hinzufügen, indem Sie ein Speicher-Repository erstellen.

Für die Konvertierung unterstützte Gastbetriebssysteme. Citrix Hypervisor Conversion Manager unterstützt die Konvertierung von VMware VMs, auf denen jedes der von Citrix Hypervisor unterstützten Windows Gastbetriebssysteme ausgeführt wird. Eine Liste der von Citrix Hypervisor unterstützten Windows Gastbetriebssysteme finden Sie unter Unterstützung für Gastbetriebssysteme. Die folgenden Linux-Betriebssysteme werden ebenfalls unterstützt.

- RHEL 5,4/5,6/6,4/7,0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 14.04/16.04

Erfüllung der Netzwerkanforderungen

Um VMware VMs zu konvertieren, benötigt die Citrix Hypervisor Conversion Manager Virtual Appliance eine Verbindung 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 Citrix Hypervisor Pool, fügen Sie das Netzwerk vor der Konvertierung zu Citrix Hypervisor hinzu.

Zuordnen der vorhandenen Netzwerkkonfiguration

Citrix Hypervisor Conversion Manager enthält Funktionen, mit denen die manuelle Netzwerkkonfiguration reduziert werden kann, die nach der Konvertierung von vorhandenen VMware VMs in Citrix Hypervisor erforderlich ist. Citrix Hypervisor Conversion Manager beispielsweise:

- Bewahren Sie virtuelle MAC-Adressen auf den VMware s auf und verwenden Sie sie in den resultierenden Citrix Hypervisor VMs erneut. Die Beibehaltung der mit virtuellen Netzwerkadaptern verknüpften MAC-Adressen (virtuelle MAC-Adressen) kann:
  - Schutz von IP-Adressen in Umgebungen mit DHCP
  - Nutzen Sie für Softwareprogramme, deren Lizenzierung auf die virtuellen MAC-Adressen verweist
- Zuordnen (virtueller) Netzwerkadapter. Citrix Hypervisor Conversion Manager kann VMware Netzwerke Citrix Hypervisor Netzwerken zuordnen, sodass nach der Konvertierung der VMs die virtuellen Netzwerkschnittstellen entsprechend verbunden sind. Zu den Citrix Hypervisor Netzwerken, die Sie auswählen können, gehören physische Standardnetzwerke (sogenannte externe Netzwerke), VLANs, private Einzelserver-Netzwerke und serverübergreifende private Netzwerke.

  Wenn Sie VMware „Virtual Network 4“ beispielsweise Citrix Hypervisor „Network 0“ zuordnen, wird jede VMware VM, bei der ein virtueller Adapter mit „Virtual Network 4“ verbunden war, nach der Konvertierung mit „Network 0“ verbunden. Citrix Hypervisor Conversion Manager konvertiert oder migriert keine Hypervisor-Netzwerkeinstellungen. Der Assistent ändert nur die virtuellen Netzwerkschnittstellenverbindungen einer konvertierten virtuellen Maschine basierend auf den bereitgestellten Zuordnungen.

  > **Hinweis:**
  >
  > Sie müssen nicht alle VMware Netzwerke den entsprechenden Citrix Hypervisor Netzwerken zuordnen. Sie können jedoch die Netzwerke ändern, die von VMs verwendet werden, die Anzahl der Netzwerke in der neuen Citrix Hypervisor-Konfiguration reduzieren oder konsolidieren.

  Um den maximalen Nutzen aus diesen Funktionen zu ziehen, empfiehlt Citrix Folgendes:

  - Schließen Sie die Hosts vor der Installation von Citrix Hypervisor an die Netzwerke des Switches (d. h. die Ports) an, die Sie auf dem Host konfigurieren möchten.

- Stellen Sie sicher, dass der Citrix Hypervisor Pool die Netzwerke sehen kann, die erkannt werden sollen. Schließen Sie die Citrix Hypervisor Hosts an Switch-Ports an, die auf dieselben Netzwerke wie der VMware Cluster zugreifen können.

Obwohl es einfacher ist, die Citrix Hypervisor Netzwerkkarten in dieselben Netzwerke wie die Netzwerkkarten auf den VMware Hosts zu verbinden, ist dies nicht erforderlich. Wenn Sie die Netzwerkzuordnung ändern möchten, können Sie eine Citrix Hypervisor Netzwerkkarte an ein anderes physisches Netzwerk anschließen.

Vorbereiten der Netzwerkanforderungen für Citrix Hypervisor Conversion Manager

Wenn Sie die Konvertierung durchführen, müssen Sie eine Netzwerkverbindung mit dem Netzwerk erstellen, in dem sich der VMware Server befindet. Citrix Hypervisor Conversion Manager verwendet diese Verbindung für den Konvertierungsverkehr zwischen dem Citrix Hypervisor Host und dem VMware Server.

Um diese Netzwerkverbindung zu erstellen, müssen Sie zwei Aufgaben ausführen:

- Wenn Sie die Citrix Hypervisor Conversion Manager Virtual Appliance importieren, geben Sie das Netzwerk an, das Sie für den Konvertierungsdatenverkehr als virtuelle Netzwerkschnittstelle hinzugefügt haben. Sie können dies tun, indem Sie **Schnittstelle 1** so konfigurieren, dass es eine Verbindung zu diesem Netzwerk herstellt.
- Bevor Sie den Konvertierungsassistenten ausführen, fügen Sie das Netzwerk, das VMware und Citrix Hypervisor verbindet, dem Citrix Hypervisor-Host hinzu, auf dem die konvertierten VMs ausgeführt werden sollen.

Wenn Sie die Citrix Hypervisor Conversion Manager Virtual Appliance importieren, erstellt XenCenter standardmäßig eine virtuelle Netzwerkschnittstelle, die Network 0 und NIC0 (eth0) zugeordnet ist. Standardmäßig konfiguriert Citrix Hypervisor Setup NIC0 jedoch als *Verwaltungsschnittstelle*, eine Netzwerkkarte, die für den Citrix Hypervisor-Verwaltungsdatenverkehr verwendet wird. Wenn Sie ein Netzwerk für die Konvertierung hinzufügen, können Sie daher eine andere Netzwerkkarte als NIC0 auswählen. Die Auswahl eines anderen Netzwerks kann die Leistung in Pools mit ausgelasteten Pools verbessern. Weitere Informationen zur Verwaltungsoberfläche finden Sie in der XenCenter Hilfe.

So fügen Sie Citrix Hypervisor ein Netzwerkhinzu:

1. Wählen Sie im **Ressourcenbereich** in XenCenter den Pool aus, in dem Sie Citrix Hypervisor Conversion Manager ausführen möchten.
2. Klicken Sie auf die Registerkarte **Netzwerk**.
3. Klicken Sie auf **Netzwerk hinzufügen**.
4. Select auf der Seite **Typ auswählen** die Option **Externes Netzwerk** aus, und klicken Sie auf **Weiter**.

5. Geben Sie auf der Seite **Name** einen aussagekräftigen Namen für das Netzwerk ein (z. B. „VMware Netzwerk“) und eine Beschreibung.
6. Geben Sie auf der Seite **Schnittstelle** Folgendes an:
   - **NIC**. Die Netzwerkkarte, die Citrix Hypervisor zum Erstellen des Netzwerks verwenden soll. Select 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 die MTU-Box auf den Standardwert 1500.

     > **Hinweis:**Aktivieren Sie
     >
     > nicht das Kontrollkästchen **Dieses Netzwerk automatisch zu neuen virtuellen Maschinen hinzufügen**.
7. Klicken Sie auf **Fertig stellen**.

Erfüllung der Speicheranforderungen

Berücksichtigen Sie vor der Konvertierung von Stapel von VMware VMs Ihre Speicheranforderungen. Konvertierte VM-Festplatten werden in einem Citrix Hypervisor or-Speicher-Repository gespeichert.

Dieses Speicher-Repository muss groß genug sein, um die virtuellen Laufwerke für alle konvertierten VMs enthalten, die in diesem Pool ausgeführt werden sollen. Bei konvertierten Maschinen, die nur auf einem eigenständigen Host ausgeführt werden, können Sie entweder lokalen oder freigegebenen Speicher als Speicherort für die konvertierten virtuellen Laufwerke angeben. Bei konvertierten Maschinen, die in Pools ausgeführt werden, können Sie nur gemeinsam genutzten Speicher angeben.

So erstellen Sie ein Speicher-Repository:

1. Wählen Sie im **Ressourcenbereich** in XenCenter den Pool aus, in dem Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance ausführen möchten.
2. Klicken Sie auf die Registerkarte **Speicher**.
3. Klicken Sie auf **Neuer SR** , und folgen Sie den Anweisungen im Assistenten. Um weitere Anweisungen zu erhalten, drücken Sie **F1** , um die Online-Hilfe anzuzeigen.

Citrix Hypervisor Anforderungen

Sie können VMs, die mit dieser Version von Citrix Hypervisor Conversion Manager konvertiert wurden, auf den folgenden Versionen von Citrix Hypervisor ausführen:

- XenServer 7.0
- XenServer 7.1 Kumulatives Update 2
- XenServer 7.5
- XenServer 7.6
- Citrix Hypervisor 8.0

VMware Anforderungen

Citrix Hypervisor Conversion Manager kann VMware s aus den folgenden VMware-Versionen konvertieren:

- vCenter Server 5.5.0, 6.0.0 und 6.5.0
- vSphere 5.5.0, 6.0.0 und 6.5.0
- ESXi 5.5.0, 6.0.0 und 6.5.0

> **Hinweis:**
>
> Citrix Hypervisor Conversion Manager kann VMware-VMs mit vier oder mehr Festplatten nicht in Citrix Hypervisor VMs konvertieren. Ihre VMware-VMs müssen über drei oder weniger Festplatten verfügen.

Vorbereiten des Imports der virtuellen Appliance

Beachten Sie vor dem Importieren der virtuellen Appliance die folgenden Informationen und nehmen Sie gegebenenfalls die entsprechenden Änderungen an Ihrer Umgebung vor.

Laden Sie die virtuelle Appliance herunter

Die virtuelle Citrix Hypervisor Conversion Manager-Appliance ist in einem xva-Format verpackt. Sie können die virtuelle Appliance von der herunterladen[Seite Citrix Hypervisor 8.0 Premium Edition]. Speichern Sie die Datei beim Herunterladen in einem Ordner auf der lokalen Festplatte (normalerweise, aber nicht unbedingt auf dem Computer, auf dem XenCenter installiert ist). Nachdem sich die XVA-Datei auf der Festplatte befindet, können Sie sie in XenCenter importieren.

> **Hinweis:**
>
> Citrix Hypervisor Conversion Manager ist für Citrix Hypervisor Premium Edition-Kunden oder für Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unterLizenzierung. Um ein Upgrade oder eine Citrix Hypervisor 8.0 Lizenz zu erwerben, besuchen Sie die[Citrix Website].

Voraussetzungen für virtuelle Appliance

Die Citrix Hypervisor Conversion Manager Virtual Appliance erfordert mindestens:

- XenServer 7.0, XenServer 7.1 Kumulatives Update 2, XenServer 7.5, XenServer 7.6, Citrix Hypervisor 8.0
- Festplattenspeicher: 30 GB Festplattenspeicher
- Arbeitsspeicher: 6,5 GB
- Virtuelle CPU-Zuweisung: 1 vCPU

Importieren und Konfigurieren der virtuellen Citrix Hypervisor Conversion Manager-Appliance

Die Citrix Hypervisor Conversion Manager Virtual Appliance ist eine einzelne vorinstallierte VM, die auf einem Citrix Hypervisor Host ausgeführt werden kann. Überprüfen Sie vor dem Importieren die erforderlichen Informationen und Überlegungen im Abschnitt *Vorbereiten des Imports der virtuellen Appliance*.

Importieren der virtuellen Appliance in Citrix Hypervisor

Importieren Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance in den Pool oder Host, auf dem Sie die konvertierten VMs ausführen möchten. Verwenden Sie den Importassistenten des XenCenters, um die Citrix Hypervisor Conversion Manager Virtual Appliance zu **importieren** .

So importieren Sie die virtuelle Appliance in XenCenter:

1. Öffnen Sie XenCenter. Klicken Sie mit der rechten Maustaste auf den Pool (oder den Host), in den Sie das Paket der virtuellen Appliance importieren möchten, und wählen Sie **Importieren**aus.
2. Suchen Sie nach dem Paket der virtuellen Appliance.
3. Select den Pool oder einen *Home-Server* aus, auf dem die Citrix Hypervisor Conversion Manager Virtual Appliance ausgeführt werden soll.

   > **Hinweis:**
   >
   > Ein Home-Server ist der Host, der die Ressourcen für eine VM in einem Pool bereitstellt. Obwohl dies möglich ist, versucht ein Citrix Hypervisor, die VM auf diesem Host zu starten, bevor er andere Hosts ausprobiert. Wenn Sie einen Host auswählen, verwendet die virtuelle Citrix Hypervisor Conversion Manager-Appliance diesen Host als Heimserver. Wenn Sie den Pool auswählen, startet die virtuelle Appliance automatisch auf dem am besten geeigneten Host in diesem Pool.

4. Wählen Sie ein Speicher-Repository aus, auf dem das virtuelle Laufwerk für die Citrix Hypervisor Conversion Manager Virtual Appliance gespeichert werden soll, und klicken Sie dann auf **Importieren**. Informationen zum Hinzufügen eines Speicher-Repository zum Pool finden Sie im Abschnitt „Speicheranforderungen erfüllen“. „ Sie können entweder lokalen oder freigegebenen Speicher auswählen.

5. Stellen Sie sicher, dass das Netzwerk, das für die Konvertierung verwendet werden soll (das Netzwerk, das den VMware Server mit dem Citrix Hypervisor Host verbindet) als Netzwerk ausgewählt ist, das der **Schnittstelle 1** zugeordnet ist („virtuelle NIC 1”).

   - Wenn neben Schnittstelle 1 das richtige Netzwerk nicht 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 Citrix Hypervisor ein Netzwerk**hinzu.

   > **Warnung:**Konfigurieren
   >
   > Sie NIC0 NICHT für Ihr Kundennetzwerk. Weisen Sie NIC0 nur „Host-internes Management-Netzwerk. „

6. Lassen Sie das Kontrollkästchen **VM (s) nach dem Import starten** aktiviert, und klicken Sie auf **Fertig stellen** , um die virtuelle Appliance zu importieren.

7. Nach dem Importieren der XVA-Datei wird die virtuelle Citrix Hypervisor Conversion Manager-Appliance im **Ressourcenbereich** in XenCenter angezeigt.

Konfigurieren der virtuellen Citrix Hypervisor Conversion Manager-Appliance

Nachdem Sie den Import der virtuellen Citrix Hypervisor Conversion Manager-Appliance abgeschlossen haben, müssen Sie sie konfigurieren, bevor Sie VMware VMs konvertieren können. Befolgen Sie die Eingabeaufforderungen auf der Registerkarte XenCenter **Konsole** .

1. Klicken Sie nach dem Importieren der virtuellen Citrix Hypervisor Conversion Manager-Appliance auf die Registerkarte **Konsole** .

2. Geben Sie **„Ja“** ein, um die Bedingungen des Lizenzvertrags zu akzeptieren. Um die EULA abzulehnen, geben Sie **Nr.**ein.

3. Geben Sie ein neues Stammkennwort für die virtuelle Citrix Hypervisor Conversion Manager Appliance ein, und bestätigen Sie es. Citrix empfiehlt, ein sicheres Kennwort auszuwählen.
4. Geben Sie einen Hostnamen für die virtuelle Citrix Hypervisor Conversion Manager-Appliance ein.
5. Geben Sie das Domänensuffix für die virtuelle Appliance ein. Wenn z. B. der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) für die virtuelle Appliance lautet`citrix-migrate-vm.domain4.bedford4.ctx4`, geben Sie ein`domain4.bedford4.ctx4`.
6. Geben Sie **y** ein, um DHCP zu verwenden, um die IP-Adresse für die virtuelle Citrix Hypervisor Conversion Manager-Appliance automatisch abzurufen. Geben Sie andernfalls **n** ein, und geben Sie dann eine statische IP-Adresse, eine Subnetzmaske und ein Gateway für die VM ein.
7. Überprüfen Sie den Hostnamen und die Netzwerkeinstellung, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden. Dieser Schritt schließt den Konfigurationsprozess der virtuellen Appliance von Citrix Hypervisor Conversion Manager ab.
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 Citrix Hypervisor Conversion Manager Virtual Appliance anzumelden.

Nachdem Sie die Konfiguration der virtuellen Citrix Hypervisor Conversion Manager Appliance abgeschlossen haben, installieren Sie die Citrix Hypervisor Conversion Manager-Konsole. Weitere Informationen finden Sie unter Installieren der Conversion Manager-Konsole.

Installieren der Conversion Manager-Konsole

Nachdem Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance konfiguriert haben, fahren Sie mit der Installation der Citrix Hypervisor Conversion Manager-Konsole auf der lokalen Workstation fort. Die Citrix Hypervisor Conversion Manager-Konsole ist die Benutzeroberfläche, auf der Sie die meisten Konvertierungsaufgaben ausführen. In der Citrix Hypervisor Conversion Manager-Konsole können Sie einen Konvertierungsassistenten starten, mit dem Sie VMware VMs für die Konvertierung auswählen können.

> **Hinweis:**
>
> Citrix Hypervisor Conversion Manager ist für Citrix Hypervisor Premium Edition-Kunden oder für Kunden verfügbar, die über ihre Citrix Virtual Apps und Desktops Zugriff auf Citrix Hypervisor haben. Weitere Informationen zur Citrix Hypervisor-Lizenzierung finden Sie unter Lizenzierung. Um ein Upgrade oder eine Citrix Hypervisor or-Lizenz zu erwerben, besuchen Sie die[Citrix Website].

Systemanforderungen

Unterstützte Gastbetriebssysteme:

Citrix Hypervisor Conversion Manager unterstützt die Konvertierung von VMware VMs, auf denen jedes der von Citrix Hypervisor unterstützten Windows Gastbetriebssysteme ausgeführt wird. Eine Liste der von Citrix Hypervisor unterstützten Windows Gastbetriebssysteme finden Sie unter Unterstützung für Gastbetriebssysteme. Die folgenden Linux-Betriebssysteme werden ebenfalls unterstützt.

- RHEL 5,4/5,6/6,4/7,0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 14.04/16.04

Softwareanforderungen:

Microsoft .NET Framework 4.6

Festplattenspeicher für die Installation erforderlich:

10 MB

Installation

Die Citrix Hypervisor Conversion Manager-Konsole wird auf demselben Computer installiert, auf dem XenCenter ausgeführt wird.

> **Wichtig:**
>
> - Entfernen Sie vor der Installation der Citrix Hypervisor Conversion Manager-Konsole alle anderen Versionen der Konsole vom Computer.
> - Die Citrix Hypervisor Conversion Manager-Konsole hängt vom Browser für Proxy-Einstellungen ab. Wenn Citrix Hypervisor, ESXi und vCenter nur über einen Proxy-Server erreicht werden können, müssen die Details des Proxyservers in den Proxyeinstellungen des Browsers eingegeben werden. Wenn Citrix Hypervisor, ESXi und vCenter ohne Proxy-Server erreicht werden können und der Benutzer den Proxy des Browsers für den Zugriff auf das Internet festgelegt hat, müssen die Adressen von Citrix Hypervisor, ESXi und vCenter in der Proxyausnahme der Proxyeinstellungen des Browsers hinzugefügt werden.

So installieren Sie die Citrix Hypervisor Conversion Manager-Konsole:

1. Doppelklicken Sie auf **convui_setup.msi**.
2. Klicken Sie auf der Seite **Willkommen beim Setup-Assistenten für Citrix Hypervisor Conversion Manager** auf **Weiter** .

3. Überprüfen Sie die Lizenzvereinbarung und wählen Sie **Ich akzeptiere die Bedingungen im Lizenzvertrag** , um die Bedingungen der Vereinbarung zu akzeptieren. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Zielordner** aus, an der die Conversion Manager-Konsole installiert werden soll, und klicken Sie auf **Weiter** .

   > **Hinweis:**
   >
   > Standardmäßig ist die Conversion Manager-Konsole in installiert`C:\Program Files (x86)\Citrix\XCM`.

5. Klicken Sie auf **Installieren** , um die Conversion Manager-Konsole zu installieren.
6. Klicken Sie auf **Fertig stellen**.

So entfernen Sie die Citrix Hypervisor Conversion Manager-Konsole:

1. Öffnen Sie die Windows -Systemsteuerung.
2. Öffnen Sie **Programme und Funktionen**.
3. Select **Citrix Hypervisor Conversion Manager**aus.
4. Klicken Sie auf **Deinstallieren**.

VMware VMs konvertieren

Wenn Sie VMware VMs konvertieren, werden sie in den Citrix Hypervisor-Pool oder den eigenständigen Host importiert, auf dem Sie die Citrix Hypervisor Conversion Manager Virtual Appliance ausführen. Konvertierte VMs behalten ihre ursprünglichen VMware Einstellungen für virtuellen Prozessor und virtuellen Speicher bei.

Die Verwendung von Citrix Hypervisor Conversion Manager zum Konvertieren von VMs erfordert die folgenden Aufgaben:

1. Starten der Citrix Hypervisor Conversion Manager-Konsole.
2. Herstellen einer Verbindung mit einem Citrix Hypervisor Host.
3. Starten des Assistenten zu einem neuen Konvertierungsauftrag, der die Angabe von VMware Server-Anmeldeinformationen und die Auswahl von VMs und dem Speicher-Repository erfordert.

> **Hinweise:**
>
> - Citrix Hypervisor Conversion Manager unterstützt die Konvertierung von VMware VMs mit unterschiedlichem Speicher wie Thin Provisioning, Thick Provisioning, IDE und SCSI.
> - Citrix Hypervisor Conversion Manager erfordert nicht, dass VMware Tools auf den Quell-VMs installiert sind. Sie können die Konvertierung auf VMware VMs durchführen, unabhängig

> davon, ob VMware Tools installiert sind oder nicht.
>
> - Citrix Hypervisor Conversion Manager kann VMware-VMs mit vier oder mehr Festplatten nicht in Citrix Hypervisor VMs konvertieren. Ihre VMware-VMs müssen über drei oder weniger Festplatten verfügen.

Aufgabe 1: Starten der Citrix Hypervisor Conversion Manager-Konsole

So starten Sie die Citrix Hypervisor Conversion Manager-Konsole:

1. Wählen Sie im Startmenü **Alle Programme** > **Citrix > CitrixHypervisor Conversion Manager** aus.

   > **Hinweis:**
   >
   > Sie können nur eine Instanz von Citrix Hypervisor Conversion Manager pro Computer ausführen.

2. Fahren Sie **mit Citrix Hypervisor verbinden**fort.

Aufgabe 2: Herstellen einer Verbindung mit einem Citrix Hypervisor Host

Wenn Sie die Citrix Hypervisor Conversion Manager-Konsole starten, müssen Sie sie mit einem Citrix Hypervisor Host verbinden.

Stellen Sie vor dem Start sicher, dass Sie über die Anmeldeinformationen für den Citrix Hypervisor Pool (oder den eigenständigen Host) verfügen. Entweder sind die Anmeldeinformationen des Stammkontos oder ein rollenbasiertes Zugriffssteuerungskonto (RBAC) mit konfigurierter Pooladministratorrolle zulässig.

So stellen Sie eine Verbindung zu einem Citrix Hypervisor Hosther:

1. Wenn das Dialogfeld **Verbindung mit Citrix Hypervisor** herstellen beim Starten der Citrix Hypervisor Conversion Manager-Konsole nicht angezeigt wird, klicken Sie auf die Schaltfläche **Verbinden** in der Symbolleiste.
2. Geben **Sie im Dialogfeld Verbindung mit Citrix Hypervisor** herstellen die folgenden Details ein:

- **Server**. Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für den Citrix Hypervisor Host ein, auf den Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance importiert haben. Um die IP-Adresse zu finden, wählen Sie den Host im XenCenter Ressourcenbereich aus, und klicken Sie auf die Registerkarte **Suchen** .
- **Benutzername**. Geben Sie den Benutzernamen für ein Citrix Hypervisor Konto für den Pool (oder den eigenständigen Host) ein. Dieses Konto muss entweder das Stammkonto für den Host oder Pool sein oder die RBAC-Rolle „Pool Admin“ haben.

Ausführliche Informationen zu RBAC finden Sie unterÜbersicht über RBAC.

- **Passwort**. Geben Sie das Kennwort für dieses Konto ein, und klicken Sie auf **Verbinden**.

  Nachdem Sie eine Verbindung mit dem Citrix Hypervisor Host erfolgreich hergestellt haben, zeigt Citrix Hypervisor Conversion Manager die Seite **Aufträge** an.

Aufgabe 3: Starten eines neuen Konvertierungsauftrags

Bevor Sie mit der Konvertierung beginnen, stellen Sie sicher, dass Folgendes zutrifft:

- Sie verfügen über die Anmeldeinformationen für den VMware Server, der die VMs enthält, die Sie konvertieren möchten. Für die Konvertierung müssen Sie die Citrix Hypervisor Conversion Manager-Konsole mit dem VMware Server verbinden.
- Die zu konvertierende virtuelle VMware Maschine wird ausgeschaltet.
- Der Citrix Hypervisor-Pool (oder Host), auf dem die konvertierten VMs ausgeführt werden, ist mit einem Speicher-Repository verbunden. Das Speicher-Repository muss genügend Speicherplatz für die konvertierten virtuellen Laufwerke enthalten.
- Die virtuellen Laufwerke der zu konvertierenden virtuellen Maschine haben eine Größe von weniger als 2 TiB.
- Citrix Hypervisor-Pool (oder Host) verfügt über Netzwerke, die von den konvertierten VMs verwendet werden.

So konvertieren Sie VMware VMs:

1. Klicken Sie im Fenster **Aufträge** auf die Schaltfläche **Konvertieren** .
2. Geben Sie auf der Seite **Anmeldeinformationen** Folgendes ein, und klicken Sie dann auf **Verbinden** :

   Server. Geben Sie die IP-Adresse oder den FQDN für den VMware Server ein, der die VMs enthält, die Sie in Citrix Hypervisor 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 besitzen.

   Passwort. Geben Sie das Kennwort für das Benutzerkonto ein, das Sie im Feld **Benutzername** angegeben haben.
3. Wählen Sie auf der Seite **Speicher-Repository** das Speicher-Repository aus, das Sie während der Konvertierung verwenden möchten. In diesem Speicher-Repository werden die VMs und die virtuellen Laufwerke, die Sie erstellen, dauerhaft gespeichert.
4. Wählen Sie auf der Seite **Virtuelle Maschinen** die VMware s aus, die Sie konvertieren möchten, und klicken Sie auf **Weiter** .

Wenn Sie die zu konvertierenden VMs auswählen, erhöht sich der rote Kreiskeil, um anzugeben, welcher Anteil des verfügbaren Speichers für die virtuellen Laufwerke der konvertierten virtuellen Maschine verbraucht werden soll.

Während der Konvertierung lädt Citrix Hypervisor Conversion Manager aktualisierte Kernel für Linux-VMs herunter, die nicht aktualisiert werden. Wenn kein Zugriff auf das Internet besteht, installiert Citrix Hypervisor Conversion Manager den Kernel vom folgenden Speicherort der Citrix Hypervisor Conversion Manager-Appliance.

```
/opt/vpxxcm/conversion/linuxv2v/${
 distro }
 /
```

In der folgenden Tabelle sind die Kernelversionen für die verschiedenen Linux-Betriebssysteme aufgeführt, die während der Konvertierung unterstützt werden.

Betriebssystem	32-bit/64-bit	Empfohlene Kernel-Versionsnummer
CentOS 5.5	32-bit	2.6.18-412(kernel-Xen)
CentOS 6.3	32-bit	2.6.32-642
CentOS 6.4	32-bit	2.6.32-642
CentOS 6.5	32-bit	2.6.32-642
RHEL 5,4	32-bit	2.6.18-164
RHEL 5,6	32-bit	2.6.18-412
RHEL 6,4	32-bit	2.6.32-642
SLES 11 SP3	32-bit	3.0.76-0
SLES 11 SP4	32-bit	3.0.101-63
Ubuntu 14.04	32-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren
Ubuntu 16.04	32-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren
RHEL 5,4	64-bit	2.6.18-411
RHEL 5,6	64-bit	2.6.18-411
RHEL 6,4	64-bit	2.6.32-642

Betriebssystem	32-bit/64-bit	Empfohlene Kernel-Versionsnummer
RHEL 7,0	64-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren
CentOS 5.5	64-bit	2.6.18-412 (Kernel-XEN)
CentOS 6.3	64-bit	2.6.32-642
CentOS 6.4	64-bit	2.6.32-642
CentOS 6.5	64-bit	2.6.32-642
CentOS 7.0	64-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren
SLES 11 SP3	64-bit	3.0.76-0
SLES 11 SP4	64-bit	3.0.101-59
Ubuntu 14.04	64-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren
Ubuntu 16.04	64-bit	Keine Internetverbindung erforderlich, um den Xen Kernel zu aktualisieren

5. *(Optional.) Führen Sie auf der Seite **Netzwerke** eine oder mehrere der folgenden Aufgaben aus, um anzugeben, wie Citrix Hypervisor Conversion Manager die virtuellen Netzwerkadapter in den zu konvertierenden VMs konvertiert :*

   Ändern Sie alle Citrix Hypervisor Netzwerke, denen VMware Netzwerkadapter zugeordnet sind. Citrix Hypervisor Conversion Manager erkennt die virtuellen Netzwerkadapter auf den zu konvertierenden VMs und ermöglicht es Ihnen, diese Adapter mit Netzwerken in Citrix Hypervisor zu verknüpfen. Nach der Konvertierung verfügen die neuen VMs über virtuelle Netzwerkschnittstellen, die eine Verbindung zu den in diesem Schritt angegebenen Citrix Hypervisor Netzwerken herstellen.

   Akzeptieren Sie die standardmäßigen Netzwerkzuordnungen. Wenn Sie beim Importieren der virtuellen Citrix Hypervisor Conversion Manager-Appliance das physische VMware Netzwerk oder VLAN angegeben haben, sollten Sie die Netzwerke auf dieser Seite unter den Standardeinstellungen belassen.

   Select das Kontrollkästchen Virtuelle MAC-Adresse beibehalten. Citrix Hypervisor kann

virtuelle MAC-Adressen automatisch generieren, wenn Sie VMs erstellen oder importieren. Sie können jedoch die virtuellen MAC-Adressen auf Ihren VMware s beibehalten, um IP-Adressen in Umgebungen mit DHCP beizubehalten. Weitere Informationen finden Sie im Abschnitt **Vorbereiten der Citrix Hypervisor Conversion Manager-Netzwerkanforderungen**.

6. Überprüfen Sie auf der Seite Zusammenfassung die Konvertierungsdetails, und klicken Sie auf Fertig stellen. Während die Konvertierung ausgeführt wird, wird der Status auf der Seite **Jobs** angezeigt.

   > **Hinweis:**Die
   >
   > Konvertierung von ESXi oder vSphere kann je nach Größe der virtuellen Laufwerke mehrere Minuten dauern.

Aufgabe 4: Schritte nach der Konvertierung

Öffnen Sie nach der Konvertierung XenCenter, und führen Sie die folgenden Schritte auf den neu konvertierten VMs aus:

Auf Windows Computern:

1. Auf Windows VMs müssen Sie je nach Microsoft-Lizenzmodell möglicherweise die Windows-Lizenz der VM reaktivieren. Dies geschieht, weil das Windows Betriebssystem die Konvertierung als Hardwareänderung wahrnimmt.
2. Installieren Sie auf Windows VMs Citrix VM Tools, um Hochgeschwindigkeits-E/A-Vorgänge für verbesserte Festplatten- und Netzwerkleistung zu erhalten. Citrix VM-Tools ermöglichen auch bestimmte Funktionen und Funktionen, einschließlich sauberes Herunterfahren, Neustart, Anhalten und Live-Migrieren von VMs.

Wenn Sie mit einer VM arbeiten, auf der Citrix VM Tools nicht installiert sind, wird auf der Registerkarte **Allgemein** im Eigenschaftenbereich die Meldung Citrix VM Tools nicht installiert angezeigt. Bei Windows VMs können Sie auf diesen Text doppelklicken, um zur VM-Konsole zu wechseln, die Citrix VM Tools-ISO zu laden und den Citrix VM Tools-Installationsassistenten zu starten.

> **Hinweis:**
>
> Citrix VM Tools müssen auf jeder VM installiert sein, damit die VM über eine vollständig unterstützte Konfiguration verfügt. Obwohl VMs ohne Citrix VM Tools funktionieren, kann ihre Leistung beeinträchtigt werden.

Aktivieren von VNC auf Linux-Computern

Führen Sie auf Linux-VMs die folgenden Schritte aus, um den VNC-Server zu konfigurieren.

> **Hinweis:**
>
> Das VNC-Passwort muss mindestens sechs Zeichen lang sein.

Für CentOS 5.5 und RHEL 5.4/5.6

1. Passen Sie die RHEL-basierte VMs Firewall an, um den VNC-Port zu öffnen, indem Sie den folgenden Befehl verwenden:

```
system-config-securitylevel-tui
```

2. Select **Anpassen** und fügen Sie **5900** zur Liste **Weitere Ports hinzu. Alternativ können Sie die Firewall bis zum nächsten Neustart deaktivieren, indem Sie den folgenden Befehl ausführen:

```
service iptables stop
```

3. Führen Sie für CentOS 5.5 und RHEL 5.4/5.6 Folgendes aus, wenn die VNC-Grafikkonsole nicht ordnungsgemäß angezeigt wird:

```
init 5
```

   Überprüfen Sie dann, ob die Grafikkonsole ordnungsgemäß angezeigt wird.

Für CentOS 6.3/6.4/6.5 und RHEL 6.4

1. Festlegen des VNC-Kennworts

```
vncpasswd
```

2. Starten des VNC-Servers

```
service vncserver start
```

3. Öffnen Sie für Firewall-Einstellungen die Datei /etc/sysconfig/iptables und fügen Sie die folgende Zeile hinzu:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

   > **Hinweis:**
   >
   > Fügen Sie die obige Zeile nach:`-A INPUT -j REJECT \--reject-with icmp-host-prohibited`:

4. Geben Sie den folgenden Befehl ein, um iptables neu zu starten:

```
>Dienst iptables Neustart
```


Für SLES Linux Enterprise Server 11 SP3 bis SP4

1. Legen Sie das VNC-Kennwort in der Startkonsole fest.

   ```
   vncpasswd
   ```

   Antwort`n` auf die Frage`Would you like to enter a view-only password(y/n)? n`

2. Konfigurieren Sie die Feuerwand-Einstellungen wie folgt:

   a) Öffnen Sie eine Textkonsole auf der VM und führen Sie das YaST-Dienstprogramm aus:

   ```
   yast
   ```

   b) Verwenden Sie die Pfeiltasten, um **Sicherheit und Benutzer** im linken Menü auszuwählen, dann Tab in das rechte Menü und verwenden Sie die Pfeiltasten, um **Firewall** auszuwählen. Drücken Sie die **Eingabetaste**.

   c) Wählen Sie im **Firewall-Bildschirm** im linken Menü mit den Pfeiltasten **Benutzerdefinierte Regeln** aus, und drücken **Sie dann die EINGABETASTE**.

   d) Klicken Sie auf die Schaltfläche **Hinzufügen** im Abschnitt **Benutzerdefinierte zulässige Regeln** , und drücken **Sie dann die EINGABETASTE** .

   e) Geben Sie im Feld **Quellnetzwerk** den Wert **0/0** ein. Tabulatortaste in das Feld **Zielport** , und geben Sie **5900** ein.

   f) Klicken Sie auf die Schaltfläche **Hinzufügen** , und drücken Sie dann die **Eingabetaste** .

   g) Tabulatortaste zur Schaltfläche **Weiter** und drücken **Sie die Eingabetaste** . Klicken Sie im Fenster **Zusammenfassung** auf die Schaltfläche **Fertig stellen** , und drücken **Sie die Eingabetaste** . Schließlich, auf dem obersten YaST-Bildschirm, Tab auf die Schaltfläche **Beenden** und drücken **Sie die Eingabetaste** .

3. Klicken Sie auf **Zur grafischen Konsole wechseln**.

4. Wenn die grafische Konsole nicht korrekt angezeigt wird, wechseln Sie zur **Textkonsole** und führen Sie den Befehl aus:

   ```
   /etc/init.d/vncserver restart
   ```

5. Klicken Sie auf **Zur grafischen Konsole wechseln**.

> **Hinweise:**
>
> - Führen Sie für andere Probleme mit der grafischen Konsolenanzeige Folgendes aus:`/etc/init.d/vncserver restart`.
> - Die Konvertierung von VMs mit IDE-Festplatten wird für SLES 11 SP3 in SP4 nicht unterstützt.

Andere Konvertierungsaufgaben

In diesem Abschnitt werden weitere Aufgaben aufgeführt, die Sie beim Konvertieren von VMs möglicherweise ausführen möchten. Zu diesen Aufgaben gehören das Löschen von Aufträgen, das Speichern einer Zusammenfassung von Aufträgen, das Wiederholen von Aufträgen, das Abbrechen von Aufträgen und das Anzeigen der Protokolldatei.

So löschen Sie alle Aufträge

Wählen Sie im Menü „ **Aufträge** “ die Option „ **Aufträge löschen** “.

So speichern Sie eine Zusammenfassung der Aufträge

Klicken Sie im Menü **Datei** auf **Jobübersicht speichern** .

So wiederholen Sie einen Auftrag

Klicken Sie auf **Aufträge wiederholen**.

> **Hinweis:**
>
> Die Option **Aufträge wiederholen** ist nur für fehlgeschlagene oder abgebrochene Aufträge aktiviert.

So brechen Sie einen Auftrag ab

Klicken Sie auf **Aufträge abbrechen**.

> **Hinweis:**
>
> Aufträge abbrechen ist nur für Warteschlange oder ausgeführte Aufträge aktiviert.

So speichern Sie die Citrix Hypervisor Conversion Manager-Anwendungsprotokolldatei

1. Wählen Sie im Menü **Hilfe** die Option **Support-Protokolldateien speichern** aus.
2. Wenn Sie dazu aufgefordert werden, geben Sie an, wo die Protokolldateien für Citrix Hypervisor Conversion Manager Console (`XCMUI.log`) und Citrix Hypervisor Conversion Manager Virtual Appliance (`XCM.log`) -Protokolle gespeichert werden sollen.

So zeigen Sie Konvertierungsdetails an

1. Select den Auftrag im Fenster Citrix Hypervisor Conversion **Manager-Aufträge** aus.

2. Klicken Sie im Bereich **Auftragsübersicht** auf den Link **Zusätzliche Protokollinformationen abrufen** .

Die Citrix Hypervisor Conversion Manager-Konsole ruft das Protokoll von der virtuellen Citrix Hypervisor Conversion Manager Appliance ab und zeigt das Ergebnis in einem Texteditor an.

So erhalten Sie Protokolldetails

Protokolle für Windows s- und Linux-Gäste sind in der `/var/log/conversion/convsvc.log` Datei vorhanden. Wenn die Konvertierung fehlschlägt, klicken Sie auf die Schaltfläche **Zusätzliche Protokollinformationen abrufen** . Für Linux-VMs sind zusätzliche Protokolle in vorhanden `/var/log/conversion/linuxxenfix.log`.

Problembehandlung bei der Konvertierung

Dieser Abschnitt enthält Informationen zur Problembehandlung bei der Konvertierung und konvertierten VMs.

Probleme beim Starten einer konvertierten VM

Im Allgemeinen läuft die Konvertierung reibungslos, und Citrix Hypervisor Conversion Manager konvertiert VMs ohne Probleme. In einigen seltenen Fällen können jedoch Fehler auftreten, wenn Sie versuchen, konvertierte VMs zu öffnen. Die folgenden Abschnitte enthalten einige Hinweise zur Behebung von Fehlern und anderen Problemen.

Blauer Bildschirm mit Windows STOP Code 0x0000007B

Dieser Stoppcode weist darauf hin, dass Citrix Hypervisor Conversion Manager kein Windows Gerät konfigurieren konnte, das zum ersten Mal in Citrix Hypervisor von entscheidender Bedeutung ist. Speichern Sie die Protokolle und senden Sie sie an den technischen Support von Citrix, um weitere Informationen zu erhalten.

Windows Produktaktivierung

Je nach Lizenzmodell kann eine Fehlermeldung bei der Systemaktivierung angezeigt werden, wenn Sie versuchen, eine Windows VM zu starten.

> **Hinweis:**
>
> Die Konvertierung von ESXi oder vSphere kann je nach Größe der virtuellen Laufwerke mehrere Minuten dauern.

Verlorene Netzwerkeinstellungen in einer Windows VM

Wenn Sie eine Windows VM von einem ESXi-Server in Citrix Hypervisor 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-Festplatte kann nicht gestartet werden

Wenn eine VMware VM von einer SCSI-Festplatte gestartet wird, aber auch eine oder mehrere IDE-Festplatten konfiguriert sind, wird die VM möglicherweise nicht gestartet, wenn Sie sie in Citrix Hypervisor konvertieren. Dies liegt daran, dass der Migrationsprozess den IDE-Festplatten niedrigere Gerätenummern als SCSI-Festplatten zuweist. Citrix Hypervisor startet jedoch von der Festplatte, 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 der virtuellen Festplatte, die das Betriebssystem enthält, neu gestartet wird.

So ändern Sie die Position des virtuellen Laufwerks, das das Betriebssystem enthält:

1. Wählen Sie im Bereich XenCenter Ressourcen die ausgeschalteten Gast-VM aus.
2. Select die Registerkarte **Speicher** .
3. Wählen Sie auf der Seite **Virtuelle Laufwerke** das virtuelle Laufwerk aus, das das Betriebssystem enthält, und klicken Sie dann auf **Eigenschaften** .
4. Klicken Sie im** Dialogfeld Eigenschaften von ***operating_system* auf die Registerkarte ****operating_system*** , um 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 Linux-VMs Fehler auftreten, entfernen Sie die konvertierte VM, starten Sie die virtuelle Citrix Hypervisor Conversion Manager-Appliance neu, und versuchen Sie es erneut. Protokolle von fehlgeschlagenen Konvertierungen werden in **/var/log/xensource.log**gespeichert. Wenn Sie sich an den Citrix Support wenden, um Probleme zu lösen, empfehlen wir, die Protokolldatei zur Fehlerbehebung bereitzustellen.

Kopiert!
Failed!

vSwitch und Controller

October 16, 2019

Der vSwitch bietet Transparenz, Sicherheit und Kontrolle für virtualisierte Citrix Hypervisor Netzwerkumgebungen. Es besteht aus folgenden Komponenten:

- Der *vSwitch*, ein virtualisierungsorientierter Switch, der auf jedem Citrix Hypervisor ausgeführt wird
- Der *vSwitch Controller*, ein zentralisierter Server, der das Verhalten jedes einzelnen vSwitches verwaltet und koordiniert, um das Erscheinungsbild eines einzelnen vSwitches bereitzustellen.

Der vSwitch Controller unterstützt feinkörnige Sicherheitsrichtlinien zur Steuerung des Datenverkehrs, der an und von einer VM gesendet wird. Es bietet einen detaillierten Überblick über das Verhalten und die Leistung für den gesamten Datenverkehr in der virtuellen Netzwerkumgebung. Ein vSwitch vereinfacht die IT-Administration in Ihrer Umgebung erheblich. Bei Verwendung von vSwitch bleiben die VM-Konfiguration und -Statistiken an eine VM gebunden, selbst wenn sie von einem physischen Host auf einen anderen migriert wird.

Erste Schritte

Anforderungen

- Mindestens ein in XenCenter konfigurierter Citrix Hypervisor Ressourcenpool
- Ausreichende Kapazität in diesem Pool für die Bereitstellung der virtuellen vSwitch Controller Appliance

Die Anforderungen für den Host, auf dem der Controller ausgeführt wird, werden im nächsten Abschnitt beschrieben.

Prozess

Das Einrichten des vSwitch Controller umfasst die folgenden Aufgaben:

1. Bereitstellen der virtuellen vSwitch Controller Appliance
2. Zugriff auf den vSwitch Controller
3. Konfigurieren der vSwitch Controller IP-Adresse
4. Ressourcenpools hinzufügen
5. Konfigurieren der hohen Verfügbarkeit (optional)

> **Hinweis:**
>
> Diese Version von vSwitch Controller funktioniert mit allen unterstützten Versionen von Citrix Hypervisor.

Bereitstellen der virtuellen vSwitch Controller Appliance

Der Citrix Hypervisor or-Server, auf dem der vSwitch Controller ausgeführt wird, muss die folgenden Mindestanforderungen erfüllen:

- 2 CPUs
- 2 GB DRAM
- 16 GB Festplatte

Die minimal zulässige VM-Konfiguration für die vSwitch Controller Appliance und die Standardkonfiguration beim Import ist:

- 2 vCPUs
- 2 GB DRAM
- 16 GB Festplatte

Diese Konfiguration unterstützt Pools mit bis zu 16 Citrix Hypervisor or-Servern und 256 Virtual Interfaces (VIFs), die mit dem vSwitch Controller verbunden sind. Bei größeren Pools (bis zum maximal unterstützten Grenzwert von insgesamt 64 Citrix Hypervisor or-Servern für alle Pools und 1024 VIFs) ändern Sie die VM-Konfiguration folgendermaßen:

- 4 vCPUs
- 4 GB DRAM
- 16 GB Festplatte

> **Hinweis:**
>
> - Wenn der Datenträger der Appliance auf einem Netzwerkspeicher gespeichert ist und den Netzwerkverkehr des zugrunde liegenden Citrix Hypervisor Hosts steuert, kann ein Deadlock in geladenen Situationen auftreten, und der Netzwerkverkehr des gesamten Pools kann angehalten werden. Um dies zu verhindern, empfiehlt Citrix Kunden dringend, die DVSC-Festplatte auf einem lokalen Speicher zu speichern oder die Appliance in einen anderen Pool zu verschieben, der nicht von diesem DVSC gesteuert wird.
> - Für jeden Pool müssen Sie die Poolgröße auf 16 Hosts oder weniger beschränken.
> - Der vSwitch Controller wird in Pools, die die Citrix Hypervisor PVS-Beschleunigerfunktion verwenden, nicht unterstützt.

Die vSwitch Controller VM kann in einem Ressourcenpool ausgeführt werden, den sie verwaltet. Im Allgemeinen wird diese Konfiguration so ausgeführt, als ob die vSwitch Controller VM separat ausgeführt würde. Es kann jedoch etwas länger dauern (bis zu zwei Minuten), um alle vSwitches zu verbinden, wenn eine Controller Migration oder ein Neustart stattfindet. Diese Zeit liegt an Unterschieden in der Art und Weise, wie die einzelnen vSwitches Steuerungsverbindungen leiten.

Importieren Sie zum Installieren des vSwitch Controller das bereitgestellte VM-Image der virtuellen Appliance in einen Citrix Hypervisor Ressourcenpool. Schließen Sie während des Imports die VIF der im-

portierten VM an ein Netzwerk an, über das Sie den Host oder Pool erreichen können, den Sie steuern möchten.

Nachdem die VM importiert wurde, starten Sie sie, um mit der Konfiguration des DVS zu beginnen.

Zugriff auf die Befehlszeilenschnittstelle des vSwitch Controller

Sie können über XenCenter oder über einen SSH-Client auf die vSwitch Controller er-Befehlszeilenschnittstelle (CLI) zugreifen. Wenn die vSwitch Controller VM zum ersten Mal gestartet wird, zeigt die Konsole in XenCenter die IP-Adresse an, die für den Remote-Zugriff auf den Controller verwendet werden soll. Wenn die VM keine IP-Adresse erhalten hat, gibt die Textkonsole an, dass eine Adresse über die CLI zugewiesen werden muss. In beiden Fällen zeigt die Textkonsole eine Anmeldeaufforderung an, um sich lokal in der XenCenter Konsole bei der CLI anzumelden. Eine vollständige Dokumentation der verfügbaren CLI-Befehle ist in enthaltenBefehlszeilenschnittstelle.

Zugriff auf die Benutzeroberfläche des vSwitch Controller

Greifen Sie über einen Webbrowser oder lokal in der XenCenter er-Konsole auf die vSwitch Controller er-GUI zu.

Wenn die vSwitch Controller VM gestartet wird, zeigt die Konsole in XenCenter die IP-Adresse an, die für den Remote-Zugriff auf die GUI verwendet werden soll. Wenn die VM keine IP-Adresse erhalten hat, kann die GUI erst lokal oder remote verwendet werden, wenn eine zugewiesen wurde. Die Konsole enthält Anweisungen zum lokalen Festlegen der IP-Adresse in der Befehlszeilenschnittstelle. Nachdem die Controller-VM die IP-Adresse hat, können Sie lokal in der XenCenter Konsole auf die GUI zugreifen.

> **Hinweis:**
>
> Wenn VNC deaktiviert ist, kann auf die vSwitch Controller GUI nur über einen Webbrowser zugegriffen werden.

Remote-Zugriff auf die vSwitch Controller GUI

So greifen Sie remote auf die vSwitch Controller Schnittstelle zu:

1. Öffnen Sie einen Browser und geben Sie die folgende URL ein, wobei *Server* die IP-Adresse oder den Hostnamen der Schnittstelle der Controller-VM ist:`https://server-name:443/`
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf **Anmelden**. Der Standardbenutzername und das Kennwort des **Administrators sind admin** und **admin** .

> **Hinweis:**
>
> Standardmäßig verwendet der vSwitch Controller Webserver ein selbstsigniertes Zertifikat. Das Zertifikat kann dazu führen, dass Browser einen Sicherheitsfehler anzeigen, wenn sie eine Verbindung mit der GUI herstellen. Sie können den Fehler sicher ignorieren und das Zertifikat in Ihrem Browser installieren.
>
> Folgende Browser werden unterstützt: Firefox 3.x, Safari 4.x, Internet Explorer 7 und 8. Andere moderne Browser mit ähnlichen Funktionen (zum Beispiel Opera oder Google Chrome) werden nicht unterstützt, funktionieren aber möglicherweise. Internet Explorer 9 behebt bekannte Speicher- und Ressourcenlecks. Es hat jedoch keine vollständige Prüfung erhalten.
>
> Wenn Sie sich zum ersten Mal anmelden, werden Sie vom System aufgefordert, das standardmäßige Administratorkennwort zu ändern. Es ist wichtig, dass Sie ein starkes Administratorkennwort erstellen, um die Sicherheit der Umgebung zu schützen.

Konfigurieren der vSwitch Controller IP-Adresse

Wenn der vSwitch Controller zum ersten Mal gestartet wird, versucht er, eine IP-Adresse mit DHCP abzurufen. Es wird jedoch empfohlen, eine statische IP-Adresse zuzuweisen. Wenn DHCP konfiguriert ist, können Ressourcenpools nicht auf den Fail-Sabe-Modus eingestellt werden.

So weisen Sie eine statische IP-Adresse zu:

1. Greifen Sie lokal auf die vSwitch Controller Schnittstelle zu.
2. Select die Registerkarte **Einstellungen** und dann **IP-Konfiguration** im Seitenbereich. Die aktuellen Einstellungen werden angezeigt.
3. Select **Konfiguration ändern**, geben Sie die neuen IP-Adressinformationen an und wählen Sie **Änderungen vornehmen**aus.
4. Starten Sie die virtuelle vSwitch Controller Appliance neu.

Ressourcenpools hinzufügen

Durch Hinzufügen eines Ressourcenpools kann der vSwitch Controller automatisch mit der Verwaltung aller Citrix Hypervisor or-Server in diesem Pool beginnen.

So fügen Sie einen Ressourcenpool hinzu:

1. Öffnen Sie unter **Sichtbarkeit und Steuerung**die Registerkarte **Status**, und wählen Sie **Alle Ressourcenpools**in der Ressourcenstruktur, um die Seite **Status**für alle Ressourcenpools zu öffnen.

2. Klicken Sie auf **Ressourcenpool hinzufügen**. Wenn Sie nicht über die richtige Lizenz zum Hinzufügen eines anderen Ressourcenpools verfügen, wird eine Fehlermeldung angezeigt.
3. Geben Sie die IP-Adresse oder den DNS-Namen des Citrix Hypervisor ormasterservers in das Feld **Pool Master Server (DNS/IP)** ein.
4. Geben Sie den Benutzernamen und das Kennwort für den Administratorzugriff auf den Server ein.

   Der Benutzer muss über vollständige Verwaltungsfunktionen im Ressourcenpool verfügen. Der vSwitch Controller kann den Pool nicht ordnungsgemäß verwalten, wenn das Konto über eingeschränkte Funktionen verfügt.

   In der Regel ist dieses Konto der Benutzer benannt`root`, kann jedoch ein anderer Name sein, wenn die RBAC-Funktionen der Citrix Hypervisor Plattform verwendet werden.
5. Aktivieren Sie das Kontrollkästchen **Steal** nur, wenn Sie eine vorhandene vSwitch Controller Konfiguration für diesen Ressourcenpool außer Kraft setzen möchten.
6. Klicken Sie auf **Verbinden**.

Der vSwitch Controller verwendet den angegebenen Benutzernamen und das Kennwort, um mit dem Poolmasterserver über das XAPI-Protokoll zu kommunizieren. Wenn eine Kommunikation hergestellt wird, wird der neue Ressourcenpool zusammen mit allen zugeordneten Ressourcen zur Ressourcenstruktur hinzugefügt. Wenn die vSwitch Controller VM nicht mit dem Poolmaster kommunizieren kann, wird eine Fehlermeldung angezeigt, die den Fehler beschreibt.

> **Hinweis:**
>
> Damit der vSwitch Controller mit dem Citrix Hypervisor Ressourcenpool kommunizieren kann, muss der Citrix Hypervisor-Ressourcenpool den **Abwärtskompatibilitätsmodus**verwenden. Dieser Modus ist die Standardeinstellung. Sie können diese Einstellung auf der Seite „ **Pool-Eigenschaften** “ in XenCenter angeben. Weitere Informationen finden Sie in der *XenCenter Hilfe*.

Konfigurieren der Hochverfügbarkeit

Um sicherzustellen, dass Citrix Hypervisor-Server immer einen aktiven vSwitch Controller erreichen können, verwenden Sie Citrix Hypervisor Hochverfügbarkeit für die vSwitch Controller-VM. Weitere Informationen zum Aktivieren der Hochverfügbarkeit auf Citrix Hypervisor finden Sie unterHohe Verfügbarkeit. Der kontinuierliche Betrieb des vSwitch Controller ist für den Betrieb von Netzwerken für alle VMs von entscheidender Bedeutung. Um eine hohe Verfügbarkeit der vSwitch Controller M zu gewährleisten, setzen Sie ihre`restart-priority` auf 1 und`ha-always-run` auf true.

Kopiert!
Failed!

Verwalten von vSwitch

October 16, 2019

Mit der grafischen Benutzeroberfläche von vSwitch Controller können Sie verschiedene Verwaltungsaufgaben ausführen, darunter:

- Status- und Flussstatistiken für Elemente im virtuellen Netzwerk anzeigen
- Richten Sie VM-Zugriffssteuerung, Servicequalität und Datenspiegelungsrichtlinien ein
- Ändern der Konfiguration der virtuellen vSwitch Controller Appliance

Schnittstellenübersicht

Die vSwitch Controller GUI verfügt über drei verschiedene Panels. Diese Panels sind in der nächsten Abbildung dargestellt.

Oberteil

Der obere Bereich ist immer sichtbar, wenn Sie die GUI verwenden und enthält eine Statusleiste und eine Reihe von Hauptnavigationssymbolen.

Statusleiste

Die graue Statusleiste am oberen Rand des vSwitch Controller Fensters enthält die folgenden Informationen und Funktionen (von links nach rechts):

- Version: Aktuelle Version des vSwitch Controller.
- Online-Hilfe: Klicken Sie hier, um einen Onlinehilfebereich oben im Controller-Fenster anzuzeigen oder zu schließen.
- Abmelden: Klicken Sie hier, um sich von der vSwitch Controller GUI abzumelden.
- Benutzer: Zeigt den Benutzernamen des aktuell angemeldeten Benutzers an.
- Symbol „Aktualisieren“: Klicken Sie auf, um die Informationen auf der Seite zu aktualisieren.
- Wiedergabe/Pause: Klicken Sie hier, um einzuschalten, ob die GUI Daten auf dem Bildschirm mithilfe von Hintergrundaktualisierungen automatisch aktualisiert. Im Wiedergabemodus werden die angezeigten Daten automatisch alle 15 Sekunden aktualisiert. Im Pause-Modus werden die meisten Daten nicht aktualisiert. Einige Elemente werden jedoch aktualisiert, insbesondere der Ressourcenbaum. Der Hintergrund der Statusleiste hinter den Schaltflächen wird orange und im Pause-Modus wird in der Statusleiste ein Indikator „Datenaktualisierungen angehalten“ angezeigt.

Oben Symbole

Klicken Sie auf die oberen Symbole, um auf die wichtigsten Funktionsbereiche innerhalb der GUI zuzugreifen.

- Dashboard: Zeigen Sie zusammenfassende Statistiken und Informationen zu Netzwerk- und Administratorereignissen an. Siehe Überwachen des Netzwerkstatus mit dem Dashboard.
- Sichtbarkeit und Kontrolle: Anzeigen von Netzwerkstatus und -statistiken oder Konfigurieren von Zugriffssteuerungs-, QoS- und Datenspiegelungsrichtlinien für virtuelle Netzwerke. Siehe Sichtbarkeit und Kontrolle virtueller Netzwerke.
- Einstellungen: Führen Sie vSwitch Controller Wartungs- und Verwaltungsfunktionen. Siehe Verwalten und Verwalten des vSwitch Controller.

Seitenwand

Die Seitenwand ist nur im Abschnitt Sichtbarkeit und Steuerung und Einstellungen verfügbar.

Für den Abschnitt Sichtbarkeit und Steuerung enthält der Seitenbereich eine Ressourcenstruktur, die Sie zum Durchsuchen von Netzwerkelementen in der virtuellen Netzwerkumgebung verwenden können. Ähnlich wie die Ressourcenstruktur in XenCenter sind Elemente hierarchisch organisiert und bieten eine einfache Möglichkeit, Elemente innerhalb des Systems zu durchsuchen. Um einen Abschnitt der Ressourcenstruktur zu erweitern, klicken Sie auf den seitlichen Pfeil neben dem Knotentext. Ein erweiterter Knoten ist mit einem nach unten gerichteten Pfeil markiert, auf den Sie klicken können, um zu reduzieren.

Wenn Sie ein Element aus der Ressourcenstruktur auswählen, werden im Hauptfenster Status- und Konfigurationsdaten für diesen Knoten in der Struktur angezeigt. Wenn Sie z. B. eine VM aus der Ressourcenstruktur auswählen und im Abschnitt **Sichtbarkeit und KontrolleStatus** auswählen, werden im Hauptfenster Statusinformationen über die ausgewählte VM angezeigt.

Der Ressourcenbaum enthält eine Suchfunktion. Um den Inhalt anhand einer Suchzeichenfolge zu filtern, geben Sie Text in das Suchfeld ein und drücken **Sie die EINGABETASTE**. Klicken Sie auf das **X-Symbol** , um die Suche zu löschen. Suchvorgänge unterstützen Platzhalter (∗ für ein oder mehrere Zeichen und? für ein einzelnes Zeichen). Wenn keine Platzhalter verwendet werden, führt das System eine Teilzeichensuche durch, als ob sich ein∗ Platzhalter am Anfang und am Ende der Suchzeichenfolge befindet. Beispielsweise findet die Suche „Lab“ alle Elemente mit „Lab“ im Namen, wie „Laboratory-1” und „New-Lab-5. „

Für den Abschnitt „Einstellungen“ enthält die Seitenleiste Symbole, mit denen Sie auswählen können, welchen Bereich der vSwitch Controller er-Konfiguration der Benutzer anzeigen oder ändern möchte.

Verwenden der Ressourcenstruktur

Auf der höchsten Ebene werden die folgenden Elemente in der Ressourcenstruktur angezeigt:

- Alle Ressourcenpools: Liste aller verfügbaren Ressourcenpools. Diese Liste ist die oberste Ressource zum Durchsuchen aller Citrix Hypervisor or-Server, Netzwerke, VMs und VIFs, die Teil jedes Ressourcenpools sind.
- Adressgruppen: Benannte Gruppen von IP-Adressen und Subnetzbereichen. Diese Gruppen werden für folgende Zwecke verwendet:
  - So beschränken Sie die Anwendung einer Regel im Bereich Zugriffssteuerung
  - So beschränken Sie den Bereich einer Abfrage im Abschnitt „ **Flow Statistics** “
- VM-Gruppen: Benannte Gruppen von VMs, die verwendet werden sollen, um die Status- und Flussstatistiken einer bestimmten Sammlung von VMs zu vereinfachen.

Wenn Sie einen Ressourcenpool in der Ressourcenstruktur erweitern, werden die folgenden Elemente angezeigt:

- Pool-weite Netzwerke: Diese Liste enthält alle Netzwerke im Ressourcenpool und ähnelt der Liste auf der Registerkarte Netzwerk von XenCenter. Sie können die Liste erweitern, um die einzelnen Netzwerke anzuzeigen, ein Netzwerk erweitern, um die VMs in diesem Netzwerk anzuzeigen, und eine VM erweitern, um ihre VIFs in diesem Netzwerk anzuzeigen.
- Citrix Hypervisor -Server. Diese Liste ähnelt der Serverhierarchie in XenCenter. Sie können die Liste erweitern, um alle Server im Pool anzuzeigen, und einen einzelnen Servereintrag erweitern, um die mit dem Server verknüpften Netzwerke, VMs und VIFs anzuzeigen. Die Liste Servernetzwerke ähnelt dem, was angezeigt wird, wenn Sie in XenCenter auf einen Server klicken und die Registerkarte Netzwerk auswählen.
- Alle VMs: In dieser Liste werden alle VMs im Ressourcenpool angezeigt, unabhängig davon, ob sie für einen einzelnen Server konfiguriert sind. Sie können die Liste erweitern, um die einzelnen VMs anzuzeigen, und eine VM erweitern, um ihre VIFs anzuzeigen.

Rechtsklick-Kontextmenüs auf Knoten sind auf den meisten Knoten verfügbar, um eine einfache Möglichkeit zum Hinzufügen, Ändern und Löschen von Elementen in der Ressourcenstruktur zu bieten.

Farbcodierte Symbole

Farbcodierte Symbole im Ressourcenbaum zeigen den Status von Baumknoten unter dem Knoten „Alle Ressourcenpools“ der obersten Ebene an. Ähnlich wie XenCenter basieren diese Farbcodes auf Daten, die über XAPI von jedem Poolmaster abgerufen werden. Wenn sich ein Knotenstatus ändert, wird das Symbol wie folgt aktualisiert:

- Grün: Ein grünes Symbol zeigt an, dass die Ressource im Netzwerk aktiv ist und vom vSwitch Controller ordnungsgemäß verwaltet wird.

- Rot: Bei einem Ressourcen-Pool-Knoten gibt das rote Zeichen an, dass keine XAPI-Verbindung zum Poolmaster hergestellt werden kann. Wenn der Ressourcen-Pool-Knoten grün ist, zeigt ein rotes Symbol für jeden darunter liegenden Knoten an, dass das Element derzeit im Netzwerk nicht aktiv ist. Beispielsweise wird das Element ausgeschaltet oder getrennt.
- Orange: Ein orangefarbenes Symbol zeigt an, dass der Knoten oder eines seiner abhängigen Elemente nicht ordnungsgemäß verbunden oder verwaltet ist. Auf der Statusseite für die zugeordnete Ressource wird eine Fehlermeldung angezeigt, die das Problem beschreibt.

Die Farbcodes in den Baummenüelementen werden auch auf der Seite Status für den Knoten angezeigt. Ausführliche Informationen zu den Farbcodes und Statusinformationen finden Sie unterBeheben von vSwitch Controller Problemen.

Datenbereich des Hauptfelds

Der Datenbereich des Hauptbereichs enthält Statusinformationen, Statistiken und Konfigurationseinstellungen.

- Dashboard: Es gibt kein Seitenmenü und der Datenbereich des Hauptbereichs nimmt den gesamten Bereich unterhalb des oberen Bereichs ein. Das Dashboard-Hauptfenster bietet einen Überblick über alle virtuellen Netzwerke, die vom vSwitch Controller verwaltet werden.
- Sichtbarkeit und Steuerung: Das Hauptfenster nimmt die rechte Seite des Fensters unterhalb des oberen Bereichs ein. Das Bedienfeld enthält Registerkarten oben, die den folgenden wichtigen Sichtbarkeits- und Kontrollfunktionen entsprechen:
  - Status: Zeigt detaillierte Statusinformationen für den ausgewählten Ressourcenbauknoten an.
  - Flussstatistik: Zeigen Sie ein Diagramm und Daten zur Netzwerkaktivität für den ausgewählten Knoten an.
  - Zugriffssteuerung: Richten Sie Zugriffssteuerungsrichtlinien für den ausgewählten Knoten ein.
  - Port-Konfiguration: Richten Sie Quality of Service und Datenspiegelungsrichtlinien für den ausgewählten Knoten ein.
- Einstellungen: Das Hauptfeld nimmt die rechte Seite des Fensters unter dem oberen Panel ein. Im Einstellungs-Hauptfenster werden Details zum Anzeigen oder Konfigurieren von vSwitch Controller Einstellungen basierend auf dem im Seitenbereich ausgewählten Unterabschnitt angezeigt.

Im Abschnitt Sichtbarkeit und Steuerung ändern sich die im Hauptfenster angezeigten Daten, um die Hierarchieebene und das spezifische Element, das Sie im Seitenbereich ausgewählt haben, zu widerspiegeln.

Wenn Sie beispielsweise einen Ressourcenpool im Seitenbereich auswählen und auf die Registerkarte Zugriffssteuerung klicken, wird im Hauptfenster Folgendes angezeigt:

- Die globale Sicherheitsrichtlinie für die Zugriffskontrolle
- Die Richtlinie für den ausgewählten Ressourcenpool

Wenn Sie im Seitenbereich eine virtuelle Schnittstelle (VIF) auswählen und auf die Registerkarte Zugriffssteuerung klicken, wird das Hauptfenster angezeigt:

- Die globale Sicherheitsrichtlinie für die Zugriffskontrolle
- Die Richtlinie für den Ressourcenpool, der die VIF enthält
- Die Richtlinie für die VM, die die VIF enthält
- Die Richtlinie für das ausgewählte VIF

Überwachen des Netzwerkstatus mit dem Dashboard

Das Dashboard enthält zusammenfassende Statistiken und Informationen zu Ereignissen in der virtuellen Netzwerkumgebung. Um das Dashboard anzuzeigen, klicken Sie oben in der vSwitch Controller Schnittstelle auf das **Dashboard-Symbol** .

Das Dashboard ist in die in diesem Abschnitt beschriebenen Bereiche unterteilt. Die Informationen werden automatisch alle paar Sekunden aktualisiert.

Serverstatistik

Dieser Abschnitt enthält die folgenden allgemeinen Informationen zum vSwitch Controller.

- Up-Zeit: Länge der Zeit seit dem letzten Start des vSwitch Controller.
- CPU-Last: Aktueller Prozentsatz der CPU-Auslastung für die virtuelle vSwitch Controller Appliance.

Netzwerkstatistik

In diesem Abschnitt wird eine Bestandsaufnahme der Netzwerkelemente (Ressourcenpools, Citrix Hypervisor or-Server, Netzwerke und VMs) für jede der folgenden Kategorien angezeigt:

- Verwaltet: Anzahl der Elemente dieses Typs, die sich gemäß XAPI im laufenden Zustand befinden und derzeit vom vSwitch Controller verwaltet werden.
- Aktiv: Anzahl der Elemente dieses Typs, die sich gemäß XAPI in einem laufenden Zustand befinden. Enthält verwaltete und nicht verwaltete Elemente.
- Summe: Anzahl der Elemente dieses Typs (aktiv oder nicht), die über XAPI bekannt sind.

Wenn das System konfiguriert und ordnungsgemäß funktioniert, sind die verwalteten und aktiven Zählungen identisch. Die Gesamtanzahl ist immer gleich oder größer als die verwaltete und aktive Anzahl. Komponenten, die ausgeschaltet sind, werden nicht als vom Controller verwaltet angezeigt.

Aktuelle Netzwerkereignisse

In diesem Abschnitt werden die neuesten Ereignisse aufgeführt, die seit dem letzten Neustart des vSwitch Controller in den verwalteten virtuellen Netzwerken aufgetreten sind. Verwenden Sie die Bildlaufleiste auf der rechten Seite, um durch die Liste zu blättern. Das letzte Ereignis wird zuerst aufgeführt. Im Laufe der Zeit werden ältere Ereignisse aus der Liste gelöscht.

Für jedes Netzwerkereignis werden folgende Informationen gemeldet:

- Priority: Relative Bedeutung des Ereignisses.
- Datum/Uhrzeit: Datum und Uhrzeit des Auftretens des Ereignisses.
- Ereignis: Beschreibung des Ereignisses. Sie können in einer Ereignisbeschreibung auf Hyperlinks klicken, um auf die entsprechenden Sichtbarkeits- und Kontrollstatusseiten der im Ereignis erwähnten Netzwerkelemente zuzugreifen.

Netzwerkereignisse können für einen dauerhafteren Datensatz auf einen Syslog-Server exportiert werden. Weitere Informationen finden Sie unter Exportieren von Syslog-Dateien.

Jüngste administrative Ereignisse

In diesem Abschnitt werden Ereignisse aufgeführt, die innerhalb des vSwitch Controller aufgetreten sind, häufig infolge einer Änderung der Konfiguration innerhalb der Benutzeroberfläche durch einen Administrator. Verwenden Sie die Bildlaufleiste auf der rechten Seite, um durch die Liste zu blättern. Das letzte Ereignis wird zuerst aufgeführt. Im Laufe der Zeit werden ältere Ereignisse aus der Liste gelöscht.

Für jedes administrative Ereignis werden folgende Informationen gemeldet:

- Priority: Relative Bedeutung des Ereignisses.
- Datum/Uhrzeit: Datum und Uhrzeit des Auftretens des Ereignisses.
- Ereignis: Beschreibung des Ereignisses. Sie können in einer Ereignisbeschreibung auf Hyperlinks klicken, um auf die Seiten Sichtbarkeit und Kontrollstatus der im Ereignis erwähnten Netzwerkelemente zuzugreifen.

Netzwerkereignisse können für einen dauerhafteren Datensatz auf einen Syslog-Server exportiert werden. Weitere Informationen finden Sie unter Exportieren von Syslog-Dateien.

Durchsatz-, Fluss- und Bitratendiagramme

Diese Diagramme zeigen Informationen über das Verhalten der aktivsten VMs und Protokolle an.

Die Diagramme zeigen die folgenden Informationen an:

- Aggregierter Durchsatz (Bit/s) für die letzte Stunde

- Aggregate Paketrate (Pakete/Sek) für die letzte Stunde
- Aggregierte Verbindungsrate (Flows/s) für die letzte Stunde

Kopiert!
Failed!

Sichtbarkeit und Kontrolle virtueller Netzwerke

October 16, 2019

Im Abschnitt Sichtbarkeit und Kontrolle können Sie das Netzwerkverhalten überwachen und die Netzwerkrichtlinie konfigurieren. Um auf die Seiten zuzugreifen, wählen Sie oben auf der vSwitch Controller-Schnittstelle das Symbol **Sichtbarkeit und Steuerung** aus.

Status anzeigen

Die Registerkarte **Status** enthält detaillierte Informationen in Tabellenform über den Knoten, der in der Ressourcenstruktur ausgewählt ist. Die Art der dargestellten Informationen variiert je nach ausgewähltem Knoten. Die meisten einzelnen Tabelleneinträge sind Links. Sie können auf diese Links klicken, um die Statusseite anzuzeigen, die für diesen Tabelleneintrag gilt.

Alle Bytezahlen und Fehlerzahlen werden auch dann akkumuliert, wenn ein Citrix Hypervisor or-Server neu gestartet oder eine VM neu gestartet oder migriert wird. Die Farbcodes folgen den gleichen Regeln wie die Farbcodes in der Seitenwand. Siehe Farbcodierte Symbole.

Globale Ebene

Auf globaler Ebene wird auf der Seite Status eine Tabelle mit allen Ressourcenpools mit den folgenden Informationen angezeigt:

- Ressourcenpool: Name des Ressourcenpools.
- # Server: Anzahl der Server im Pool.
- # Netzwerke: Anzahl der Netzwerke im Pool.
- # VMs: Anzahl der VMs im Pool.
- Status: Farbcodiertes Symbol, das den aktuellen Poolstatus anzeigt.

Durch Klicken auf das Zahnradsymbol auf der rechten Seite einer Zeile können Sie den Ressourcenpool ändern.

Auf dieser Seite können Sie auch verfügbare Ziel-VLANs für Portkonfigurationsrichtlinien angeben. Siehe Richten Sie Portkonfigurationsrichtlinien ein.

Ressourcenpoolebene

Für einen ausgewählten Ressourcenpool enthält die Seite Status die folgenden Informationen:

- Status: Farbcodiertes Symbol, das den aktuellen Poolstatus anzeigt.
- Poolmaster: IP-Adresse oder DNS-Name des Masterservers im Pool.
- Pool-weite Netzwerke: Anzahl der Netzwerke im Pool.
- Citrix Hypervisor: Anzahl der Server im Pool.
- Alle VMs: Anzahl der VMs im Pool.
- Serverliste: Liste der Server im Pool, einschließlich Servername, Anzahl der Netzwerke, Anzahl der VMs und Status.

Zusätzlich zur Anzeige von Statusinformationen können Sie konfigurieren, wie die Citrix Hypervisor or-Server im Pool Netflow-Daten weiterleiten. Select die folgenden Kontrollkästchen, und klicken Sie auf **Netflow-Konfiguration speichern**:

- vSwitch Controller (standardmäßig ausgewählt): leitet Netflow-Informationen an den vSwitch Controller weiter, um sie durch den Abschnitt „Flow Statistics“ der GUI zu verwenden. Wenn Sie dieses Kontrollkästchen deaktivieren, werden die Netflow-Daten nicht an den vSwitch Controller gesendet, und auf den Seiten „Flow Statistics“ werden keine Daten angezeigt.
- Externer Netflow-Controller: Ermöglicht die Weiterleitung von Netflow-Daten an einen externen Netflow-Collector von Drittanbietern. Geben Sie die IP-Adresse des externen Collectors ein.

Ausfallsicherer Modus

Verwenden Sie den Abschnitt **Fehlermodus** , um zu konfigurieren, wie ein vSwitch die Zugriffssteuerungsregeln erzwingt, wenn er keine Verbindung mit seinem vSwitch Controller herstellen kann. Es ist wichtig, ein hohes Maß an vSwitch Controller Verfügbarkeit aufrechtzuerhalten, um Datenverlust zu vermeiden. In Zeiten, in denen der vSwitch Controller nicht verfügbar ist, gelten die folgenden Fehlermodi:

- Fail-Open: Der gesamte Datenverkehr ist zulässig, zuvor definierte ACLs gelten erst dann, wenn der vSwitch wieder eine Verbindung mit dem vSwitch Controller herstellen kann.
- Ausfallsicher: Vorhandene ACLs gelten weiterhin.

Im normalen Betrieb verwaltet der vSwitch Verbindungen zu seinem konfigurierten vSwitch Controller, um Netzwerkverwaltungs- und Statusinformationen auszutauschen. Wenn der vSwitch Controller nicht verfügbar ist, wartet der vSwitch bis zu einem Inaktivitäts-Timeout, bei dem der Netzwerkverkehr unterbrochen wird. Nach dem Inaktivitäts-Timeout wechselt der vSwitch in den konfigurierten Fail-Modus.

Im ausfallsicheren Modus werden vorhandene ACLs weiterhin angewendet, nachdem der vSwitch die Verbindung zum konfigurierten vSwitch Controller verliert. Datenverkehr, der nicht mit vorhandenen ACLs übereinstimmt, wird verweigert. Alle ACLs auf jeder Ebene der vom Controller dargestell-

ten Richtlinienhierarchie werden als Regelsätze für VIFs im vSwitch erzwungen. Daher können neue VIFs, die im ausfallsicheren Modus angezeigt werden, während der Controller nicht verfügbar ist, erst kommunizieren, wenn der Controller wieder verfügbar ist. Vorhandene VIFs, die getrennt und dann neu angeschlossen werden, haben das gleiche Verhalten wie neue VIFs. Diese Situation tritt auf, auch wenn übergeordnete ACL-Richtlinienregeln (global, pro Ressourcenpool, pro Netzwerk oder pro VM), die die Kommunikation auf vorhandenen VIFs zulassen, vorhanden sind. Darüber hinaus kann der vSwitch Controller ACLs basierend auf den erlernten IP-Adressen definieren. Im ausfallsicheren Modus werden Pakete, die von einer VM mit einer IP-Adresse gesendet werden, die der Controller nicht mit der VM verknüpft hat, bevor sie nicht verfügbar wurde, verweigert. Beispielsweise kann eine vorhandene VM, die eine neue IP-Adresse verwendet, erst kommunizieren, wenn der Controller wieder erreichbar ist. Weitere Beispiele, bei denen Datenverkehr im ausfallsicheren Modus verweigert wird, sind:

- Neu gesteckte VIFs
- Eine neue VM
- Eine migrierte VM (z. B. Live-Migration oder Workload Balancing)
- VMs auf Hosts, die einem Pool hinzugefügt wurden
- Anwendungen, die wie ein Router funktionieren

Wenn der vSwitch im ausfallsicheren Modus neu gestartet wird und der Controller nach dem Start des vSwitch immer noch nicht verfügbar ist, gehen alle ACLs verloren und der gesamte Datenverkehr wird verweigert. Der vSwitch bleibt im ausfallsicheren Modus, bis eine Verbindung mit dem Controller wieder hergestellt wird und ACLs vom Controller an den vSwitch gedrückt werden.

> **Warnhinweis:**
>
> Das Entfernen eines Ressourcenpools aus der vSwitch Controller Verwaltung im ausfallsicheren Modus kann dazu führen, dass der vSwitch Netzwerkkonnektivität verliert und eine Notfall-Reset-Situation erzwungen wird. Um diese Situation zu verhindern, entfernen Sie einen Ressourcenpool nur, wenn sein Status grün ist.

Sie können auf dieser Seite auch verfügbare Ziel-VLANs für Portkonfigurationsrichtlinien angeben. Weitere Informationen finden Sie unter Richten Sie Portkonfigurationsrichtlinien ein.

Serverebene

Für einen ausgewählten Server enthält die Seite Status die folgenden Informationen:

- Serverstatus: Farbcodiertes Symbol, das den aktuellen Serverstatus anzeigt.
- Servernetzwerke: Anzahl der Netzwerke im Ressourcenpool.
- MAC-Adresse: MAC-Adresse der Server-Management-Schnittstelle.
- IP-Adresse: IP-Adresse der Serververwaltungsschnittstelle.

- vSwitch-Version: Build- und Versionsnummer des vSwitches, der auf diesem Citrix Hypervisor ausgeführt wird.
- Servernetzwerke: Liste aller Netzwerke, die dem Server zugeordnet sind. Diese Informationen umfassen:
  - Die Anzahl der VMs auf dem Server, die dieses Netzwerk verwenden
  - Die zugeordnete physikalische Schnittstelle,
  - Das VLAN
  - Die Anzahl der übertragenen und empfangenen Bytes
  - Die Anzahl der Fehler
  - Der Status
- Server-VMs: Liste aller VMs, die dem Server zugeordnet sind. Für jede VIF auf der VM umfassen diese Informationen auch:
  - Die MAC-Adresse
  - Das Netzwerk
  - Die IP-Adresse
  - Die Gesamtzahl der seit dem Starten der VM übertragenen und empfangenen Bytes
  - Der Status

Auf dieser Seite können Sie auch verfügbare Ziel-VLANs für Portkonfigurationsrichtlinien angeben. Siehe Richten Sie Portkonfigurationsrichtlinien ein.

Netzwerkebene

Auf der Registerkarte Status für Pool-weite Netzwerke werden zusammenfassende Informationen zu jedem Netzwerk im Ressourcenpool aufgeführt. Auf der Registerkarte Status für ein einzelnes Netzwerk werden Informationen über das Netzwerk selbst aufgeführt. Die Registerkarte enthält Hyperlink-Tabellen mit Informationen über die physischen Schnittstellen und VM-Schnittstellen, die derzeit mit dem Netzwerk verbunden sind.

Das Statussymbol kann in folgenden Farben angezeigt werden:

- Grün, wenn das Netzwerk aktiv und ordnungsgemäß vom vSwitch Controller verwaltet wird
- Rot, wenn das Netzwerk keine verbundenen Schnittstellen hat
- Orange, wenn eine Fehlerbedingung vorliegt. Der zugehörige Text beschreibt den Fehler.

Für Pool-weite Netzwerke werden folgende Informationen angezeigt:

- Netzwerkname: Bestimmtes Netzwerk.
- VMs: Anzahl der VMs, die dem Netzwerk zugeordnet sind.
- Citrix Hypervisor: Server für das Netzwerk.
- Physische Schnittstelle: Server-Schnittstelle für das Netzwerk.
- Pakete übertragen (Tx) und empfangen (Rx): Aggregierte Leistungsindikatoren über alle VIFs im angegebenen Netzwerk.

- Fehler: Aggregierte Leistungsindikatoren über alle VIFs im angegebenen Netzwerk.
- Status: Farbcodiertes Symbol, das das aktuelle Netzwerk anzeigt.

Für ein ausgewähltes Netzwerk werden folgende Informationen dargestellt:

- Netzwerkstatus: Farbcodiertes Symbol, das das aktuelle Netzwerk anzeigt.
- VMs: Anzahl der VMs, die dem Netzwerk zugeordnet sind.
- Physische Schnittstellen: Liste der physischen Schnittstellen, einschließlich VLAN, Anzahl der übertragenen und empfangenen Bytes, Fehler und Status.
- Switching von Citrix Hypervisor (nur in serverübergreifenden privaten Netzwerken vorhanden): Gibt den aktuellen aktiven Switching-Host für das Netzwerk an.
  Ein serverübergreifendes privates Netzwerk ermöglicht die Kommunikation zwischen VMs im selben Ressourcenpool, ohne dass eine zusätzliche Konfiguration des physischen Netzwerks erforderlich ist. Die VMs können auf verschiedenen Hosts ausgeführt werden. Diese Fähigkeit wird erreicht, indem ein „Switching-Host“ GRE-Tunnel zu jedem der anderen Hosts im Pool einrichtet. Die GRE Tunnel sind in einer Sterntopologie aufgebaut. Die anderen Hosts verfügen über eine aktive VM, die im privaten Netzwerk ausgeführt wird.
  Wenn ein Switching-Host nicht verfügbar ist oder gelöscht wird, wird automatisch ein neuer Switching-Host ausgewählt und neue GRE-Tunnel konfiguriert. Vernetzung/de-de/citrix-hypervisor/networking.html[()]Weitere Informationen zu serverübergreifenden privaten Netzwerken finden Sie unter.
- VM-Schnittstellen: Liste der VMs, einschließlich MAC-Adresse, IP-Adresse, Anzahl der übertragenen und empfangenen Bytes und Status.

Auf dieser Seite können Sie auch verfügbare Ziel-VLANs für Portkonfigurationsrichtlinien angeben. Weitere Informationen finden Sie unter Richten Sie Portkonfigurationsrichtlinien ein.

Ebene der virtuellen Maschine (VM)

Die folgenden Informationen werden für alle VMs angezeigt:

- VM-Name: Name der spezifischen VM.
- MAC-Adresse: MAC-Adresse, die der VM zugewiesen ist.
- Netzwerkname: Netzwerk, dem die VM zugewiesen ist.
- Erkannte IP-Adresse: der VM zugewiesene IP-Adressen.
- Pakete übertragen (Tx) und empfangen (Rx): Aggregierte Leistungsindikatoren über alle VIFs auf der angegebenen VM.
- Fehler: Aggregierte Leistungsindikatoren über alle VIFs auf der angegebenen VM.

Für eine ausgewählte VM werden auf der Seite Status die folgenden Informationen angezeigt:

- Status: Farbcodiertes Symbol, das den aktuellen VM-Status anzeigt.
- Ressourcenpool: Ressourcenpool, zu dem die VM gehört.

- Servername: Name des Servers, dem die VM zugewiesen ist. Diese Informationen sind leer, wenn die VM nicht ausgeführt wird und nicht an einen bestimmten Server gebunden ist.
- VM-Gruppenmitgliedschaft: Liste der administrativen Gruppen, denen die VM zugewiesen ist.
- VM-Schnittstellen: Liste der VIFs auf der VM. Diese Informationen umfassen:
  - MAC-Adresse
  - Netzwerkname
  - Erkannte IP-Adresse
  - Übertragen und Empfangen von Bytes, Paket- und Fehlerzählungen
  - Status
- Netzwerkereignisse: Liste der Netzwerkereignisse, die die VM betreffen, einschließlich Priorität, Datum/Uhrzeit und Beschreibung.

Ebene der virtuellen Schnittstelle (VIF)

Für ein ausgewähltes VIF enthält die Seite Status die folgenden Informationen:

- Status: Farbcodiertes Symbol, das den aktuellen VIF-Status anzeigt.
- Ressourcenpool: Ressourcenpool, zu dem das VIF gehört.
- Netzwerk: Netzwerk, zu dem das VIF gehört.
- VM-Name: VM, zu der das VIF gehört.
- MAC-Adresse: MAC-Adresse des VIF.
- IP-Adresse: IP-Adresse des VIF.
- Senden und Empfangen von Bytes, Paketen und Fehlern: Datenverkehr zählt für die VIF.
- Switch-Port-ACL-Statistiken: Im Gegensatz zu Sende- und Empfangszählungen sind die ACL-Trefferanzahl momentane Statistiken, die aus den ACL-Regelstatistiken des aktuellen vSwitch gelesen werden. Daher führen Richtlinienänderungen und VM-Aktionen wie Suspendierung, Herunterfahren oder Migration dazu, dass diese Statistiken zurückgesetzt werden.Für die vSwitch-ACL-Statistiken muss eine IP-Adresse im Netzwerk identifiziert werden und Statistiken für IP-basierte Protokolle sammeln können. Wenn Sie feststellen, dass IP-basierte Regeln nicht berücksichtigt werden, stellen Sie sicher, dass eine IP-Adresse im Feld IP-Adresse angezeigt wird.

Anzeigen von Flow-Statistiken

Standardmäßig sendet der vSwitch auf jedem verwalteten Citrix Hypervisor Netflow-Daten an den vSwitch Controller, der diese Daten verwendet, um Flow-Statistiktabellen und -Diagramme zu generieren. Der vSwitch generiert Netflow-Datensätze für alle IPv4-Flows nach fünf Sekunden ohne Aktivität oder 60 Sekunden Gesamtaktivität.

Die Datenrate eines Flows wird als Gesamtverkehr des Flows dargestellt, der über die Dauer des Flows gemittelt wird. Wenn ein Flow beispielsweise 10 Sekunden dauert, wobei 900 KB in der ersten

Sekunde gesendet und 10 KB in jeder der neun verbleibenden Sekunden gesendet werden, werden die resultierenden Daten so dargestellt, als ob die Rate 100 KB/s für den gesamten Flusszeitraum betrug.

Netflow verwendet UDP-Datagramme, um NetFlow-Datensätze zwischen einem Switch und einem Collector zu transportieren (z. B. dem vSwitch Controller). Da NetFlow UDP-Datagramme verwendet, kann der Collector normalerweise nicht wissen, warum ein NetFlow-Datensatz nicht empfangen wurde. Verfallene Datensätze können zu nichtdeterministischen Daten mit Flow Statistics Tabellen oder Diagrammen führen. Angenommen, ein Netzwerk, das 10 Flows pro Sekunde generiert, verfügt über eine einzelne 1-GB-Dateiübertragung, die 10 Sekunden dauert. Das Netzwerk erzeugt insgesamt 202 Flows (100 Hping-Reize, 100 Hping-Antworten, 1 Dateiübertragungsstimulus und 1 Dateiübertragungsantwort). Wenn 50% der UDP-Datagramme gelöscht werden, besteht eine Wahrscheinlichkeit von 50/50, dass der Collector entweder 1 GB Daten oder 2 KB meldet.

Da jeder vSwitch in einem Pool Netflow-Datensätze generiert, führen Quellen und Ziele, die auf verschiedenen Citrix Hypervisor or-Servern ausgeführt werden, zu zwei Datensätzen, wodurch die Statistikanzahl verdoppelt wird.

Deaktivieren Sie die Flow-Transparenz in Bereitstellungen von mehr als 100 VMs, um eine Überlastung der virtuellen vSwitch Controller Appliance und des Netzwerkes zu vermeiden, das zum Senden von NetFlow-Datensätzen verwendet wird.

Auf der Registerkarte „ **Flow-Statistiken** “ werden ein Diagramm und eine zugehörige Tabelle angezeigt, in der die Flows für den ausgewählten Knoten angezeigt werden.

Verwenden Sie die Listen oben auf der Seite, um Folgendes anzugeben:

- Richtung: Bidirektional, Inward, Outbound
- Einheiten: Bytes, Bits, Pakete, Flows
- Die oberen oder unteren Elemente (höchste oder niedrigste Werte) einer der folgenden Gruppierungen:
  - VMs: VMs, die sich im Ressourcenpool als Quellen/Ziele für den Datenverkehr befinden
  - IP-Adressen: IP-Adressen als Quelle oder Ziel für den Datenverkehr
  - Protokolle: IP-Protokollverkehr wie ICMP, TCP und UDP

    > **Hinweis:**
    > Ethernet-Layer-Protokolle (z. B. ARP) werden aufgrund der Einschränkungen im Netflow-Protokoll, das zum Generieren von Ergebnissen verwendet wird, nicht angezeigt.

  - Anwendung: Protokollverkehr auf Anwendungsebene, identifiziert durch TCP/UDP-Port oder ICMP-Typ/Code
- Datenverkehr (nach Typ): VMs, IP-Adresse, Protokolle, Anwendungen (nach Protokolltyp und Portnummer angezeigt, diese Informationen können Sie den Dienst ableiten)
- Zeitintervall.

In der Tabelle unterhalb des Diagramms werden einige oder alle der folgenden Informationen angezeigt, je nach Typ des in der Liste ausgewählten Elements:

- VM
- IP
- Eingehende Bytes
- Eingangsdatenrate (KBit/s)
- Ausgehende Bytes
- Ausgehende Datenrate (KBit/s)
- Bytes insgesamt
- Gesamte Datenrate (bps)

Wenn NetFlow nicht an den vSwitch Controller weitergeleitet wird, wird auf der Registerkarte „Flow Statistics“ ein blauer Statustext angezeigt:`One or more selected pools are not configured to forward NetFlow records to vSwitch Controller`

Um die Weiterleitung neu zu konfigurieren, klicken Sie auf den blauen Statustext, um eine Liste der Ressourcenpools anzuzeigen. Select den gewünschten Ressourcenpool aus der Liste aus, um zur Poolstatusseite zu navigieren. Auf der Statusseite können Sie NetFlow-Datenweiterleitung konfigurieren.

Verwalten von Adressgruppen

Sie können Adressgruppen einrichten, um die IP-Adressen anzugeben, die als Quelle oder Ziel für ACLs und für die Berichterstellung von Flussstatistiken verwendet werden sollen.

So fügen Sie eine Adressgruppe hinzu:

1. Wählen Sie unter **Sichtbarkeit und Steuerung**in der Ressourcenstruktur (Seitenbereich) die Option **Adressgruppen**aus, um die Seite Status für alle Adressgruppen zu öffnen.
2. Klicken Sie auf **Gruppe erstellen**.
3. Geben Sie den Namen für die Identifizierung der Gruppe und eine optionale Beschreibung ein.
4. Klicken Sie auf **Gruppe erstellen**. Die neue Gruppe wird der Liste der Adressgruppen hinzugefügt.
5. Select die neue Gruppe in der Ressourcenstruktur aus, um die **Statusseite** zu öffnen.
6. Klicken Sie auf die Schaltfläche **Mitglieder hinzufügen** .
7. Geben Sie im Popup-Fenster eine oder mehrere IP-Adressen oder Subnetze an (durch Kommas getrennt). Beispiel: 192.168.12.5, 192.168.1.0/24
8. Klicken Sie auf **Hinzufügen**. Fügen Sie bei Bedarf weitere Netzwerke hinzu. Jede Adressengruppe wird als Knoten unter dem Netzwerk in der Liste Adressgruppen hinzugefügt.

Die neue Adressgruppe ist jetzt für ACL-Richtlinien und Flussstatistiken verfügbar.

Sie können eine vorhandene Adressgruppe entfernen, indem Sie in der Zeile der Alle Adressgruppen für diese Adressgruppe auf den Link Entfernen klicken.

Sie können auch den Namen oder die Beschreibung der und die Adressgruppe aktualisieren:

1. Select die neue Gruppe in der Ressourcenstruktur aus, um die **Statusseite** zu öffnen.
2. Klicken Sie auf die Schaltfläche **Gruppe ändern** .
3. Ändern Sie im sich öffnenden Dialog den Namen und die Beschreibung.
4. Klicken Sie auf die Schaltfläche **Gruppe ändern** , um die Änderungen zu speichern.

Verwalten von Gruppen virtueller Maschinen

Eine VM-Gruppe ist eine Gruppe von VMs, die Sie als Gruppe zum Anzeigen von Status- und Flussstatistiken identifizieren. Jede VM in einer VM-Gruppe muss sich bereits in einem Ressourcenpool befinden. Die Gruppen sind ansonsten unabhängig von Ressourcenpools und Servern.

So fügen Sie eine VM-Gruppe hinzu:

1. Wählen Sie unter **Sichtbarkeit und Steuerung**die Option **VM-Gruppen**in der Ressourcenstruktur (Seitenbereich) aus, um die Seite Status für alle VM-Gruppen zu öffnen.
2. Klicken Sie auf die Schaltfläche Gruppe erstellen.
3. Geben Sie den Namen für die Identifizierung der Gruppe und eine optionale Beschreibung ein.
4. Klicken Sie auf **Gruppe erstellen**. Die neue Gruppe wird der Liste der VM-Gruppen hinzugefügt.
5. Select die neue Gruppe in der Ressourcenstruktur aus, um die **Statusseite** zu öffnen.
6. Klicken Sie auf **Mitglied hinzufügen**.
7. Wählen Sie im Popup-Fenster die VM aus der Liste aus.
8. Klicken Sie auf **Hinzufügen**. Fügen Sie bei Bedarf weitere VMs hinzu. Jede VM wird als Unterknoten unter der Gruppe in der Liste VM-Gruppen hinzugefügt.

Für jede VM-Gruppe stehen folgende Rechtsklickoptionen zur Verfügung:

- VM zu Gruppe hinzufügen: Fügen Sie ein neues Gruppenmitglied hinzu.
- Name/Beschreibung ändern: Ändern Sie den Namen oder die Beschreibung.
- Gruppe entfernen: Löschen Sie die Gruppe.

Konfigurationshierarchie der DVS-Richtlinie

Verwenden Sie die Registerkarten Zugriffssteuerung und Portkonfiguration in **Sichtbarkeit & Steuerung** , um Zugriffssteuerungs-, QoS- und Datenspiegelungsrichtlinien innerhalb der virtuellen Netzwerkumgebung zu konfigurieren. Während alle Richtlinien auf VIF-Ebene angewendet werden, stellt vSwitch Controller ein hierarchisches Richtlinienmodell bereit, das das Deklarieren von Standardrichtlinien für eine Sammlung von VIFs unterstützt. Der vSwitch Controller bietet auch eine Möglichkeit, diese Standardrichtlinie zu überschreiben, indem bei Bedarf feinkörnige Ausnahmen erstellt werden. Beispielsweise können Sie eine bestimmte VM von der standardmäßigen Ressourcenpool-Richtlinie ausnehmen.

Ähnlich wie die in der Ressourcenstruktur verwendete Hierarchie weist die Richtlinienhierarchie die folgenden Ebenen auf:

- Global (allgemeinste Ebene): Enthält alle VIFs in allen Ressourcenpools.
- Ressourcenpools: Alle VIFs in einem bestimmten Ressourcenpool.
- Netzwerke: Alle VIFs, die an ein bestimmtes Netzwerk angeschlossen sind.
- VMs: Alle VIFs, die an eine bestimmte VM angeschlossen sind
- VIFs (spezifischste Stufe): Ein einzelnes VIF.

> **Hinweis:**
>
> Citrix Hypervisor-Server sind nicht in der Richtlinienhierarchie enthalten, da Richtlinien unabhängig davon gelten müssen, welche Citrix Hypervisor in einem Ressourcenpool eine VM ausführt.

Einrichten von Zugriffssteuerungsrichtlinien

Wählen Sie die Registerkarte **Zugriffssteuerung** , um Richtlinien einzurichten, die VM-Datenverkehr basierend auf Paketattributen zulassen oder verweigern.

Eine ACL-Richtlinie besteht aus einer Reihe von Regeln, die jeweils Folgendes umfassen:

- Aktion: Gibt an, ob Datenverkehr, der der Regel entspricht, zulässig ist (Zulassen) oder gelöscht (Verweigern).
- Protokoll: Netzwerkprotokoll, für das die Regel gilt. Sie können die Regel auf alle Protokolle anwenden (Beliebig), eine vorhandene Protokollliste auswählen oder ein neues Protokoll angeben.
- Richtung: Verkehrsrichtung, für die die Regel gilt. Lesen Sie den Text der Regeln von links nach rechts: „nach“ bedeutet Datenverkehr, der von der VM ausgehend ist, während „von“ Datenverkehr, der an die VM eingeht.
- Remoteadressen: Gibt an, ob die Regel auf den Datenverkehr zu/von einer bestimmten Gruppe von Remote-IP-Adressen beschränkt ist.

Die Verwaltung von ACL-Richtlinien folgt eng mit der Ressourcenstrukturhierarchie. Sie können Richtlinien auf jeder unterstützten Ebene der Hierarchie angeben. Auf jeder Ebene sind die Regeln wie folgt organisiert:

- Obligatorische Regeln: Diese Regeln werden vor untergeordneten Richtlinienregeln ausgewertet. Die einzigen Regeln, die Vorrang vor ihnen haben, sind obligatorische Regeln von übergeordneten (weniger spezifischen) Richtlinien. Obligatorische Regeln werden verwendet, um Regeln anzugeben, die untergeordnete (spezifischere) Richtlinien nicht überschreiben können.
- Untergeordnete Regeln: Der Platzhalter für untergeordnete Richtlinien gibt den Speicherort in der Regelreihenfolge an, in der Regeln in untergeordneten Richtlinien ausgewertet werden. Es teilt die obligatorischen Regeln von den Standardregeln.

- Standardregeln: Diese Regeln werden zuletzt ausgewertet, nachdem alle obligatorischen Regeln und alle untergeordneten Policy-Standardregeln. Sie haben nur Vorrang vor Standardregeln übergeordneter Richtlinien. Sie werden verwendet, um Verhalten anzugeben, das nur angewendet wird, wenn eine spezifischere untergeordnete Richtlinie kein widersprüchliches Verhalten angibt.

Global Access Control List (ACL) -Regeln

Um globale ACL-Regeln einzurichten, klicken Sie in der **Ressourcenstruktur auf Alle Ressourcenpools** . Auf der Seite werden alle ACL-Regeln aufgeführt, die auf globaler Ebene definiert sind.

Resource Pool-Zugriffssteuerungslistenregeln (ACL)

Um ACL-Regeln für einen Ressourcenpool einzurichten, wählen Sie den Ressourcenpool in der Ressourcenstruktur aus.

Die Seite zeigt einen erweiterbaren Balken für globale Richtlinien und einen erweiterten Bereich für Ressourcenpoolregeln. Wenn Sie auf die Schaltfläche **Alle erweitern** klicken, können Sie sehen, wie die Ressourcenpoolregeln in das globale Richtlinienframework eingebettet sind.

ACL-Regeln (Network Access Control List)

Um ACL-Regeln auf Netzwerkebene einzurichten, klicken Sie in der Ressourcenstruktur auf das Netzwerk.

Die Seite zeigt Folgendes:

- Ein erweiterbarer Balken für globale Regeln
- Ein erweiterbarer Balken für den Ressourcenpool, zu dem das Netzwerk gehört
- Ein erweiterter Bereich für Netzwerkregeln

Wenn Sie auf **Alle erweitern**klicken, können Sie sehen, wie die Netzwerkrichtlinien in das Ressourcenrichtlinien-Framework und in das globale Richtlinienframework eingebettet sind.

VM-Zugriffssteuerungslisten-Regeln (ACL)

Um Richtlinien auf VM-Ebene einzurichten, klicken Sie in der Ressourcenstruktur auf die VM.

Die Seite zeigt Folgendes:

- Ein erweiterbarer Balken für globale Regeln
- Erweiterbare Balken für den Ressourcenpool und das Netzwerk, zu dem die VM gehört

- Ein erweiterter Bereich für VM-Regeln

Wenn Sie auf die Schaltfläche **Alle erweitern** klicken, können Sie sehen, wie die VM-Regeln in das Netzwerk, den Ressourcenpool und das globale Framework eingebettet sind.

Wenn eine VM VIFs in mehreren Netzwerken enthält, wird rechts neben der Beispielleiste für das Netzwerk ein Link „Netzwerk ändern“ angezeigt. Mit diesem Link können Sie die Regeln für jede Richtlinie auf Netzwerkebene anzeigen, die für eine VIF auf dieser VM gelten könnten.

VIF-Zugriffssteuerungslisten-Regeln (ACL)

Um Richtlinien auf VIF-Ebene einzurichten, klicken Sie in der Ressourcenstruktur auf das VIF. Da Richtlinien nur auf VIF-Ebene verpackt und angewendet werden, müssen Sie die VIF-Seiten anzeigen, um den vollständigen Richtlinienkontext anzuzeigen.

Die Seite zeigt Folgendes:

- Erweiterbare Balken für globale Regeln
- Erweiterbare Balken für den Ressourcenpool, das Netzwerk und die VM, zu der das VIF gehört
- Ein erweiterter Bereich für VIF-Regeln

Wenn Sie auf die Schaltfläche **Alle erweitern** klicken, können Sie sehen, wie die VIF-Regeln in die VM, das Netzwerk, den Ressourcenpool und das globale Framework eingebettet sind.

Zugriffssteuerungsliste (ACL) -Regelerzwingungsreihenfolge

Obwohl ACLs auf verschiedenen Ebenen der Richtlinienkonfigurationshierarchie definiert werden können, werden ACLs pro VIF-Basis erzwungen. Für die tatsächliche Erzwingung wird die Hierarchie in der in diesem Abschnitt beschriebenen Reihenfolge kombiniert und auf jedes VIF angewendet. Um die aktuell angewendeten Regeln für eine VIF und die zugehörigen Statistiken anzuzeigen, wählen Sie die VIF in der Ressourcenstruktur aus. Zeigen Sie die ACL-Liste auf der Registerkarte Status an.

Die Vollstreckungsbefehl lautet wie folgt:

1. Obligatorische Regeln auf globaler Ebene
2. Obligatorische Regeln für den Ressourcenpool, der das VIF enthält
3. Obligatorische Regeln für das Netzwerk, das das VIF enthält
4. Obligatorische Regeln für die VM, die das VIF enthält
5. Regeln für das VIF, das das VIF enthält
6. Standardregeln für die VM, die das VIF enthält
7. Standardregeln für das Netzwerk, das das VIF enthält
8. Standardregeln für den Ressourcenpool, der das VIF enthält
9. Standardregeln für die globale, die das VIF enthält

Die erste Regel, die übereinstimmt, wird ausgeführt, und es werden keine weiteren Regeln ausgewertet.

> **Hinweis:**
>
> Wenn ein vSwitch Controller nicht verfügbar ist, erzwingt der Ressourcenpool Zugriffssteuerungsregeln basierend auf dem konfigurierten Fehlermodus. Weitere Informationen zum Ausfallmodus eines Ressourcenpools finden Sie im Abschnitt „Ressourcenpoolebene“ unter „Status anzeigen“.

Zugriffssteuerungslisten (ACL) -Regeln definieren

Um eine neue ACL-Regel zu definieren, wählen Sie mithilfe der Ressourcenstruktur den Knoten auf der entsprechenden Ebene in der Richtlinienkonfigurationshierarchie aus. Sie können Regeln auf jeder Ebene für diese Ebene und für höhere Ebenen hinzufügen. Wenn Sie beispielsweise einen Ressourcenpool auswählen, können Sie Regeln für diesen Ressourcenpool und globale Regeln hinzufügen.

Wenn Sie einen Ressourcenstrukturknoten auswählen, der keiner Ebene in der Richtlinienkonfigurationshierarchie entspricht, wird eine Meldung angezeigt. Die Nachricht enthält Links zum Auswählen einer anderen Ebene.

Neue Regeln können auf folgende Weise hinzugefügt werden:

- Um eine obligatorische Regel hinzuzufügen, klicken Sie auf das Zahnradsymbol in der Kopfleiste für die Ebene und wählen Sie **Neue obligatorische ACL hinzufügen**.
- Um eine Standardregel hinzuzufügen, klicken Sie auf das Zahnradsymbol in der Kopfleiste für die Ebene und wählen Sie **Neue Standard-ACL hinzufügen**.
- Um eine Regel oberhalb eines vorhandenen Regeleintrags hinzuzufügen, klicken Sie auf das Zahnradsymbol für den Eintrag und wählen Sie „ **Neue ACL hinzufügen**“.
- Um eine Regel unterhalb eines vorhandenen Regeleintrags hinzuzufügen, klicken Sie auf das Zahnradsymbol für den Eintrag und wählen Sie „ **Neue ACL hinzufügen“ unten**.

Die neue Regel wird der Seite mit den folgenden Standardeinstellungen hinzugefügt:

- Aktion: Zulassen
- Protokoll: Beliebig
- Richtung: zu/Von
- Remote-Adressen: Beliebig
- Beschreibung: None

Um ein bestimmtes Feld innerhalb einer Regel zu ändern, klicken Sie auf den Link, der den aktuellen Feldwert darstellt, und wenden Sie die Änderungen an, wie in der folgenden Liste beschrieben. Wenn Sie eine Änderung anwenden, wird die Regel aktualisiert, um die Werte anzuzeigen.

- **Aktion:** Klicken Sie auf den Link und wählen Sie „ **Aktion zum Verweigern ändern“ oder „Zu zulässigeAktion ändern“** .
- **Protokoll:** Klicken Sie auf und wählen Sie eine der folgenden Optionen:
  - Wählen Sie „ **Beliebiges Protokoll** zuordnen“, um die Regel auf alle Protokolle anzuwenden.
  - Wählen Sie **Vorhandenes Protokoll verwenden** , um ein Protokoll anzugeben. Select das Protokoll aus der Liste aus, und klicken Sie auf **Protokoll verwenden**.
  - Wählen Sie **Neues Protokoll verwenden** , um benutzerdefinierte Protokollmerkmale anzugeben. Geben Sie die folgenden Informationen im Popup-Fenster an, und klicken Sie auf **Speichern und verwenden**:
    * Ethertype: Select IP oder geben Sie einen anderen Ethertyp ein.
    * IP-Protokoll: Select eines der aufgelisteten Protokolle aus, oder geben Sie ein anderes ein.
    * Zielport (nur TCP/UDP): Geben Sie eine Portnummer ein, oder geben Sie **Beliebig**an.
    * Quellport (nur TCP/UDP): Geben Sie eine Portnummer ein, oder geben Sie **Beliebig**an. Wenn Sie eine Anwendung definieren, die einen bekannten Serverport verwendet, definieren Sie diesen bekannten Port als Zielport, und belassen Sie den Quellport als **Beliebig**. Sie können diesen Ansatz beispielsweise für HTTP verwenden, das Port 80 verwendet.
    * ICMP-Typ (nur ICMP): Wählen Sie „ **Beliebig** “, oder geben Sie einen bestimmten ICMP-Typ-Protokolltyp (ICMP) ein.
    * ICMP-Code (nur ICMP): Wählen Sie „ **Beliebig** “, oder geben Sie einen bestimmten ICMP-Code ein.
    * Antwortverkehr abgleichen: Geben Sie an, ob Rückkehrverkehr automatisch als Teil der Regel zulässig ist. Wenn die Regel beispielsweise UDP-Zielport 7777 Datenverkehr von der VM zu einer angegebenen Remoteadresse zulässt und Antwortverkehr übereinstimmen ausgewählt ist, ist UDP-Datenverkehr auch **vom** Quellport 7777 der Remoteadresse zur VM zulässig. Aktivieren Sie diese Option für jedes UDP-Protokoll, das eine bidirektionale Kommunikation erfordert (die Option ist immer für TCP aktiviert).
    * Einmalige Verwendung vs. Mehrfachverwendungen: Select aus, ob dieses Protokoll nur für die aktuelle Regel verwendet werden soll oder es der Liste der Protokolle im Protokollmenü hinzugefügt werden soll.
  - Wählen Sie **Aktuelles Protokoll anzeigen/ändern** , um Eigenschaften für ein bereits definiertes Protokoll zu ändern.
- **Richtung:** Wählen Sie aus, ob die Regel **von** oder **auf** die angegebenen Remoteadressen oder beides angewendet wird.
- **Remoteadressen:** So geben Sie die Remoteadressen an:
  1. Klicken Sie auf den Link **Beliebig** , um ein Popup-Fenster zu öffnen, in dem die verfügbaren Adressgruppen aufgeführt sind.

2. Select eine oder mehrere Adressgruppen aus, und verschieben Sie sie mit den Pfeilen in die Spalte **Ausgewählt** .
3. Mit den Schaltflächen **Alle** können Sie alle Gruppen auswählen oder deaktivieren.
4. Um eine IP-Adresse oder ein Subnetz anzugeben, das nicht Teil einer vorhandenen Adressgruppe ist, geben Sie die Adresse oder das Subnetz ein (x.x.x.x oder x.x.x/n). Klicken Sie auf **Hinzufügen**. Wiederholen Sie dies, um weitere Adressen hinzuzufügen.
5. Klicken Sie auf **Fertig**.

- **Beschreibung:** So fügen Sie eine Textbeschreibung der Regel hinzu:
  1. Klicken Sie auf die Schaltfläche **Beschreibung** .
  2. Klicken Sie auf den Eintrag (<**Keine**> wenn keine aktuelle Beschreibung vorhanden ist). Ein Texteingabebereich wird angezeigt. Geben Sie den Text ein und drücken Sie **Geben Sie ein**.
- **Regeldetails:** Klicken Sie auf die Schaltfläche **Regeldetails** , um eine kurze Zusammenfassung der Regel anzuzeigen.

Klicken Sie auf **Richtlinienänderungen speichern** , um die neuen Regeln anzuwenden. Wenn Sie dies tun, werden die Änderungen sofort innerhalb der virtuellen Netzwerkumgebung wirksam. Wenn Sie die Regeln noch nicht gespeichert haben, können Sie auf **Änderungen rückgängig machen** klicken, um die von Ihnen benannten Änderungen rückgängig zu machen.

Wenn Sie eine ACL ändern, werden alle Hintergrundaktualisierungen für die vSwitch Controller GUI angehalten. Wenn ein anderer Administrator die Richtlinie gleichzeitig ändert und Änderungen vor Ihnen festlegt, aktualisieren Sie die Seite, um die neue Richtlinie vom Server abzurufen. Geben Sie Ihre Änderungen erneut ein.

Sie können die Reihenfolge der Regeln in einer Ebene ändern, indem Sie auf das Zahnradsymbol für die Regel klicken und „ **Nach oben** “ oder „ **Nach unten** “ wählen. Sie können keine Regel zwischen Ebenen in der Hierarchie verschieben. Um eine Regel zu entfernen, klicken Sie auf das Zahnradsymbol und wählen Sie **Löschen**. Klicken Sie auf die Schaltfläche **Beschreibung** , um die ACL-Beschreibung anzuzeigen. Oder die Schaltfläche „ **Regel** “, um die von Ihnen erstellte ACL-Regel anzuzeigen.

ACL-Regeln werden immer aus der Sicht der virtuellen Schnittstelle der VM interpretiert, selbst wenn sie in der Richtlinienhierarchie höher konfiguriert sind. Dieses Verhalten ist wichtig, wenn Sie über die Bedeutung des Felds „Remoteadressen“ in den Regeln nachdenken.

Wenn beispielsweise eine VM in einem Pool die IP-Adresse 10.1.1.1 hat, erwarten Sie möglicherweise eine Regel für den Pool, die angibt, dass „Alle Protokolle nach IP 10.1.1.1” verweigern, um zu verhindern, dass Datenverkehr auf die VM gelangt. Dieses Verhalten ist für alle anderen VMs im Ressourcenpool der Fall, da jede VM die Regel erzwingt, wenn die VM überträgt. Computer, die sich außerhalb des Ressourcenpools befinden, *können* jedoch mit der VM mit der IP-Adresse 10.1.1.1 kommunizieren. Dieses Verhalten liegt daran, dass keine Regeln das Übertragungsverhalten der externen Maschinen steuern. Es liegt auch daran, dass die VIF der VM mit der IP-Adresse 10.1.1.1 eine Regel aufweist, die den Übertragungsverkehr mit dieser Adresse abnimmt. Die Regel löscht jedoch

keinen *Empfangsverkehr* mit dieser Adresse.

Wenn das Richtlinienverhalten unerwartet ist, zeigen Sie die Registerkarte Status für die virtuelle Schnittstelle an, auf der der gesamte Regelsatz aller Richtlinienebenen visualisiert wird.

Richten Sie Portkonfigurationsrichtlinien ein

Verwenden Sie die Registerkarte **Portkonfiguration** , um Richtlinien zu konfigurieren, die für die VIF-Ports gelten. Die folgenden Richtlinientypen werden unterstützt:

- QoS: Quality of Service (QoS) -Richtlinien steuern die maximale Übertragungsrate für eine VM, die mit einem DVS-Port verbunden ist.
- Datenverkehrsspiegelung: RSPAN-Richtlinien (Remote Switched Port Analyzer) unterstützen die Spiegelung des Datenverkehrs, der auf einem VIF an ein VLAN gesendet oder empfangen wird, um Anwendungen zur Datenüberwachung zu unterstützen.
- Deaktivieren der MAC-Adress-Spoofprüfung: Richtlinien für die Überprüfung der MAC-Adresse steuern, ob die MAC-Adressenerzwingung bei Datenverkehr aus einem VIF durchgeführt wird. Wenn der vSwitch Controller ein Paket mit einer unbekannten MAC-Adresse aus einem VIF erkennt, werden das Paket und der gesamte nachfolgende Datenverkehr aus dem VIF entfernt. Die Richtlinien für die Überprüfung von MAC-Adressen sind standardmäßig aktiviert. Deaktivieren Sie diese Richtlinien auf VIFs, die Software wie den Netzwerklastenausgleich auf Microsoft Windows -Servern ausführen.

> **Warnhinweis:**
>
> Die Aktivierung von RSPAN ohne korrekte Konfiguration Ihres physischen und virtuellen Netzwerks kann zu einem schwerwiegenden Netzwerkausfall führen. Lesen Sie die Anweisungen inRSPAN konfigurierensorgfältig durch, bevor Sie diese Funktion aktivieren.

Sie können QoS und Traffic Mirroring Port-Richtlinien auf globaler Ebene, Ressourcenpool, Netzwerk, VM und VIF konfigurieren. Wenn Sie einen Knoten in der Ressourcenstruktur auswählen und die Registerkarte **Portkonfiguration** auswählen, wird die Konfiguration für jede übergeordnete Ebene in der Hierarchie angezeigt. Es kann jedoch nur die Konfiguration auf der ausgewählten Richtlinienebene geändert werden. Wenn Sie beispielsweise eine VM auswählen, werden auf der Registerkarte **Portkonfiguration** die Werte angezeigt, die auf globaler Ebene, Ressourcenpool und Netzwerkebene konfiguriert sind. Auf der Registerkarte können Sie den Wert auf VM-Ebene ändern.

QoS und Traffic Mirroring Konfigurationen auf einer bestimmten Ebene überschreiben die Konfigurationen auf den höheren Ebenen. Wenn eine Konfiguration außer Kraft gesetzt wird, zeigt die Registerkarte **Port-Konfiguration** die übergeordnete Konfiguration durchgestrichen an. Die nächste Abbildung zeigt beispielsweise eine QoS-Konfiguration auf Netzwerkebene, die die Konfiguration auf Ressourcenpoolebene außer Kraft setzt.

Um Port-Richtlinien zu konfigurieren, wählen Sie den Knoten in der Ressourcenstruktur und wählen Sie die Registerkarte **Port-Konfiguration** . Wenn Sie einen Knoten auswählen, der keine Portkonfigurationsrichtlinien unterstützt, wird eine Meldung mit Verknüpfungen zu Knoten angezeigt, die die Portkonfiguration unterstützen.

QoS konfigurieren

Wählen Sie für QoS-Richtlinien aus den folgenden Optionen:

- QoS-Richtlinie vom übergeordneten Element übernehmen (Standard): Wendet die Richtlinie von der höheren (d. h. weniger spezifischen) Hierarchieebene an. Diese Option ist auf globaler Ebene nicht vorhanden.
- Vererbte QoS-Richtlinie deaktivieren: Ignoriert alle Richtlinien, die auf höheren (d. h. weniger spezifischen) Ebenen festgelegt sind, so dass alle in dieser Richtlinienebene enthaltenen VIFs keine QoS-Konfiguration haben.
- QoS-Limit anwenden: Select ein Zinslimit (mit Einheiten) und eine Aufzahlungsgröße (mit Einheiten) aus. Der Datenverkehr zu allen in dieser Richtlinienstufe enthaltenen VIFs ist auf die angegebene Rate begrenzt, wobei einzelne Bursts auf die angegebene Anzahl von Paketen beschränkt sind.

> **Warnhinweis:**
>
> Wenn Sie eine zu kleine Burstgröße relativ zum Ratenlimit festlegen, kann verhindert werden, dass ein VIF genügend Datenverkehr sendet, um das Ratenlimit zu erreichen. Dieses Verhalten ist besonders wahrscheinlich für Protokolle, die Staukontrolle wie TCP durchführen.
>
> Die Burstrate muss mindestens größer sein als die Maximum Transmission Unit (MTU) des lokalen Netzwerks.
>
> Das Setzen von QoS auf eine unangemessen niedrige Burstrate auf jeder Schnittstelle, auf der sich der vSwitch Controller befindet, kann dazu führen, dass die Kommunikation mit dem vSwitch Controller verloren geht. Dieser Kommunikationsverlust erzwingt eine Notfall-Reset-Situation.
>
> Deaktivieren Sie die QoS-Richtlinie auf VM-Ebene, um zu verhindern, dass eine geerbte Erzwingung stattfindet.

Klicken Sie auf **Portkonfigurationsänderungen speichern** , um die Änderungen zu implementieren, oder klicken Sie auf **Änderungen rückgängig machen** , um nicht gespeicherte Änderungen zu entfernen. Die Richtlinie tritt unmittelbar nach dem Speichern in Kraft.

RSPAN konfigurieren

> **Warnhinweis:**
>
> Die Konfiguration von RSPAN, wenn der Server mit einem Switch verbunden ist, der VLANs nicht versteht oder nicht ordnungsgemäß für die Unterstützung des RSPAN-VLANs konfiguriert ist, kann Datenverkehrsduplizierung und Netzwerkausfälle verursachen. Überprüfen Sie die Dokumentation und Konfiguration Ihrer physischen Switches, bevor Sie die RSPAN-Funktion aktivieren. Diese Überprüfung ist besonders wichtig auf höheren Ebenen der Hierarchie, wo mehrere physische Switches beteiligt sein könnten.

Die Aktivierung von RSPAN erfordert eine Reihe von Schritten, die unten beschrieben sind:

Identifizieren Sie Ihr RSPAN-VLAN

Wenn RSPAN auf einem VIF aktiviert ist, erstellt der vSwitch für dieses VIF eine Kopie jedes Pakets, das an oder von diesem VIF gesendet wird. Der vSwitch überträgt die Kopie dieses Pakets, das mit dem VLAN-Wert als Ziel-VLAN gekennzeichnet ist. Ein Administrator platziert dann einen Host, der Überwachung durchführt, auf dem Switch-Port, der für die Verwendung des Ziel-VLAN konfiguriert ist. Wenn die Überwachungshostschnittstelle den Promiscuous-Modus verwendet, kann der gesamte Datenverkehr angezeigt werden, der an und von den für die Verwendung von RSPAN konfigurierten VIFs gesendet wird.

Konfigurieren des physischen Netzwerks mit dem Ziel-VLAN

Es ist wichtig, das physische Netzwerk korrekt zu konfigurieren, um den RSPAN-Datenverkehr zu kennen, um Netzwerkausfälle zu vermeiden. Aktivieren Sie RSPAN nur, wenn die physische Switching-Infrastruktur, die alle RSPAN-fähigen VIFs verbindet, so konfiguriert werden kann, dass das Lernen im Ziel-VLAN deaktiviert wird. Weitere Informationen finden Sie in der Dokumentation Ihres Switch-Herstellers.

Darüber hinaus muss der auf dem Ziel-VLAN gesendete Datenverkehr von jedem der vSwitches an die Überwachungshosts weitergeleitet werden. Wenn Ihre physische Infrastruktur viele Switches in einer Hierarchie enthält, muss für diese Weiterleitung das Ziel-VLAN zwischen den verschiedenen Switches abgeschaltet werden. Weitere Informationen finden Sie in der Dokumentation Ihres Switch-Herstellers.

Konfigurieren des vSwitch Controller mit dem Ziel-VLAN

Informieren Sie den vSwitch Controller über jedes Ziel-VLAN, bevor Sie diese VLAN-ID für die RSPAN-Portkonfiguration verwenden. Sie können verfügbare Ziel-VLAN-IDs auf Ressourcenpool-, Netzwerk- oder Serverebene angeben. Ziel-VLANs, die auf einer Ebene der Hierarchie hinzugefügt wurden, sind verfügbar, wenn die RSPAN-Portkonfiguration auf dieser Ebene und auf allen unteren Ebenen der Hi-

erarchie konfiguriert wird. Die richtige Stufe zum Angeben eines Ziel-VLAN hängt davon ab, wie weit Sie Ihre physische Infrastruktur so konfiguriert haben, dass sie dieses Ziel-VLAN kennt.

So geben Sie verfügbare Ziel-VLANs an:

1. Öffnen Sie unter **Sichtbarkeit und Kontrolle**die Registerkarte **Status**für alle Ressourcenpools, einen bestimmten Ressourcenpool, einen bestimmten Server oder ein bestimmtes Netzwerk.
2. Klicken Sie im Bereich **RSPAN-Ziel-VLAN-IDs** auf **+** , und geben Sie die VLAN-ID ein.
3. Wiederholen Sie dies, um weitere VLAN-IDs hinzuzufügen.
4. Klicken Sie auf **Ziel-VLAN-Änderung speichern**.

Die VLANs stehen nun auf der Registerkarte Port-Konfiguration zur Auswahl, wie in diesem Abschnitt beschrieben.

Ändern der Portkonfiguration, um RSPAN für einen Satz von VIFs zu aktivieren

Um RSPAN-Richtlinien auf der Registerkarte **Port-Konfiguration** zu konfigurieren, wählen Sie den entsprechenden Knoten in der Ressourcenstruktur aus, und wählen Sie eine der folgenden Optionen:

- RSPAN-Richtlinie vom übergeordneten Element erben (Standard): Wendet die Richtlinie von der nächsthöheren (d. h. weniger spezifischen) Hierarchieebene an.
- Vererbte RSPAN-Richtlinie deaktivieren: Ignoriert alle Richtlinien, die auf höheren (d. h. weniger spezifischen) Ebenen festgelegt sind, so dass alle in dieser Richtlinienebene enthaltenen VIFs keine RSPAN-Konfiguration haben.
- RSPAN-Datenverkehr auf VLAN: Wählen Sie ein VLAN aus der Liste der Ziel-VLANs aus. Die einzigen Ziel-VLANs, die in der Liste angezeigt werden, sind die VLANs, die für Richtlinienebenen konfiguriert sind, die den aktuell ausgewählten Knoten enthalten.

Konfigurieren der MAC-Adress-Spoofprüfung

Um die Erzwingung von MAC-Adressen zu deaktivieren, wählen Sie **MAC-Adress-Spoofprüfung aus**. Die Erzwingung kann nur auf VIF-Basis konfiguriert werden und übernimmt keine übergeordneten Konfigurationen.

Änderungen speichern

Klicken Sie auf Portkonfigurationsänderungen speichern, um die Änderungen zu implementieren, oder klicken Sie auf **Änderungen rückgängig machen** , um nicht gespeicherte Änderungen zu entfernen. Die Richtlinie tritt unmittelbar nach dem Speichern in Kraft.

Kopiert!
Failed!

Verwalten und Verwalten des vSwitch Controller

October 16, 2019

Verwenden Sie die Seiten **„Einstellungen“** , um Verwaltungs- und Wartungsfunktionen auf dem vSwitch Controller auszuführen. Um auf die Seiten „Einstellungen“ zuzugreifen, wählen Sie das Symbol „ **Einstellungen** “ im oberen Bereich des vSwitch Controller Fensters.

Konfigurieren der IP-Adresseinstellungen

Verwenden Sie die Seite „ **IP-Konfiguration** “, um die IP-Adresse des vSwitch Controller zu überprüfen und zu konfigurieren. Wenn der vSwitch Controller zum ersten Mal gestartet wird, erhält er eine IP-Adresse über DHCP. Es wird jedoch empfohlen, eine statische IP-Adresse zuzuweisen. Wenn DHCP konfiguriert ist, können Ressourcenpools nicht auf den ausfallsicheren Modus eingestellt werden.

So zeigen Sie die Controller-IP-Adresse an und konfigurieren Sie sie:

1. Wählen Sie unter **Einstellungen IP-Konfiguration**, um die aktuelle Konfiguration anzuzeigen.
2. Um die Konfiguration zu ändern, klicken Sie auf **Konfiguration ändern**.
3. Select **Manuelle Konfiguration** , um eine statische IP-Adresse zuzuweisen.
4. Geben Sie folgende Informationen ein:
   - Neue IP-Adresse
   - Netzmaske
   - Gateway-IP-Adresse
   - (Optional) Eine oder zwei DNS-Server-IP-Adressen

     > **Hinweis:**
     > Um die Namensauflösung auf dem Controller zu aktivieren, muss mindestens eine DNS-Server-IP-Adresse angegeben werden.
5. Klicken Sie auf **Änderungen vornehmen** , um die Änderungen zu implementieren.

> **Warnhinweis:**
>
> Nach dem Ändern der IP-Adresse des vSwitch Controller wird möglicherweise eine Fehlermeldung angezeigt: Pool verwaltet von *old_ip_address*. Diese Fehlermeldung wird in der Spalte **Status** der Pools angezeigt, die der vSwitch Controller verwaltet. Wenn diese Meldung angezeigt wird, müssen Sie den Controller anweisen, die Pools erneut zu verwalten.
>
> Klicken Sie auf der Registerkarte **Alle Ressourcenpools** auf das Zahnradsymbol neben der Spalte **Status** der Ressourcenpools. Select **Pool stehlen**aus.

Standardmäßig verwendet die virtuelle vSwitch Controller Appliance ein selbstsigniertes SSL-Zertifikat für Verbindungen mit dem vSwitch, der auf jedem Citrix Hypervisor ausgeführt wird.

Sie können eine Zertifizierungsstelle erhalten, die Ihnen ein signiertes Zertifikat für Ihre vSwitch-Verbindungen zur Verfügung stellt. Befolgen Sie die Anweisungen der Zertifizierungsstelle, die Sie beim Generieren des zu signierenden öffentlichen/privaten Schlüsselpaars verwenden möchten. Senden Sie den Schlüssel an die Behörde. Nachdem Sie das signierte Zertifikat von der Behörde erhalten haben, führen Sie die Schritte in diesem Abschnitt aus.

Klicken Sie unter **Einstellungen**auf **Server- und Zertifikatverwaltung**.

Klicken Sie auf **OVS-Zertifikat aktualisieren**.

Wählen Sie die SSL/TLS-Zertifikatsdatei aus.

Klicken Sie nach dem Hochladen der Datei auf **Zertifikat aktualisieren**.

So zeigen Sie Informationen zum vSwitch SSL-Sicherheitszertifikat an:

1. Klicken Sie unter **Einstellungen**auf **Server- und Zertifikatverwaltung**.
2. Klicken Sie **auf OVS-Zertifikat anzeigen**.

Diese Informationen enthalten auch, wenn das Zertifikat abläuft.

Nachdem Sie das vSwitch-SSL-Zertifikat aktualisiert haben, lädt der vSwitch jedes Servers im Pool automatisch das neue Zertifikat herunter, wenn Sie neue Pools für die Verwaltung hinzufügen. Für vSwitches, die auf vorhandenen Pools unter Verwaltung ausgeführt werden, müssen Sie jedoch ihre SSL-Zertifikate manuell aktualisieren.

Kopieren Sie auf dem Citrix Hypervisor or-Server das SSL-Zertifikat nach`/etc/openvswitch/vswitchd.cacert`

Starten Sie den Citrix Hypervisor -Server neu.

Konfigurieren des Controller-Hostnamens

Verwenden Sie die Seite IP-Konfiguration, um den Hostnamen des Controller und die DNS-Domäne zu überprüfen und zu konfigurieren. Standardmäßig ist der Hostname des Controllers`dvsc`, und der DNS-Domänenname ist nicht zugewiesen.

Wählen Sie unter **Einstellungen IP-Konfiguration**, um die aktuelle Konfiguration anzuzeigen.

Klicken Sie auf **Hosteinstellungen ändern**.

Geben Sie den gewünschten Hostnamen und Domainnamen in die entsprechenden Felder ein.

Der Wert des Domänennamens wird sowohl für den Domänennamen des Hosts als auch für die Domäne verwendet, um nach nicht qualifizierten Hostnamen zu suchen.

Klicken Sie auf **Änderungen vornehmen** , um die Änderungen zu speichern, oder wählen Sie **Abbrechen** .

Sammeln von Informationen für Fehlerberichte

So sammeln Sie Informationen für Fehlerberichte:

1. Klicken Sie unter **Einstellungen** auf **Server- und Zertifikatverwaltung** .
2. Klicken Sie auf **Alle Protokolle sammeln und zippen** , um alle relevanten vSwitch Controller Protokolle zu einer ZIP-Datei zum Download hinzuzufügen.
3. Wenn der ZIP-Vorgang abgeschlossen ist, klicken Sie auf den **hier** Link im Popup-Fenster, um die Datei dump.tar.gz herunterzuladen.
4. Klicken Sie nach dem Herunterladen auf **Schließen** , um das Popup-Fenster zu schließen.

Starten Sie die vSwitch Controller -Software neu

Um die vSwitch Controller -Software neu zu starten, klicken Sie unter Einstellungen auf **Server- und Zertifikatverwaltung** , und klicken Sie dann auf **Netzwerkcontroller neu starten** . Wenn der Neustart abgeschlossen ist, wird die Anmeldeseite geöffnet.

Verwalten von Administratorkonten

Mehrere Benutzerkonten können verwendet werden, um bestimmten Benutzern eingeschränkte Berechtigungen beim Zugriff auf die GUI zu gewähren. Einträge im Protokoll „Administrative Ereignisse“ enthalten den Namen des Benutzers, der die Aktion ausgeführt hat. Mit mehreren Benutzern kann ermittelt werden, wer kürzlich eine Konfigurationsänderung vorgenommen hat.

So fügen Sie Benutzerkonten für den Zugriff auf den vSwitch Controller hinzu und ändern Sie Benutzerpasswörter:

1. Wählen Sie unter **Einstellungen**die Option **Administrative Konten**aus.
2. Klicken Sie auf **Konto erstellen**.
3. Geben Sie einen Benutzernamen und ein Kennwort ein, und geben Sie das Kennwort zur Bestätigung erneut ein. Geben Sie eine der folgenden Benutzerrechte an:
   - Superuser: Alle Privilegien.
   - Lese-/Schreibzugriff: Alle Berechtigungen, mit Ausnahme der Möglichkeit, andere Benutzerkonten zu ändern und Snapshots wiederherzustellen.
   - Schreibgeschützt: Kann die meisten Informationen in der GUI sehen, aber nichts im vSwitch Controller mit Ausnahme des eigenen Kennworts des Benutzers ändern.
4. Klicken Sie auf **Benutzer hinzufügen**.

Um ein Benutzerkennwort zu ändern, klicken Sie auf den Link **Kennwort** für den Benutzer. Geben Sie ein neues Kennwort ein und bestätigen Sie es, und klicken Sie auf **Kennwort ändern**.

Um einen Benutzer zu entfernen, klicken Sie auf den Link **Entfernen** für den Benutzer. Sie können den Admin-Benutzer nicht entfernen.

Verwalten von Konfigurations-Snapshots

Snapshots bieten einen Mechanismus zum Speichern der aktuellen vSwitch Controller Konfiguration, sodass Sie diese exakte Konfiguration zu einem späteren Zeitpunkt wiederherstellen können. Es kann nützlich sein, das System zu fotografieren, bevor größere Konfigurationsänderungen vorgenommen werden. Standardmäßig erstellt das System automatisch alle 12 Stunden einen automatischen Snapshot.

Klicken Sie unter **Einstellungen** auf **Konfigurations-Snapshots** , um die Liste der Konfigurationssicherungen und der Wiederherstellung aus der Sicherung anzuzeigen. Die Seite listet alle letzten Sicherungen auf, wobei die zuletzt aufgeführten zuerst aufgeführt sind. Automatische Sicherungen werden zweimal täglich und jedes Mal, wenn der vSwitch Controller neu gestartet wird. Beim Wiederherstellen von einer Sicherung wird die aktuelle IP-Konfiguration des vSwitch Controller nicht aktualisiert. Informationen zum Ändern der vSwitch Controller IP-Adresse finden Sie unterKonfigurieren der IP-Adresseinstellungen.

Um die Konfiguration aus einer Sicherung wiederherzustellen, klicken Sie auf das Zahnradsymbol für den Snapshot und wählen Sie In **Snapshot wiederherstellen**. Wenn Sie gefragt werden, ob Sie fortfahren möchten, klicken Sie auf **Ja, Wiederherstellen**.

Um eine Sicherung bei Bedarf zu erstellen, klicken Sie auf **Neuen Snapshot erstellen**. Sie können eine optionale Beschreibung eingeben, um den Snapshot zu identifizieren. Klicken Sie auf **Snapshot erstellen**. Die neue Sicherung wird am Anfang der Liste hinzugefügt.

Um einen Snapshot herunterzuladen, der auf einem anderen System gespeichert wird, klicken Sie auf das Zahnradsymbol für den Snapshot und wählen Sie **Herunterladen**. Befolgen Sie die Anweisungen in den Popup-Fenstern, um die Snapshot-Datei zu speichern.

Um einen zuvor gespeicherten Snapshot auf den Controller hochzuladen, klicken Sie auf **Snapshot hochladen**. Wählen Sie die Snapshot-Datei aus, und klicken Sie auf **Snapshot hochladen**. Der hochgeladene Snapshot wird der Liste auf der Seite Konfigurations-Snapshots hinzugefügt.

Um einen Snapshot zu löschen, klicken Sie auf das Zahnradsymbol für den Snapshot und wählen Sie **Snapshot löschen**. Klicken Sie auf **Snapshot löschen**, wenn Sie gefragt werden, ob Sie fortfahren möchten.

Die Snapshot-Tabelle enthält auch Informationen zur Softwareversion und Kompatibilität. Kompatibilität gibt an, ob die Daten im Snapshot mit der aktuellen Softwareversion kompatibel sind. Es zeigt eine grüne Anzeige, wenn es kompatibel ist, und eine rote Anzeige, falls nicht. Um einen inkompatiblen Snapshot wiederherzustellen, müssen Sie zunächst die Software in eine kompatible Version ändern, wie in der Spalte Softwareversion aufgeführt.

Standardmäßig erstellt das System alle 12 Stunden einen Konfigurationssnapshot. Diese Snapshots werden mit der Beschriftung **Automatische periodische Momentaufnahme**aufgeführt. Darüber hinaus werden bei jedem Neustart des vSwitch Controller Konfigurations-Snapshots erstellt. Diese Snap-

shots werden mit der Beschriftung „ **Startsnapshot“**aufgeführt. Systeminitiierte Snapshots werden automatisch gelöscht, wenn sie älter als 30 Tage sind. Wenn Sie einen Snapshot manuell erstellen, geben Sie ein eindeutiges Beschreibungslabel ein, damit es nicht als systeminitiierter Snapshot verwechselt und nach 30 Tagen gelöscht wird. Wenn ein vom System initiierter Snapshot länger als 30 Tage aufbewahrt werden muss, laden Sie ihn herunter und laden Sie ihn dann erneut hoch, indem Sie ein eindeutiges Beschreibungslabel verwenden.

Hinzufügen von NTP-Servern (Network Time Protocol)

Die virtuelle vSwitch Controller Appliance verwendet eine Verbindung zu externen NTP-Servern (Network Time Protocol), um ihre Zeiteinstellungen zu verwalten. Der Controller verfügt über bereits konfigurierte Standardserver. Da diese NTP-Server möglicherweise nicht optimal für Ihre Umgebung sind, können Sie sie gemäß den folgenden Anweisungen durch einen lokalen NTP-Server ersetzen.

So fügen Sie einen NTP-Server hinzu:

1. Wählen Sie unter **Einstellungen**die Option **Zeit & NTP**aus.
2. Klicken Sie auf **Server hinzufügen**.
3. Geben Sie die IP-Adresse des Servers ein und klicken Sie auf **Hinzufügen**.
4. Fügen Sie nach Bedarf weitere Server hinzu.

Um einen NTP-Server zu entfernen, klicken Sie auf den Link **Entfernen** .

Exportieren von Syslog-Dateien

Verwenden Sie die Seite „Syslog“, um Server hinzuzufügen, die Remote-Syslog-Nachrichten empfangen, die aus Administrator- und Netzwerkereignismeldungen bestehen, die vom System generiert werden. Die neuesten Syslog-Einträge werden ebenfalls im Dashboard angezeigt.

So fügen Sie Syslog-Server hinzu:

1. Wählen Sie unter **EinstellungenSyslog**aus.
2. Klicken Sie auf **Serveradresse hinzufügen**.
3. Geben Sie die IP-Adresse des Servers ein und klicken Sie auf **Hinzufügen**.
4. Fügen Sie nach Bedarf weitere Server hinzu.

Um einen Server zu entfernen, klicken Sie auf den Link **Entfernen** .

Kopiert!
Failed!

Befehle

October 16, 2019

In diesem Abschnitt werden die CLI-Befehle für vSwitch Controller beschrieben. Sie können lokal über die Textkonsole der Controller VM in XenCenter auf die CLI zugreifen. Um remote auf die CLI zuzugreifen, verwenden Sie eine SSH-Clientanwendung und stellen Sie eine Verbindung mit dem Hostnamen oder der IP-Adresse des Controllers auf Port 22 her.

Während einer CLI-Sitzung können Sie Hilfe zu CLI-Befehlen auf eine der folgenden Arten erhalten:

- Geben Sie **help ein,** und drücken Sie dann die **EINGABETASTE** .
- Geben Sie einen Teil eines Befehls ein, gefolgt von einem Leerzeichen und einem Fragezeichen (?) , und drücken Sie dann die **EINGABETASTE**.

Die Schnittstelle unterstützt die Fertigstellung des Befehlsarguments, wenn Sie die **Tabulatortaste** drücken. Im Allgemeinen können Sie Befehle auf den kürzesten, eindeutigen String auf jeder Ebene abkürzen, um die Eingabe zu reduzieren. Sie können den Befehlsverlauf innerhalb der aktuellen Sitzung zugreifen, indem Sie die **Pfeiltasten** .

Lebenszyklusbefehle

So halten Sie den vSwitch Controller an

```
1 halt controller
```

Mit diesem Befehl wird die vSwitch Controller Appliance angehalten, indem der Controller ordnungsgemäß heruntergefahren wird.

So starten Sie den Controller neu

```
1 restart controller appliance
```

Mit diesem Befehl wird die gesamte Controller-Appliance heruntergefahren und neu gestartet.

Dieser Befehl dient hauptsächlich zur Fehlerbehebung. Im Allgemeinen wird der`halt` Befehl verwendet, um die Controller-Appliance auszuschalten.

So starten Sie den Controller Daemon neu


```
restart controller daemon
```

Mit diesem Befehl werden die Prozesse heruntergefahren und neu gestartet, die die Controller-Funktionen implementieren.

Dieser Befehl dient hauptsächlich zur Fehlerbehebung.

Festlegen von Befehlen

Verwenden Sie diesen Befehl, um den vSwitch-Controller zu konfigurieren.

So legen Sie den Hostnamen der Controller-Appliance fest

```
set controller hostname hostname
```

Mit diesem Befehl wird der Hostname der Controller-Appliance festgelegt.

Wenn der angegebene Hostname ein oder mehrere Periodenzeichen enthält („. „), wird der Hostname der Appliance *vor* der ersten Periode auf die Zeichenfolge gesetzt. Der Domänenname der Appliance wird *nach* der ersten Periode auf die Zeichenfolge festgelegt.

So legen Sie die IP-Adresse der Controller Verwaltungsschnittstelle über DHCP fest

```
set controller management-interface config dhcp
```

Mit diesem Befehl wird die IP-Adresse der Controller Verwaltungsschnittstelle mithilfe von DHCP festgelegt. Wenn DHCP konfiguriert ist, können Ressourcenpools nicht auf den ausfallsicheren Modus eingestellt werden.

Dieser Befehl wird bei der Ausführung wirksam, sodass der Remote-Zugriff auf die CLI verloren geht, wenn sich die Adresse ändert.

So legen Sie eine statische IP-Adresse für die Controller Verwaltungsschnittstelle fest

```
set controller management-interface config static
                            IP-address
                        netmask
                        gateway-IP
                            [dns-server-IP]
                            [dns-server-IP2
                        dns-search]]‘
```


Mit diesem Befehl wird eine statische IP-Adresse für die Controller Verwaltungsschnittstelle festgelegt. Die DNS-Konfigurationsinformationen sind optional. Die Möglichkeit, einen DNS-Suchpfad anzugeben, erfordert die Spezifikation von zwei DNS-Servern.

Dieser Befehl wird bei der Ausführung wirksam, sodass der Remote-Zugriff auf die CLI verloren geht, wenn sich die Adresse ändert.

Anzeigebefehle

Verwenden Sie diese Befehle, um Informationen zur aktuellen vSwitch-Controller-Konfiguration anzuzeigen.

So zeigen Sie den aktuellen Controller Hostnamen an

```
1 show controller hostname
```

So zeigen Sie eine Zusammenfassung der aktuellen Konfiguration und des Status der Management-Schnittstelle an

```
1 show controller management-interface
```

So zeigen Sie Konfigurationswerte für die Management-Schnittstelle an

```
1 show controller management-interface config
```

So zeigen Sie das aktuelle Standard-Gateway für den Controller an

```
1 show controller management-interface default-gateway
```

So zeigen Sie die aktuelle DNS-Konfiguration für den Controller an

```
1 show controller management-interface dns-server
```


So zeigen Sie die aktuelle IP-Adresse der Controller Verwaltungsschnittstelle an

```
show controller management-interface ip-address
```

So zeigen Sie die aktuelle Netzmaske der Controller Verwaltungsschnittstelle an

```
show controller management-interface netmask
```

So zeigen Sie die Softwareversion des Controller an

```
show controller version
```

Andere Befehle

So beenden Sie die aktuelle CLI-Sitzung

```
exit
```

So erhalten Sie Informationen zu Befehlen

```
help
```

So führen Sie ein Upgrade oder ein Downgrade der vorhandenen Version des Controller durch

```
install controller software-update scp-format-remote-filename
```

Dieser Befehl kopiert sicher eine Controller-Update-Datei vom angegebenen Remotestandort und installiert diese Version anstelle der vorhandenen Version.

Dieser Befehl kann verwendet werden, um Softwareversionen zu installieren, die sowohl Upgrades als auch Downgrades sind. Upgrades migrieren die Konfiguration automatisch auf die neue Version. Downgrades werden auf den neuesten kompatiblen Konfigurationssnapshot oder auf eine leere Konfiguration zurückgesetzt, wenn kein kompatibler Snapshot vorhanden ist.

So pingen Sie ein bestimmtes Remote-System an

```
ping name-or-IP-address [count]
```

Dieser Befehl sendet ICMP-Echo-Anfragen an das durch den Namen oder die IP-Adresse identifizierte entfernte System und wartet auf Antworten. Wenn keine Anzahl angegeben ist, werden Anfragen einmal pro Sekunde gesendet, bis sie mit Strg-C unterbrochen werden. Wenn eine Anzahl angegeben wird, wird diese Anzahl von Pings gesendet.

Kopiert!
Failed!

Beheben von vSwitch Controller Problemen

October 16, 2019

Dieser Abschnitt enthält Informationen zur Problembehandlung bei vSwitch Controller Problemen.

Status des Ressourcenbauknotens

In der folgenden Tabelle werden die Statussymbole für jeden Ressourcentyp beschrieben. Diese Symbole werden in der Ressourcenstruktur und auf der Seite Status für das Element angezeigt.

Artikel/Statussymbole	Beschreibung
VIFs	
rot	Die zugeordnete virtuelle Maschine (VM) wird heruntergefahren oder nicht erreichbar.
Grün	Virtuelle Schnittstelle (VIF) ist verfügbar und wird verwaltet.
Orange	VM wird ausgeführt, aber der Citrix Hypervisor, auf dem sich die VIF befindet, ist nicht mit dem vSwitch Controller verbunden.
VMs	
rot	Die VM wird heruntergefahren oder nicht erreichbar.
Grün	VM befindet sich im ausgeführten Zustand und VIFs werden verwaltet.

Artikel/Statussymbole	Beschreibung
Orange	VM wird ausgeführt, aber der Citrix Hypervisor, auf dem sich die VM befindet, ist nicht korrekt mit dem vSwitch Controller verbunden. Dieser Status hängt vom kollektiven Zustand der jeweiligen VIFs ab.
Servernetzwerke	
rot	Citrix Hypervisor wird heruntergefahren oder nicht erreichbar, oder keine VMs verfügen über VIFs, die dem Netzwerk zugeordnet sind.
Grün	Citrix Hypervisor ist korrekt mit dem vSwitch Controller verbunden.
Orange	Citrix Hypervisor ist nicht korrekt für die Verbindung mit dem vSwitch Controller konfiguriert (abhängig vom kollektiven Status der zugeordneten physischen Schnittstellen und VIFs).
Citrix Hypervisor	
rot	Citrix Hypervisor wird heruntergefahren oder nicht erreichbar.
Grün	Citrix Hypervisor ist korrekt mit dem vSwitch Controller verbunden.
Orange	Citrix Hypervisor ist nicht für die Verbindung mit dem vSwitch Controller konfiguriert (abhängig vom kollektiven Status der zugeordneten physischen Schnittstellen und VIFs).
Pool-weite Netzwerke	
rot	Master Citrix Hypervisor wird heruntergefahren oder nicht erreichbar.
Grün	Master Citrix Hypervisor ist so konfiguriert, dass eine Verbindung mit dem vSwitch Controller hergestellt wird und die Verbindung funktioniert.

Artikel/Statussymbole	Beschreibung
Orange	Master Citrix Hypervisor ist nicht für die Verbindung mit dem vSwitch Controller konfiguriert (abhängig vom kollektiven Status der zugeordneten physischen Schnittstellen und VIFs).
Ressourcenpools	
rot	Master Citrix Hypervisor wird heruntergefahren oder nicht erreichbar.
Grün	Master Citrix Hypervisor ist so konfiguriert, dass eine Verbindung mit dem vSwitch Controller hergestellt wird und die Verbindung funktioniert.
Orange	Master Citrix Hypervisor ist nicht für die Verbindung mit dem vSwitch Controller konfiguriert (abhängig vom kollektiven Status der zugeordneten physischen Schnittstellen und VIFs).

Beheben von Zugriffsrichtlinienproblemen

Die folgenden Vorschläge helfen bei der Fehlerbehebung, wenn Zugriffssteuerungsrichtlinien nicht ordnungsgemäß funktionieren:

1. Select die Seite **Status** für die VIF einer VM aus, auf die sich die Richtlinie auswirken soll. Zeigen Sie die Trefferanzahl für jede Regel an, während Sie Datenverkehr generieren, den die Richtlinie nicht ordnungsgemäß verarbeitet. Identifizieren Sie die Regel, die der Datenverkehr tatsächlich trifft, anstelle der Regel, von der er erwartet wird. Für Debugging-Zwecke können Sie eine Standardregel hinzufügen, die dem gesamten Datenverkehr als Standardregel mit niedrigster Priorität auf globaler Ebene entspricht.

   > **Hinweis:**
   >
   > Diese Regel kann entweder eine Zulassungs- oder Ablehnungsaktion haben, abhängig vom gewünschten Netzwerkverhalten beim Debuggen. Löschen Sie diese Regel nach dem Debuggen.

2. Wenn der Datenverkehr eine Regel mit niedrigerer Priorität als die von Ihnen erwartete, überprüfen Sie sorgfältig die Kriterien für den Regelabgleich. Ist die Verkehrsrichtung korrekt

angegeben? Sind die Remote-Hosts richtig identifiziert? Ist das Protokoll korrekt definiert? Ist beispielsweise das Protokoll, das einen UDP-Port anstelle eines TCP-Ports angibt oder umgekehrt?

3. Wenn der Datenverkehr eine Regel mit höherer Priorität als erwartet trifft, lösen Sie den Konflikt zwischen dieser Regel und der Regel, von der der Datenverkehr erwartet wurde. Sie können Konflikte lösen, indem Sie Regeln mehr oder weniger detaillierter definieren oder die relativen Prioritäten der beiden Regeln ändern. Beispielsweise können Sie eine Regel so einstellen, dass sie nur auf eine bestimmte Gruppe von Remote-IP-Adressen angewendet wird.
4. Wenn die VM über mehrere VIFs verfügt, überprüfen Sie, ob sie den Datenverkehr auf dem VIF sendet und empfängt, für den die Richtlinie gilt. Verwenden Sie gegebenenfalls RSPAN, um Datenverkehr vom VIF zu einem Netzwerkanalysator zu spiegeln. Sie können diesen gespiegelten Datenverkehr verwenden, um sicherzustellen, dass Datenverkehr vorhanden ist, der der Regel entsprechen soll.

> **Hinweis:**
>
> Wenn ein vSwitch Controller nicht verfügbar ist, erzwingt der Ressourcenpool Zugriffssteuerungsregeln basierend auf dem konfigurierten Fehlermodus. Weitere Informationen zum Ausfallmodus eines Ressourcenpools finden Sie im Abschnitt „Ressourcenpoolebene“ unter „Status anzeigen“.

Erstellen eines Fehlerberichts

Um Probleme effizient zu beheben, sammeln Sie Informationen aus Citrix Hypervisor und vSwitch Controller, die an dem Problem beteiligt sind. Sammeln Sie diese Informationen so schnell wie möglich, nachdem das Problem auftritt. Senden Sie die Informationen zusammen mit Ihrem Fehlerbericht.

- Fügen Sie für jeden Citrix Hypervisor, der an dem Problem beteiligt ist, einen Serverstatusbericht hinzu. Informationen zum Generieren von Serverstatusberichten finden Sie unterGesundheitscheck
- Fügen Sie ein Protokollpaket aus dem vSwitch Controller ein, indem Sie auf der Seite **Server- und Zertifikatwartungseinstellungenauf Alle Protokolle sammeln und zippen** klicken. Weitere Informationen finden Sie unter Sammeln von Informationen für Fehlerberichte.

Controller Fehlermeldungen

Folgende Fehlermeldungen können angezeigt werden:

- **Verbindung mit Pool herstellen** - Wird angezeigt, wenn ein neuer Pool hinzugefügt wird und der vSwitch Controller noch nicht erfolgreich mit dem Poolmaster verbunden ist. ODER Wird

angezeigt, wenn der vSwitch Controller neu gestartet wird und noch nicht erfolgreich mit dem Poolmaster verbunden ist. Wenn innerhalb von 30 Sekunden keine erfolgreiche Verbindung hergestellt wird, wird diese Meldung durch „Poolverbindung fehlgeschlagen“ ersetzt.

- **Netzwerksteuerkanäle getrennt** - Citrix Hypervisor ist nicht korrekt mit dem vSwitch Controller verbunden.
- **Fehlende Pool-Adresse** - Für den Pool ist kein DNS-Name oder keine IP-Adresse verfügbar.
- **Poolverbindung fehlgeschlagen** - Diese Meldung wird in den folgenden Situationen angezeigt:
  - Es liegt ein Netzwerkproblem zwischen dem Controller und dem Poolmaster vor
  - Fehler bei der DNS-Namensauflösung
  - Es gibt einen ungültigen DNS-Namen oder eine Pool-Master-IP-Adresse.
  - Der Poolmaster ist ausgefallen oder falsch konfiguriert
- **Nicht unterstützte Poolversion** - Der DNS-Name oder die IP-Adresse, die für den Pool konfiguriert ist, wird nicht in eine kompatible Version von Citrix Hypervisor aufgelöst.
- **Doppelter Pool: Pool deaktiviert** - Der Pool meldet dieselbe XAPI-UUID wie ein anderer Pool, der sich bereits in der vSwitch Controller Datenbank befindet.
- **Fehler bei der Poolauthentifizierung** - vSwitch Controller konnte sich nicht mit dem angegebenen Benutzernamen und Kennwort beim Poolmaster authentifizieren.
- **Poolidentität geändert** - Der Pool wurde neu installiert und stimmt nicht mit dem Status des übereinstimmenden Pools überein.
- **Pool-Synchronisierungsfehler** - Bei Verwendung von XAPI zur Kommunikation mit dem Poolmaster wurde ein nicht unterstützter Vorgang angezeigt.
- **Unbekannter Fehler** - Ursache des Fehlers ist nicht bekannt.

Kopiert!
Failed!

Befehlszeilenschnittstelle

October 16, 2019

Mit der *xe* CLI können Sie Systemverwaltungsaufgaben skriptieren und automatisieren. Verwenden Sie die CLI, um Citrix Hypervisor in eine vorhandene IT-Infrastruktur zu integrieren.

Installation der xe CLI

Die xe-Befehlszeilenschnittstelle wird standardmäßig auf allen Citrix Hypervisor or-Servern installiert und ist in XenCenter enthalten. Eine eigenständige Remote-CLI ist auch für Linux verfügbar.

Unter Windows

Unter Windows wird der`xe.exe` Befehl zusammen mit XenCenter installiert.

Um den`xe.exe` Befehl zu verwenden, öffnen Sie eine Windows Eingabeaufforderung und ändern Sie die Verzeichnisse in das Verzeichnis, in dem sich die`xe.exe` Datei befindet (normalerweise`C:\Program Files\Citrix\XenCenter`). Wenn Sie den`xe.exe` Installationsspeicherort zu Ihrem Systempfad hinzufügen, können Sie den Befehl verwenden, ohne in das Verzeichnis wechseln zu müssen.

Unter Linux

Bei RPM-basierten Distributionen (z. B. Red Hat) können Sie den eigenständigen xe-Befehl aus dem RPM installieren, der`client_install/xapi-xe-BUILD.x86_64.rpm` auf der Citrix Hypervisor Hauptinstallations-ISO benannt ist.

Verwenden Sie den folgenden Befehl, um vom RPM aus zu installieren:

```
1 rpm -ivh xapi-xe-BUILD.x86_64.rpm
```

Sie können Parameter in der Befehlszeile verwenden, um den Citrix Hypervisor or-Server, den Benutzernamen und das Kennwort zu definieren, die beim Ausführen von xe-Befehlen verwendet werden sollen. Sie haben jedoch auch die Möglichkeit, diese Informationen als Umgebungsvariable festzulegen. Zum Beispiel:

```
1 export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password
     =<password>"
```

> **Hinweis:**
>
> Die remote xe CLI unter Linux hängt möglicherweise ab, wenn versucht wird, Befehle über eine sichere Verbindung auszuführen, und diese Befehle beinhalten Dateiübertragung. In diesem Fall können Sie den Befehl mithilfe des`--no-ssl` Parameters über eine unsichere Verbindung zum Citrix Hypervisor or-Server ausführen.

Hilfe zu xe-Befehlen erhalten

Die grundlegende Hilfe ist für CLI-Befehle auf dem Host verfügbar, indem Sie Folgendes eingeben:

```
1 xe help command
```

Eine Liste der am häufigsten verwendeten xe-Befehle wird angezeigt, wenn Sie Folgendes eingeben:


```
xe help
```

Oder eine Liste aller xe-Befehle wird angezeigt, wenn Sie Folgendes eingeben:

```
xe help --all
```

Grundlegende x-Syntax

Die grundlegende Syntax aller Citrix Hypervisor xe CLI-Befehle lautet:

```
xe command-name argument=value argument=value
```

Jeder spezifische Befehl enthält einen eigenen Satz von Argumenten, die in der Form sind`argument=value`. Einige Befehle haben erforderliche Argumente, und die meisten haben einige optionale Argumente. Normalerweise nimmt ein Befehl Standardwerte für einige der optionalen Argumente an, wenn er ohne diese aufgerufen wird.

Wenn der xe-Befehl remote ausgeführt wird, werden zusätzliche Argumente verwendet, um eine Verbindung herzustellen und zu authentifizieren. Diese Argumente nehmen auch die Form an`argument=argument_value`.

Das`server` Argument wird verwendet, um den Hostnamen oder die IP-Adresse anzugeben. Die`username` Argumente`password` und werden verwendet, um Anmeldeinformationen anzugeben.

Ein`password-file` Argument kann anstelle des Kennworts direkt angegeben werden. In diesem Fall versucht der Befehl xe, 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 das Kennwort direkt in der Befehlszeile anzugeben.

Das optionale`port` Argument kann verwendet werden, um den Agent-Port auf dem Remote-Server von Citrix Hypervisor anzugeben (Standardwert 443).

Beispiel: Auf dem lokalen Citrix Hypervisor -Server:

```
xe vm-list
```

Beispiel: Auf dem Remote-Server von Citrix Hypervisor:

```
xe vm-list -user username -password password -server hostname
```

Für Remoteverbindungsargumente ist auch eine Kurzschrift verfügbar:

- `-u` Benutzername
- `-pw` Passwort

- `-pwf` Passwortdatei
- `-p` Port
- `-s` Server

Beispiel: Auf einem entfernten Citrix Hypervisor -Server:

```
1 xe vm-list -u myuser -pw mypassword -s hostname
```

Argumente werden auch der Umgebungsvariable XE_EXTRA_ARGS in Form von durch Kommas getrennten Schlüssel/Wert-Paaren entnommen. Um beispielsweise Befehle einzugeben, die auf einem Citrix Hypervisor or-Server ausgeführt werden, führen Sie zuerst den folgenden Befehl aus:

```
1 export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=
    pass"
```

Nach dem Ausführen dieses Befehls müssen Sie nicht mehr die Remote-Citrix Hypervisor or-Serverparameter in jedem ausgeführten xe-Befehl angeben.

Die Verwendung der Umgebungsvariable XE_EXTRA_ARGS ermöglicht auch die Tabulatorvervollständigung von xe-Befehlen, wenn sie für einen entfernten Citrix Hypervisor or-Server ausgegeben werden, der standardmäßig deaktiviert ist.

Sonderzeichen und Syntax

Um Argument/Wert-Paare in der`xe` Befehlszeile anzugeben, schreiben Sie:`argument=value`

Verwenden Sie keine Anführungszeichen, wenn der Wert Leerzeichen enthält. Zwischen dem Argumentnamen, dem Gleichheitszeichen (=) und dem Wert sollte kein Leerzeichen vorhanden sein. 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 dem Citrix Hypervisor or-Server verwenden, verfügen Befehle über eine Funktion zur Tabulatorvervollständigung, die der Funktion in der Standard-Linux-Bash-Shell ähnelt. Wenn Sie beispielsweise die **TAB-TASTE** eingeben`xe vm-l` und dann drücken, wird der Rest des Befehls angezeigt. Wenn mehr als ein Befehl mit beginnt`vm-l`, werden die Möglichkeiten durch Drücken von **TAB**ein zweites Mal aufgelistet. Diese Funktion ist nützlich, wenn Objekt-UUIDs in Befehlen angegeben werden.

> **Hinweis:**
>
> Die Tabulatorvervollständigung funktioniert normalerweise nicht, wenn Befehle auf einem Citrix Hypervisor or-Server ausgeführt werden. Wenn Sie jedoch die Variable XE_EXTRA_ARGS auf

> dem Computer festlegen, auf dem Sie die Befehle eingeben, ist die Tabulatorvervollständigung aktiviert. Weitere Informationen finden Sie unter Grundlegende x-Syntax.

Befehlstypen

Die CLI-Befehle können in zwei Hälften geteilt werden. Low-Level-Befehle befassen sich mit der Auflistung und Parametermanipulation von API-Objekten. Befehle höherer Ebene werden verwendet, um mit VMs oder Hosts in einer abstrakten Ebene zu interagieren.

Die Low-Level-Befehle sind:

- *class*-list
- *Klasse*-param-get
- *class*-param-set
- *Klasse*-param-list
- *Klasse*-param-add
- *Klasse*-param-remove
- *Klasse*-param-clear

Wo *Klasse* eine der folgenden ist:

- `bond`
- `console`
- `host`
- `host-crashdump`
- `host-cpu`
- `network`
- `patch`
- `pbd`
- `pif`
- `pool`
- `sm`
- `sr`
- `task`
- `template`

- vbd
- vdi
- vif
- vlan
- vm

Nicht jeder Wert der *Klasse* hat den vollständigen Satz von *Klassenbefehlen* -param-*action* . Einige Werte der *Klasse* haben einen kleineren Satz von Befehlen.

Parametertypen

Die Objekte, die mit den xe-Befehlen adressiert werden, verfügen über Parametersätze, die sie identifizieren und deren Status definieren.

Die meisten Parameter nehmen einen einzelnen Wert an. Beispielsweise enthält der`name-label` Parameter einer VM einen einzelnen Zeichenfolgenwert. In der Ausgabe von Parameterlistenbefehlen`xe vm-param-list`, z. B. gibt ein Wert in Klammern an, ob Parameter schreibgeschützt (RW) oder schreibgeschützt (RO) sind.
Die Ausgabe von`xe vm-param-list` auf einer angegebenen VM kann folgende Zeilen haben:

```
user-version ( RW): 1
 is-control-domain (RO): false
```

Der erste Parameter,`user-version`, ist beschreibbar und hat den Wert 1. Das zweite`is-control-domain`„ ist schreibgeschützt und hat den Wert false.

Die beiden anderen Parametertypen sind mehrwertig. Ein *Set-Parameter* enthält eine Liste von Werten. Ein *Kartenparameter* ist ein Satz von Schlüssel/Wert-Paaren. Sehen Sie sich beispielsweise die folgende Beispielausgabe des`xe vm-param-list` auf einer angegebenen VM an:

```
Plattform (MRW): acpi: true; apic: true; pae: true; nx: false
allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
hard_shutdown; hard_reboot; suspendieren
```

Der`platform` Parameter enthält eine Liste von Elementen, die Schlüssel/Wert-Paare darstellen. Den Schlüsselnamen folgt ein Doppelpunkt (:). Jedes Schlüssel/Wert-Paar wird durch ein Semikolon (;) vom nächsten getrennt. Das M, das dem RW vorangestellt ist, gibt an, dass dieser Parameter ein Kartenparameter ist und lesbar und beschreibbar ist. Der`allowed-operations` Parameter verfügt über eine Liste, aus der eine Reihe von Elementen besteht. Das S, das dem RO vorangestellt ist, zeigt an, dass es sich um einen eingestellten Parameter handelt und lesbar, aber nicht beschreibbar ist.

Um nach einem Kartenparameter zu filtern oder einen Kartenparameter festzulegen, verwenden Sie einen Doppelpunkt (:), um den Kartenparameternamen und das Schlüssel/Wert-Paar zu trennen. Um beispielsweise den Wert des`foo` Schlüssels des`other-config` Parameters einer VM auf festzulegen`baa` , lautet der Befehl

```
1 xe vm-param-set uuid=VM uuid other-config:foo=baa
```

> **Hinweis:**
>
> In früheren Versionen wurde das Bindestrich (-) verwendet, um Kartenparameter anzugeben. Diese Syntax funktioniert immer noch, ist aber veraltet.

Low-Level-Parameterbefehle

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 und *class*-param-list. Jeder dieser Befehle verwendet einen`uuid` Parameter, um das jeweilige Objekt anzugeben. Da diese Befehle als Low-Level-Befehle gelten, müssen sie die UUID und nicht die VM-Namensbezeichnung verwenden.

- **`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.

- **`class`**`-param-get uuid=uuid param-name=parameter param-key=key`

  Gibt den Wert eines bestimmten Parameters zurück. Bei einem Zuordnungsparameter wird durch die Angabe des Paramschlüssels der Wert abgerufen, der diesem Schlüssel in der Karte zugeordnet ist. Wenn paramkey nicht angegeben ist oder wenn der Parameter ein Satz ist, gibt der Befehl eine Zeichenfolgendarstellung des Satzes oder der Zuordnung zurück.

- **`class`**`-param-set uuid=uuid param=value`

  Legt den Wert eines oder mehrerer Parameter fest.

- **`class`**`-param-add uuid=uuid param-name=parameter key=value param-key=key`

  Fügt entweder einer Karte oder einem Set-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.

- **`class`**`-param-remove uuid=uuid param-name=parameter param-key=key`

  Entfernt entweder ein Schlüssel/Wert-Paar aus einer Karte oder einen Schlüssel aus einem Satz.

- **`class`**`-param-clear uuid=uuid param-name=parameter`

  Löscht einen Satz oder eine Karte vollständig.

Low-Level-Listenbefehle

Der Befehl *class*-list listet die Objekte des Typs *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 filtern, so dass es nur eine Teilmenge ausgibt
- Die Parameter, die gedruckt werden, können geändert werden.

Um die Parameter zu ändern, die gedruckt werden, geben Sie die *Argumentparameter* als kommagetrennte Liste der erforderlichen Parameter an. Zum Beispiel:

```
1 xe vm-list params=name-label,other-config
```

Um alle Parameter aufzulisten, verwenden Sie alternativ die Syntax:

```
1 xe vm-list params=all
```

Der Befehl list zeigt nicht einige Parameter an, die teuer zu berechnen sind. Diese Parameter werden beispielsweise wie folgt dargestellt:

```
1 allowed-VBD-devices (SRO): <expensive field>
```

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 Werten ab, die in der Befehlszeile angegeben sind. Dabei werden nur Objekte gedruckt, die allen angegebenen Einschränkungen entsprechen. Zum Beispiel:

```
1 xe vm-list HVM-boot-policy="BIOS order" power-state=halted
```

Dieser Befehl listet nur die VMs auf, für die *sowohl* das Feld den Wert *angehaltenpower-state* hat als auch das Feld die *BIOS-ReihenfolgeHVM-boot-policy aufweist* .

Sie können die Liste auch nach dem Wert von Schlüsseln in Zuordnungen oder nach der Existenz von Werten in einem Satz filtern. Die Syntax für die Filterung basierend auf Schlüsseln in Karten ist`map-name:key=value`. Die Syntax für die Filterung basierend auf Werten, die in einem Satz vorhanden sind, ist`set-name:contains=value`.

Beim Skripting wird die Befehlszeile durch eine nützliche Technik übergeben`--minimal`, wodurch`xe` nur das erste Feld in einer kommagetrennten Liste gedruckt wird. Beispielsweise gibt der Befehl`xe vm-list --minimal` auf einem Host mit drei installierten VMs die drei UUIDs der VMs an:

```
1     a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-
         af10baea96b7, \
```



```
2      42c044de-df69-4b30-89d9-2c199564581d
```

Geheimnisse

Citrix Hypervisor bietet einen Geheimnismechanismus, um zu verhindern, dass Kennwörter im Befehlszeilenverlauf oder in API-Objekten im Klartext gespeichert werden. XenCenter verwendet diese Funktion automatisch und kann auch über die xe-CLI für alle Befehle verwendet werden, für die ein Kennwort erforderlich ist.

> Hinweis
>
> Kennwortgeheimnisse können nicht zur Authentifizierung mit einem Citrix Hypervisor Host von einer Remote-Instanz der xe-CLI verwendet werden.

Führen Sie zum Erstellen eines geheimen Objekts den folgenden Befehl auf dem Citrix Hypervisor Host aus.

```
1 xe secret-create value=my-password
```

Ein Geheimnis wird erstellt und auf dem Citrix Hypervisor Host gespeichert. Der Befehl gibt die UUID des geheimen Objekts aus. Beispiel: `99945d96-5890-de2a-3899-8c04ef2521db`. _secret“ Hängen Sie an den Namen des Passwort-Arguments an, um diese UUID an einen beliebigen Befehl zu übergeben, der ein Kennwort erfordert.

Beispiel: Auf dem Citrix Hypervisor Host, auf dem Sie den geheimen Schlüssel 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”
```

xe-Befehlsreferenz

In diesem Abschnitt werden die Befehle nach den Objekten gruppiert, die der Befehl adressiert. Diese Objekte werden alphabetisch aufgelistet.

Appliance-Befehle

Befehle zum Erstellen und Ändern von VM-Appliances (auch vApps genannt). Weitere Informationen finden Sie unter vApps.

Einheitenparameter

Appliance-Befehle haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die Appliance uid	Erforderlich
name-description	Beschreibung der Appliance	Optional
paused		Optional
force	Herunterfahren erzwingen	Optional

appliance-assert-can-be-recovered

```
appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid
    =vdi-uuid
```

Prüft, ob Speicher verfügbar ist, um diese VM-Appliance/vApp wiederherzustellen.

appliance-create

```
appliance-create name-label=name-label [name-description=name-
    description]
```

Erstellt eine Appliance/vApp. Zum Beispiel:

```
xe appliance-create name-label=my_appliance
```

Hinzufügen von VMs zur Appliance:

```
    xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
```

appliance-destroy

```
appliance-destroy uuid=appliance-uuid
```

Zerstört eine Appliance/vApp. Zum Beispiel:

```
xe appliance-destroy uuid=appliance-uuid
```


appliance-recover

```
appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
   paused=true|false]
```

Wiederherstellen einer VM-Appliance/vApp aus der Datenbank, die im mitgelieferten VDI enthalten ist.

appliance-shutdown

```
appliance-shutdown uuid=appliance-uuid [force=true|false]
```

Beenden Sie alle VMs in einer Appliance/vApp. Zum Beispiel:

```
xe appliance-shutdown uuid=appliance-uuid
```

appliance-start

```
appliance-start uuid=appliance-uuid [paused=true|false]
```

Startet eine Appliance/vApp. Zum Beispiel:

```
xe appliance-start uuid=appliance-uuid
```

Überwachungsbefehle

Überwachungsbefehle laden alle verfügbaren Datensätze der RBAC-Überwachungsdatei im Pool herunter. Wenn der optionale Parameter vorhandensince 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 *Dateiname*	Erforderlich
since	Spezifischer Datum/Zeitpunkt	Optional

audit-log-get

```
audit-log-get [since=timestamp] filename=filename
```

Führen Sie beispielsweise den folgenden Befehl aus, um Überwachungsdatensätze des Pools seit einem genauen Zeitstempel in Millisekunden 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
```

Bonding-Befehle

Befehle für die Arbeit mit Netzwerkanleihen, für Widerstandsfähigkeit mit physischem Schnittstellen-Failover. Weitere Informationen finden Sie unter Vernetzung.

Das Bindungsobjekt ist ein Referenzobjekt, das *Master-* und *Member-PIF* zusammenklebt. Die Master-PIF ist die Klebungsschnittstelle, die als Gesamt-PIF verwendet werden muss, um sich auf die Bindung zu beziehen. Bei den Mitglied-PIFs handelt es sich um eine Gruppe von zwei oder mehr physikalischen Schnittstellen, die zu der High-Level-gebundenen Schnittstelle kombiniert wurden.

Anleihungsparameter

Anleihen haben folgende Parameter:

Parametername	Beschreibung	Typ
uuid	Eindeutige Bezeichner/Objektreferenz für die Bindung	Schreibgeschützt
master	UUID für die Master-Anleihe PIF	Schreibgeschützt
members	Satz von UUIDs für die zugrunde liegenden gebundenen PIF	Schreibgeschützt

bond-create


```
bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,pif_uuid_2
    ,...
```

Erstellen Sie eine gebundene Netzwerkschnittstelle im Netzwerk, das aus einer Liste vorhandener PIF-Objekte angegeben wurde. Der Befehl schlägt in einem der folgenden Fälle fehl:

- Wenn PIF bereits in einer anderen Anleihe sind
- Wenn ein Mitglied ein VLAN-Tag gesetzt hat
- Wenn sich die referenzierten PIF nicht auf demselben Citrix Hypervisor or-Server befinden
- Wenn weniger als 2 PIF geliefert werden

bond-destroy

```
bond-destroy uuid=bond_uuid
```

Löscht eine gebundene Schnittstelle, die durch ihre UUID angegeben wird, von einem Host.

bond-set-mode

```
bond-set-mode uuid=bond_uuid mode=bond_mode
```

Ändern Sie den Bond-Modus.

CD-Befehle

Befehle zum Arbeiten mit physischen CD/DVD-Laufwerken auf Citrix Hypervisor or-Servern.

CD-Parameter

CDs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Eindeutige Bezeichner/Objektreferenz für die CD	Schreibgeschützt
name-**label**	Name der CD	Lese-/Schreibzugriff
name-description	Beschreibungstext für die CD	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
allowed-operations	Eine Liste der Vorgänge, die auf dieser CD ausgeführt werden können	Schreibgeschützte Parameter
current-operations	Eine Liste der Vorgänge, die derzeit auf dieser CD ausgeführt werden	Schreibgeschützte Parameter
sr-uuid	Die eindeutige Bezeichner/Objektreferenz für die SR, die diese CD enthält, ist Teil von	Schreibgeschützt
sr-name-**label**	Der Name für die SR dieser CD ist Teil von	Schreibgeschützt
vbd-uuids	Eine Liste der eindeutigen Bezeichner für die VBDs auf VMs, die eine Verbindung zu dieser CD herstellen	Schreibgeschützte Parameter
crashdump-uuids	Nicht auf CDs verwendet. Da Crashdumps nicht auf CDs geschrieben werden können	Schreibgeschützte Parameter
virtual-size	Größe der CD, wie sie für VMs angezeigt wird (in Byte)	Schreibgeschützt
physical-utilisation	Menge des physischen Speicherplatzes, den das CD-Image auf der SR belegt (in Bytes)	Schreibgeschützt
type	Für CDs auf Benutzer festlegen	Schreibgeschützt
sharable	Gibt an, ob das CD-Laufwerk gemeinsam verwendet werden kann. Der Standardwert ist**false**.	Schreibgeschützt
read-only	Ob die CD schreibgeschützt ist, wenn**false**, ist das Gerät beschreibbar. Immer wahr für CDs.	Schreibgeschützt

Parametername	Beschreibung	Typ
storage-lock	Der Wert ist **true** , wenn dieser Datenträger auf Speicherebene gesperrt ist.	Schreibgeschützt
parent	Verweis auf die übergeordnete Festplatte, wenn diese CD Teil einer Kette ist.	Schreibgeschützt
missing	Der Wert ist **true** , wenn der SR-Scanvorgang diese CD als nicht auf der Festplatte gemeldet hat.	Schreibgeschützt
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die CD angeben	Kartenparameter mit Lese-/Schreibzugriff
location	Der Pfad, auf dem das Gerät eingehängt ist	Schreibgeschützt
managed	Wert ist **true** , wenn das Gerät verwaltet wird	Schreibgeschützt
xenstore-data	Daten, die in den Xenstore-Baum eingefügt werden sollen	Schreibgeschützte Kartenparameter
sm-config	Namen und Beschreibungen von Speicher-Manager-Gerätekonfigurationsschlüsseln	Schreibgeschützte Kartenparameter
is-a-snapshot	Wert ist **true** , wenn es sich bei dieser Vorlage um einen CD-Schnappschuss handelt.	Schreibgeschützt
snapshot_of	Die UUID der CD, die diese Vorlage ein Snapshot von	Schreibgeschützt
snapshots	Die UUIDs aller Snapshots, die von dieser CD erstellt wurden	Schreibgeschützt

Parametername	Beschreibung	Typ
snapshot_time	Der Zeitstempel des Snapshot-Vorgangs	Schreibgeschützt

cd-list

```
cd-list [params=param1,param2,...] [parameter=parameter_value]
```

Listen Sie die CDs und ISOs (CD-Imagedateien) auf dem Citrix Hypervisor-Server oder -pool auf und filtern Sie das optionale Argumentparams.

Wenn das optionale Argument verwendetparams 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. Wennparams nicht verwendet wird, zeigt die zurückgegebene Liste eine Standardteilmenge aller verfügbaren Parameter an.

Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts CD-Parameter aufgeführten sein.

Clusterbefehle

Befehle zum Arbeiten mit gruppierten Pools.

Cluster-Pools sind Ressourcenpools, für die das Cluster-Feature aktiviert ist. Verwenden Sie diese Pools mit GFS2 SRs. Weitere Informationen finden Sie unter Cluster-Pools

Die Cluster- und Cluster-Host-Objekte können mit den Standardobjekt-Auflistungsbefehlen (xe cluster-list undxe cluster-host-list) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle.
Befehle zum Arbeiten mit gruppierten Pools.

Clusterparameter

Cluster haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für den Cluster	Schreibgeschützt

Parametername	Beschreibung	Typ
`cluster-hosts`	Eine Liste eindeutiger Bezeichner/Objektreferenzen für die Hosts im Cluster	Schreibgeschützte Parameter
`cluster-token`	Der geheime Schlüssel, der von xapi-clusterd verwendet wird, wenn er auf anderen Hosts mit sich selbst spricht	Schreibgeschützt
`cluster-stack`	Der Technologie-Stack, der die Clustering-Funktionen bereitstellt. Mögliche Werte sind`corosync`.	Schreibgeschützt
`allowed-operations`	Listet die in diesem Zustand zulässigen Vorgänge auf. Diese Liste ist nur beratend, und der Clusterstatus hat sich möglicherweise geändert, wenn ein Client dieses Feld liest.	Schreibgeschützte Parameter
`current-operations`	Listet die derzeit in Bearbeitung befindlichen Vorgänge auf. Diese Liste ist nur beratend, und der Clusterstatus hat sich möglicherweise geändert, wenn ein Client dieses Feld liest.	Schreibgeschützte Parameter
`token-timeout`	Das Timeout des Corosync-Token in Sekunden	Schreibgeschützt
`token-timeout-coefficient`	Der Corosync-Token Timeout-Koeffizient in Sekunden	Schreibgeschützt
`pool-auto-join`	True, wenn neue Poolmitglieder automatisch mit dem Cluster verbunden werden. Dies ist auf eingestellt`true`.	Schreibgeschützt

Parametername	Beschreibung	Typ
cluster-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Cluster angeben.	Schreibgeschützte Kartenparameter
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Cluster angeben.	Kartenparameter mit Lese-/Schreibzugriff

cluster-host-create

```
cluster-host-create cluster-uuid=cluster_uuid host-uuid=host_uuid pif-
    uuid=pif_uuid
```

Fügen Sie einem vorhandenen Cluster einen Host hinzu.

cluster-host-destroy

```
cluster-host-destroy uuid=host_uuid
```

Zerstören Sie einen Clusterhost und verlassen Sie den Cluster effektiv.

cluster-host-disable

```
cluster-host-disable uuid=cluster_uuid
```

Deaktivieren der Clustermitgliedschaft für einen aktivierten Clusterhost.

cluster-host-enable

```
cluster-host-enable uuid=cluster_uuid
```

Aktivieren der Clustermitgliedschaft für einen deaktivierten Clusterhost.

cluster-host-force-destroy

```
cluster-host-force-destroy uuid=cluster_host
```

Zerstören Sie ein Cluster-Hostobjekt mit Nachdruck und verlassen Sie den Cluster effektiv.

cluster-pool-create

```
cluster-pool-create network-uuid=network_uuid [cluster-stack=
    cluster_stack] [token-timeout=token_timeout] [token-timeout-
    coefficient=token_timeout_coefficient]
```

Erstellen Sie einen Pool-weiten Cluster.

cluster-pool-destroy

```
cluster-pool-destroy cluster-uuid=cluster_uuid
```

Zerstöre den Pool-weiten Cluster. Der Pool existiert weiterhin, ist aber nicht mehr gruppiert und kann keine GFS2-SRs mehr verwenden.

cluster-pool-force-destroy

```
cluster-pool-force-destroy cluster-uuid=cluster_uuid
```

Erzwingen Sie, den Pool-weiten Cluster zu zerstören.

cluster-pool-resync

```
cluster-pool-resync cluster-uuid=cluster_uuid
```

Synchronisieren Sie einen Cluster über einen Pool hinweg.

Konsolenbefehle

Befehle zum Arbeiten mit Konsolen.

Die Konsolenobjekte können mit dem Standardbefehl (`xe console-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle.

Konsolenparameter

Konsolen haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die Konsole	Schreibgeschützt
`vm-uuid`	Die eindeutige Bezeichner/Objektreferenz der VM, auf der diese Konsole geöffnet ist	Schreibgeschützt
`vm-name-label`	Der Name der VM, auf der diese Konsole geöffnet ist	Schreibgeschützt
`protocol`	Protokoll, das von dieser Konsole verwendet wird. Mögliche Werte sind`vt100`: VT100-Terminal,`rfb`: Remote Framebuffer Protocol (wie in VNC verwendet) oder`rdp`: Remote Desktop Protocol	Schreibgeschützt
`location`	URI für den Konsolendienst	Schreibgeschützt
`other-config`	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die Konsole angeben.	Kartenparameter mit Lese-/Schreibzugriff

`console`

```
1 console
```

An eine bestimmte Konsole anhängen.

Diagnosebefehle

Befehle zum Sammeln von Diagnoseinformationen von Citrix Hypervisor.

diagnostic-compact

```
diagnostic-compact
```

Führen Sie eine große GC-Sammlung und Heap-Komprimierung durch.

diagnostic-db-log

```
diagnostic-db-log
```

Starten Sie die Protokollierung der Datenbankvorgänge. Warnung: Einmal gestartet, kann diese nicht gestoppt werden.

diagnostic-db-stats

```
diagnostic-db-stats
```

Drucken von Datenbankstatistiken.

diagnostic-gc-stats

```
diagnostic-gc-stats
```

GC-Statistiken drucken.

diagnostic-license-status

```
diagnostic-license-status
```

Hilfe bei der Diagnose von Poolweiten Lizenzierungsproblemen.

diagnostic-net-stats

```
diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2
    ...]
```

Drucken von Netzwerkstatistiken.

diagnostic-timing-stats

```
diagnostic-timing-stats
```

Zeitstatistiken drucken.

diagnostic-vdi-status

```
diagnostic-vdi-status uuid=vdi_uuid
```

Fragen Sie den Sperr- und Freigabestatus eines VDI ab.

diagnostic-vm-status

```
diagnostic-vm-status uuid=vm_uuid
```

Fragen Sie die Hosts ab, auf denen die VM starten kann, und überprüfen Sie den Freigabe-/Sperrstatus aller VBDs.

Disaster Recovery-Befehle

Befehle zum Wiederherstellen von VMs nach einer Katastrophe

drtask-create

```
drtask-create type=type sr-whitelist=sr-white-list device-config=device
    -config
```

Erstellt eine Disaster Recovery-Aufgabe. So stellen Sie beispielsweise eine Verbindung zu einer iSCSI-SR in Vorbereitung auf die Disaster Recovery her:

```
xe drtask-create type=lvmoiscsi device-config:target=target-ip-address
    \
     device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
     sr-whitelist=sr-uuid-list
```

> **Hinweis:**

> Der Befehl`sr-whitelist` listet SR-UUIDs auf. Der `drtask-create` Befehl führt nur eine SR ein und stellt eine Verbindung mit einer der UUIDs auf der weißen Liste her.

drtask-destroy

```
drtask-destroy uuid=dr-task-uuid
```

Zerstört eine Disaster Recovery-Aufgabe und vergisst die eingeführte SR.

vm-assert-can-be-recovered

```
vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

Prüft, ob Speicher verfügbar ist, um diese VM wiederherzustellen.

appliance-assert-can-be-recovered

```
appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid
    =vdi-uuid
```

Überprüft, ob der Speicher (der die App/vApp-Festplatte enthält) sichtbar ist.

appliance-recover

```
appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [force
    =true|false]
```

Wiederherstellen einer Appliance/vApp aus der Datenbank, die im mitgelieferten VDI enthalten ist.

vm-recover

```
vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true|false]
```

Stellt eine VM aus der Datenbank wieder her, die im mitgelieferten VDI enthalten ist.

sr-enable-database-replication

```
sr-enable-database-replication uuid=sr_uuid
```

Aktiviert die XAPI-Datenbankreplikation auf die angegebene (gemeinsam genutzte) SR.

sr-disable-database-replication

```
sr-disable-database-replication uuid=sr_uuid
```

Deaktiviert die XAPI-Datenbankreplikation auf die angegebene SR.

Beispielnutzung

Das folgende Beispiel zeigt die DR-CLI-Befehle im Kontext:

Aktivieren Sie am primären Standort die Datenbankreplikation:

```
xe sr-database-replication uuid=sr=uuid
```

Stellen Sie nach einer Katastrophe am sekundären Standort eine Verbindung zum SR her. Der`device-config` Befehl hat die gleichen 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
```

Suchen Sie nach Datenbank-VDIs auf der SR:

```
xe vdi-list sr-uuid=sr-uuid type=Metadata
```

Abfrage eines Datenbank-VDI für vorhandene VMs:

```
xe vm-list database:vdi-uuid=vdi-uuid
```

Wiederherstellen einer VM:

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

Zerstören Sie den DR-Task. Alle von der DR-Task eingeführten und von VMs nicht benötigten SRs werden vernichtet:


```
xe drtask-destroy uuid=drtask-uuid
```

Ereignisbefehle

Befehle zum Arbeiten mit Ereignissen.

Eventklassen

Ereignisklassen sind in der folgenden Tabelle aufgeführt:

Klassenname	Beschreibung
pool	Ein Pool physischer Hosts
vm	Eine virtuelle Maschine
host	Ein physischer Host
network	Ein virtuelles Netzwerk
vif	Eine virtuelle Netzwerkschnittstelle
pif	Eine physische Netzwerkschnittstelle (separate VLANs werden als mehrere PIFs dargestellt)
sr	Ein Speicher-Repository
vdi	Ein virtuelles Laufwerk-Image
vbd	Ein virtuelles Blockgerät
pbd	Die physischen Blockgeräte, über die Hosts auf SRs zugreifen

`event-wait`

```
event-wait class=class_name [param-name=param_value] [param-name=/=
    param_value]
```

Blockiert die Ausführung anderer Befehle, bis ein Objekt vorhanden ist, das die in der Befehlszeile angegebenen Bedingungen erfüllt. Das Argument `x=y` bedeutet „warten, bis Feld x Wert y nimmt“ und `x=/=y` bedeutet „warten, bis Feld x einen anderen Wert als y nimmt.“

Beispiel: Warten Sie, bis eine bestimmte VM ausgeführt wird.


```
xe event-wait class=vm name-label=myvm power-state=running
```

Blockiert andere Befehle, bis eine VM aufgerufenmyvm wird in derpower-state „läuft. „

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)
```

Blockiert 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 jeder der am Anfang dieses AbschnittsEreignisklassenaufgeführten sein. Bei den Parametern kann es sich um einen der in der *CLI-Befehlsklasse*-param-list aufgeführten Parameter handeln.

GPU-Befehle

Befehle für die Arbeit mit physischen GPUs, GPU-Gruppen und virtuellen GPUs.

Die GPU-Objekte können mit den Standardobjektlistenbefehlen aufgelistet werden:xe pgpu-listxe gpu-group-list““, undxe vgpu-list“. Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle.

Physische GPU-Parameter

Physische GPUS (PGPU) haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die PGPU	Schreibgeschützt
vendor-name	Der Herstellername der PGPU	Schreibgeschützt
device-name	Der vom Hersteller diesem PGPU Modell zugewiesene Name	Schreibgeschützt

Parametername	Beschreibung	Typ
gpu-group-uuid	Der eindeutige Bezeichner/Objektreferenz für die GPU-Gruppe, der diese PGPU automatisch von Citrix Hypervisor zugewiesen wurde. Identische PGPU über Hosts in einem Pool sind gruppiert	Schreibgeschützt
gpu-group-name-**label**	Der Name der GPU-Gruppe, der die PGPU zugewiesen ist	Schreibgeschützt
host-uuid	Der eindeutige Bezeichner/Objektreferenz für den Citrix Hypervisor or-Server, mit dem die PGPU verbunden ist	Schreibgeschützt
host-name-**label**	Der Name des Citrix Hypervisor or-Servers, mit dem die PGPU verbunden ist	Schreibgeschützt
pci-id	PCI-Bezeichner	Schreibgeschützt
dependencies	Listet die abhängigen PCI-Geräte auf, die an dieselbe VM übergeben wurden	Kartenparameter mit Lese-/Schreibzugriff
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die PGPU angeben	Kartenparameter mit Lese-/Schreibzugriff
supported-VGPU-types	Liste der virtuellen GPU-Typen, die von der zugrunde liegenden Hardware unterstützt werden	Schreibgeschützt
enabled-VGPU-types	Liste der virtuellen GPU-Typen, die für diese PGPU aktiviert wurden	Lesen/Schreiben

Parametername	Beschreibung	Typ
resident-VGPUs	Liste der auf dieser PGPU ausgeführten VGPUs	Schreibgeschützt

pgpu-disable-dom0-access

```
pgpu-disable-dom0-access uuid=uuid
```

Deaktivieren Sie den PGPU Zugriff auf dom0.

pgpu-enable-dom0-access

```
pgpu-enable-dom0-access uuid=uuid
```

Aktivieren 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	Schreibgeschützt
name-**label**	Der Name der GPU-Gruppe	Lese-/Schreibzugriff
name-description	Der beschreibende Text der GPU-Gruppe	Lese-/Schreibzugriff
VGPU-uuids	Listet die eindeutigen Bezeichner/Objektreferenzen für die virtuellen GPUs in der GPU-Gruppe auf	Schreibgeschützte Parameter
PGPU-uuids	Listet die eindeutigen Bezeichner/Objektreferenzen für die PGPU in der GPU-Gruppe auf	Schreibgeschützte Parameter

Parametername	Beschreibung	Typ
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die GPU-Gruppe angeben	Kartenparameter mit Lese-/Schreibzugriff
supported-VGPU-types	Vereinigung aller von der zugrunde liegenden Hardware unterstützten virtuellen GPU-Typen	Schreibgeschützt
enabled-VGPU-types	Vereinigung aller virtuellen GPU-Typen, die auf den zugrunde liegenden PGPU aktiviert wurden	Schreibgeschützt
allocation-algorithm	Tiefe-ersten/Breadth-erste Einstellung für die Zuweisung virtueller GPUs auf PGPU innerhalb der Gruppe	Enum-Parameter mit Lese-/Schreibzugriff

GPU-Gruppenvorgänge

Befehle für die Arbeit mit GPU-Gruppen

gpu-group-create

```
gpu-group-create name-label=name_for_group [name-description=
    description]
```

Erstellt eine neue (leere) GPU-Gruppe, in die PGPU verschoben werden können.

gpu-group-destroy

```
gpu-group-destroy uuid=uuid_of_group
```

Zerstört die GPU-Gruppe; nur für leere Gruppen zulässig.

gpu-group-get-remaining-capacity


```
gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-uuid=
    uuid_of_vgpu_type
```

Gibt zurück, wie viele weitere virtuelle GPUs des angegebenen Typs in dieser GPU-Gruppe instanziiert werden können.

gpu-group-param-set

```
gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
    first|depth-first
```

Ändert den Algorithmus, den die GPU-Gruppe verwendet, um PGPU virtuelle GPUs zuzuweisen.

gpu-group-param-get-uuid

```
gpu-group-param-get-uuid uuid=uuid_of_group param-name=supported-vGPU-
    types|enabled-vGPU-types
```

Gibt die unterstützten oder aktivierten Typen für diese GPU-Gruppe zurück.

Virtuelle GPU-Parameter

Virtuelle GPUs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die virtuelle GPU	Schreibgeschützt
vm-uuid	Der eindeutige Bezeichner/Objektreferenz für die VM, der die virtuelle GPU zugewiesen ist	Schreibgeschützt
vm-name-**label**	Der Name der VM, der die virtuelle GPU zugewiesen ist	Schreibgeschützt
gpu-group-uuid	Die eindeutige Bezeichner/Objektreferenz für die GPU-Gruppe, in der die virtuelle GPU enthalten ist	Schreibgeschützt

Parametername	Beschreibung	Typ
gpu-group-name-**label**	Der Name der GPU-Gruppe, in der die virtuelle GPU enthalten ist	Schreibgeschützt
currently-attached	True, wenn eine VM mit GPU-Pass-Through ausgeführt wird, andernfalls false	Schreibgeschützt
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die virtuelle GPU angeben	Kartenparameter mit Lese-/Schreibzugriff
type-uuid	Die eindeutige Bezeichner/Objektreferenz für den virtuellen GPU-Typ dieser virtuellen GPU	Kartenparameter mit Lese-/Schreibzugriff
type-model-name	Modellname, der dem virtuellen GPU-Typ zugeordnet ist	Schreibgeschützt

Parameter des virtuellen GPU-Types

> **Hinweis:**
>
> GPU-Passthrough und virtuelle GPUs sind nicht mit Livemigration, Speicher-Livemigration oder VM Suspend kompatibel, sofern nicht unterstützte Software und Grafikkarten von GPU-Anbietern vorhanden sind. VMs ohne diese Unterstützung können nicht migriert werden, um Ausfallzeiten zu vermeiden. Informationen zur NVIDIA vGPU Kompatibilität mit Livemigration, Speicher-Livemigration und VM Suspend finden Sie unterGrafik.

Virtuelle GPU-Typen haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für den virtuellen GPU-Typ	Schreibgeschützt

Parametername	Beschreibung	Typ
vendor-name	Name des virtuellen GPU-Anbieters	Schreibgeschützt
model-name	Modellname, der dem virtuellen GPU-Typ zugeordnet ist	Schreibgeschützt
freeze-frame	Framebuffer-Größe des virtuellen GPU-Typs, in Byte	Schreibgeschützt
max-heads	Maximale Anzahl von Bildschirmen, die vom virtuellen GPU-Typ unterstützt werden	Schreibgeschützt
supported-on-PGPUs	Liste der PGPU, die diesen virtuellen GPU-Typ unterstützen	Schreibgeschützt
enabled-on-PGPUs	Liste der PGPU, für die dieser virtuelle GPU-Typ aktiviert ist	Schreibgeschützt
VGPU-uuids	Liste der virtuellen GPUs dieses Typs	Schreibgeschützt

Virtuelle GPU-Vorgänge

vgpu-create

```
1 vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [vgpu-
     type-uuid=uuid_of_vgpu-type]
```

Erstellt eine virtuelle GPU. Mit diesem Befehl wird die VM an die angegebene GPU-Gruppe angehängt und optional den virtuellen GPU-Typ angegeben. Wenn kein virtueller GPU-Typ angegeben wird, wird der Typ „Pass-Through“ angenommen.

vgpu-destroy

```
1 vgpu-destroy uuid=uuid_of_vgpu
```

Zerstören Sie 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
```

Mit`false` dieser Option wird die VNC-Konsole für eine VM deaktiviert, während sie an`disablevnc=1` den Anzeigeemulator weitergeleitet wird. Standardmäßig ist VNC aktiviert.

Host-Befehle

Befehle für die Interaktion mit dem Citrix Hypervisor or-Server.

Citrix Hypervisor or-Server sind die physischen Server, auf denen die Citrix Hypervisor or-Software ausgeführt wird. Auf ihnen werden VMs unter der Kontrolle einer speziellen privilegierten virtuellen Maschine ausgeführt, die als Steuerdomäne oder Domäne 0 bezeichnet wird.

Die Citrix Hypervisor or-Serverobjekte können mit den Standardbefehlen aufgelistet werden:xe host-listxe host-cpu-list"", undxe host-crashdump-list"). Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle.

Host-Selektoren

Mehrere der hier aufgeführten Befehle verfügen über einen gemeinsamen Mechanismus zur Auswahl eines oder mehrerer Citrix Hypervisor or-Server, auf denen der Vorgang ausgeführt werden soll. Am einfachsten ist die Angabe des Argumentshost=`uuid_or_name_label`. Sie können Citrix Hypervisor auch angeben, indem Sie die vollständige Liste der Hosts nach den Werten der Felder filtern. Durch Angeben werden beispielsweiseenabled=`true` alle Citrix Hypervisor or-Server ausgewählt, derenenabled Feld gleich ist`true` . Wenn mehrere Citrix Hypervisor or-Server übereinstimmen und der Vorgang auf mehreren Citrix Hypervisor or-Servern ausgeführt werden kann, müssen Sie angeben,`--multiple` um den Vorgang auszuführen. Die vollständige Liste der Parameter, die abgeglichen werden können, wird am Anfang dieses Abschnitts beschrieben. Sie können diese Liste der Befehle erhalten, indem Sie den Befehl ausführen`xe host-list params=all`. Wenn keine Parameter für die Auswahl von Citrix Hypervisor or-Servern angegeben werden, wird der Vorgang auf allen Citrix Hypervisor-Servern ausgeführt.

Host-Parameter

Citrix Hypervisor -Server verfügen über die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Der eindeutige Bezeichner/Objektreferenz für den Citrix Hypervisor or-Server	Schreibgeschützt
name-**label**	Der Name des Citrix Hypervisor -Servers	Lese-/Schreibzugriff
name-description	Die Beschreibungszeichenfolge des Citrix Hypervisor -Servers	Schreibgeschützt
enabled	Wert ist**false** , wenn deaktiviert. Dadurch wird verhindert, dass neue VMs auf den Hosts gestartet werden, und die Hosts werden für das Herunterfahren oder Neustart vorbereitet. Wert ist**true** , wenn der Host aktiviert ist	Schreibgeschützt
API-version-major	Hauptversionsnummer	Schreibgeschützt
API-version-minor	Nebenversionsnummer	Schreibgeschützt
API-version-vendor	Identifizierung des API-Anbieters	Schreibgeschützt
API-version-vendor-implementation	Details zur Implementierung des Anbieters	Schreibgeschützte Kartenparameter
logging	Protokollierungskonfiguration	Kartenparameter mit Lese-/Schreibzugriff
suspend-image-sr-uuid	Die eindeutige Bezeichner/Objektreferenz für die SR, in der suspendierte Bilder platziert werden	Lese-/Schreibzugriff
crash-dump-sr-uuid	Die eindeutige Bezeichner/Objektreferenz für die SR, in der Crash-Dumps platziert werden	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
software-version	Liste der Versionsparameter und deren Werte	Schreibgeschützte Kartenparameter
capabilities	Liste der Xen Versionen, die auf dem Citrix Hypervisor or-Server ausgeführt werden können	Schreibgeschützte Parameter
other-config	Eine Liste der Schlüssel/Wert-Paare, die zusätzliche Konfigurationsparameter für den Citrix Hypervisor or-Server angeben	Kartenparameter mit Lese-/Schreibzugriff
chipset-info	Eine Liste von Schlüssel/Wert-Paaren, die Informationen über den Chipsatz angeben	Schreibgeschützte Kartenparameter
hostname	Hostname des Citrix Hypervisor or-Servers	Schreibgeschützt
address	IP-Adresse des Citrix Hypervisor or-Servers	Schreibgeschützt
license-server	Eine Liste von Schlüssel/Wert-Paaren, die Informationen zum Lizenzserver angeben. Der Standardport für die Kommunikation mit Citrix Produkten ist 27000. Informationen zum Ändern von Portnummern aufgrund von Konflikten finden Sie unterPortnummern ändern	Schreibgeschützte Kartenparameter
supported-bootloaders	Liste der Bootloader, die der Citrix Hypervisor or-Server unterstützt, z. B. pygrub, eliloader	Schreibgeschützte Parameter

Parametername	Beschreibung	Typ
memory-total	Gesamtmenge des physischen Arbeitsspeichers auf dem Citrix Hypervisor or-Server in Byte	Schreibgeschützt
memory-free	Gesamtmenge des verbleibenden physischen Arbeitsspeichers, der VMs zugewiesen werden kann, in Byte	Schreibgeschützt
host-metrics-live	True, wenn der Host betriebsbereit ist	Schreibgeschützt
logging	Dersyslog_destination Schlüssel kann auf den Hostnamen eines Remote Listening Syslog-Dienstes gesetzt werden.	Kartenparameter mit Lese-/Schreibzugriff
allowed-operations	Listet die in diesem Zustand zulässigen Vorgänge auf. Diese Liste ist nur beratend, und der Serverstatus hat sich möglicherweise geändert, wenn ein Client dieses Feld liest.	Schreibgeschützte Parameter
current-operations	Listet die derzeit in Bearbeitung befindlichen Vorgänge auf. Diese Liste ist nur beratend, und der Serverstatus hat sich möglicherweise geändert, wenn ein Client dieses Feld liest.	Schreibgeschützte Parameter
patches	Satz von Host-Patches	Schreibgeschützte Parameter
blobs	Binärer Datenspeicher	Schreibgeschützt

Parametername	Beschreibung	Typ
memory-free-computed	Eine konservative Schätzung der maximalen Speichermenge, die auf einem Host frei ist	Schreibgeschützt
ha-statefiles	Die UUIDs aller HA-Statusdateien	Schreibgeschützt
ha-network-peers	Die UUIDs aller Hosts, die die VMs auf diesem Host hosten könnten, wenn ein Fehler auftritt	Schreibgeschützt
external-auth-type	Typ der externen Authentifizierung, z. B. Active Directory.	Schreibgeschützt
external-auth-service-name	Der Name des externen Authentifizierungsdienstes	Schreibgeschützt
external-auth-configuration	Konfigurationsinformationen für den externen Authentifizierungsdienst.	Schreibgeschützte Kartenparameter

Citrix Hypervisor or-Server enthalten einige andere Objekte, die auch Parameterlisten enthalten.

CPUs auf Citrix Hypervisor or-Servern weisen die folgenden Parameter auf:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die CPU	Schreibgeschützt
number	Die Nummer des physischen CPU-Kerns innerhalb des Citrix Hypervisor or-Servers	Schreibgeschützt
vendor	Die Herstellerzeichenfolge für den CPU-Namen	Schreibgeschützt
speed	Die CPU-Takt in Hz	Schreibgeschützt

Parametername	Beschreibung	Typ
`modelname`	Die Herstellerzeichenfolge für das CPU-Modell, z. B. „Intel (R) Xeon (TM) CPU 3.00 GHz“	Schreibgeschützt
`stepping`	Die CPU-Revisionsnummer	Schreibgeschützt
`flags`	Die Flags der physischen CPU (eine dekodierte Version des Feature-Feldes)	Schreibgeschützt
`Utilisation`	Die aktuelle CPU-Auslastung	Schreibgeschützt
`host-uuid`	Die UUID, wenn der Host, in dem sich die CPU befindet	Schreibgeschützt
`model`	Die Modellnummer der physischen CPU	Schreibgeschützt
`family`	Die Nummer der physischen CPU-Familie	Schreibgeschützt

Crash Dumps auf Citrix Hypervisor or-Servern weisen die folgenden Parameter auf:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den Crashdump	Schreibgeschützt
`host`	Citrix Hypervisor -Server, dem der Crashdump entspricht	Schreibgeschützt
`timestamp`	Zeitstempel des Datums und der Uhrzeit, an der der Absturz aufgetreten ist, in der Form`yyyymmdd-hhmmss-ABC`, wobei *ABC*der Zeitzonenindikator ist, z. B. GMT	Schreibgeschützt
`size`	Größe des Crashdump, in Bytes	Schreibgeschützt

host-all-editions

```
host-all-editions
```

Eine Liste aller verfügbaren Editionen abrufen

host-apply-edition

```
host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition=”
    free” ”per-socket” ”xendesktop”]
```

Weist die Citrix Hypervisor or-Lizenz einem Hostserver zu. Wenn Sie eine Lizenz zuweisen, kontaktiert Citrix Hypervisor den Lizenzserver und fordert den angegebenen Lizenztyp an. Wenn eine Lizenz verfügbar ist, wird sie dann vom Lizenzserver ausgecheckt.

Verwenden Sie für Citrix Hypervisor für Citrix Virtual Desktops Editionen”xendesktop”.

Informationen zur Erstkonfiguration der Lizenzierung finden Sie unter auchlicense-server-address undlicense-server-port.

host-backup

```
host-backup file-name=backup_filename host=host_name
```

Laden Sie eine Sicherung der Steuerdomäne des angegebenen Citrix Hypervisor or-Servers auf den Computer herunter, von dem der Befehl aufgerufen wird. Speichern Sie es dort als Datei mit dem Namenfile-name.

> **Wichtig:**
>
> Während derxe host-backup Befehl funktioniert, wenn er auf dem lokalen Host ausgeführt wird (dh ohne einen bestimmten Hostnamen angegeben), verwenden Sie ihn nicht auf diese Weise. Dies würde die Kontrolldomänenpartition mit der Sicherungsdatei füllen. Verwenden Sie nur den Befehl von einem externen Rechner, auf dem Sie Speicherplatz für die Sicherungsdatei haben.

host-bugreport-upload

```
host-bugreport-upload [host-selector=host_selector_value...] [url=
    destination_url http-proxy=http_proxy_name]
```


Generieren Sie einen neuen Fehlerbericht (mit xen-bugtool, mit allen optionalen Dateien enthalten) und laden Sie sie auf die Support-FTP-Site oder an einen anderen Ort hoch.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

Optionale Parameter sind `http-proxy`: Verwenden Sie den angegebenen HTTP-Proxy und `url`: Upload zu dieser Ziel-URL. Wenn keine optionalen Parameter verwendet werden, wird kein Proxyserver identifiziert, und das Ziel ist die standardmäßige Support-FTP-Site.

host-call-plugin

```
host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args=
    args]
```

Ruft die Funktion innerhalb des Plugins auf dem angegebenen Host mit optionalen Argumenten auf.

host-compute-free-memory

```
host-compute-free-memory
```

Berechnet die Menge des freien Speichers auf dem Host.

host-compute-memory-overhead

```
host-compute-memory-overhead
```

Berechnet den Virtualisierungsspeicher-Overhead eines Hosts.

host-cpu-info

```
host-cpu-info [uuid=uuid]
```

Listet Informationen über die physischen CPUs des Hosts auf.

host-crashdump-destroy

```
host-crashdump-destroy uuid=crashdump_uuid
```

Löschen Sie einen durch seine UUID angegebenen Host-Crashdump vom Citrix Hypervisor or-Server.

host-crashdump-upload

```
host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [http-
    proxy=http_proxy_name]
```

Laden Sie ein crashdump auf die Support-FTP-Site oder einen anderen Speicherort hoch. Wenn keine optionalen Parameter verwendet werden, wird kein Proxyserver identifiziert, und das Ziel ist die standardmäßige Support-FTP-Site. Optionale Parameter sind `http-proxy`: Verwenden Sie den angegebenen HTTP-Proxy und `url`: Upload zu dieser Ziel-URL.

host-declare-dead

```
host-declare-dead uuid=host_uuid
```

Erklären Sie, dass der Host tot ist, ohne ihn explizit zu kontaktieren.

> **Warnhinweis:**
>
> Dieser Aufruf ist gefährlich und kann Datenverlust verursachen, wenn der Host nicht tatsächlich tot ist.

host-disable

```
host-disable [host-selector=host_selector_value...]
```

Deaktiviert die angegebenen Citrix Hypervisor or-Server, wodurch verhindert wird, dass neue VMs auf ihnen gestartet werden. Mit dieser Aktion werden die Citrix Hypervisor or-Server für das Herunterfahren oder Neustart vorbereitet.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (sieheHost-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-disable-display

```
host-disable-display uuid=host_uuid
```

Deaktivieren Sie die Anzeige für den Host.

host-disable-local-storage-caching

```
host-disable-local-storage-caching
```

Deaktivieren Sie das lokale Speicher-Caching auf dem angegebenen Host.

host-dmesg

```
host-dmesg [host-selector=host_selector_value...]
```

Abrufen eines Xen`dmesg` (die Ausgabe des Kernelringpuffers) von angegebenen Citrix Hypervisor or-Servern.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-emergency-ha-disable

```
host-emergency-ha-disable  [--force]
```

Deaktivieren Sie HA auf dem lokalen Host. Nur zur Wiederherstellung eines Pools mit einem defekten HA-Setup verwendet werden.

host-emergency-management-reconfigure

```
host-emergency-management-reconfigure interface=
    uuid_of_management_interface_pif
```

Konfigurieren Sie die Verwaltungsschnittstelle dieses Citrix Hypervisor or-Servers neu. Verwenden Sie diesen Befehl nur, wenn sich der Citrix Hypervisor or-Server im Notfallmodus befindet. Der Notfallmodus bedeutet, dass der Host ein Mitglied in einem Ressourcenpool ist, dessen Master aus dem Netzwerk verschwunden ist und nach mehreren Wiederholungen nicht kontaktiert werden kann.

host-enable

```
host-enable [host-selector=host_selector_value...]
```


Aktiviert die angegebenen Citrix Hypervisor or-Server, wodurch neue VMs auf ihnen gestartet werden können.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-enable-display

```
host-enable-display uuid=host_uuid
```

Anzeige für den Host aktivieren.

host-enable-local-storage-caching

```
host-enable-local-storage-caching  sr-uuid=sr_uuid
```

Aktivieren Sie das lokale Speicher-Caching auf dem angegebenen Host.

host-evacuate

```
host-evacuate [host-selector=host_selector_value...]
```

Live migriert alle ausgeführten VMs auf andere geeignete Hosts in einem Pool. Zuerst lösen Sie den Host mithilfe deshost-disable Befehls auf.

Wenn der evakuierte Host der Poolmaster ist, muss ein anderer Host als Poolmaster ausgewählt werden. Verwenden Sie denpool-designate-**new**-master Befehl, um den Poolmaster mit deaktiviertem HA zu ändern. Weitere Informationen finden Sie unter pool-bezeichnen-neu-master.

Wenn HA aktiviert ist, besteht Ihre einzige Option darin, den Server herunterzufahren, wodurch HA zufällig einen neuen Master wählt. Weitere Informationen finden Sie unter Host-Shutdown.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-forget

```
host-forget uuid=host_uuid
```


Der XAPI-Agent vergisst den angegebenen Citrix Hypervisor or-Server, ohne ihn explizit zu kontaktieren.

Verwenden Sie den`--force` Parameter, um zu vermeiden, dass Sie aufgefordert werden, zu bestätigen, dass Sie diesen Vorgang wirklich ausführen möchten.

> **Warnhinweis:**
>
> Verwenden Sie diesen Befehl nicht, wenn HA im Pool aktiviert ist. Deaktivieren Sie zuerst HA und aktivieren Sie es dann erneut, nachdem Sie den Host vergessen haben.

Dieser Befehl ist nützlich, wenn der Citrix Hypervisor or-Server zum „Vergessen“ nicht mehr vorhanden ist. Wenn der Citrix Hypervisor or-Server jedoch live ist und Teil des Pools ist, verwenden Sie`xe pool-eject` stattdessen.

host-get-cpu-features

```
host-get-cpu-features {
 features=pool_master_cpu_features }
  [uuid=host_uuid]
```

Druckt eine hexadezimale Darstellung der physischen CPU-Funktionen des Hosts.

host-get-server-certificate

```
host-get-server-certificate
```

Holen Sie sich das installierte SSL-Zertifikat des Servers.

host-get-sm-diagnostics

```
host-get-sm-diagnostics uuid=uuid
```

Zeigt SM-Diagnoseinformationen pro Host an.

host-get-system-status

```
host-get-system-status filename=name_for_status_file [entries=
    comma_separated_list] [output=tar.bz2|zip] [host-selector=
    host_selector_value...]
```


Laden Sie Systemstatusinformationen in die angegebene Datei herunter. Der optionale Parameterentries ist eine durch Kommas getrennte Liste von Systemstatuseinträgen, die aus dem vomhost-get-system-status-capabilities Befehl zurückgegebenen Capabilities XML-Fragment entnommen werden. Weitere Informationen finden Sie unter Host-get-system-status-Funktionen. Wenn nicht angegeben, werden alle Systemstatusinformationen in der Datei gespeichert. Der Parameteroutput kann *tar.bz2* (Standardeinstellung) oder *zip* sein. Wenn dieser Parameter nicht angegeben ist, wird die Datei intar.bz2 Form gespeichert.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben).

host-get-system-status-capabilities

```
host-get-system-status-capabilities [host-selector=host_selector_value
    ...]
```

Abrufen der Systemstatusfunktionen für die angegebenen Hosts. 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>
```

Jede Capability-Entity kann die folgenden Attribute haben.

- key Ein eindeutiger Bezeichner für die Fähigkeit.
- content-type Kann entweder text/plain oder application/data sein. Gibt an, ob eine Benutzeroberfläche die Einträge für den menschlichen Verzehr rendern kann.
- **default**-checked Kann entweder Ja oder Nein sein. Gibt an, ob eine Benutzeroberfläche diesen Eintrag standardmäßig auswählen soll.
- min-size,max-sizeGibt einen ungefähren Bereich für die Größe dieses Eintrags in Byte an. -1 gibt an, dass die Größe unwichtig ist.

- `min-time`,`max-time`Geben Sie einen ungefähren Bereich für die Zeit in Sekunden an, die benötigt wird, um diesen Eintrag zu erfassen. -1 gibt an, dass die Zeit unwichtig ist.
- `pii` Persönlich identifizierbare Informationen. Gibt an, ob der Eintrag Informationen enthält, die den Systembesitzer identifizieren können, oder Details seiner Netzwerktopologie. Das Attribut kann einen der folgenden Werte haben:
  - `no`: keine PII ist in diesen Einträgen enthalten
  - `yes`: PII ist wahrscheinlich oder sicher in diesen Einträgen
  - `maybe`: Sie können diese Einträge für 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.

  Passwörter dürfen niemals in einen Fehlerbericht aufgenommen werden, unabhängig von der PII Deklaration.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben).

host-get-thread-diagnostics

```
1 host-get-thread-diagnostics uuid=uuid
```

Zeigt Diagnoseinformationen pro Host Thread an.

host-get-vms-which-prevent-evacuation

```
1 host-get-vms-which-prevent-evacuation uuid=uuid
```

Gibt eine Liste der VMs zurück, die die Evakuierung eines bestimmten Hosts verhindern und die Gründe für jeden anzeigen.

host-is-in-emergency-mode

```
1 host-is-in-emergency-mode
```

Gibt zurück**`true`** , wenn sich der Host, mit dem die CLI spricht, im Notfallmodus befindet,**`false`** andernfalls. Dieser CLI-Befehl funktioniert direkt auf Slave-Hosts, selbst wenn kein Master-Host vorhanden ist.

host-license-add

```
host-license-add [license-file=path/license_filename] [host-uuid=
    host_uuid]
```

Verwenden Sie für Citrix Hypervisor (kostenlose Edition), um eine lokale Lizenzdatei zu analysieren und sie dem angegebenen Citrix Hypervisor or-Server hinzuzufügen.

host-license-remove

```
host-license-remove [host-uuid=host_uuid]
```

Entfernen Sie alle Lizenzierungen, die auf einen Host angewendet werden.

host-license-view

```
host-license-view [host-uuid=host_uuid]
```

Zeigt den Inhalt der Citrix Hypervisor-Serverlizenz an.

host-logs-download

```
host-logs-download [file-name=logfile_name] [host-selector=
    host_selector_value...]
```

Laden Sie eine Kopie der Protokolle der angegebenen Citrix Hypervisor or-Server herunter. Die Kopie wird standardmäßig in einer Zeitstempeldatei mit dem Namen gespeichert`hostname-yyyy-mm-dd T hh:mm:ssZ.tar.gz`. Sie können einen anderen Dateinamen mit dem optionalen Parameter *filename*angeben.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

> **Wichtig:**
>
> Während der`xe host-logs-download` Befehl funktioniert, wenn er auf dem lokalen Host ausgeführt wird (dh ohne einen bestimmten Hostnamen angegeben), verwenden Sie ihn *nicht* auf diese Weise. Dadurch wird die Partition der Steuerdomäne mit der Kopie der Protokolle umk-

> lammert. Der Befehl sollte *nur* von einem externen Rechner aus verwendet werden, auf dem Sie Platz haben, um die Kopie der Protokolle zu speichern.

host-management-disable

```
host-management-disable
```

Deaktiviert den Host-Agent, der eine externe Verwaltungsnetzwerkschnittstelle überwacht, und trennt alle verbundenen API-Clients (z. B. XenCenter). Dieser Befehl funktioniert direkt auf dem Citrix Hypervisor or-Server, mit dem die CLI verbunden ist. Der Befehl wird nicht an den Poolmaster weitergeleitet, wenn er auf einen Citrix Hypervisor or-Server eines Mitglieds angewendet wird.

> **Warnhinweis:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden. Nachdem dieser Befehl ausgeführt wurde, können Sie keine Remoteverbindung mit der Steuerdomäne über das Netzwerk herstellen, um den Host-Agent erneut zu aktivieren.

host-management-reconfigure

```
host-management-reconfigure [interface=device] [pif-uuid=uuid]
```

Konfiguriert den Citrix Hypervisor or-Server so neu, dass die angegebene Netzwerkschnittstelle als Verwaltungsschnittstelle verwendet wird, d. h. die Schnittstelle, die für die Verbindung mit XenCenter verwendet wird. Der Befehl schreibt den MANAGEMENT_INTERFACE Schlüssel in um `/etc/xensource-inventory`.

Wenn der Gerätename einer Schnittstelle (die über eine IP-Adresse verfügen muss) angegeben wird, wird der Citrix Hypervisor or-Server sofort neu bindet. Dieser Befehl funktioniert sowohl im Normal- als auch im Notfallmodus.

Wenn die UUID eines PIF-Objekts angegeben wird, bestimmt der Citrix Hypervisor or-Server, welche IP-Adresse erneut an sich gebunden werden soll. Es darf sich nicht im Notbetrieb befinden, wenn dieser Befehl ausgeführt wird.

> **Warnhinweis:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden, und stellen Sie sicher, dass Sie über Netzwerkkonnektivität auf der neuen Schnittstelle verfügen. Verwenden Sie `xe pif-reconfigure`, um eine zuerst einzurichten. Andernfalls können nachfolgende CLI-Befehle den Citrix Hypervisor or-Server nicht erreichen.

host-power-on

```
host-power-on [host=host_uuid]
```

Schaltet Citrix Hypervisor or-Server mit aktivierter *Host-Einschaltfunktion* ein. Aktivieren Sie vor der Verwendung dieses Befehls `host-set-power-on` auf dem Host.

host-reboot

```
host-reboot [host-selector=host_selector_value...]
```

Starten Sie die angegebenen Citrix Hypervisor -Server neu. Die angegebenen 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 mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

Wenn die angegebenen Citrix Hypervisor or-Server Mitglieder eines Pools sind, wird der Verlust der Konnektivität beim Herunterfahren gehandhabt, und der Pool wird wiederhergestellt, wenn die Citrix Hypervisor or-Server zurückkehren. Die anderen Mitglieder und der Master funktionieren weiterhin.

Wenn Sie den Master herunterfahren, ist der Pool außer Betrieb, bis eine der folgenden Aktionen auftritt:

- Sie machen eines der Mitglieder in den Master
- Der ursprüngliche Master wird neu gestartet und wieder online.

  Wenn der Master wieder online ist, verbinden sich die Mitglieder erneut und synchronisieren sich mit dem Master.

host-restore

```
host-restore [file-name=backup_filename] [host-selector=
    host_selector_value...]
```

Stellen Sie eine Sicherung mit dem Namen`file-name` der Citrix Hypervisor-Serversteuerungssoftware wieder her. Die Verwendung des Wortes „restore“ bedeutet hier nicht eine vollständige Wiederherstellung im üblichen Sinne, sondern bedeutet lediglich, dass die komprimierte Sicherungsdatei unkomprimiert und auf die sekundäre Partition entpackt wurde. Nachdem Sie eine getan haben`xe host-restore`, müssen Sie die CD installieren booten und die Option Aus Sicherung wiederherstellen verwenden.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-send-debug-keys

```
host-send-debug-keys  host-uuid=host_uuid keys=keys
```

Senden Sie angegebene Hypervisor-Debug-Schlüssel an den angegebenen Host.

host-set-hostname-live

```
host-set-hostname host-uuid=uuid_of_host hostname=new_hostname
```

Ändern Sie den Hostnamen des von angegebenen Citrix Hypervisor or-Servershost-uuid. Mit diesem Befehl wird sowohl der Hostname in der Steuerdomänendatenbank als auch der tatsächliche Linux-Hostname des Citrix Hypervisor or-Servers dauerhaft festgelegt. Der Wert von *hostname* ist *nicht* identisch mit dem Wert des Felds *name_label* .

host-set-power-on-mode

```
host-set-power-on-mode host=host_uuid power-on-mode={
 "" | "wake-on-lan" | "iLO" | "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 ]
```

Aktivieren Sie diese Option, um die Funktion „ *Host Power On* “ auf Citrix Hypervisor Hosts zu aktivieren, die mit Remote-Stromversorgungslösungen kompatibel sind. Wenn Sie denhost-set-power-on Befehl verwenden, müssen Sie den Typ der Energieverwaltungslösung auf dem Host angeben (d. h. den Einschaltmodus). Geben Sie dann Konfigurationsoptionen mit dem Argument power-on-config und den zugehörigen Schlüssel-Wert-Paaren an.

Geben Sie den Schlüssel an, um die Secrets-Funktion zum Speichern Ihres Kennworts zu verwenden" power_on_password_secret". Weitere Informationen finden Sie unter Geheimnisse.

host-shutdown


```
host-shutdown [host-selector=host_selector_value...]
```

Fahren Sie die angegebenen Citrix Hypervisor -Server herunter. Die angegebenen Citrix Hypervisor or-Server 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 mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

Wenn die angegebenen Citrix Hypervisor or-Server Mitglieder eines Pools sind, wird der Verlust der Konnektivität beim Herunterfahren gehandhabt, und der Pool wird wiederhergestellt, wenn die Citrix Hypervisor or-Server zurückkehren. Die anderen Mitglieder und der Master funktionieren weiterhin.

Wenn Sie den Master herunterfahren, ist der Pool außer Betrieb, bis eine der folgenden Aktionen auftritt:

- Sie machen eines der Mitglieder in den Master
- Der ursprüngliche Master wird neu gestartet und wieder online.

  Wenn der Master wieder online ist, verbinden sich die Mitglieder erneut und synchronisieren sich mit dem Master.

Wenn HA für den Pool aktiviert ist, wird eines der Mitglieder automatisch in einen Master umgewandelt. Wenn HA deaktiviert ist, müssen Sie den gewünschten Server mit dem`pool-designate-new-master` Befehl manuell als Master festlegen. Weitere Informationen finden Sie unter pool-bezeichnen-neu-master.

host-sm-dp-destroy

```
host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
```

Versuchen Sie, einen Speicherdatenpfad auf einem Host zu zerstören und zu bereinigen. Wenn angegeben`allow-leak=true` wird, werden alle Datensätze des Datenpfads gelöscht, auch wenn er nicht sauber heruntergefahren werden konnte.

host-sync-data

```
host-sync-data
```

Synchronisieren Sie die auf dem Poolmaster gespeicherten Nicht-Datenbankdaten mit dem benannten Host.

host-syslog-reconfigure

```
host-syslog-reconfigure [host-selector=host_selector_value...]
```

Konfigurieren Sie densyslog Daemon auf den angegebenen Citrix Hypervisor or-Servern neu. Mit diesem Befehl werden die imlogging Host-Parameter definierten Konfigurationsinformationen angewendet.

Die Hosts, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt (siehe Host-Selektoren oben). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein.

host-data-source-list

```
host-data-source-list [host-selectors=host selector value...]
```

Listen Sie die Datenquellen auf, die für einen Host aufgezeichnet werden können.

Select mithilfe des Standardauswahlmechanismus die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen Hosts ausgeführt.

Datenquellen haben zwei Parameter —standard undenabled . Dieser Befehl gibt die Werte der Parameter aus:

- Wenn eine Datenquelle auf enabled festgelegt ist **true**, werden die Metriken derzeit in der Performance-Datenbank aufgezeichnet.
- Wenn eine Datenquelle aufstandard festgelegt ist**true** , werden die Metriken *standardmäßig* in der Performance-Datenbank aufgezeichnet. Der Wert von enabled wird auch **true** für diese Datenquelle auf festgelegt.
- Wenn eine Datenquelle aufstandard festgelegt ist**false** , werden die Metriken *nicht* standardmäßig in der Performance-Datenbank aufgezeichnet. Der Wert von enabled wird auch **false** für diese Datenquelle auf festgelegt.

Führen Sie den host-data-source-record Befehl aus, um Datenquellen-Metriken in der Performance-Datenbank aufzuzeichnen. Dieser Befehl wird enabled auf festgelegt **true**. Um zu stoppen, führen Sie den aus host-data-source-forget. Dieser Befehl wird enabled auf festgelegt **false**.

host-data-source-record


```
host-data-source-record data-source=name_description_of_data_source [
    host-selectors=host_selector_value...]
```

Zeichnen Sie die angegebene Datenquelle für einen Host auf.

Dieser Vorgang schreibt die Informationen aus der Datenquelle in die Datenbank für persistente Performance-Metriken der angegebenen Hosts. Aus Performance-Gründen unterscheidet sich diese Datenbank von der normalen Agent-Datenbank.

Select mithilfe des Standardauswahlmechanismus die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen Hosts ausgeführt.

`host-data-source-forget`

```
host-data-source-forget data-source=name_description_of_data_source [
    host-selectors=host_selector_value...]
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für einen Host und vergessen Sie alle aufgezeichneten Daten.

Select mithilfe des Standardauswahlmechanismus die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen Hosts ausgeführt.

`host-data-source-query`

```
host-data-source-query data-source=name_description_of_data_source [
    host-selectors=host_selector_value...]
```

Zeigt die angegebene Datenquelle für einen Host an.

Select mithilfe des Standardauswahlmechanismus die Hosts aus, auf denen dieser Vorgang ausgeführt werden soll (siehe Host-Selektoren). Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts Host-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen Hosts ausgeführt.

Protokollierungsbefehle

Befehle zum Arbeiten mit Protokollen.

log-get

```
log-get
```

Gibt das Protokoll zurück, das aktuell im String-Logger gespeichert ist.

log-get-keys

```
log-get-keys
```

Listen Sie die Schlüssel auf, die der Logger kennt.

log-reopen

```
log-reopen
```

Öffnen Sie alle Logger erneut (verwenden Sie dies für das Drehen von Dateien).

log-set-output

```
log-set-output output=output [key=key] [level=level]
```

Setzen Sie alle Logger auf die angegebene Ausgabe (nil, stderr, string, file:*filename*, syslog:*something*).

Nachrichtenbefehle

Befehle zum Arbeiten mit Nachrichten. Nachrichten werden erstellt, um Benutzer über wichtige Ereignisse zu benachrichtigen, und werden in XenCenter als Warnungen angezeigt.

Die Nachrichtenobjekte können mit dem Standardbefehl (`xe message-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

Meldungsparameter

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die Nachricht	Schreibgeschützt
name	Der eindeutige Name der Nachricht	Schreibgeschützt
priority	Die Nachrichtenpriorität. Höhere Zahlen weisen eine höhere Priorität auf	Schreibgeschützt
class	Die Nachrichtenklasse, z. B. VM.	Schreibgeschützt
obj-uuid	Die uuid des betroffenen Objekts.	Schreibgeschützt
timestamp	Die Uhrzeit, zu der die Nachricht generiert wurde.	Schreibgeschützt
body	Der Nachrichteninhalt.	Schreibgeschützt

message-create

```
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]]
```

Erstellt eine Nachricht.

message-destroy

```
message-destroy [uuid=message_uuid]
```

Zerstört eine vorhandene Nachricht. Sie können ein Skript erstellen, um alle Nachrichten zu zerstören. Zum Beispiel:

```
# Dismiss all alerts   \
    IFS=",”; for m in $(xe message-list params=uuid --minimal); do  \
    xe message-destroy uuid=$m  \
    done
```


Netzwerkbefehle

Befehle zum Arbeiten mit Netzwerken.

Die Netzwerkobjekte können mit dem Standardbefehl (`xe network-list`) aufgelistet und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

Netzwerkparameter

Netzwerke haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das Netzwerk	Schreibgeschützt
`name-label`	Der Name des Netzwerks	Lese-/Schreibzugriff
`name-description`	Der Beschreibungstext des Netzwerks	Lese-/Schreibzugriff
`VIF-uuids`	Eine Liste eindeutiger Bezeichner der VIFs (virtuelle Netzwerkschnittstellen), die von VMs an dieses Netzwerk angeschlossen sind	Schreibgeschützte Parameter
`PIF-uuids`	Eine Liste der eindeutigen Bezeichner der PIFs (physische Netzwerkschnittstellen), die von Citrix Hypervisor or-Servern an dieses Netzwerk angeschlossen sind	Schreibgeschützte Parameter
`bridge`	Name der diesem Netzwerk entsprechenden Bridge auf dem lokalen Citrix Hypervisor or-Server	Schreibgeschützt

Parametername	Beschreibung	Typ
default-locking-mode	Ein Netzwerkobjekt, das mit VIF-Objekten für die ARP-Filterung verwendet wird. Setzen Sie aufunlocked , um alle Filterregeln zu entfernen, die dem VIF zugeordnet sind. Stellen Sie diese Einstellungdisabled so ein, dass der VIF den gesamten Datenverkehr löscht.	Lese-/Schreibzugriff
purpose	Satz von Zwecken, für die der Citrix Hypervisor or-Server dieses Netzwerk verwendet. Legen Sie festnbd , dass das Netzwerk zum Herstellen von NBD-Verbindungen verwendet wird.	Lese-/Schreibzugriff
other-config: staticroutes	Kommagetrennte Liste von ***Subnetz/Netzmaske/Gateway-formatierten***Einträgen, die die Gateway-Adresse angeben, über die Subnetze weitergeleitet werden sollen. Wenn Sie z. B.other-config :**static**-routes auf 172.16.0.0/15/192.168.0.3,172.18. festlegen, wird der Datenverkehr auf 172.16.0.0/15 über 192.168.0.3 und der Datenverkehr auf 172.18.0.0/16 über 192.168.0.4 geleitet.	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
other-config: ethtoolautoneg	Setzen Sie auf „no“, um die automatische Verhandlung der physischen Schnittstelle oder Brücke zu deaktivieren. Der Standardwert ist ja.	Lese-/Schreibzugriff
other-config:ethtool-rx	Auf „Ein“ setzen, um die Empfangsprüfsumme zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-tx	Setzen Sie auf ein, um die Prüfsumme der Übertragung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-sg	Setzen Sie auf ein, um Scatter sammeln zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-tso	Setzen Sie auf ein, um die TCP-Segmentierung Offload zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-ufo	Setzen Sie auf ein, um die UDP-Fragmentabladung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-gso	Setzen Sie auf ein, um generische Segmentierungsabladung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
blobs	Binärer Datenspeicher	Schreibgeschützt

network-create

```
network-create name-label=name_for_network [name-description=
    descriptive_text]
```


Erstellt ein Netzwerk.

network-destroy

```
network-destroy uuid=network_uuid
```

Zerstört ein vorhandenes Netzwerk.

SR-IOV-Befehle

Befehle für die Arbeit mit SR-IOV.

Die network-sriov-Objekte können mit dem standardmäßigen Objektlistenbefehl (`xe network-sriov-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

SR-IOV-Parameter

SR-IOV hat die folgenden Parameter:

Parametername	Beschreibung	Typ
`physical-PIF`	Die PIF, um SR-IOV zu aktivieren.	Schreibgeschützt
`logical-PIF`	Ein SR-IOV-logisches PIF. Benutzer können diesen Parameter verwenden, um ein SR-IOV-VLAN-Netzwerk zu erstellen.	Schreibgeschützt
`requires-reboot`	Wenn auf True festgelegt, wird der Host neu gestartet, um die SR-IOV-Aktivierung in Kraft zu setzen.	Schreibgeschützt
`remaining-capacity`	Anzahl der verbleibenden verfügbaren VFs.	Schreibgeschützt

network-sriov-create


```
network-sriov-create network-uuid=network_uuid pif-uuid=
    physical_pif_uuid
```

Erstellt ein SR-IOV-Netzwerkobjekt für eine bestimmte physische PIF und aktiviert SR-IOV auf der physischen PIF.

`network-sriov-destroy`

```
network-sriov-destroy uuid=network_sriov_uuid
```

Entfernt ein Netzwerk SR-IOV-Objekt und deaktiviert SR-IOV auf seiner physischen PIF.

Zuweisen eines SR-IOV-VF

```
xe vif-create device=device_index mac=vf_mac_address network-uuid=
    sriov_network vm-uuid=vm_uuid
```

Weist einer VM ein VF aus einem SR-IOV-Netzwerk zu.

SDN-Controller Befehle

Befehle für die Arbeit mit dem SDN-Controller.

`sdn-controller-forget`

```
sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
    port=tcp_port]
```

Einführung eines SDN-Controllers.

`sdn-controller-introduce`

```
sdn-controller-forget uuid=uuid
```

Entfernen Sie einen SDN-Controller.

Tunnelbefehle

Befehle für die Arbeit mit Tunneln.

`tunnel-create`

```
tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
```

Erstellen Sie einen neuen Tunnel auf einem Host.

`tunnel-destroy`

```
tunnel-destroy uuid=uuid
```

Zerstöre einen Tunnel.

Patch-Befehle

Befehle zum Arbeiten mit Patches.

`patch-apply`

```
patch-apply uuid=patch_uuid host-uuid=host_uuid
```

Wenden Sie den zuvor hochgeladenen Patch auf den angegebenen Host an.

`patch-clean`

```
patch-clean uuid=uuid
```

Löschen Sie eine zuvor hochgeladene Patch-Datei.

`patch-destroy`

```
patch-destroy uuid=uuid
```

Entfernen Sie einen nicht angewendeten Patchdatensatz und Dateien vom Server.

patch-pool-apply

```
patch-pool-apply uuid=uuid
```

Wenden Sie den zuvor hochgeladenen Patch auf alle Hosts im Pool an.

patch-pool-clean

```
patch-pool-clean uuid=uuid
```

Löschen Sie eine zuvor hochgeladene Patch-Datei auf allen Hosts im Pool.

patch-precheck

```
patch-precheck uuid=uuid host-uuid=host_uuid
```

Führen Sie die Vorprüfungen aus, die im Patch enthalten sind, der zuvor auf den angegebenen Host hochgeladen wurde.

patch-upload

```
patch-upload file-name=file_name
```

Laden Sie eine Patchdatei auf den Server hoch.

PBD-Befehle

Befehle zum Arbeiten mit PBDs (Physical Block Devices). PBDs sind die Softwareobjekte, über die der Citrix Hypervisor or-Server auf Speicher-Repositories (SRs) zugreift.

Die PBD-Objekte können mit dem Standard-Objektlistenbefehl (`xe pbd-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

PBD-Parameter

PBDs haben folgende Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für die PBD.	Schreibgeschützt
sr-uuid	Das Speicher-Repository, auf das die PBD verweist	Schreibgeschützt
device-config	Zusätzliche Konfigurationsinformationen, die dem SR-Backend-Treiber eines Hosts zur Verfügung gestellt werden	Schreibgeschützte Kartenparameter
currently-attached	True, wenn der SR auf diesem Host angehängt ist, andernfalls False	Schreibgeschützt
host-uuid	UUID des physischen Computers, auf dem die PBD verfügbar ist	Schreibgeschützt
host	Das Hostfeld ist veraltet. Verwenden Sie stattdessen host_uuid.	Schreibgeschützt
other-config	Zusätzliche Konfigurationsinformationen.	Kartenparameter mit Lese-/Schreibzugriff

pbd-create

```
pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:key
    =corresponding_value]
```

Erstellen Sie eine PBD auf dem Citrix Hypervisor or-Server. Der schreibgeschützte`device-config` Parameter kann nur bei der Erstellung festgelegt werden.

Um eine Zuordnung von ‘path’ zu ‘/tmp’ hinzuzufügen, sollte die Befehlszeile das Argument`device-config:path=/tmp`

Eine vollständige Liste der unterstützten Geräte-Konfigurations-Schlüssel/Wert-Paare für jeden SR-Typ finden Sie unterSpeicher.

pbd-destroy

```
pbd-destroy uuid=uuid_of_pbd
```

Zerstören Sie die angegebene PBD.

pbd-plug

```
pbd-plug uuid=uuid_of_pbd
```

Versucht, die PBD mit dem Citrix Hypervisor or-Server zu verbinden. Wenn dieser Befehl erfolgreich ist, sollten die referenzierte SR (und die darin enthaltenen VDIs) für den Citrix Hypervisor or-Server sichtbar werden.

pbd-unplug

```
pbd-unplug uuid=uuid_of_pbd
```

Versuchen Sie, die PBD vom Citrix Hypervisor or-Server zu trennen.

PIF-Befehle

Befehle für die Arbeit mit PIF (Objekte, die die physischen Netzwerkschnittstellen darstellen).

Die PIF-Objekte können mit dem Standardbefehl (`xe pif-list`) aufgelistet und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

PIF-Parameter

PIF haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die PIF	Schreibgeschützt
`device machine-readable`	Name der Schnittstelle (z. B. eth0)	Schreibgeschützt

Parametername	Beschreibung	Typ
MAC	Die MAC-Adresse des PIF	Schreibgeschützt
other-config	Zusätzliche name:value PIF-Konfigurationspaare.	Kartenparameter mit Lese-/Schreibzugriff
physical	Wenn true, zeigt die PIF auf eine tatsächliche physische Netzwerkschnittstelle	Schreibgeschützt
currently-attached	Ist die PIF derzeit an diesem Host angeschlossen? **true** oder **false**	Schreibgeschützt
MTU	Maximale Übertragungseinheit des PIF in Byte.	Schreibgeschützt
VLAN	VLAN-Tag für den gesamten Datenverkehr, der diese Schnittstelle durchläuft. -1 gibt an, dass kein VLAN-Tag zugewiesen ist	Schreibgeschützt
bond-master-of	Die UUID der Bindung dieses PIF ist der Master (falls vorhanden)	Schreibgeschützt
bond-slave-of	Die UUID der Bindung dieses PIF ist der Slave von (falls vorhanden)	Schreibgeschützt
management	Ist diese PIF als Verwaltungsschnittstelle für die Steuerdomäne bestimmt	Schreibgeschützt
network-uuid	Die eindeutige Bezeichner/Objektreferenz des virtuellen Netzwerks, mit dem diese PIF verbunden ist	Schreibgeschützt
network-name-**label**	Der Name des virtuellen Netzwerks, mit dem diese PIF verbunden ist	Schreibgeschützt

Parametername	Beschreibung	Typ
host-uuid	Der eindeutige Bezeichner/Objektreferenz des Citrix Hypervisor or-Servers, mit dem diese PIF verbunden ist	Schreibgeschützt
host-name-**label**	Der Name des Citrix Hypervisor or-Servers, mit dem diese PIF verbunden ist	Schreibgeschützt
IP-configuration-mode	Typ der verwendeten Netzw-erkadressenkonfiguration; DHCP oder statisch	Schreibgeschützt
IP	IP-Adresse des PIF. Hier definiert, wenn der IP-Konfigurations-Modus statisch ist; nicht definiert, wenn DHCP	Schreibgeschützt
netmask	Netzmaske des PIF. Hier definiert, wenn der IP-Konfigurations-Modus statisch ist; nicht definiert, wenn er von DHCP bereitgestellt wird	Schreibgeschützt
gateway	Gateway-Adresse des PIF. Hier definiert, wenn der IP-Konfigurations-Modus statisch ist; nicht definiert, wenn er von DHCP bereitgestellt wird	Schreibgeschützt
DNS	DNS-Adresse des PIF. Hier definiert, wenn der IP-Konfigurations-Modus statisch ist; nicht definiert, wenn er von DHCP bereitgestellt wird	Schreibgeschützt

Parametername	Beschreibung	Typ
io_read_kbs	Durchschnittliche Lesegeschote in KB/s für das Gerät	Schreibgeschützt
io_write_kbs	Durchschnittliche Schreibrate in KB/s für das Gerät	Schreibgeschützt
carrier	Verbindungsstatus für dieses Gerät	Schreibgeschützt
vendor-id	Die dem NIC-Hersteller zugewiesene ID	Schreibgeschützt
vendor-name	Name des NIC-Anbieters	Schreibgeschützt
device-id	Die vom Hersteller diesem NIC-Modell zugewiesene ID	Schreibgeschützt
device-name	Der vom Hersteller diesem NIC-Modell zugewiesene Name	Schreibgeschützt
speed	Datenübertragungsrate der NIC	Schreibgeschützt
duplex	Duplexmodus der NIC; voll oder halb	Schreibgeschützt
pci-bus-path	PCI-Buspfadadresse	Schreibgeschützt
other-config: ethtoolspeed	Legt die Geschwindigkeit der Verbindung in Mbit/s fest	Lese-/Schreibzugriff
other-config: ethtoolautoneg	Setzen Sie auf „no“, um die automatische Verhandlung der physischen Schnittstelle oder Brücke zu deaktivieren. Der Standardwert ist ja.	Lese-/Schreibzugriff
other-config: ethtoolduplex	Legt die Duplexfunktion des PIF fest, entweder voll oder halb.	Lese-/Schreibzugriff
other-config:ethtool-rx	Auf „Ein“ setzen, um die Empfangsprüfsumme zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
other-config:ethtool-tx	Setzen Sie auf ein, um die Prüfsumme der Übertragung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-sg	Setzen Sie auf ein, um Scatter sammeln zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-tso	Setzen Sie auf ein, um die TCP-Segmentierung Offload zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-ufo	Setzen Sie auf ein, um die udp-Fragmentabladung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:ethtool-gso	Setzen Sie auf ein, um generische Segmentierungsabladung zu aktivieren, aus, um zu deaktivieren	Lese-/Schreibzugriff
other-config:domain	Kommagetrennte Liste zum Festlegen des DNS-Suchpfads	Lese-/Schreibzugriff
other-config:bondmiimon	Intervall zwischen den Prüfungen der Verknüpfungsfähigkeit in Millisekunden	Lese-/Schreibzugriff
other-config:bonddowndelay	Anzahl der Millisekunden, die nach dem Verlust des Links gewartet werden müssen, bevor der Link wirklich verschwunden ist. Dieser Parameter ermöglicht einen vorübergehenden Verbindungsverlust	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
`other-config: bondupdelay`	Anzahl der Millisekunden, die gewartet werden müssen, nachdem der Link auftaucht, bevor er wirklich in Erwägung zieht. Ermöglicht das Flattern von Links. Der Standardwert ist`31s` , dass die Switches Zeit für die Weiterleitung des Datenverkehrs zulassen.	Lese-/Schreibzugriff
`disallow-unplug`	True, wenn diese PIF eine dedizierte Speicher-NIC ist, andernfalls false	Lese-/Schreibzugriff

> **Hinweis:**
>
> Änderungen an den`other-config` Feldern eines PIF werden erst nach einem Neustart wirksam. Alternativ können Sie die`xe pif-unplug` Befehle`xe pif-plug` und verwenden, um die PIF-Konfiguration neu zu schreiben.

pif-forget

```
pif-forget uuid=uuid_of_pif
```

Zerstören Sie das angegebene PIF-Objekt auf einem bestimmten Host.

pif-introduce

```
pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=
    interface_name
```

Erstellen Sie ein PIF-Objekt, das eine physische Schnittstelle auf dem angegebenen Citrix Hypervisor or-Server darstellt.

pif-plug

```
pif-plug uuid=uuid_of_pif
```


Versuchen Sie, die angegebene physikalische Schnittstelle aufzurufen.

pif-reconfigure-ip

```
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]
```

Ändern Sie die IP-Adresse des PIF. Setzen Sie für die statische IP-Konfiguration denmode `Parameter aufstatic` , mit demgatewayIP““ , undnetmask“ Parameter, die auf die entsprechenden Werte festgelegt sind. Um DHCP zu verwenden, setzen Sie den`mode` Parameter auf`DHCP` und lassen Sie die statischen Parameter nicht definiert.

> **Hinweis:**
>
> Die Verwendung statischer IP-Adressen auf physischen Netzwerkschnittstellen, die mit einem Port eines Switches verbunden sind, das Spanning Tree Protocol verwendet und STP Fast Link deaktiviert (oder nicht unterstützt), führt zu einem Zeitraum, in dem kein Datenverkehr stattfindet.

pif-reconfigure-ipv6

```
pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode [gateway=
    network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=
    dns_address]
```

Konfigurieren Sie die IPv6-Adresseinstellungen auf einem PIF neu.

pif-scan

```
pif-scan host-uuid=host_uuid
```

Suchen Sie nach neuen physischen Schnittstellen auf dem Citrix Hypervisor or-Server.

pif-set-primary-address-type

```
pif-set-primary-address-type  uuid=uuid primary_address_type=
    address_type
```

Ändern Sie den primären Adresstyp, der von dieser PIF verwendet wird.

pif-unplug

```
pif-unplug uuid=uuid_of_pif
```

Versuchen Sie, die angegebene physikalische Schnittstelle herunterzufahren.

Poolbefehle

Befehle zum Arbeiten mit Pools. Ein *Pool* ist ein Aggregat aus einem oder mehreren Citrix Hypervisor or-Servern. Ein Pool verwendet ein oder mehrere freigegebene Speicher-Repositories, sodass die VMs, die auf einem Host im Pool ausgeführt werden, in nahezu Echtzeit auf einen anderen Host im Pool migriert werden können. Diese Migration erfolgt, während die VM noch ausgeführt wird, ohne dass sie heruntergefahren und wieder hochgefahren werden muss. Jeder Citrix Hypervisor or-Server ist wirklich ein Pool, der standardmäßig aus einem einzelnen Mitglied besteht. Wenn Ihr Citrix Hypervisor or-Server mit einem Pool verbunden ist, wird er als Mitglied festgelegt, und der Pool, dem er beigetreten ist, wird zum Master für den Pool.

Das Singleton-Pool-Objekt kann mit dem Standard-Objekt-Auflistungsbefehl (`xe pool-list`) aufgelistet werden. Seine Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

Pool-Parameter

Pools haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den Pool	Schreibgeschützt
`name-label`	Der Name des Pools	Lese-/Schreibzugriff
`name-description`	Die Beschreibungszeichenfolge des Pools	Lese-/Schreibzugriff
`master`	Der eindeutige Bezeichner/Objektreferenz des Citrix Hypervisor or-Servers, der als Master des Pools festgelegt ist	Schreibgeschützt

Parametername	Beschreibung	Typ
default-SR	Die eindeutige Bezeichner/Objektreferenz der Standard-SR für den Pool	Lese-/Schreibzugriff
crash-dump-SR	Die eindeutige Bezeichner/Objektreferenz der SR, in der alle Absturzabbilder für Pool-Mitglieder gespeichert werden	Lese-/Schreibzugriff
metadata-vdis	Alle bekannten Metadaten-VDIs für den Pool	Schreibgeschützt
suspend-image-SR	Die eindeutige Bezeichner/Objektreferenz der SR, in der suspendierte VMs auf Pool-Mitgliedern gespeichert werden	Lese-/Schreibzugriff
other-config	Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für den Pool angeben	Kartenparameter mit Lese-/Schreibzugriff
supported-sr-types	SR-Typen, die dieser Pool verwenden kann	Schreibgeschützt
ha-enabled	True, wenn HA für den Pool aktiviert ist, andernfalls false	Schreibgeschützt
ha-configuration	Reserviert für die zukünftige Nutzung.	Schreibgeschützt
ha-statefiles	Listet die UUIDs der VDIs auf, die von HA zur Ermittlung des Speicherzustands verwendet werden	Schreibgeschützt
ha-host-failures-to-tolerate	Die Anzahl der Hostfehler, die vor dem Senden einer Systemwarnung toleriert werden müssen	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
ha-plan-exists-for	Die Anzahl der Host-Ausfälle, die tatsächlich behandelt werden können, entsprechend den Berechnungen des HA-Algorithmus	Schreibgeschützt
ha-allow-overcommit	True, wenn der Pool überschrieben werden darf, andernfalls False	Lese-/Schreibzugriff
ha-overcommitted	True, wenn der Pool überschrieben ist	Schreibgeschützt
blobs	Binärer Datenspeicher	Schreibgeschützt
live-patching-disabled	Setzen Sie auf False, um Live-Patching zu aktivieren. Setzen Sie auf True, um Live-Patching zu deaktivieren.	Lese-/Schreibzugriff
igmp-snooping-enabled	Setzen Sie auf True, um IGMP-Snooping zu aktivieren. Setzen Sie auf False, um IGMP-Snooping zu deaktivieren.	Lese-/Schreibzugriff

pool-apply-edition

```
pool-apply-edition edition=edition [uuid=uuid] [license-server-address=
    address] [license-server-port=port]
```

Wenden Sie eine Edition über den Pool.

pool-certificate-install

```
pool-certificate-install filename=file_name
```

Installieren Sie ein SSL-Zertifikat, pool-weit.

pool-certificate-list

```
pool-certificate-list
```

Liste aller installierten SSL-Zertifikate.

pool-certificate-sync

```
pool-certificate-sync
```

Synchronisieren Sie SSL-Zertifikate und Zertifikatsperrlisten von Master zu Slaves.

pool-certificate-uninstall

```
pool-certificate-uninstall name=name
```

Deinstallieren Sie ein SSL-Zertifikat.

pool-crl-install

```
pool-crl-install filename=file_name
```

Installieren Sie eine SSL-Zertifikatssperrliste, pool-weit.

pool-crl-list

```
pool-crl-list
```

Listen Sie alle installierten SSL-Zertifikatsperrlisten auf.

pool-crl-uninstall

```
pool-crl-uninstall name=name
```

Deinstallieren Sie eine SSL-Zertifikatssperrliste.

pool-deconfigure-wlb

```
pool-deconfigure-wlb
```

Entfernen Sie die Konfiguration für den Arbeitslastausgleich dauerhaft.

pool-designate-new-master

```
pool-designate-new-master host-uuid=uuid_of_new_master
```

Weisen Sie den angegebenen Citrix Hypervisor or-Server an, der Master eines vorhandenen Pools zu werden. Dieser Befehl führt eine geordnete Übergabe der Rolle des Master-Hosts an einen anderen Host im Ressourcenpool durch. Dieser Befehl funktioniert nur, wenn der aktuelle Master online ist. Es ist kein Ersatz für die unten aufgeführten Notmodusbefehle.

pool-disable-external-auth

```
pool-disable-external-auth [uuid=uuid] [config=config]
```

Deaktiviert die externe Authentifizierung in allen Hosts in einem Pool.

pool-disable-local-storage-caching

```
pool-disable-local-storage-caching uuid=uuid
```

Deaktivieren Sie das lokale Speicher-Caching im gesamten Pool.

pool-disable-redo-log

```
pool-disable-redo-log
```

Deaktivieren Sie das Redo Log, wenn es verwendet wird, es sei denn, HA ist aktiviert.

pool-disable-ssl-legacy

```
pool-disable-ssl-legacy [uuid=uuid]
```

Setzen Sie ssl-legacy auf jedem Host auf False.

pool-dump-database

```
pool-dump-database file-name=filename_to_dump_database_into_(on_client)
```

Laden Sie eine Kopie der gesamten Pooldatenbank herunter und speichern Sie sie in eine Datei auf dem Client.

pool-enable-external-auth

```
pool-enable-external-auth  auth-type=auth_type service-name=
    service_name [uuid=uuid] [config:=config]
```

Aktiviert die externe Authentifizierung in allen Hosts in einem Pool. Beachten Sie, dass einige Werte des auth-Typs bestimmte config: -Werte erfordern.

pool-enable-local-storage-caching

```
pool-enable-local-storage-caching uuid=uuid
```

Aktivieren Sie das lokale Speicher-Caching im gesamten Pool.

pool-enable-redo-log

```
pool-ensable-redo-log sr-uuid=sr_uuid
```

Aktivieren Sie das Redo Log für die angegebene SR, wenn sie verwendet wird, es sei denn, HA ist aktiviert.

pool-enable-ssl-legacy

```
pool-enable-ssl-legacy [uuid=uuid]
```

Setzen Sie ssl-legacy auf jedem Host auf True. „

pool-eject

```
pool-eject host-uuid=uuid_of_host_to_eject
```

Weisen Sie den angegebenen Citrix Hypervisor or-Server an, einen vorhandenen Pool zu verlassen.

pool-emergency-reset-master

```
pool-emergency-reset-master master-address=address_of_pool_master
```

Weisen Sie einen Citrix Hypervisor or-Server an, seine Master-Adresse auf den neuen Wert zurückzusetzen und eine Verbindung zu ihm herzustellen. Führen Sie diesen Befehl nicht auf Master-Hosts aus.

pool-emergency-transition-to-master

```
pool-emergency-transition-to-master
```

Weisen Sie einen Citrix Hypervisor or-Server an, der Poolmaster zu werden. Der Citrix Hypervisor or-Server akzeptiert diesen Befehl erst, nachdem der Host in den Notfallmodus übergegangen ist. Der Notfallmodus bedeutet, dass er Mitglied eines Pools ist, dessen Master aus dem Netzwerk verschwunden ist und nach einiger Anzahl von Wiederholungen nicht kontaktiert werden kann.

Wenn das Hostkennwort 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

```
pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
```

Aktivieren Sie Hochverfügbarkeit im Ressourcenpool, wobei die angegebene SR-UUID als zentrales Speicher-Heartbeat-Repository verwendet wird.

pool-ha-disable

```
pool-ha-disable
```

Deaktiviert die Hochverfügbarkeitsfunktion im Ressourcenpool.

pool-ha-compute-hypothetical-max-host-failures-to-tolerate

Berechnen Sie die maximale Anzahl von Hostfehlern, die unter der aktuellen Poolkonfiguration toleriert werden sollen.

pool-ha-compute-max-host-failures-to-tolerate

```
pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=
    vm_uuid] [restart-priority=restart_priority]
```

Berechnen Sie die maximale Anzahl von Hostfehlern, die mit den bereitgestellten, vorgeschlagenen geschützten VMs toleriert werden sollen.

pool-initialize-wlb

```
pool-initialize-wlb wlb_url=url wlb_username=wlb_username wlb_password=
    wlb_password xenserver_username=username xenserver_password=password
```

Initialisieren Sie den Arbeitslastausgleich für den aktuellen Pool mit dem Ziel-WLB-Server.

pool-join

```
pool-join master-address=address master-username=username master-
    password=password
```

Weisen Sie Ihren Citrix Hypervisor or-Server an, einem vorhandenen Pool beizutreten.

pool-management-reconfigure

```
pool-management-reconfigure [network-uuid=network-uuid]
```

Konfiguriert die Verwaltungsschnittstelle aller Hosts im Pool neu, um die angegebene Netzwerkschnittstelle zu verwenden, d. h. die Schnittstelle, die für die Verbindung mit XenCenter verwendet wird. Der Befehl schreibt den Schlüssel MANAGEMENT_INTERFACE/`etc/xensource-inventory` für alle Hosts im Pool um.

Wenn der Gerätename einer Schnittstelle (die über eine IP-Adresse verfügen muss) angegeben wird, wird der Citrix Hypervisor Masterhost sofort neu bindet. Dieser Befehl funktioniert sowohl im Normal- als auch im Notfallmodus.

Von der angegebenen Netzwerk-UUID wird die UUID des PIF-Objekts identifiziert und dem Citrix Hypervisor or-Server zugeordnet, der bestimmt, welche IP-Adresse an sich selbst gebunden werden soll. Es darf sich nicht im Notbetrieb befinden, wenn dieser Befehl ausgeführt wird.

> **Warnhinweis:**
>
> Seien Sie vorsichtig, wenn Sie diesen CLI-Befehl außerhalb des Hosts verwenden, und stellen Sie sicher, dass Sie über Netzwerkkonnektivität auf der neuen Schnittstelle verfügen. Verwenden Sie `xe pif-reconfigure`, um eine zuerst einzurichten. Andernfalls können nachfolgende CLI-Befehle den Citrix Hypervisor or-Server nicht erreichen.

pool-recover-slaves

```
pool-recover-slaves
```

Weisen Sie den Poolmaster an, die Master-Adresse aller Mitglieder zurückzusetzen, die derzeit im Notfallmodus ausgeführt werden. Dieser Befehl wird in der Regel verwendet, nachdem verwendet`pool-emergency-transition-to-master` wurde, um eines der Elemente als neuen Master festzulegen.

pool-restore-database

```
pool-restore-database file-name=filename_to_restore_from_on_client [dry
    -run=true|false]
```

Laden Sie eine Datenbanksicherung (erstellt mit`pool-dump-database`) in einen Pool hoch. Beim Empfang des Uploads startet der Master selbst mit der neuen Datenbank neu.

Es gibt auch eine *Trockenlaufoption* , mit der Sie überprüfen können, ob die Pooldatenbank wiederhergestellt werden kann, ohne den Vorgang tatsächlich auszuführen. Standardmäßig`dry-run` ist auf false gesetzt.

pool-retrieve-wlb-configuration

```
pool-retrieve-wlb-configuration
```

Ruft die Pool-Optimierungskriterien vom Workload-Balancing-Server ab.

pool-retrieve-wlb-diagnostics

```
pool-retrieve-wlb-diagnostics [filename=file_name]
```

Ruft die Diagnose vom Workload-Balancing-Server ab.

pool-retrieve-wlb-recommendations

```
pool-retrieve-wlb-recommendations
```

Ruft VM-Migrationsempfehlungen für den Pool vom Workload-Balancing-Server ab.

pool-retrieve-wlb-report

```
pool-retrieve-wlb-report report=report [filename=file_name]
```

Ruft Berichte vom Workload-Balancing-Server ab.

pool-send-test-post

```
pool-send-test-post dest-host=destination_host dest-port=
    destination_port body=post_body
```

Senden Sie den gegebenen Körper mit HTTPS an den angegebenen Host und Port und drucken Sie die Antwort. Dies wird zum Debuggen der SSL-Schicht verwendet.

pool-send-wlb-configuration

```
pool-send-wlb-configuration [config:=config]
```

Legt die Pool-Optimierungskriterien für den Workload-Balancing-Server fest.

pool-sync-database

```
pool-sync-database
```

Erzwingen Sie, dass die Pooldatenbank über alle Hosts im Ressourcenpool synchronisiert wird. Dieser Befehl ist im normalen Betrieb nicht erforderlich, da die Datenbank regelmäßig automatisch repliziert wird. Wie auch immer, kann der Befehl nützlich sein, um sicherzustellen, dass Änderungen schnell repliziert werden, nachdem ein erheblicher Satz von CLI-Operationen durchgeführt wurde.

Pooligmp-snooping

```
pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|false]
```

Aktiviert oder deaktiviert IGMP-Snooping in einem Citrix Hypervisor Pool.

PVS Accelerator-Befehle

Befehle für die Arbeit mit dem PVS Accelerator.

pvs-cache-storage-create

```
pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid
    size=size
```

Konfigurieren Sie einen PVS-Cache auf einer bestimmten SR für einen bestimmten Host.

pvs-cache-storage-destroy

```
pvs-cache-storage-destroy uuid=uuid
```

Entfernen Sie einen PVS-Cache.

pvs-proxy-create

```
pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
```

Konfigurieren Sie einen VM/VIF für die Verwendung eines PVS-Proxy.

pvs-proxy-destroy

```
pvs-proxy-destroy uuid=uuid
```

Entfernen (oder ausschalten) eines PVS-Proxy für diese VIF/VM.

pvs-server-forget

```
pvs-server-forget uuid=uuid
```

Vergessen Sie einen PVS-Server.

pvs-server-introduce

```
pvs-server-introduce addresses=adresses first-port=first_port last-port
    =last_port pvs-site-uuid=pvs_site_uuid
```

Einführung eines neuen PVS-Servers.

pvs-site-forget

```
pvs-site-forget uuid=uuid
```

Vergessen Sie eine PVS-Website.

pvs-site-introduce

```
pvs-site-introduce name-label=name_label [name-description=
    name_description] [pvs-uuid=pvs_uuid]
```

Einführung neuer PVS-Website.

Storage Manager-Befehle

Befehle zum Steuern von Storage Manager-Plugins.

Die Speichermanager-Objekte können mit dem Befehl zur Standardobjektauflistung (`xe sm-list`) aufgelistet werden. Die Parameter können mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

SM-Parameter

SMs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
uuid	Die eindeutige Bezeichner/Objektreferenz für das SM-Plugin	Schreibgeschützt
name-**label**	Der Name des SM-Plugins	Schreibgeschützt
name-description	Die Beschreibungszeichenfolge des SM-Plugins	Schreibgeschützt
type	Der SR-Typ, mit dem dieses Plugin eine Verbindung herstellt	Schreibgeschützt
vendor	Name des Anbieters, der dieses Plugin erstellt hat	Schreibgeschützt
copyright	Copyright-Erklärung für dieses SM-Plugin	Schreibgeschützt
required-api-version	Minimale SM-API-Version auf dem Citrix Hypervisor or-Server erforderlich	Schreibgeschützt
configuration	Namen und Beschreibungen der Gerätekonfigurationss-chlüssel	Schreibgeschützt
capabilities	Funktionen des SM-Plugins	Schreibgeschützt
driver-filename	Der Dateiname des SR-Treibers.	Schreibgeschützt

Snapshot-Befehle

Befehle zum Arbeiten mit Snapshots.

`snapshot-clone`

```
1 snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-
    description=description]
```

Erstellen Sie eine neue Vorlage, indem Sie einen vorhandenen Snapshot klonen und einen schnellen Festplattenklonvorgang auf Speicherebene verwenden, sofern verfügbar.

snapshot-copy

```
snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-
    description=name_description] [sr-uuid=sr_uuid]
```

Erstellen Sie eine neue Vorlage, indem Sie eine vorhandene VM kopieren, ohne den schnellen Festplattenklonvorgang auf Speicherebene zu verwenden (auch wenn diese verfügbar ist). Die Disk-Images der kopierten VM sind garantiert „vollständige Bilder“ - d.h. nicht Teil einer KuW-Kette.

snapshot-destroy

```
snapshot-destroy  [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

Einen Schnappschuss zerstören. Dadurch bleibt der mit dem Snapshot verknüpfte Speicher intakt. Um auch Speicher zu löschen, verwenden Sie snapshot-uninstall.

snapshot-disk-list

```
snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-
    params=vbd_params] [vdi-params=vdi_params]
```

Listen Sie die Datenträger auf den ausgewählten virtuellen Rechnern auf.

snapshot-export-to-template

```
snapshot-export-to-template filename=file_name snapshot-uuid=
    snapshot_uuid  [preserve-power-state=true|false]
```

Exportieren Sie einen Snapshot *in Dateiname*.

snapshot-reset-powerstate

```
snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--
    force]
```

Erzwingen Sie, dass der VM-Powerstate nur in der Management-Toolstack-Datenbank angehalten wird. Dieser Befehl wird verwendet, um einen Snapshot wiederherzustellen, der als „suspendiert“ markiert ist. Dies ist eine potenziell gefährliche Operation: Sie müssen sicherstellen, dass Sie das Speicherbild nicht mehr benötigen (dh Sie können Ihren Snapshot nicht mehr fortsetzen).

snapshot-revert

```
snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

Stellen Sie eine vorhandene VM in einen vorherigen Status mit Checkpoint- oder Snapshott-Status zurück.

snapshot-uninstall

```
snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

Deinstallieren Sie einen Snapshot. Dieser Vorgang zerstört die VDIs, die als RW markiert sind und nur mit diesem Snapshot verbunden sind. Um den VM-Eintrag einfach zu zerstören, verwenden Sie snapshot-destroy.

SR-Befehle

Befehle zur Steuerung von SRs (Storage Repositories).

Die SR-Objekte können mit dem Befehl zur Standardobjektauflistung (`xe sr-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

SR-Parameter

SRs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die SR	Schreibgeschützt
`name-label`	Der Name der SR	Lese-/Schreibzugriff
`name-description`	Die Beschreibungszeichenfolge der SR	Lese-/Schreibzugriff
`allowed-operations`	Liste der zulässigen Vorgänge auf der SR in diesem Zustand	Schreibgeschützte Parameter

Parametername	Beschreibung	Typ
current-operations	Liste der Vorgänge, die derzeit auf dieser SR ausgeführt werden	Schreibgeschützte Parameter
VDIs	Eindeutige Bezeichner/Objektreferenz für die virtuellen Laufwerke in dieser SR	Schreibgeschützte Parameter
PBDs	Eindeutige Bezeichner/Objektreferenz für die an diese SR angeschlossenen PBDs	Schreibgeschützte Parameter
physical-utilisation	Physischer Speicherplatz, der derzeit auf dieser SR in Bytes belegt wird. Für Thin Provisioned Datenträgerformate kann die physische Auslastung geringer sein als die virtuelle Zuweisung	Schreibgeschützt
physical-size	Physische Gesamtgröße des SR in Byte	Schreibgeschützt
type	Typ des SR, der verwendet wird, um den SR-Back-End-Treiber anzugeben, der verwendet werden soll	Schreibgeschützt
introduced-by	Die drtask (falls vorhanden), die die SR eingeführt hat	Schreibgeschützt

Parametername	Beschreibung	Typ
content-type	Der Typ des SR-Inhalts. Wird verwendet, um ISO-Bibliotheken von anderen SRs zu unterscheiden. Für Speicher-Repositories, die eine Bibliothek von ISOs speichern, muss der Inhaltstyp auf iso gesetzt werden. In anderen Fällen empfiehlt es sich, diesen Parameter entweder auf leer oder auf den Zeichenfolgenbenutzer zu setzen.	Schreibgeschützt
shared	True, wenn diese SR von mehreren Citrix Hypervisor or-Servern gemeinsam genutzt werden kann; andernfalls False	Lese-/Schreibzugriff
other-config	Liste der Schlüssel/Wert-Paare, die zusätzliche Konfigurationsparameter für die SR angeben	Kartenparameter mit Lese-/Schreibzugriff
host	Der Hostname des Speicher-Repositorys	Schreibgeschützt
virtual-allocation	Summe der Werte virtueller Größe aller VDIs in diesem Speicher-Repository (in Byte)	Schreibgeschützt
sm-config	SM-abhängige Daten	Schreibgeschützte Kartenparameter
blobs	Binärer Datenspeicher	Schreibgeschützt

sr-create

```
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]
```

Erstellt einen SR auf dem Datenträger, führt ihn in die Datenbank ein und erstellt eine PBD, die den SR an den Citrix Hypervisor or-Server anfügt. Wenn auf festgelegt`shared` ist**`true`** , wird für jeden Citrix Hypervisor or-Server im Pool eine PBD erstellt. Wenn nicht angegeben oder auf festgelegt`shared` ist**`false`** , wird eine PBD nur für den mit angegebenen Citrix Hypervisor or-Server erstellt`host-uuid` .

Die genauen `device-config` Parameter unterscheiden sich je nach Gerät `type`. Einzelheiten zu diesen Parametern für die verschiedenen Speicher-Back-Ends finden Sie unter Speicher.

sr-data-source-forget

```
sr-data-source-forget data-source=data_source
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für einen SR, und vergessen Sie alle aufgezeichneten Daten.

sr-data-source-list

```
sr-data-source-list”
```

Listen Sie die Datenquellen auf, die für eine SR aufgezeichnet werden können.

sr-data-source-query

```
sr-data-source-query data-source=data_source
```

Fragen Sie den zuletzt gelesenen Wert aus einer SR-Datenquelle ab.

sr-data-source-record

```
sr-data-source-record  data-source=data_source
```

Zeichnen Sie die angegebene Datenquelle für einen SR auf.

sr-destroy

```
sr-destroy uuid=sr_uuid
```

Zerstört die angegebene SR auf dem Citrix Hypervisor or-Server.

sr-enable-database-replication

```
sr-enable-database-replication uuid=sr_uuid
```

Aktiviert die XAPI-Datenbankreplikation auf die angegebene (gemeinsam genutzte) SR.

sr-disable-database-replication

```
sr-disable-database-replication uuid=sr_uuid
```

Deaktiviert die XAPI-Datenbankreplikation auf die angegebene SR.

sr-forget

```
sr-forget uuid=sr_uuid
```

Der XAPI-Agent vergisst eine bestimmte SR auf dem Citrix Hypervisor or-Server. Wenn der XAPI-Agent einen SR vergisst, wird der SR getrennt, und Sie können nicht auf VDIs zugreifen, aber er bleibt auf dem Quellmedium intakt (die Daten gehen nicht verloren).

sr-introduce

```
sr-introduce name-label=name physical-size=physical_size type=type
    content-type=content_type uuid=sr_uuid
```

Platziert einfach einen SR-Datensatz in die Datenbank. `device-config` Hiermit können Sie zusätzliche Parameter in Form angeben`device-config:parameter_key=parameter_value` , z. B.:

```
xe sr-introduce device-config:device=/dev/sdb1
```

> **Hinweis:**
>
> Dieser Befehl wird nie im normalen Betrieb verwendet. Dieser erweiterte Vorgang kann nützlich sein, wenn ein SR nach der Erstellung als freigegeben neu konfiguriert werden muss oder um die

> Wiederherstellung von verschiedenen Ausfallszenarien zu erleichtern.

sr-probe

```
sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=
    value]
```

Führt einen Backend-spezifischen Scan mit den bereitgestelltendevice-config Schlüsseln durch. Wenn der für das SR-Back-End abgeschlossendevice-config ist, gibt dieser Befehl eine Liste der SRs zurück, die auf dem Gerät vorhanden sind. Wenn diedevice-config Parameter nur teilweise sind, wird ein Back-End-spezifischer Scan durchgeführt, der Ergebnisse zurückgibt, die Sie bei der Verbesserung der verbleibendendevice-config Parameter leiten. Die Scan-Ergebnisse werden als Backend-spezifisches XML zurückgegeben, das auf der CLI gedruckt wird.

Die genauen device-config Parameter unterscheiden sich je nach Gerät type. Einzelheiten zu diesen Parametern für die verschiedenen Speicher-Back-Ends finden Sie unter Speicher.

sr-probe-ext

```
sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config] [
    sm-config:-sm_config]
```

Führen Sie eine Speichersonde durch. Die Device-Config-Parameter können z.B. durch device-config:devs=/dev/sdb1 angegeben werden. Im Gegensatz zu sr-probe gibt dieser Befehl Ergebnisse für jeden SR-Typ in demselben lesbaren Format zurück.

sr-scan

```
sr-scan uuid=sr_uuid
```

Erzwingen Sie einen SR-Scan, indem Sie die XAPI-Datenbank mit VDIs synchronisieren, die im zugrunde liegenden Speichersubstrat vorhanden sind.

sr-update

```
sr-update uuid=uuid
```

Aktualisieren Sie die Felder des SR-Objekts in der Datenbank.

lvhd-enable-thin-provisioning

```
lvhd-enable-thin-provisioning  sr-uuid=sr_uuid initial-allocation=
   initial_allocation allocation-quantum=allocation_quantum
```

Aktivieren Sie Thin-Provisioning auf einem LVHD SR.

Betreff Befehle

Befehle für die Arbeit mit Themen.

session-subject-identifier-list

```
session-subject-identifier-list
```

Gibt eine Liste aller Benutzer-Betreff-IDs aller extern authentifizierten vorhandenen Sitzungen zurück.

session-subject-identifier-logout

```
session-subject-identifier-logout subject-identifier=subject_identifier
```

Melden Sie sich alle extern authentifizierten Sitzungen ab, die einer Benutzer-Betreff-ID zugeordnet sind.

session-subject-identifier-logout-all

```
session-subject-identifier-logout-all
```

Melden Sie sich alle extern authentifizierten Sitzungen ab.

subject-add

```
subject-add subject-name=subject_name
```

Fügen Sie der Liste der Themen, die auf den Pool zugreifen können, einen Betreff hinzu.

subject-remove

```
subject-remove subject-uuid=subject_uuid
```

Entfernen Sie einen Betreff aus der Liste der Themen, die auf den Pool zugreifen können.

subject-role-add

```
subject-role-add uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

Hinzufügen einer Rolle zu einem Betreff.

subject-role-remove

```
subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
    role_uuid]
```

Entfernen einer Rolle aus einem Betreff.

secret-create

```
secret-create value=value
```

Erstelle ein Geheimnis.

secret-destroy

```
secret-destroy uuid=uuid
```

Zerstöre ein Geheimnis.

Aufgabenbefehle

Befehle zum Arbeiten mit lang laufenden asynchronen Aufgaben. Bei diesen Befehlen handelt es sich um Aufgaben wie Starten, Beenden und Anhalten einer virtuellen Maschine. Die Aufgaben bestehen in der Regel aus einer Reihe anderer atomarer Teilaufgaben, die gemeinsam den angeforderten Vorgang ausführen.

Die Aufgabenobjekte können mit dem Standardbefehl (`xe task-list`) und mit den Standard-parameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

Vorgangsparameter

Aufgaben haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die Aufgabe	Schreibgeschützt
`name-label`	Der Name der Aufgabe	Schreibgeschützt
`name-description`	Die Beschreibungszeichenfolge der Aufgabe	Schreibgeschützt
`resident-on`	Die eindeutige Bezeichner/Objektreferenz des Hosts, auf dem die Aufgabe ausgeführt wird	Schreibgeschützt
`status`	Status der Aufgabe	Schreibgeschützt
`progress`	Wenn der Vorgang noch ausstehend ist, enthält dieses Feld den geschätzten Prozentsatz, der abgeschlossen ist, von 0 bis 1. Wenn die Aufgabe erfolgreich oder erfolglos abgeschlossen wurde, ist der Wert 1.	Schreibgeschützt

Parametername	Beschreibung	Typ
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 nicht definiert	Schreibgeschützt
result	Wenn der Vorgang erfolgreich abgeschlossen wurde, enthält dieses Feld den Ergebniswert, entweder Void oder einen Objektreferenz. Andernfalls ist der Wert dieses Parameters nicht definiert.	Schreibgeschützt
error_info	Wenn der Task fehlgeschlagen ist, enthält dieser Parameter den Satz der zugeordneten Fehlerzeichenfolgen. Andernfalls ist der Wert dieses Parameters nicht definiert	Schreibgeschützt
allowed_operations	Liste der in diesem Zustand zulässigen Vorgänge	Schreibgeschützt
created	Zeitpunkt der Erstellung der Aufgabe	Schreibgeschützt
finished	Zeitaufgabe abgeschlossen (d. h. erfolgreich oder fehlgeschlagen). Wenn der Aufgabenstatus ausstehend ist, hat der Wert dieses Feldes keine Bedeutung	Schreibgeschützt
subtask_of	Enthält die UUID der Aufgaben, die dieser Task eine Teilaufgabe von	Schreibgeschützt

Parametername	Beschreibung	Typ
subtasks	Enthält die UUIDs aller Teilaufgaben dieser Aufgabe	Schreibgeschützt

task-cancel

```
task-cancel [uuid=task_uuid]
```

Die angegebene Aufgabe soll abbrechen und zurückgeben.

Vorlagenbefehle

Befehle zum Arbeiten mit VM-Vorlagen.

Vorlagen sind im Wesentlichen VMs mit dem `is-a-template` Parameter auf **`true`**. Eine Vorlage ist ein „Gold-Image“, das alle verschiedenen Konfigurationseinstellungen enthält, um eine bestimmte VM zu instanziieren. Citrix Hypervisor wird mit einem Basissatz von Vorlagen ausgeliefert, bei denen es sich um generische „rohe“ VMs handelt, die eine Installations-CD des Betriebssystemherstellers starten können (z. B. RHEL, CentOS, SLES, Windows). Sie können VMs erstellen, 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 standardmäßigen Objektlistenbefehl (`xe template-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

> **Hinweis:**
>
> Vorlagen können nicht direkt in VMs konvertiert werden, indem der `is-a-template` Parameter auf festgelegt wird **`false`**. Das Festlegen des `is-a-template` Parameters auf **`false`** wird nicht unterstützt und führt zu einer virtuellen Maschine, die nicht gestartet werden kann.

VM-Vorlagenparameter

Vorlagen haben die folgenden Parameter:

- `uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die Vorlage
- `name-` **`label`** (Lese-/Schreibzugriff) der Name der Vorlage
- `name-description` (Lese-/Schreibzugriff) der Beschreibungszeichenfolge der Vorlage

- `user-version` (Lese-/Schreibzeichenfolge) für Ersteller von VMs und Vorlagen, um Versionsinformationen zu setzen
- `is-a-template` (read/write) true, wenn diese VM eine 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 VMs konvertiert werden.
- `is-control-domain` (schreibgeschützt) true, wenn dies eine Steuerdomäne ist (Domäne 0 oder eine Treiberdomäne)
- `power-state` (schreibgeschützt) Stromzustand. Der Wert wird immer für eine Vorlage angehalten
- `memory-dynamic-max` (schreibgeschützt) dynamischer maximaler Speicher in Byte.
  `Derzeit nicht verwendet, aber wenn geändert, muss die folgende Einschränkung beachtet werden:memory_static_max>=memory_dynamic_max>=“““‘memory_dynamic_min .‘`
- `memory-dynamic-min` (Lese-/Schreibzugriff) dynamischer Mindestspeicher in Bytes.
  Derzeit nicht verwendet, aber wenn geändert,`memory-dynamic-max` müssen die gleichen Einschränkungen für eingehalten werden.
- `memory-static-max` (Lese-/Schreibzugriff) statisch festgelegter (absoluter) maximaler Speicher in Bytes. Dieses Feld ist der Hauptwert, der verwendet wird, um die Speichermenge zu bestimmen, die einer VM zugewiesen ist.
- `memory-static-min` (Lese-/Schreibzugriff) statisch festgelegter (absoluter) Mindestspeicher in Bytes.
  Dieses Feld stellt den absoluten Mindestspeicher dar und`memory-static-min` muss kleiner sein als`memory-static-max` .
  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)
- -Konfigurationsparameter `VCPUs-params` (Lese-/Schreibzuordnungsparameter) für die ausgewählte vCPU-Richtlinie.

  Sie können das Anheften einer vCPU optimieren mit:

  ```
  1  xe template-param-set uuid=<template_uuid> vCPUs-params:mask
       =1,2,3
  ```

  Eine aus dieser Vorlage erstellte VM wird nur auf physischen CPUs 1, 2 und 3 ausgeführt.

Sie können auch die vCPU-Priorität (xen-Scheduling) mit den Parametern cap und weight optimieren. Zum Beispiel:

```
xe template-param-set uuid=<template_uuid> VCPUs-params:weight
   =512 xe template-param-set uuid=<template_uuid> VCPUs-params:
   cap=100
```

Eine VM, die auf dieser Vorlage mit einem Gewicht von 512 basiert, erhält doppelt so viel CPU wie eine Domain mit einem Gewicht von 256 auf einem beanspruchten Host. Die zulässigen Gewichtungen liegen zwischen 1 und 65535 und der Standardwert ist 256.

Die Kappe behebt optional die maximale CPU-Menge, die eine VM auf Basis dieser Vorlage belegen kann, selbst wenn der Citrix Hypervisor or-Server über Leerlauf-CPU-Zyklen verfügt. Die Obergrenze wird in Prozent einer physischen CPU ausgedrückt: 100 ist 1 physische CPU, 50 ist eine halbe CPU, 400 ist 4 CPUs usw. Der Standardwert 0 bedeutet, dass keine obere Obergrenze vorhanden ist.

- `VCPUs-max` (Lese-/Schreibzugriff) maximale Anzahl von vCPUs
- `VCPUs-at-startup` (Lese-/Schreibzugriff) Startnummer von vCPUs
- `actions-after-crash` (Lese-/Schreibvorgang) -Aktion, die ausgeführt wird, wenn eine auf dieser Vorlage basierende VM abstürzt
- `console-uuids` (schreibgeschützte Parameter) virtuelle Konsolengeräte
- `platform` (Lese-/Schreibzuordnungsparameter) plattformspezifische Konfiguration

  So deaktivieren Sie die Emulation eines parallelen Ports für HVM-Gäste (z. B. Windows Gäste):

  ```
  xe vm-param-set uuid=<vm_uuid> platform:parallel=none
  ```

  So deaktivieren Sie die Emulation eines seriellen Ports für HVM-Gäste:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
  ```

  So deaktivieren Sie die Emulation eines USB-Controllers und eines USB-Tablet-Geräts für HVM-Gäste:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:usb=false
  xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
  ```

- Liste der in diesem Zustand zulässigen Operationen `allowed-operations` (read only set parameter)
- `current-operations` (Read Only Set Parameter) Liste der Vorgänge, die derzeit in dieser Vorlage ausgeführt werden

- `allowed-VBD-devices` (read only set parameter) Liste der verfügbaren VBD-Bezeichner, die durch ganze Zahlen im Bereich 0—15 dargestellt werden. Diese Liste ist nur informativ, und andere Geräte können verwendet werden (aber möglicherweise nicht funktionieren).
- `allowed-VIF-devices` (read only set parameter) Liste der zur Verwendung verfügbaren VIF-Bezeichner, dargestellt durch ganze Zahlen im Bereich 0—15. Diese Liste ist nur informativ, und andere Geräte können verwendet werden (aber möglicherweise nicht funktionieren).
- `HVM-boot-policy` (Lese-/Schreibzugriff) die Boot-Richtlinie für HVM-Gäste. Entweder BIOS-Reihenfolge oder eine leere Zeichenfolge.
- `HVM-boot-params` (Lese-/Schreibzuordnungsparameter) steuert der Orderschlüssel die HVM-Gaststartreihenfolge, die als Zeichenfolge dargestellt wird, wobei jedes Zeichen eine Boot-Methode ist: d für die CD/DVD, c für die Root-Diskette und n für den Netzwerk-PXE-Start. Der Standardwert ist dc.
- `PV-kernel` (Lese-/Schreibzugriff) Pfad zum Kernel
- `PV-ramdisk` (Lese-/Schreibzugriff) Pfad zum initrd
- `PV-args` (Lese-/Schreibzeichenfolge) von Kernel-Befehlszeilenargumenten
- `PV-legacy-args` (Lese-/Schreibzeichenfolge), um Legacy-VMs basierend auf dieser Vorlage booten zu lassen
- `PV-bootloader` (Lese-/Schreibzugriff) Name oder Pfad zum Bootloader
- `PV-bootloader-args` (Lese-/Schreib-) Zeichenfolge mit verschiedenen Argumenten für den Bootloader
- `last-boot-CPU-flags` (schreibgeschützt) beschreibt die CPU-Flags, auf denen eine VM, die auf dieser Vorlage basiert, zuletzt gestartet wurde; nicht für eine Vorlage aufgefüllt
- `resident-on` (schreibgeschützt) der Citrix Hypervisor or-Server, auf dem sich eine auf dieser Vorlage basierende VM befindet. Erscheint wie `not in database` für eine Vorlage
- `affinity` (Lese-/Schreibzugriff) des Citrix Hypervisor or-Servers, auf dem eine VM basierend auf dieser Vorlage Vorgabe ausgeführt werden kann. Wird vom `xe vm-start` Befehl verwendet, um zu entscheiden, wo die VM ausgeführt werden soll.
- `other-config` (Lese-/Schreibzuordnungsparameter) Liste der Schlüssel/Wert-Paare, die zusätzliche Konfigurationsparameter für die Vorlage angeben
- `start-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu dem die Metriken für eine VM auf der Grundlage dieser Vorlage gelesen wurden, in der Form`yyyymmddThh:mm:ss z` , wobei z der einbuchstabige militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT). Legen Sie für eine Vorlage auf `1 Jan 1970 Z` (Anfang der Unix/POSIX-Epoche) fest

- `install-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu dem die Metriken für eine VM auf der Grundlage dieser Vorlage gelesen wurden, in der Form`yyyymmddThh:mm:ss z` , wobei z der einbuchstabige militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT). Legen Sie für eine Vorlage auf `1 Jan 1970 Z` (Anfang der Unix/POSIX-Epoche) fest
- `memory-actual` (schreibgeschützt) der tatsächliche Speicher, der von einer VM verwendet wird, basierend auf dieser Vorlage; 0 für eine Vorlage
- `VCPUs-number` (schreibgeschützt) die Anzahl der virtuellen CPUs, die einer VM basierend auf dieser Vorlage zugewiesen sind; 0 für eine Vorlage
- `VCPUs-Utilization` (Read Only Map-Parameter) Liste der virtuellen CPUs und deren Gewichtung schreibgeschützte Map-Parameter OS-Version der Version des Betriebssystems für eine VM basierend auf dieser Vorlage. Erscheint wie `not in database` für eine Vorlage
- `PV-drivers-version` (schreibgeschützte Zuordnungsparameter) die Versionen der paravirtualisierten Treiber für eine VM basierend auf dieser Vorlage. Erscheint wie `not in database` für eine Vorlage
- `PV-drivers-detected` (schreibgeschützt) für die neueste Version der paravirtualisierten Treiber für eine VM basierend auf dieser Vorlage. Erscheint wie `not in database` für eine Vorlage
- `memory` (schreibgeschützte Zuordnungsparameter) Memory-Metriken, die vom Agenten auf einer VM basierend auf dieser Vorlage gemeldet werden. Erscheint wie `not in database` für eine Vorlage
- `disks` (schreibgeschützte Zuordnungsparameter) Datenträgermetriken, die vom Agenten auf einer VM basierend auf dieser Vorlage gemeldet werden. Erscheint wie `not in database` für eine Vorlage
- `networks` (schreibgeschützte Zuordnungsparameter) Netzwerkmetriken, die vom Agenten auf einer VM basierend auf dieser Vorlage gemeldet werden. Erscheint wie `not in database` für eine Vorlage
- `other` (schreibgeschützte Zuordnungsparameter) andere Metriken, die vom Agenten auf einer VM basierend auf dieser Vorlage gemeldet werden. Erscheint wie `not in database` für eine Vorlage
- `guest-metrics-last-updated` (schreibgeschützt) Zeitstempel, wenn der In-Gast-Agent das letzte Schreiben in diese Felder durchgeführt hat. In der Form`yyyymmddThh:mm:ss z`, wobei z der einbuchstabige militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT)
- `actions-after-shutdown` (Lese-/Schreibvorgang) -Aktion, die nach dem Herunterfahren der VM ausgeführt werden soll
- `actions-after-reboot` (Lese-/Schreibvorgang) -Aktion, die nach dem Neustart der VM ausgeführt werden soll

- `possible-hosts` (schreibgeschützt) Liste der Hosts, die möglicherweise die VM hosten könnten
- `HVM-shadow-multiplier` (Lese-/Schreib-) Multiplikator angewendet auf die Menge an Schatten, die dem Gast zur Verfügung gestellt wird
- `dom-id` (schreibgeschützt) Domain-ID (falls verfügbar, andernfalls -1)
- `recommendations` (schreibgeschützt) XML-Spezifikation der empfohlenen Werte und Bereiche für Eigenschaften dieser VM
- `xenstore-data` (Lese-/Schreibzuordnungsparameter) -Daten, die in den xenstore-Baum (*/local/domain/domid* /vmdata) eingefügt werden, nachdem die VM erstellt wurde.
- `is-a-snapshot` (schreibgeschützt) True, wenn es sich bei dieser Vorlage um einen VM-Snapshot handelt
- `snapshot_of` (schreibgeschützt) die UUID der VM, die diese Vorlage ein Snapshot von
- `snapshots` (schreibgeschützt) die UUIDs aller Snapshots, die aus dieser Vorlage erstellt wurden
- `snapshot_time` (schreibgeschützt) der Zeitstempel des letzten VM-Snapshots
- `memory-target` (schreibgeschützt) die Zielmenge des Speichersatzes für diese Vorlage
- `blocked-operations` (Kartenparameter mit Lese-/Schreibzugriff) listet die Vorgänge auf, die für diese Vorlage nicht ausgeführt werden können
- `last-boot-record` (schreibgeschützt) Datensatz der letzten Boot-Parameter für diese Vorlage im XML-Format
- `ha-always-run` (read/write) True, wenn eine Instanz dieser Vorlage immer auf einem anderen Host neu gestartet wird, wenn ein Fehler des Hosts auftritt, auf dem er sich befindet. Dieser Parameter ist jetzt veraltet. Verwenden Sie stattdessen den `ha-restartpriority` Parameter.
- `ha-restart-priority` (schreibgeschützt) Neustart oder Best-Effort-Lese-/Schreib-BLOBs binärer Datenspeicher
- `live` (schreibgeschützt), die nur für eine laufende VM relevant ist.

template-export

```
template-export template-uuid=uuid_of_existing_template filename=
    filename_for_new_template
```

Exportiert eine Kopie einer angegebenen Vorlage in eine Datei mit dem angegebenen neuen Dateinamen.

template-uninstall

```
template-uninstall template-uuid=template_uuid [--force]
```

Deinstallieren Sie eine benutzerdefinierte Vorlage. Dieser Vorgang zerstört die VDIs, die von dieser Vorlage als „Eigentum“ gekennzeichnet sind.

Aktualisierungsbefehle

Der folgende Abschnitt enthält Update-Befehle für Citrix Hypervisor Server.

Die Aktualisierungsobjekte können mit dem Befehl zur Standardobjektauflistung (`xe update-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

Aktualisierungsparameter

Citrix Hypervisor -Serverupdates verfügen über die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für das Update	Schreibgeschützt
`host`	Die Liste der Hosts, auf die dieses Update angewendet wird	Schreibgeschützt
`host-uuid`	Der eindeutige Bezeichner für die Abfrage des Citrix Hypervisor or-Servers	Schreibgeschützt
`name-label`	Der Name des Updates	Schreibgeschützt
`name-description`	Die Beschreibungszeichenfolge des Updates	Schreibgeschützt
`applied`	Gibt an, ob die Aktualisierung angewendet wurde; true oder false	Schreibgeschützt
`installation-size`	Die Größe der Aktualisierung in Bytes	Schreibgeschützt

Parametername	Beschreibung	Typ
after-apply-guidance	Gibt an, ob der XAPI-Toolstack oder der Host einen Neustart erfordert	Schreibgeschützt
version	Die Version des Updates	Schreibgeschützt

update-upload

```
1 update-upload file-name=update_filename
```

Laden Sie eine angegebene Update-Datei auf den Citrix Hypervisor or-Server hoch. Dieser Befehl bereitet ein Update vor, das angewendet werden soll. Bei Erfolg wird die UUID des hochgeladenen Updates gedruckt. Wenn das Update zuvor hochgeladen wurde, wird stattdessen einUPDATE_ALREADY_EXISTS Fehler zurückgegeben und der Patch wird nicht erneut hochgeladen.

update-precheck

```
1 update-precheck uuid=update_uuid host-uuid=host_uuid
```

Führen Sie die im angegebenen Update enthaltenen Vorprüfungen auf dem angegebenen Citrix Hypervisor or-Server aus.

update-destroy

```
1 update-destroy uuid=update_file_uuid
```

Löscht eine Update-Datei, die nicht aus dem Pool angewendet wurde. Kann verwendet werden, um eine Update-Datei zu löschen, die nicht auf die Hosts angewendet werden kann.

update-apply

```
1 update-apply host-uuid=host_uuid uuid=update_file_uuid
```

Wenden Sie die angegebene Update-Datei an.

update-pool-apply

```
update-pool-apply uuid=update_uuid
```

Wenden Sie das angegebene Update auf alle Citrix Hypervisor or-Server im Pool an.

update-introduce

```
update-introduce vdi-uuid=vdi_uuid
```

Update VDI einführen.

update-pool-clean

```
update-pool-clean uuid=uuid
```

Entfernt die Dateien des Updates von allen Hosts im Pool.

Benutzerbefehle

user-password-change

```
user-password-change old=old_password new=new_password
```

Ändert das Kennwort des angemeldeten Benutzers. Das alte Kennwortfeld ist nicht aktiviert, da Sie Supervisor-Berechtigungen benötigen, um diesen Befehl zu verwenden.

VBD-Befehle

Befehle zum Arbeiten mit VBDs (Virtual Block Devices).

Ein 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 an die VM binden (ist es bootfähig, seine Lese-/Schreibmetriken usw.). Der VDI enthält Informationen zu den physikalischen Attributen des virtuellen Laufwerks (welcher Typ von SR, ob der Datenträger gemeinsam verwendet werden kann, ob das Medium schreibgeschützt oder schreibgeschützt ist usw.).

Die VBD-Objekte können mit dem Standard-Objektlistenbefehl (`xe vbd-list`) aufgelistet werden, und die Parameter werden mit den Standardparameterbefehlen manipuliert. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

VBD-Parameter

VBDs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für die VBD	Schreibgeschützt
`vm-uuid`	Die eindeutige Bezeichner/Objektreferenz für die VM, an die diese VBD angehängt ist	Schreibgeschützt
`vm-name-label`	Der Name der VM, an die diese VBD angehängt ist	Schreibgeschützt
`vdi-uuid`	Die eindeutige Bezeichner/Objektreferenz für den VDI, dem diese VBD zugeordnet ist	Schreibgeschützt
`vdi-name-label`	Der Name des VDI, dem diese VBD zugeordnet ist	Schreibgeschützt
`empty`	Wenn`true`dieser VBD ein leeres Laufwerk darstellt	Schreibgeschützt
`device`	Das Gerät, das vom Gast gesehen wird, zum Beispiel`hda`	Schreibgeschützt
`userdevice`	Gerätenummer`vbd-create`, die durch den Geräteparameter angegeben werden, z. B. 0 für hda, 1 für hdb usw.	Lese-/Schreibzugriff
`bootable`	True, wenn diese VBD bootfähig ist	Lese-/Schreibzugriff
`mode`	Der Modus, in dem der VBD mit	Lese-/Schreibzugriff
`type`	Wie die VBD auf der VM angezeigt wird, z. B. auf Festplatte oder CD	Lese-/Schreibzugriff

Parametername	Beschreibung	Typ
currently-attached	True, wenn die VBD auf diesem Host angehängt ist, andernfalls false	Schreibgeschützt
storage-lock	True, wenn eine Sperre auf Speicherebene erworben wurde	Schreibgeschützt
status-code	Fehler-/Erfolgscode, der mit dem letzten Anfügevorgang verknüpft ist	Schreibgeschützt
status-detail	Fehler-/Erfolgsinformationen, die mit dem Status des letzten Anfügevorgangs verknüpft sind	Schreibgeschützt
qos_algorithm_type	Der zu verwendende QoS-Algorithmus	Lese-/Schreibzugriff
qos_algorithm_params	Parameter für den gewählten QoS-Algorithmus	Kartenparameter mit Lese-/Schreibzugriff
qos_supported_algorithms	Unterstützte QoS-Algorithmen für diese VBD	Schreibgeschützte Parameter
io_read_kbs	Durchschnittliche Leserate in kB pro Sekunde für diese VBD	Schreibgeschützt
io_write_kbs	Durchschnittliche Schreibrate in kB pro Sekunde für diese VBD	Schreibgeschützt
allowed-operations	Liste der in diesem Zustand zulässigen Vorgänge. Diese Liste ist nur beratend, und der Serverstatus hat sich möglicherweise geändert, wenn dieses Feld von einem Client gelesen wird.	Schreibgeschützte Parameter

Parametername	Beschreibung	Typ
current-operations	Verknüpft jede der ausgeführten Tasks, die dieses Objekt verwenden (per Verweis), mit einer current_operation-Enumeration, die die Art der Aufgabe beschreibt.	Schreibgeschützte Parameter
unpluggable	True, wenn diese VBD Hot Unplug unterstützt	Lese-/Schreibzugriff
attachable	True, wenn das Gerät angeschlossen werden kann	Schreibgeschützt
other-config	Zusätzliche Konfiguration	Kartenparameter mit Lese-/Schreibzugriff

vbd-create

```
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
    ]
```

Erstellen Sie eine VBD auf einer VM.

Die zulässigen Werte für dasdevice Feld sind ganze Zahlen 0—15, und die Zahl muss für jede VM eindeutig sein. Die aktuell zulässigen Werte können imallowed-VBD-devices Parameter auf der angegebenen VM angezeigt werden. Dies wird wieuserdevice in denvbd Parametern gesehen.

Wenn dertype istDisk ,vdi-uuid ist erforderlich. Der Modus kannRO oderRW für einen Datenträger sein.

Wenn dertype istCD ,vdi-uuid ist optional. Wenn kein VDI angegeben wird, wird eine leere VBD für die CD erstellt. Der Modus mussRO für eine CD sein.

vbd-destroy

```
vbd-destroy uuid=uuid_of_vbd
```

Zerstören Sie die angegebene VBD.

Wenn der`other-config:owner` Parameter für die VBD auf gesetzt ist**`true`**, wird auch der zugehörige VDI zerstört.

`vbd-eject`

```
vbd-eject uuid=uuid_of_vbd
```

Entfernen Sie das Medium aus dem Laufwerk, das durch eine VBD dargestellt wird. Dieser Befehl funktioniert nur, wenn das Medium einen Wechseldatentyp hat (eine physische CD oder ein ISO). Andernfalls `VBD_NOT_REMOVABLE_MEDIA` wird eine Fehlermeldung zurückgegeben.

`vbd-insert`

```
vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
```

Legen Sie neue Medien in das Laufwerk ein, das durch eine VBD dargestellt wird. Dieser Befehl funktioniert nur, wenn das Medium einen Wechseldatentyp hat (eine physische CD oder ein ISO). Andernfalls `VBD_NOT_REMOVABLE_MEDIA` wird eine Fehlermeldung zurückgegeben.

`vbd-plug`

```
vbd-plug uuid=uuid_of_vbd
```

Versuchen Sie, die VBD anzuhängen, während sich die VM im ausgeführten Zustand befindet.

`vbd-unplug`

```
vbd-unplug uuid=uuid_of_vbd
```

Versucht, die VBD von der VM zu trennen, während sie sich im laufenden Zustand befindet.

VDI-Befehle

Befehle zum Arbeiten mit VDIs (Virtual Disk Images).

Ein VDI ist ein Softwareobjekt, das den Inhalt des virtuellen Laufwerks darstellt, das von einer VM angezeigt wird. Dies unterscheidet sich von der VBD, bei der es sich um ein Objekt handelt, das eine VM mit dem VDI verbindet. Der VDI enthält Informationen zu den physikalischen Attributen des virtuellen Laufwerks (welcher Typ von SR, ob der Datenträger gemeinsam verwendet werden kann,

ob das Medium schreibgeschützt oder schreibgeschützt ist usw.). Die VBD hat die Attribute, die den VDI an die VM binden (ist es bootfähig, seine Lese-/Schreibmetriken usw.).

Die VDI-Objekte können mit dem Standard-Objektlistenbefehl (`xe vdi-list`) aufgelistet werden und die Parameter mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

VDI-Parameter

VDIs haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`uuid`	Die eindeutige Bezeichner/Objektreferenz für den VDI	Schreibgeschützt
`name-label`	Der Name des VDI	Lese-/Schreibzugriff
`name-description`	Die Beschreibungszeichenfolge des VDI	Lese-/Schreibzugriff
`allowed-operations`	Eine Liste der in diesem Zustand zulässigen Vorgänge	Schreibgeschützte Parameter
`current-operations`	Eine Liste der Vorgänge, die derzeit auf diesem VDI ausgeführt werden	Schreibgeschützte Parameter
`sr-uuid`	SR, in dem sich der VDI befindet	Schreibgeschützt
`vbd-uuids`	Eine Liste der VBDs, die sich auf diesen VDI beziehen	Schreibgeschützte Parameter
`crashdump-uuids`	Liste der Absturzabbilder, die auf diesen VDI verweisen	Schreibgeschützte Parameter
`virtual-size`	Größe der Festplatte, wie der VM dargestellt, in Bytes. Je nach Speicher-Backend-Typ kann die Größe nicht exakt eingehalten werden	Schreibgeschützt
`physical-utilisation`	Menge des physischen Speicherplatzes, den der VDI auf der SR belegt, in Byte	Schreibgeschützt

Parametername	Beschreibung	Typ
type	Typ des VDI, z. B. System oder Benutzer	Schreibgeschützt
sharable	True, wenn dieser VDI freigegeben werden kann	Schreibgeschützt
read-only	True, wenn dieser VDI nur schreibgeschützt bereitgestellt werden kann	Schreibgeschützt
storage-lock	True, wenn dieser VDI auf Speicherebene gesperrt ist	Schreibgeschützt
parent	Verweist auf den übergeordneten VDI, wenn dieser VDI Teil einer Kette ist	Schreibgeschützt
missing	True, wenn der SR-Scanvorgang diesen VDI als nicht vorhanden gemeldet hat	Schreibgeschützt
other-config	Zusätzliche Konfigurationsinformationen für diesen VDI	Kartenparameter mit Lese-/Schreibzugriff
sr-name-**label**	Name des enthaltenden Speicher-Repositorys	Schreibgeschützt
location	Standortinformationen	Schreibgeschützt
managed	True, wenn der VDI verwaltet wird	Schreibgeschützt
xenstore-data	Daten, die in den xenstore-Baum (**/local/domain/0/backend/vb id**/smdata) eingefügt werden sollen, nachdem der VDI angehängt wurde. Die SM-Back-Ends setzen dieses Feld normalerweise auf vdi_attach.	Schreibgeschützte Kartenparameter
sm-config	SM-abhängige Daten	Schreibgeschützte Kartenparameter

Parametername	Beschreibung	Typ
is-a-snapshot	True, wenn es sich bei diesem VDI um einen VM-Speicher-Snapshot handelt	Schreibgeschützt
snapshot_of	Die UUID des Speichers dieses VDI ist ein Snapshot von	Schreibgeschützt
snapshots	Die UUIDs aller Snapshots dieses VDI	Schreibgeschützt
snapshot_time	Der Zeitstempel des Snapshot-Vorgangs, der diesen VDI erstellt hat	Schreibgeschützt
metadata-of-pool	Die uuid des Pools, der diese Metadaten-VDI erstellt hat	Schreibgeschützt
metadata-latest	Flag, das angibt, ob der VDI die neuesten bekannten Metadaten für diesen Pool enthält	Schreibgeschützt
cbt-enabled	Flag, das angibt, ob die geänderte Blockverfolgung für den VDI aktiviert ist	Lese-/Schreibzugriff

vdi-clone

```
1 vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
```

Erstellen Sie eine neue, beschreibbare Kopie des angegebenen VDI, die direkt verwendet werden kann. Es ist eine Variantevdi-copy , die High-Speed-Image-Klon-Einrichtungen verfügbar machen kann, wo sie existieren.

Verwenden Sie den optionalen driver-params Zuordnungsparameter, um zusätzliche herstellerspezifische Konfigurationsinformationen an den Back-End-Speichertreiber zu übergeben, auf dem der VDI basiert. Weitere Informationen finden Sie in der Dokumentation des Speicherherstellertreibers.

vdi-copy


```
vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
```

Kopieren Sie einen VDI in eine angegebene SR.

vdi-create

```
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
```

Erstellen Sie einen VDI.

Der `virtual-size` Parameter kann in Bytes oder mit den IEC-Standardsuffixe KiB, MiB, GiB und TiB angegeben werden.

> **Hinweis:**
>
> SR-Typen, die Thin Provisioning von Festplatten unterstützen (z. B. lokale VHD und NFS), erzwingen keine virtuelle Zuweisung von Festplatten. Achten Sie bei der übermäßigen Zuweisung von virtuellem Festplattenspeicher auf einem SR auf große Sorgfalt. Wenn ein überlasteter SR voll wird, muss der Speicherplatz entweder auf dem SR-Zielsubstrat oder durch Löschen nicht verwendeter VDIs in der SR zur Verfügung gestellt werden.
>
> Einige SR-Typen können den`virtual-size` Wert aufrunden, um ihn durch eine konfigurierte Blockgröße teilbar zu machen.

vdi-data-destroy

```
vdi-data-destroy uuid=uuid_of_vdi
```

Löschen Sie die Daten, die mit dem angegebenen VDI verknüpft sind, behalten Sie jedoch die geänderten Block-Tracking-Metadaten bei.

> **Hinweis:**
>
> Wenn Sie die geänderte Blockverfolgung verwenden, um inkrementelle Sicherungen des VDI zu erstellen, stellen Sie sicher, dass Sie den`vdi-data-destroy` Befehl verwenden, um Snapshots zu löschen, aber die Metadaten beizubehalten. Verwenden Sie diese Option `vdi-destroy` nicht für Snapshots von VDIs, bei denen die Blockverfolgung aktiviert wurde.

vdi-destroy

```
vdi-destroy uuid=uuid_of_vdi
```

Zerstören Sie den angegebenen VDI.

> **Hinweis:**
>
> Wenn Sie die geänderte Blockverfolgung verwenden, um inkrementelle Sicherungen des VDI zu erstellen, stellen Sie sicher, dass Sie den`vdi-data-destroy` Befehl verwenden, um Snapshots zu löschen, aber die Metadaten beizubehalten. Verwenden Sie diese Option`vdi-destroy` nicht für Snapshots von VDIs, bei denen die Blockverfolgung aktiviert wurde.
>
> Bei lokalen VHD- und NFS-SR-Typen wird Speicherplatz nicht sofort freigegeben`vdi-destroy`, sondern regelmäßig während eines Speicher-Repository-Scanvorgangs. Wenn Sie die Bereitstellung gelöschter Speicherplatz erzwingen müssen, rufen Sie [`sr-scan`] (#sr -scan) manuell auf.

vdi-disable-cbt

```
vdi-disable-cbt uuid=uuid_of_vdi
```

Deaktivieren Sie die geänderte Blockverfolgung für den VDI.

vdi-enable-cbt

```
vdi-enable-cbt uuid=uuid_of_vdi
```

Aktivieren Sie die geänderte Blockverfolgung für den VDI.

> **Hinweis:**
>
> Sie können die geänderte Blockverfolgung nur auf lizenzierten Instanzen von Citrix Hypervisor Premium Edition aktivieren.

vdi-export

```
vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=
    format] [base=uuid_of_base_vdi] [--progress]
```

Exportieren Sie einen VDI in den angegebenen Dateinamen. Sie können einen VDI in einem der folgenden Formate exportieren:

- raw
- vhd

Das VHD-Format kann *dünn*sein. Wenn innerhalb des VDI nicht zugewiesene Blöcke vorhanden sind, werden diese Blöcke möglicherweise aus der VHD-Datei weggelassen, wodurch die VHD-Datei kleiner wird. Sie können aus allen unterstützten VHD-basierten Speichertypen (EXT, NFS) in das VHD-Format exportieren.

Wenn Sie denbase Parameter angeben, exportiert dieser Befehl nur die Blöcke, die sich zwischen dem exportierten VDI und dem Basis-VDI geändert haben.

vdi-forget

```
vdi-forget uuid=uuid_of_vdi
```

Entfernt bedingungslos einen VDI-Eintrag aus der Datenbank, ohne das Speicher-Back-End zu berühren. Im normalen Betrieb sollten Sie stattdessen [vdi-destroy] (#vdi -destroy) verwenden.

vdi-import

```
vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format=
    format] [--progress]
```

Importieren Sie einen VDI. Sie können einen VDI aus einem der folgenden Formate importieren:

- raw
- vhd

vdi-introduce

```
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]
```

Erstellen Sie ein VDI-Objekt, das ein vorhandenes Speichergerät darstellt, ohne Speicher tatsächlich zu ändern oder zu erstellen. Dieser Befehl wird hauptsächlich intern verwendet, um Hot-Plug–Speichergeräte automatisch einzuführen.

vdi-list-changed-blocks

```
vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=second
   -vdi-uuid
```

Vergleichen Sie zwei VDIs und geben Sie die Liste der Blöcke zurück, die sich zwischen den beiden als base64-codierte Zeichenfolge geändert haben. Dieser Befehl funktioniert nur für VDIs, bei denen die Blockverfolgung aktiviert wurde.

Weitere Informationen finden Sie unter Blockverfolgung geändert.

vdi-pool-migrate

```
vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
```

Migrieren Sie einen VDI zu einer bestimmten SR, während der VDI an einen laufenden Gast angeschlossen ist. (Massenspeicher-Live-Migration)

Weitere Informationen finden Sie unter Migrieren von VMs.

vdi-resize

```
vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
```

Ändern Sie die Größe des durch UUID angegebenen VDI.

vdi-snapshot

```
vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
```

Erzeugt eine Lese-/Schreibversion eines VDIs, die als Referenz für Backup- oder Vorlagenerstellungszwecke oder beides verwendet werden kann. Verwenden Sie den Snapshot, um eine Sicherung durchzuführen, anstatt Backup-Software innerhalb der VM zu installieren und auszuführen. Die VM wird weiterhin ausgeführt, während externe Sicherungssoftware den Inhalt des Snapshots auf das Sicherungsmedium streamt. Ebenso kann ein Snapshot als „Goldbild“ verwendet werden, auf dem eine Vorlage basiert. Eine Vorlage kann mit beliebigen VDIs erstellt werden.

Verwenden Sie den optionalen `driver-params` Zuordnungsparameter, um zusätzliche herstellerspezifische Konfigurationsinformationen an den Back-End-Speichertreiber zu übergeben, auf dem der VDI basiert. Weitere Informationen finden Sie in der Dokumentation des Speicherherstellertreibers.

Ein Klon eines Snapshots sollte immer einen beschreibbaren VDI erzeugen.

vdi-unlock

```
vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
```

Versucht, die angegebenen VDIs zu entsperren. Wenn an den Befehl übergeben`force=true` wird, erzwingt es die Entsperrung.

vdi-update

```
vdi-update uuid=uuid
```

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 Befehl zur Standardobjektauflistung (`xe vif-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

VIF-Parameter

VIFs haben die folgenden Parameter:

- `uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die VIF
- `vm-uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die VM, auf der sich diese VIF befindet
- `vm-name-label` (schreibgeschützt) der Name der VM, auf der sich diese VIF befindet
- `allowed-operations` (schreibgeschützter Parameter) eine Liste der in diesem Zustand zulässigen Operationen
- `current-operations` (schreibgeschützter Parameter) eine Liste der Vorgänge, die derzeit auf diesem VIF ausgeführt werden
- `device` (schreibgeschützte) Ganzzahlbeschriftung dieses VIF, die die Reihenfolge angibt, in der VIF-Back-Ends erstellt wurden
- `MAC` (schreibgeschützte) MAC-Adresse von VIF, wie sie der VM zugänglich gemacht wird

- `MTU` (schreibgeschützt) Maximale Übertragungseinheit des VIF in Byte.

  Dieser Parameter ist schreibgeschützt, aber Sie können die MTU-Einstellung mit dem`mtu` Schlüssel mit dem Parameter`other-config` map überschreiben. 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
  ```

- `currently-attached` (schreibgeschützt) true, wenn das Gerät angeschlossen ist
- `qos_algorithm_type` (Lese-/Schreib-) QoS-Algorithmus zu verwenden
- `qos_algorithm_params` (Lese-/Schreibzugriffsparameter) für den gewählten QoS-Algorithmus
- `qos_supported_algorithms` (read only set parameter) unterstützte QoS-Algorithmen für diese VIF
- `MAC-autogenerated` (schreibgeschützt) True, wenn die MAC-Adresse des VIF automatisch generiert wurde
- `other-config` (Lese-/Schreibzuordnungsparameter) zusätzliche`key:value` Konfigurationspaare
- `other-config:ethtoolrx` (Lese-/Schreibzugriff) auf ein gesetzt, um Empfangsprüfsumme zu aktivieren, aus, um zu deaktivieren
- `other-config:ethtooltx` (Lese-/Schreibzugriff) auf ein gesetzt, um die Prüfsumme der Übertragung zu aktivieren, aus, um zu deaktivieren
- `other-config:ethtoolsg` (Lese-/Schreibzugriff) auf ein gesetzt, um Scatter sammeln zu aktivieren, aus, um zu deaktivieren
- `other-config:ethtooltso` (Lese-/Schreibzugriff) auf ein gesetzt, um TCP-Segmentierungsabladung zu aktivieren, aus, um zu deaktivieren
- `other-config:ethtoolufo` (Lese-/Schreibzugriff) auf ein gesetzt, um die udp-Fragmentabladung zu aktivieren, aus, um zu deaktivieren
- `other-config:ethtoolgso` (Lese-/Schreibzugriff) auf ein gesetzt, um generische Segmentierungsabladung zu aktivieren, aus, um zu deaktivieren
- `other-config:promiscuous` (read/write) true auf ein VIF, um auf der Brücke promiscuous zu sein, so dass es den gesamten Verkehr über die Brücke sieht. Nützlich, um ein Intrusion Detection System (IDS) oder ähnliches in einer VM auszuführen.
- `network-uuid` (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz des virtuellen Netzwerks, mit dem diese VIF verbunden 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 diese VIF
- `io_write_kbs` (schreibgeschützt) durchschnittliche Schreibrate in KB/s für diese VIF
- `locking_mode` (Lese-/Schreibzugriff) Beeinflusst die VIFs Fähigkeit, Datenverkehr zu/aus einer Liste von MAC- und IP-Adressen zu filtern. Benötigt zusätzliche Parameter.
- `locking_mode:default` (Lese-/Schreibzugriff) variiert je nach Standardsperrmodus für das VIF-Netzwerk.

  Wenn der Standardsperrmodus auf festgelegt ist`disabled`, wendet Citrix Hypervisor eine Filterregel an, sodass die VIF keinen Datenverkehr senden oder empfangen kann. Wenn der Standardsperrmodus auf eingestellt ist`unlocked`, entfernt Citrix Hypervisor alle Filterregeln, die dem VIF zugeordnet sind. Weitere Informationen finden Sie unter Netzwerkbefehle.
- `locking_mode:locked` (Lese-/Schreibzugriff) Auf der VIF ist nur Datenverkehr zulässig, der an die angegebene MAC- und IP-Adressen gesendet wird. Wenn keine IP-Adressen angegeben werden, ist kein Datenverkehr zulässig.
- `locking_mode:unlocked` (Lese-/Schreibzugriff) Es werden keine Filter auf Datenverkehr angewendet, der zum VIF oder aus dem VIF geht.
- `locking_mode:disabled` (Lese-/Schreibzugriff) Citrix Hypervisor wendet eine Filterregel an, sodass die VIF den gesamten Datenverkehr löscht.

`vif-create`

```
vif-create vm-uuid=uuid_of_the_vm device=see below network-uuid=
    uuid_of_network_to_connect_to [mac=mac_address]
```

Erstellen eines VIF auf einer VM.

Die entsprechenden Werte für das`device` Feld sind im Parameter`allowed-VIF-devices` auf der angegebenen VM aufgeführt. Bevor dort VIFs vorhanden sind, sind die zulässigen Werte ganze Zahlen von 0-15.

Der`mac` Parameter ist die Standard-MAC-Adresse im Formular`aa:bb:cc:dd:ee:ff` . Wenn Sie es nicht angegeben lassen, wird eine entsprechende zufällige MAC-Adresse erstellt. Sie können auch explizit eine zufällige MAC-Adresse festlegen, indem Sie angeben`mac=random`.

`vif-destroy`


```
vif-destroy uuid=uuid_of_vif
```

Zerstöre ein VIF.

vif-move

```
vif-move uuid=uuid network-uuid=network_uuid
```

Verschieben Sie die VIF in ein anderes Netzwerk.

vif-plug

```
vif-plug uuid=uuid_of_vif
```

Versuchen Sie, die VIF anzuhängen, während sich die VM im ausgeführten Zustand befindet.

vif-unplug

```
vif-unplug uuid=uuid_of_vif
```

Versucht, die VIF von der VM zu trennen, während sie ausgeführt wird.

vif-configure-ipv4

Konfigurieren Sie IPv4-Einstellungen für diese virtuelle Schnittstelle. Legen Sie die IPv4-Einstellungen wie folgt fest:

```
vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
    gateway=gateway_address
```

Zum Beispiel:

```
VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
    192.168.1.1")
```

Säubern Sie die IPv4-Einstellungen wie folgt:

```
vif-configure-ipv4 uuid=uuid_of_vif mode=none
```


vif-configure-ipv6

Konfigurieren Sie IPv6-Einstellungen für diese virtuelle Schnittstelle. Legen Sie die IPv6-Einstellungen wie folgt fest:

```
vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
    gateway=gateway_address
```

Zum Beispiel:

```
VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
    "fd06:7768:b9e5:8b00::1")
```

Säubern Sie IPv6-Einstellungen wie folgt:

```
vif-configure-ipv6 uuid=uuid_of_vif mode=none
```

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 zugeordnetes virtuelles Netzwerk verfügen. Weitere Informationen finden Sie unter PIF-Befehle. Verwenden Sie zum Beispiel, um VLANs aufzulisten`xe pif-list`.

vlan-create

```
vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
    uuid_of_network
```

Erstellen Sie ein VLAN auf dem Citrix Hypervisor or-Server.

pool-vlan-create

```
pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
    uuid_of_network
```

Erstellen Sie ein VLAN auf allen Hosts in einem Pool, indem Sie bestimmen, auf welcher Schnittstelle (z. B.`eth0`) sich das angegebene Netzwerk befindet (auf jedem Host) und ein neues PIF-Objekt je Host entsprechend erstellen und anschließen.

`vlan-destroy`

```
vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
```

Zerstören Sie ein VLAN. Erfordert die UUID der PIF, die das VLAN darstellt.

VM-Befehle

Befehle zum Steuern von VMs und deren Attributen.

VM-Selektoren

Mehrere der hier aufgeführten Befehle verfügen über einen gemeinsamen Mechanismus zum Auswählen einer oder mehrerer VMs, auf denen der Vorgang ausgeführt werden soll. Der einfachste Weg ist die Bereitstellung des Argumentsvm=name_or_uuid. Eine einfache Möglichkeit, die UUID einer tatsächlichen VM zu erhalten, besteht beispielsweise darin, ausgeführt zu werdenxe vm-list power-state=running. (Ruft die vollständige Liste der Felder ab, die mit dem Befehl abgeglichen werden könnenxe vm-list params=all.) Wenn Sie beispielsweise festlegen, werden VMspower-state=haltedausgewählt, derenpower-stateParameter gleich halted. 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 Befehl zur Standardobjektauflistung (xe vm-list) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

VM-Parameter

VMs verfügen über die folgenden Parameter:

> **Hinweis:**
>
> Alle beschreibbaren VM-Parameterwerte können während der Ausführung der VM geändert werden, aber neue Parameter werden *nicht* dynamisch angewendet und können erst angewendet werden, wenn die VM neu gestartet wird.

- appliance (Lese-/Schreibzugriff) die Appliance/vApp, zu der die VM gehört
- uuid (schreibgeschützt) die eindeutige Bezeichner/Objektreferenz für die VM
- name-**label** (Lese-/Schreibzugriff) der Name der VM

- `name-description` (Lese-/Schreibzugriff) der Beschreibungszeichenfolge der VM
- `order start order` (Lese-/Schreibzugriff) für vApp-Start/Herunterfahren und für den Start nach HA-Failover
- `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-/Schreibzeichenfolge) für Ersteller von VMs und Vorlagen, um Versionsinformationen zu setzen
- `is-a-template` (Lese-/Schreibzugriff) False, es sei denn, diese VM ist eine Vorlage. 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 VMs konvertiert werden.
- `is-control-domain` (schreibgeschützt) True, wenn dies eine Steuerdomäne ist (Domäne 0 oder eine Treiberdomäne)
- `power-state` (schreibgeschützt) Stromzustand
- `start-delay` (Lese-/Schreibzugriff) die Verzögerung zu warten, bevor ein Aufruf zum Starten der VM zurückgibt
- `shutdown-delay` (Lese-/Schreibzugriff) die Verzögerung zu warten, bevor ein Aufruf zum Herunterfahren der VM zurückgibt
- `memory-dynamic-max` (Lese-/Schreibzugriff) dynamisches Maximum in Bytes
- `memory-dynamic-min` (Lese-/Schreibzugriff) dynamisches Minimum in Bytes
- `memory-static-max` (Lese-/Schreibzugriff) statisch (absolutes) Maximum in Bytes festgelegt. Wenn Sie diesen Wert ändern möchten, muss die VM heruntergefahren werden.
- `memory-static-min` (Lese-/Schreibzugriff) statisch festgelegtes (absolutes) Minimum in Bytes. Wenn Sie diesen Wert ändern möchten, muss die VM heruntergefahren werden.
- `suspend-VDI-uuid` (schreibgeschützt) der VDI, auf dem ein Suspend-Image gespeichert ist
- -Konfigurationsparameter `VCPUs-params` (Lese-/Schreibzuordnungsparameter) für die ausgewählte vCPU-Richtlinie.

  Sie können das Anheften einer vCPU mit

  ```
  1  xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
  ```

  Die ausgewählte VM wird dann nur auf physischen CPUs 1, 2 und 3 ausgeführt.
  Sie können auch die vCPU-Priorität (xen-Scheduling) mit den Parametern cap und weight optimieren. Zum Beispiel:


```
xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-
   param-set uuid=<vm_uuid> VCPUs-params:cap=100
```

Eine VM mit einem Gewicht von 512 erhalten doppelt so viel CPU wie eine Domäne mit einem Gewicht von 256 auf einem angekommenCitrix Hypervisor or-Server. Die zulässigen Gewichtungen liegen zwischen 1 und 65535 und der Standardwert ist 256. Die Kappe behebt optional die maximale CPU-Menge, die eine VM belegen kann, selbst wenn der Citrix Hypervisor or-Server über Leerlauf-CPU-Zyklen verfügt. Die Obergrenze wird in Prozent einer physischen CPU ausgedrückt: 100 ist 1 physische CPU, 50 ist eine halbe CPU, 400 ist 4 CPUs usw. Der Standardwert 0 bedeutet, dass keine obere Obergrenze vorhanden ist.

- `VCPUs-max` (Lese-/Schreibzugriff) maximale Anzahl virtueller CPUs.
- `VCPUs-at-startup` (Lese-/Schreibzugriff) Startnummer virtueller CPUs
- `actions-after-crash` (Lese-/Schreibvorgang), die ausgeführt werden soll, wenn die VM abstürzt. Für PV-Gäste gelten folgende Parameter:
  - `preserve` (nur zur Analyse)
  - `coredump_and_restart` (Record a coredump und VM neu starten)
  - `coredump_and_destroy` (Notieren Sie einen Coredump und lassen Sie VM angehalten)
  - `restart` (kein Coredump und Neustart der VM)
  - `destroy` (kein Coredump und VM angehalten lassen)
- `console-uuids` (schreibgeschützte Parameter) virtuelle Konsolengeräte
- `platform` (Lese-/Schreibzuordnungsparameter) plattformspezifische Konfiguration

  So deaktivieren Sie Virtual Desktop Agent (VDA), um Windows 10 in den Tablet-Modus zu wechseln:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
  ```

  So aktivieren Sie VDA, um Windows 10 in den Tablet-Modus zu wechseln:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
  ```

  So überprüfen Sie den aktuellen Status:

  ```
  xe vm-param-get uuid=<vm_uuid> param-name=platform param-key=
     acpi_laptop_slate
  ```

- Liste der in diesem Zustand zulässigen Operationen `allowed-operations` (read only set parameter)
- `current-operations` (schreibgeschützter Parameter) eine Liste der Vorgänge, die derzeit auf der VM ausgeführt werden

- `allowed-VBD-devices` (read only set parameter) Liste der verfügbaren VBD-Bezeichner, die durch ganze Zahlen im Bereich 0—15 dargestellt werden. Diese Liste ist nur informativ, und andere Geräte können verwendet werden (aber möglicherweise nicht funktionieren).
- `allowed-VIF-devices` (read only set parameter) Liste der zur Verwendung verfügbaren VIF-Bezeichner, dargestellt durch ganze Zahlen im Bereich 0—15. Diese Liste ist nur informativ, und andere Geräte können verwendet werden (aber möglicherweise nicht funktionieren).
- `HVM-boot-policy` (Lese-/Schreibzugriff) die Boot-Richtlinie für HVM-Gäste. Entweder BIOS-Reihenfolge oder eine leere Zeichenfolge.
- `HVM-boot-params` (Lese-/Schreibzuordnungsparameter) steuert der Orderschlüssel die HVM-Gaststartreihenfolge, die als Zeichenfolge dargestellt wird, wobei jedes Zeichen eine Boot-Methode ist: d für die CD/DVD, c für die Root-Diskette und n für den Netzwerk-PXE-Start. Der Standardwert ist dc.
- `HVM-shadow-multiplier` (Lese-/Schreibzugriff) Gleitkommawert, der den Umfang des Schattenspeicher-Overhead steuert, um der VM zu gewähren. Der Standardwert ist 1.0 (der Mindestwert), und nur fortgeschrittene Benutzer sollten diesen Wert ändern.
- `PV-kernel` (Lese-/Schreibzugriff) Pfad zum Kernel
- `PV-ramdisk` (Lese-/Schreibzugriff) Pfad zum initrd
- `PV-args` (Lese-/Schreibzeichenfolge) von Kernel-Befehlszeilenargumenten
- `PV-legacy-args` (Lese-/Schreibzeichenfolge), um ältere VMs zu starten
- `PV-bootloader` (Lese-/Schreibzugriff) Name oder Pfad zum Bootloader
- `PV-bootloader-args` (Lese-/Schreib-) Zeichenfolge mit verschiedenen Argumenten für den Bootloader
- `last-boot-CPU-flags` (schreibgeschützt) beschreibt die CPU-Flags, auf denen die VM zuletzt gestartet wurde
- `resident-on` (schreibgeschützt) der Citrix Hypervisor or-Server, auf dem sich eine VM befindet
- `affinity` (Lese-/Schreibzugriff) Der Citrix Hypervisor or-Server, auf dem die VM bevorzugt ausgeführt werden soll. Wird vom `xe vm-start` Befehl verwendet, um zu entscheiden, wo die VM ausgeführt werden soll.
- `other-config` (Kartenparameter mit Lese-/Schreibzugriff) Eine Liste von Schlüssel/Wert-Paaren, die zusätzliche Konfigurationsparameter für die VM angeben. Zum Beispiel wird eine VM automatisch nach dem Host-Boot gestartet, wenn der`other-config` Parameter das Schlüssel/Wert-Paar`auto_poweron: true` enthält
- `start-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu dem die Metriken für die VM gelesen wurden. Dieser Zeitstempel hat die Form `yyyymmddThh:mm:ss z`, wobei z der einzelne Buchstabe militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT)

- `install-time` (schreibgeschützt) Zeitstempel des Datums und der Uhrzeit, zu dem die Metriken für die VM gelesen wurden. Dieser Zeitstempel hat die Form `yyyymmddThh:mm:ss z`, wobei z der einzelne Buchstabe 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 PV (paravirtual) oder HVM (Hardware Virtual Machine) Linux-VM zugewiesen sind. Diese Nummer kann sich von unterscheiden`VCPUS-max` und kann geändert werden, ohne die VM mit dem`vm-vcpu-hotplug` Befehl neu zu starten. Weitere Informationen finden Sie unter [`vm-vcpu-hotplug`] (#vm -vcpu-hotplug). Windows VMs werden immer mit der Anzahl der vCPUs ausgeführt `VCPUsmax` und müssen neu gestartet werden, um diesen Wert zu ändern. Die Leistung sinkt stark, wenn Sie einen Wert festlegen`VCPUs-number` , der größer ist als die Anzahl der physischen CPUs auf dem Citrix Hypervisor or-Server.
- `VCPUs-Utilization` (Read Only Map-Parameter) eine Liste der virtuellen CPUs und deren Gewicht
- `os-version` (schreibgeschützte Zuordnungsparameter) die Version des Betriebssystems für die VM
- `PV-drivers-version` (schreibgeschützte Zuordnungsparameter) die Versionen der paravirtualisierten Treiber für die VM
- `PV-drivers-detected` (schreibgeschützt) für die neueste Version der paravirtualisierten Treiber für die VM
- `memory` (schreibgeschützte Zuordnungsparameter) Memory-Metriken, die vom Agent auf der VM gemeldet werden
- `disks` (schreibgeschützte Zuordnungsparameter) Datenträgermetriken, die vom Agent auf der VM gemeldet werden
- `networks` (schreibgeschützte Zuordnungsparameter) Netzwerkmetriken, die vom Agent auf der VM gemeldet werden
- `other` (schreibgeschützte Zuordnungsparameter) andere Metriken, die vom Agent auf der VM gemeldet werden
- `guest-metrics-lastupdated` (schreibgeschützt) Zeitstempel, wenn der In-Gast-Agent das letzte Schreiben in diese Felder durchgeführt hat. Der Zeitstempel ist in der Form`yyyymmddThh:mm:ss z`, wobei z der einzelne Buchstabe militärische Zeitzonenindikator ist, z. B. Z für UTC (GMT)
- `actions-after-shutdown` (Lese-/Schreibvorgang) -Aktion, die nach dem Herunterfahren der VM ausgeführt werden soll

- `actions-after-reboot` (Lese-/Schreibvorgang) -Aktion, die nach dem Neustart der VM ausgeführt werden soll
- `possible-hosts` potenzielle Hosts dieser VM schreibgeschützt
- `dom-id` (schreibgeschützt) Domain-ID (falls verfügbar, andernfalls -1)
- `recommendations` (schreibgeschützt) XML-Spezifikation der empfohlenen Werte und Bereiche für Eigenschaften dieser VM
- `xenstore-data` (Lese-/Schreibzuordnungsparameter) Daten, die in den xenstore-Baum (*/local/domain/domid* /vm-data) eingefügt werden, nachdem die VM erstellt wurde
- `is-a-snapshot` (schreibgeschützt) True, wenn diese VM ein Snapshot ist
- `snapshot_of` (schreibgeschützt) die UUID der VM, von der dieser Snapshot ist
- `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 Zielmenge des Arbeitsspeichers für diese VM
- `blocked-operations` (Lese-/Schreibzuordnungsparameter) listet die Vorgänge auf, die auf dieser VM nicht ausgeführt werden können
- `last-boot-record` (schreibgeschützt) Datensatz der letzten Boot-Parameter für diese Vorlage im XML-Format
- `ha-always-run` (Lese-/Schreibzugriff) True, wenn diese VM immer auf einem anderen Host neu gestartet wird, wenn ein Ausfall des Hosts vorliegt, auf dem er sich befindet. Dieser Parameter ist jetzt veraltet. Verwenden Sie stattdessen den `ha-restart-priority` Parameter.
- `ha-restart-priority` (Lese-/Schreibzugriff) Neustart oder best-effort
- `blobs` (schreibgeschützter) binärer Datenspeicher
- `live` (schreibgeschützt) True, wenn die VM ausgeführt wird. False, wenn HA den Verdacht hat, dass die VM nicht ausgeführt wird.

vm-assert-can-be-recovered

```
vm-assert-can-be-recovered uuid [database] vdi-uuid
```

Prüft, ob Speicher verfügbar ist, um diese VM wiederherzustellen.

vm-call-plugin

```
vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
    value]
```

Ruft die Funktion innerhalb des Plugins auf der angegebenen vm mit optionalen Argumenten auf (args:key=value). Um eine „value“ -Zeichenfolge mit Sonderzeichen (z.B. neue Zeile) zu übergeben, kann eine alternative Syntax args:key:file=local_file verwendet werden, wo der Inhalt von local_file abgerufen und „key“ als Ganzes zugewiesen wird.

vm-cd-add

```
vm-cd-add cd-name=name_of_new_cd device=
    integer_value_of_an_available_vbd [vm-selector=vm_selector_value...]
```

Fügen Sie der ausgewählten VM eine neue virtuelle CD hinzu. Der`device` Parameter sollte aus dem Wert des`allowed-VBD-devices` Parameters der VM ausgewählt werden.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden mithilfe des Standard-auswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

vm-cd-eject

```
vm-cd-eject [vm-selector=vm_selector_value...]
```

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 mithilfe des Standard-auswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

vm-cd-insert

```
vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
```


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 `xe vbd-insert` Befehl 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 mithilfe des Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

vm-cd-list

```
vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

Listet CDs auf, die mit den angegebenen VMs verbunden sind.

Die VM oder 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 VM-Parameter aufgeführten sein.

Sie können auch auswählen, welche VBD- und VDI-Parameter aufgelistet werden sollen.

vm-cd-remove

```
vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

Entfernen Sie eine virtuelle CD von den angegebenen VMs.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-checkpoint

```
vm-checkpoint new-name-label=name_label [new-name-description=
    description]
```

Überprüfen Sie eine vorhandene VM und verwenden Sie den schnellen Festplatten-Snapshot-Vorgang auf Speicherebene, sofern verfügbar.

vm-clone

```
vm-clone new-name-label=name_for_clone [new-name-description=
    description_for_clone] [vm-selector=vm_selector_value...]
```

Klonen Sie eine vorhandene VM mit dem schnellen Festplattenklonvorgang auf Speicherebene, sofern verfügbar. Geben Sie den Namen und die optionale Beschreibung für die resultierende geklonte VM mit den`new-name-label` Argumenten`new-name-description` und an.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-compute-maximum-memory

```
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...]
```

Berechnen Sie die maximale Menge an statischem Speicher, die einer vorhandenen VM zugewiesen werden kann, wobei die Gesamtmenge des physischen Arbeitsspeichers als Obergrenze verwendet wird. Der optionale Parameter`approximate` reserviert genügend zusätzlichen Speicher in der Berechnung, um später zusätzliche vCPUs in die VM hinzuzufügen.

Zum Beispiel:

```
xe vm-compute-maximum-memory vm=testvm total=‘xe host-list params=
    memory-free --minimal‘
```

Dieser Befehl verwendet den Wert des vom`memory-free` Befehl zurückgegebenen`xe host-list` Parameters, um den maximalen Speicher der VM mit dem Namen festzulegen`testvm` .

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-compute-memory-overhead

```
vm-compute-memory-overhead
```


Berechnet den Virtualisierungsspeicher-Overhead einer VM.

vm-copy

```
vm-copy new-name-label=name_for_copy [new-name-description=
    description_for_copy] [sr-uuid=uuid_of_sr] [vm-selector=
    vm_selector_value...]
```

Kopieren Sie eine vorhandene VM, ohne den schnellen Festplattenklonvorgang auf Speicherebene zu verwenden (auch wenn diese Option verfügbar ist). Die Disk-Images der kopierten VM sind garantiert *vollständige Images*, d. h. nicht Teil einer Copy-on-Write-Kette (CoW).

Geben Sie den Namen und die optionale Beschreibung für die resultierende kopierte VM mit den**new-name-label** Argumenten**new-name-description** und an.

Geben Sie die Ziel-SR für die resultierende kopierte VM mit der an`sr-uuid`. Wenn dieser Parameter nicht angegeben wird, ist das Ziel dieselbe SR, in der sich die ursprüngliche VM befindet.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-copy-bios-strings

```
vm-copy-bios-strings host-uuid=host_uuid
```

Kopieren Sie die BIOS-Strings des angegebenen Hosts auf die VM.

vm-crashdump-list

```
vm-crashdump-list [vm-selector=vm selector value...]
```

Listen Sie Crashdumps auf, die den angegebenen VMs zugeordnet 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 mithilfe des Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

vm-data-source-list

```
vm-data-source-list [vm-selector=vm selector value...]
```

Listen Sie die Datenquellen auf, die für eine VM aufgezeichnet werden können.

Select mithilfe des Standardauswahlmechanismus die VMs aus, auf denen dieser Vorgang ausgeführt werden soll. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen VMs ausgeführt.

Datenquellen haben zwei Parameter —`standard` und`enabled` —, die Sie in der Ausgabe dieses Befehls sehen können. Wenn eine Datenquelle auf `enabled` festgelegt ist **`true`**, werden die Metriken derzeit in der Performance-Datenbank aufgezeichnet. Wenn eine Datenquelle auf`standard` festgelegt ist**`true`** , werden die Metriken standardmäßig in der Performance-Datenbank aufgezeichnet (und`enabled` ist auch**`true`** auf diese Datenquelle). `Wenn eine Datenquelle aufstandard festgelegt istfalse, werden die Metriken *nicht* standardmäßig in der Performance-Datenbank aufgezeichnet (undenabledist auch auf falsefür diese Datenquelle).`

Führen Sie den `vm-data-source-record` Befehl aus, um Datenquellen-Metriken in der Performance-Datenbank aufzuzeichnen. Dieser Befehl wird `enabled` auf festgelegt **`true`**. Um zu stoppen, führen Sie den aus `vm-data-source-forget`. Dieser Befehl wird `enabled` auf festgelegt **`false`**.

vm-data-source-record

```
vm-data-source-record data-source=name_description_of_data-source [vm-
    selector=vm selector value...]
```

Zeichnen Sie die angegebene Datenquelle für eine VM auf.

Dieser Vorgang schreibt die Informationen aus der Datenquelle in die Datenbank für persistente Performance-Metriken der angegebenen VMs. Aus Performance-Gründen unterscheidet sich diese Datenbank von der normalen Agent-Datenbank.

Select mithilfe des Standardauswahlmechanismus die VMs aus, auf denen dieser Vorgang ausgeführt werden soll. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können

eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen VMs ausgeführt.

vm-data-source-forget

```
vm-data-source-forget data-source=name_description_of_data-source [vm-
    selector=vm selector value...]
```

Beenden Sie die Aufzeichnung der angegebenen Datenquelle für eine VM und vergessen Sie alle aufgezeichneten Daten.

Select mithilfe des Standardauswahlmechanismus die VMs aus, auf denen dieser Vorgang ausgeführt werden soll. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen VMs ausgeführt.

vm-data-source-query

```
vm-data-source-query data-source=name_description_of_data-source [vm-
    selector=vm_selector_value...]
```

Zeigt die angegebene Datenquelle für eine VM an.

Select mithilfe des Standardauswahlmechanismus die VMs aus, auf denen dieser Vorgang ausgeführt werden soll. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein. Wenn keine Parameter zur Auswahl von Hosts angegeben werden, wird der Vorgang auf allen VMs ausgeführt.

vm-destroy

```
vm-destroy uuid=uuid_of_vm
```

Zerstören Sie die angegebene VM. Dadurch bleibt der mit der VM verknüpfte Speicher intakt. Um den Speicher auch zu löschen, verwenden Sie`xe vm-uninstall`.

vm-disk-add

```
vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-
    selector=vm_selector_value...]
```


Fügen Sie einen Datenträger zu den angegebenen VMs hinzu. Select dendevice Parameter aus dem Wert desallowed-VBD-devices Parameters der VMs.

Der disk-size Parameter kann in Bytes oder mit den IEC-Standardsuffixe KiB, MiB, GiB und TiB angegeben werden.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-disk-list

```
vm-disk-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value
    ...]
```

Listet Datenträger auf, die mit den angegebenen VMs verbunden sind. Dievbd-params Parametervdi-params und steuern die Felder der jeweiligen Objekte, die ausgegeben werden sollen. Geben Sie die Parameter als kommagetrennte Liste oder den speziellen Schlüsselall für die vollständige Liste an.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-disk-remove

```
vm-disk-remove device=integer_label_of_disk [vm-selector=
    vm_selector_value...]
```

Entfernen Sie einen Datenträger von den angegebenen VMs und zerstören Sie ihn.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-export

```
vm-export filename=export_filename [metadata=true|false] [vm-selector=
    vm_selector_value...]
```


Exportieren Sie die angegebenen VMs (einschließlich Disk-Images) in eine Datei auf dem lokalen Computer. Geben Sie mithilfe desfilename Parameters den Dateinamen an, in den die VM exportiert werden soll. Nach der Konvention sollte der Dateiname eine.xva Erweiterung haben.

Wenn dermetadata Parameter lautet**true** , 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 die VM-Informationen neu erstellt werden können. Weitere Informationen finden Sie unter vm-Import.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-import

```
vm-import filename=export_filename [metadata=true|false] [preserve=true
    |false][sr-uuid=destination_sr_uuid]
```

Importieren Sie eine VM aus einer zuvor exportierten Datei. Wenn auf festgelegtpreserve ist**true** , bleibt die MAC-Adresse der ursprünglichen VM erhalten. Dersr-uuid bestimmt die Ziel-SR, in die die VM importiert werden soll. Wenn dieser Parameter nicht angegeben wird, wird der Standard-SR verwendet.

Derfilename Parameter kann auch auf eine VM im XVA-Format verweisen, bei der es sich um das Legacy-Exportformat von Citrix Hypervisor 3.2 handelt. Dieses Format wird von einigen Drittanbietern verwendet, um virtuelle Appliances bereitzustellen. Das XVA-Format verwendet ein Verzeichnis, um die VM-Datenfilename zu speichern. Legen Sie daher auf das Stammverzeichnis des XVA-Exports und nicht auf eine eigentliche Datei. Nachfolgende Exporte des importierten Legacy-Gastes werden automatisch auf das neue Dateiname-basierte Format aktualisiert, in dem viel mehr Daten über die Konfiguration der VM gespeichert werden.

> **Hinweis:**
>
> Das ältere verzeichnisbasierte XVA-Format behält nicht alle VM-Attribute vollständig bei. Insbesondere importierte VMs verfügen standardmäßig über keine virtuellen Netzwerkschnittstellen. Wenn eine Vernetzung erforderlich ist, erstellen Sie eine mitvif-create undvif-plug .

Wenn dies der Fallmetadata ist**true** , können Sie einen zuvor exportierten Satz von Metadaten ohne zugehörige Datenträgerblöcke importieren. Nur-Metadatenimport schlägt fehl, wenn keine VDIs gefunden werden können (benannt nach SR undVDI.location), es sei denn, die--forceOption ist angegeben. In diesem Fall wird der Import unabhängig fortgesetzt. Wenn Datenträger gespiegelt

oder außerhalb des Bandes verschoben werden können, ist der Import/Export von Metadaten eine schnelle Möglichkeit, VMs zwischen separaten Pools zu verschieben. Beispielsweise als Teil eines Disaster Recovery-Plans.

> **Hinweis:**
>
> Mehrere VM-Importe werden seriell schneller ausgeführt, als parallel.

vm-install

```
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]
```

Installieren oder Klonen einer virtuellen Maschine aus einer Vorlage. Geben Sie den Vorlagennamen entweder mit dem`template-uuid` Argument`template` oder an. Geben Sie einen SR mit dem`sr-uuid` Argument`sr-name-label` oder an. Geben Sie an, ob BIOS-gesperrte Medien mit dem`copy-bios-strings-from` Argument installiert werden sollen.

> **Hinweis:**
>
> Bei der Installation von einer Vorlage mit vorhandenen Datenträgern werden standardmäßig neue Datenträger in derselben SR wie diese vorhandenen Datenträger erstellt. Wo der SR es unterstützt, sind diese Festplatten schnelle Kopien. Wenn in der Befehlszeile ein anderer SR angegeben wird, werden dort die neuen Datenträger erstellt. In diesem Fall ist eine schnelle Kopie nicht möglich und die Festplatten sind vollständige Kopien.
>
> Wenn Sie aus einer Vorlage installieren, die keine vorhandenen Datenträger enthält, werden alle neuen Datenträger in der angegebenen SR oder die Poolstandard-SR erstellt, wenn keine SR angegeben wird.

vm-is-bios-customized

```
vm-is-bios-customized
```

Gibt an, ob die BIOS-Zeichenfolgen der VM angepasst wurden.

vm-memory-balloon

```
vm-memory-balloon target=target
```


Legen Sie das Speicherziel für eine ausgeführte VM fest. Der angegebene Wert muss innerhalb des Bereichs liegen, der durch die Werte memory_dynamic_min und memory_dynamic_max der VM definiert wird.

vm-memory-dynamic-range-set

```
vm-memory-dynamic-range-set min=min max=max
```

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 passen.

vm-memory-limits-set

```
vm-memory-limits-set static-min=static_min static-max=static_max
    dynamic-min=dynamic_min dynamic-max=dynamic_max
```

Konfigurieren Sie die Speichergrenzen einer VM.

vm-memory-set

```
vm-memory-set memory=memory
```

Konfigurieren Sie die Speicherzuweisung einer VM.

vm-memory-shadow-multiplier-set

```
vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...] [
    multiplier=float_memory_multiplier]
```

Legen Sie den Schattenspeichermultiplikator für die angegebene VM fest.

Dies ist eine erweiterte Option, die die Menge des *Schattenspeichers* ändert, der einer hardwareunterstützten VM zugewiesen ist.

Bei einigen speziellen Anwendungsarbeitsauslastungen wie Citrix Virtual Apps ist zusätzlicher Schattenspeicher erforderlich, um die volle Leistung zu erzielen.

Dieser Speicher wird als Overhead betrachtet. Es ist von den normalen Speicherberechnungen für die Buchhaltung Speicher zu einer VM getrennt. Wenn dieser Befehl aufgerufen wird, verringert sich die

Menge des freien Hostspeichers entsprechend dem Multiplikator und dasHVM_shadow_multiplier Feld wird mit dem Wert aktualisiert, den Xen der VM zugewiesen hat. Wenn nicht genügend Speicher für den Citrix Hypervisor Server frei ist, wird ein Fehler zurückgegeben.

Die VMs, auf denen dieser Vorgang ausgeführt werden soll, werden mit dem Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren.

vm-memory-static-range-set

```
vm-memory-static-range-set min=min max=max
```

Konfigurieren Sie den statischen Speicherbereich einer VM. Der statische Speicherbereich definiert harte Unter- und Obergrenzen für den Speicher einer VM. Diese Felder können nur geändert werden, wenn eine VM angehalten wird. Der statische Bereich muss den Dynamikbereich umfassen.

vm-memory-target-set

```
vm-memory-target-set target=target
```

Legen Sie das Speicherziel für eine angehalten oder ausgeführte VM fest. Der angegebene Wert muss innerhalb des Bereichs liegen, der durch die Werte memory_static_min und memory_static_max der VM definiert wird.

vm-memory-target-wait

```
vm-memory-target-wait
```

Warten Sie, bis eine ausgeführte VM ihr aktuelles Speicherziel erreicht hat.

vm-migrate

```
vm-migrate [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:=vif_uuid] [vdi=vdi_uuid]
```


Mit diesem Befehl werden die angegebenen VMs zwischen physischen Hosts migriert. Der`host` Parameter kann entweder der Name oder die UUID des Citrix Hypervisor or-Servers sein. Zum Beispiel, um die VM auf einen anderen Host im Pool zu migrieren, auf dem sich die VM-Festplatten auf Speicher befinden, der von beiden Hosts gemeinsam genutzt wird:

```
xe vm-migrate uuid=vm_uuid host-uuid=host_uuid
```

So verschieben Sie VMs zwischen Hosts im selben Pool, die keinen Speicher gemeinsam nutzen (Storage Livemigration):

```
xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \
    remote-username=username remote-password=password \
    host-uuid=desination_host_uuid vdi=vdi_uuid
```

Sie können die SR auswählen, in der jeder VDI gespeichert wird:

```
xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
    vdi1:vdi_1_uuid=destination_sr_uuid \
    vdi2:vdi_2_uuid=destination_sr2_uuid \
    vdi3:vdi_3_uuid=destination_sr3_uuid
```

Darüber hinaus können Sie auswählen, welches Netzwerk die VM nach der Migration angeschlossen werden soll:

```
xe vm-migrate uuid=vm_uuid \
    vdi1:vdi_1_uuid=destination_sr_uuid \
    vdi2:vdi_2_uuid=destination_sr2_uuid \
    vdi3:vdi_3_uuid=destination_sr3_uuid \
    vif:vif_uuid=network_uuid
```

Für die Pool-Migration:

```
xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78
    remote-username=username remote-password=password \
    host-uuid=desination_host_uuid vdi=vdi_uuid
```

Weitere Informationen zu Speicher-Livemigration, Live-Migration und Live-VDI-Migration finden Sie unterMigrieren von VMs.

Standardmäßig wird die VM auf dem anderen Host angehalten, migriert und fortgesetzt. Der`live` Parameter wählt die Live-Migration aus. Bei der Livemigration wird die VM während der Migration ausgeführt, wodurch die Ausfallzeit von virtuellen Rechnern auf weniger als eine Sekunde reduziert wird. Unter bestimmten Umständen, wie z. B. extrem speicherintensive Arbeitslasten in der VM, wird die Livemigration wieder in den Standardmodus versetzt und die VM für kurze Zeit angehalten, bevor die Speicherübertragung abgeschlossen wird.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-pause

```
vm-pause
```

Eine ausgeführte VM anhalten. Beachten Sie, dass dieser Vorgang den zugeordneten Speicher nicht freigibt (siehevm-suspend).

vm-query-services

```
vm-query-services
```

Fragen Sie die Systemdienste ab, die von den angegebenen VMs angeboten werden.

vm-reboot

```
vm-reboot [vm-selector=vm_selector_value...] [force=true]
```

Starten Sie die angegebenen VMs neu.

Die VM oder 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 VM-Parameter aufgeführten sein.

Verwenden Sie dasforce Argument, um einen ungrassigen Neustart zu verursachen. Wo das Herunterfahren dem Ziehen des Steckers auf einem physischen Server ähnlich ist.

vm-recover

```
vm-recover vm-uuid [database] [vdi-uuid] [force]
```

Stellt eine VM aus der Datenbank wieder her, die im mitgelieferten VDI enthalten ist.

vm-reset-powerstate

```
vm-reset-powerstate [vm-selector=vm_selector_value...] {
 force=true }
```

Die VM oder 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 VM-Parameter aufgeführten sein.

Dies ist ein *erweiterter* Befehl, der nur verwendet werden kann, wenn ein Mitgliedshost in einem Pool ausfällt. Sie können diesen Befehl verwenden, um den Poolmaster zu erzwingen, den Energiezustand der VMs zurückzusetzen`halted`. Im Wesentlichen erzwingt dieser Befehl die Sperre für die VM und ihre Festplatten, so dass sie als nächstes auf einem anderen Pool-Host gestartet werden kann. Dieser Aufruf *erfordert, dass* das force-Flag angegeben wird, und schlägt fehl, wenn es sich nicht in der Befehlszeile befindet.

vm-resume

```
vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=
    host_uuid]
```

Setzen Sie die angegebenen VMs fort.

Die VM oder 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 VM-Parameter aufgeführten sein.

Wenn sich die VM in einem gemeinsam genutzten SR in einem Hostpool befindet, geben Sie mit dem`on` Argument an, auf welchem Pool-Mitglied sie gestartet werden soll. Standardmäßig bestimmt das System einen geeigneten Host, der eines der Mitglieder des Pools sein kann.

vm-retrieve-wlb-recommendations

```
vm-retrieve-wlb-recommendations
```

Rufen Sie die Arbeitslastausgleichsempfehlungen für die ausgewählte VM ab.

vm-shutdown


```
vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
```

Fahren Sie die angegebene VM herunter.

Die VM oder 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 VM-Parameter aufgeführten sein.

Verwenden Sie das `force` Argument, um ein ungleichtes Herunterfahren zu verursachen, ähnlich dem Ziehen des Steckers auf einem physischen Server.

vm-snapshot

```
vm-snapshot new-name-label=name_label [new-name-description+
    name_description]
```

Snapshot einer vorhandenen VM, sofern verfügbar, unter Verwendung eines schnellen Festplatten-Snapshot-Vorgangs auf Speicherebene.

vm-snapshot-with-quiesce

```
vm-snapshot-with-quiesce new-name-label=name_label [new-name-
    description+name_description]
```

Snapshot einer vorhandenen VM mit Stillstand, wobei der schnelle Festplatten-Snapshot-Vorgang auf Speicherebene verwendet wird, sofern verfügbar.

vm-start

```
vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=
    host_uuid] [--multiple]
```

Starten Sie die angegebenen VMs.

Die VM oder 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 VM-Parameter aufgeführten sein.

Wenn sich die VMs in einem gemeinsam genutzten SR in einem Hostpool befinden, geben Sie mit demon Argument an, auf welchem Pool-Mitglied die VMs gestartet werden sollen. Standardmäßig bestimmt das System einen geeigneten Host, der eines der Mitglieder des Pools sein kann.

vm-suspend

```
vm-suspend [vm-selector=vm_selector_value...]
```

Anhalten der angegebenen VM.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-uninstall

```
vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
```

Deinstallieren Sie eine VM, indem Sie ihre Festplatten (die VDIs, die als RW gekennzeichnet sind und nur mit dieser VM verbunden sind) sowie deren Metadatendatensatz löschen. Um nur die VM-Metadaten zu zerstören, verwenden Siexe vm-destroy.

Die VM oder 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 VM-Parameter aufgeführten sein.

vm-unpause

```
vm-unpause
```

Heben Sie die Unterbrechung einer angehaltenen VM auf.

vm-vcpu-hotplug

```
vm-vcpu-hotplug new-vcpus=new_vcpu_count [vm-selector=vm_selector_value
    ...]
```


Passen Sie die Anzahl der vCPUs dynamisch an, die für eine laufende PV- oder HVM-Linux-VM verfügbar sind. Die Anzahl der vCPUs wird durch den Parameter begrenztVCPUs-max. Windows VMs werden immer mit der Anzahl der vCPUs ausgeführt VCPUs-max und müssen neu gestartet werden, um diesen Wert zu ändern.

Die PV oder HVM Linux VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden mit dem Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

> **Hinweis:**
>
> Wenn Sie Linux-VMs ohne installierte Citrix VM Tools ausführen, führen Sie den folgenden Befehl auf der VM aus,`root` um sicherzustellen, dass die neu installierten 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

```
vm-vif-list [vm-selector=vm_selector_value...]
```

Listet die VIFs der angegebenen VMs auf.

Die VM oder VMs, auf denen dieser Vorgang ausgeführt wird, werden mithilfe des Standardauswahlmechanismus ausgewählt. Weitere Informationen finden Sie unter VM-Selektoren. Die Selektoren arbeiten beim Filtern auf den VM-Datensätzen und *nicht* auf den VIF-Werten. Optionale Argumente können eine beliebige Anzahl der am Anfang dieses Abschnitts VM-Parameter aufgeführten sein.

Geplante Snapshots

Befehle zum Steuern von VM Shceduled Snapshots und deren Attribute.

Die vmss-Objekte können mit dem Befehl zur Standardobjektauflistung (`xe vmss-list`) und mit den Standardparameterbefehlen manipuliert werden. Weitere Informationen finden Sie unter Low-Level-Parameterbefehle

vmss-create

```
vmss-create enabled=True/False name-label=name type=type frequency=
   frequency retained-snapshots=value name-description=description
   schedule:schedule
```


Erstellt einen Snapshot-Zeitplan im Pool.

Zum 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
```

Snapshot-Zeitpläne haben die folgenden Parameter:

Parametername	Beschreibung	Typ
`name-label`	Name des Snapshot-Zeitplans.	Lese-/Schreibzugriff
`name-description`	Beschreibung des Snapshot-Zeitplans.	Lese-/Schreibzugriff
`type`	Festplatten-Snapshot; Speicher-Snapshot; Stillgestellter Snapshot	Lese-/Schreibzugriff
`frequency`	Stündlich; Täglich; Wöchentlich	Lese-/Schreibzugriff
`retained-snapshots`	Zu behaltende Snapshots. Reichweite: 1-10	Lese-/Schreibzugriff
`schedule`	`schedule:days` (Montag bis Sonntag),`schedule:hours` (0 bis 23),`schedule:minutes` (0, 15, 30, 45)	Lese-/Schreibzugriff

vmss-destroy

```
vmss-destroy uuid=uuid
```

Zerstört einen Snapshot-Zeitplan im Pool.

USB-Durchgang

USB-Passthrough aktivieren/deaktivieren


```
pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
```

USB-Pass-Through aktivieren/deaktivieren.

pusb-scan

```
pusb-scan host-uuid=host_uuid
```

Scannen Sie PUSB und aktualisieren Sie.

vusb-create

```
vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
```

Erstellt einen virtuellen USB im Pool. Starten Sie die VM, um den USB an die VM zu übergeben.

vusb-unplug

```
vusb-unplug uuid=vusb_uuid
```

Entsteckt USB von VM.

vusb-destroy

```
vusb-destroy uuid=vusb_uuid
```

Entfernt die virtuelle USB-Liste von VM.

Kopiert!
Failed!

SDKs und APIs

October 16, 2019

Die folgende Citrix Hypervisor Entwicklerdokumentation ist auf verfügbarhttps://developer-docs.citrix.com/.

- Management-API-Handbuch
- Handbuch zum Software-Entwicklungskit
- Handbuch zur Änderungsblockverfolgung
- Ergänzungspakete und der DDK-Leitfaden

Kopiert!
Failed!

