Citrix Hypervisor 8.2 Product Documentation for Common Criteria [CHPD]

December 9, 2021

1 Edition

Introduction

This document comprises a subset of the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation. This subset excludes some documentation related to features that are not supported in the evaluated configuration. However, this document does still include mentions of features that are not supported in the evaluated configuration. Disregard the documentation that refers to the following features:

Features not included in the evaluated configuration

> **Important:**
>
> The following features are NOT included in the CC evaluated configuration. Using any of these features takes your Citrix Hypervisor deployment out of the evaluated configuration. For more information about the features included in the CC evaluated configuration, see [CH CC ST].

- Heterogeneous Resource Pools
- Active Directory Integration
- Role Based Access Control (RBAC)
- Host BIOS Boot
- SMB Storage
- Software FCoE Storage
- Software-boot-fromiSCSI
- IntelliCache
- vSwitch
- Live migration
- Storage live migration
- vGPU live migration
- Live Memory Checkpoint (Snapshots)
- Dynamic Memory Control (Ballooning)
- High Availability
- GPU Virtualization
- GPU pass-through
- Disaster Recovery
- Health Check
- PVS Accelerator
- Dynamic Workload Balancing & Audit Reporting (WLB)
- Citrix Hypervisor Conversion Manager
- Docker Container Management
- Direct Inspect APIs
- SMT (hyper-threading)
- SNMP

In the CC evaluated configuration, SNMP is turned off. The firewall rules used by dom0 when routing network packets also prevent the use of SNMP.

Full product documentation

The full product documentation for Citrix Hypervisor 8.2 Cumulative Update 1 is available on the web at https://docs.citrix.com/en-us/citrix-hypervisor/. The online documentation is regularly updated.

What's new

About this release

About Cumulative Update 1 (CU1)

About 8.2 LTSR (initial release)

Cumulative Update 1

About this release

Citrix Hypervisor 8.2 CU1 is the first Cumulative Update for the Citrix Hypervisor 8.2 Long Term Service Release (LTSR). This article provides important information about the Citrix Hypervisor 8.2 CU1 release.

Citrix Hypervisor 8.2 CU1 is available in two commercial editions:

- Premium Edition
- Standard Edition

Citrix Hypervisor 8.2 CU1 and its subsequent hotfixes are available only to customers with Customer Success Services.

For Citrix Hypervisor 8.2 LTSR, mainstream support is available until Jun 17, 2025 on the latest cumulative update.

The Citrix Hypervisor 8.2 initial release is supported for six months following the release of Citrix Hypervisor 8.2 CU1. During this time, we will issue critical hotfixes for both Citrix Hypervisor 8.2 and Citrix Hypervisor 8.2 CU1. We will issue any functional hotfixes for Citrix Hypervisor 8.2 CU1 only.

To receive these hotfixes through XenCenter, you must also install the latest version of XenCenter and obtain a client ID. For more information, see Authenticating your XenCenter to receive updates.

Included in Citrix Hypervisor 8.2 CU1

Citrix Hypervisor 8.2 CU1 rolls-up all previously issued Citrix Hypervisor 8.2 hotfixes and simultaneously introduces new fixes for issues reported on Citrix Hypervisor 8.2. For more information, see Fixed issues in Citrix Hypervisor 8.2 CU1.

Some performance or non-functional improvements are also included. For more information, see Improvements in Citrix Hypervisor 8.2 CU1.

To minimize changes within the LTSR product, no additional features are included in Citrix Hypervisor 8.2 CU1

Improvements in Citrix Hypervisor 8.2 CU1

In addition to the rolled-up hotfixes, Citrix Hypervisor 8.2 CU1 includes some performance or non-functional improvements that are available for all licensed LTSR customers.

Support for kdump and kexec in Linux VMs

The `kdump` utility and `kexec` command are now supported on Linux VMs running on Citrix Hypervisor.

Ciphersuite changes

To improve security, weaker ciphersuites have been removed from the list of ciphersuites that are supported for SSH communication. For information about the ciphersuites that are now supported, see Communicate

with Citrix Hypervisor servers and resource pools.

Authenticated download of updates

To provide a more secure service for hotfix downloads, XenCenter now requires that you authenticate it with Citrix to automatically download and apply hotfixes.

To receive these hotfixes through XenCenter, you must also install the latest version of XenCenter and obtain a client ID JSON file. For more information, see Authenticating your XenCenter to receive updates.

XenCenter PuTTY update

The version of PuTTY embedded in XenCenter 8.2.4 is updated to 0.76.

Changes to guest operating system support

Added

Citrix Hypervisor 8.2 CU1 now supports the following new guests:

- Windows Server 2022 (with the latest Citrix VM Tools for Windows)

  > **Note:**
  >
  > At release of Citrix Hypervisor 8.2 Cumulative Update 1, Windows Server 2022 has not been validated on this platform with Server Virtualization Validation Program (SVVP).
  >
  > Windows Server 2022 is supported for production use only with Citrix VM Tools for Windows version 9.2.1 or later installed. You can get the latest version of the Citrix VM Tools for Windows from the Citrix Hypervisor Product Download page

- Rocky Linux 8 (Also available in Citrix Hypervisor 8.2 with latest hotfixes)
- Gooroom 2 (Also available in Citrix Hypervisor 8.2 with latest hotfixes)

Removed

Citrix Hypervisor 8.2 CU1 no longer supports the following guests:

- Windows Server 2012
- Windows Server 2012 R2
- Windows 8.1

Support for new processors

The following processors are now supported in Citrix Hypervisor 8.2 CU1:

- Intel® Xeon® E-23xx and E-23xxG Processors (Rocket Lake)

For more information, see the Hardware Compatibility List.

Compatibility with Citrix Hypervisor 8.2 virtual appliances

You can use the Workload Balancing 8.2 and Conversion Manager 8.2 virtual appliances with your Citrix Hypervisor 8.2 CU1 pool. To use the latest appliances with Citrix Hypervisor 8.2 CU1, ensure you use the latest version of XenCenter provided with Citrix Hypervisor 8.2

For information about the version 8.2 virtual appliances, see the Citrix Hypervisor current release product documentation.

Installation options

Citrix Hypervisor 8.2 CU1 is available to download from the Citrix Hypervisor Product Download page in the following packages:

- **Citrix Hypervisor 8.2 Cumulative Update 1 Installation** comprises only the fixes that make up the cumulative update. Use this ISO to apply the cumulative update to an existing installation of Citrix Hypervisor 8.2.
- **Citrix Hypervisor 8.2 Base Installation ISO including Cumulative Update 1** comprises both a base Citrix Hypervisor 8.2 installation and the fixes that make up the cumulative update. Use this ISO to create a fresh installation of Citrix Hypervisor 8.2 including CU1 or to upgrade from XenServer 7.1 CU2.

The following table shows the available options when moving from an existing version of XenServer or Citrix Hypervisor to Citrix Hypervisor 8.2 CU1.

Installed Version	Update using Citrix Hypervisor 8.2 Cumulative Update 1 ISO	Upgrade or fresh install using Citrix Hypervisor 8.2 Base Installation ISO including Cumulative Update 1
Citrix Hypervisor 8.2	YES	NO
XenServer 7.1 CU2	NO	YES

Note:

Always update the pool master before updating any other servers in a pool.

The latest version of XenCenter is also available to download from Citrix Hypervisor 8.2 download page.

Important:

If you use XenCenter to update your servers, complete the following prerequisites:

1. Update your XenCenter installation to the latest version supplied on the Citrix Hypervisor 8.2 download page before beginning.

2. Obtain a client ID JSON file. For more information, see Authenticating your XenCenter to receive updates.

Before beginning installation, review the System Requirements and Installation.

After installation of Citrix Hypervisor 8.2 CU1, the internal product version number is shown as 8.2.1.

Note:

If you use XenCenter to update your servers, the list of available updates shows both Citrix Hypervisor 8.2 CU1 and any currently released hotfixes for Citrix Hypervisor 8.2 that are not yet applied.

As Citrix Hypervisor 8.2 CU1 includes all the hotfixes released to date, applying it avoids having to install earlier released hotfixes for Citrix Hypervisor 8.2. For more information, see Fixed issues in Citrix Hypervisor 8.2 CU1.

For a period of six months after the release of Citrix Hypervisor 8.2 CU1, there might be further Citrix Hypervisor 8.2 critical hotfixes released that are not included in Citrix Hypervisor 8.2 CU1. These hotfixes will have equivalent hotfixes released for Citrix Hypervisor 8.2 CU1, if required. Customers on Citrix Hypervisor 8.2 can choose to apply the Citrix Hypervisor 8.2 hotfixes or to apply Citrix Hypervisor 8.2 CU1 and the equivalent hotfixes for Citrix Hypervisor 8.2 CU1.

If you choose to use the Automated Updates feature to install updates on Citrix Hypervisor 8.2, it is recommended to update XenCenter to the version available for Citrix Hypervisor 8.2 CU1 first. When Automated Update is selected, the Citrix Hypervisor 8.2 CU1 update and hotfixes available for Citrix Hypervisor 8.2 CU1 are applied. For more details, See Update your servers.

Optional components updated in Citrix Hypervisor 8.2 CU1

The following are new/updated optional components for the Citrix Hypervisor 8.2 CU1 release. All other optional components remain the same as those available with the Citrix Hypervisor 8.2 release.

- XenCenter 8.2.4
- Software Development Kit 8.2.2

Licensing

Upgrade your Citrix License Server to version 11.16 or higher in order to use all Citrix Hypervisor 8.2 licensed features.

Note:

Before upgrading to Citrix Hypervisor 8.2 Cumulative Update 1, ensure that you upgrade your Citrix License Server virtual appliance to the latest available version. Earlier versions of the Citrix License Server virtual appliance run in paravirtualized (PV) mode and are not supported on Citrix Hypervisor 8.2 Cumulative Update 1.

For more information about Citrix Hypervisor 8.2 licensing, see Licensing Overview.

Interoperability with Citrix products

Citrix Hypervisor 8.2 CU1 is interoperable with the following Citrix Virtual Apps and Desktops versions:

- Citrix Virtual Apps and Desktops 2112
- Citrix Virtual Apps and Desktops 1912 LTSR
- Citrix Virtual Apps and Desktops orchestrated by using Citrix Cloud.

We recommend that you use this Citrix Hypervisor LTSR with a Citrix Virtual Apps and Desktops LTSR.

Citrix Hypervisor 8.2 CU1 is also supported with Citrix Provisioning 2112 and 1912 LTSR.

For more information about interoperability with other Citrix products, see the Citrix Upgrade Guide.

Localization support

The localized versions of XenCenter (Simplified Chinese and Japanese) are also available in this release.

Product documentation

To access Citrix Hypervisor 8.2 LTSR product documentation, see Citrix Hypervisor Product Documentation.

What's new since XenServer 7.1

Citrix Hypervisor 8.2 is an LTSR release. If you are on our LTSR stream and are upgrading from XenServer 7.1 CU2, in addition to the features added in Citrix Hypervisor 8.2, you gain all the features that were added in the intervening current releases.

This article contains a list of all new features added since XenServer 7.1 CU2. However, features and capabilities have also been removed since the previous LTSR. For more information about removed and deprecated features, see Deprecations and removals.

Rebranding

Since Citrix Hypervisor 8.0, some of the terms used to describe Citrix Hypervisor products and features have changed. Refer to the following table for the new names.

Previous term	New term
XenServer	Citrix Hypervisor
XenServer PV Tools	Citrix VM Tools
XenMotion	Live migration
Storage XenMotion	Storage live migration
Enterprise Edition	Premium Edition
Free Edition	Express Edition

Platform refresh

The Citrix Hypervisor platform has been updated to use the following software:

- Kernel version: Linux 4.19
- Xen hypervisor version: 4.13.4
- Control domain operating system version: CentOS 7.5

As part of the update to the kernel version, the amount of memory allocated to the control domain (dom0) has increased. For more information, see Memory usage.

The kernel device drivers have also been updated to newer versions. Some hardware that was supported in previous releases might not be compatible with the newer drivers. Before upgrading to Citrix Hypervisor 8.2, check the Hardware Compatibility List.

In addition, the following appliances provided with Citrix Hypervisor have been updated to use CentOS 7.5 as their base operating system:

- Citrix Hypervisor Conversion manager virtual appliance
- Workload Balancing virtual appliance
- Demo Linux virtual appliance

Platform refresh of the Workload Balancing appliance and Conversion Manager appliance

Both of these additional components now include the following improvements:

- Platform updated to CentOS 7.7
- Performance gains from using JSON-RPC to communicate with Citrix Hypervisor
- OpenSSL updated to version 1.1.1
- Other third-party libraries updated for security and performance improvements
- TLS 1.2 is now enforced to ensure security

Changes to processor support

The following processors are now supported:

- Xeon E-23xx and E-23xxG Processors (Rocket Lake)
- Xeon 83xxH(L)/63xxH(L)/53xxH (Cooper Lake SP)
- Xeon 83xx/63xx/53xx/43xx (Ice Lake SP)
- Xeon 82xx/62xx/52xx/42xx/32xx (CascadeLake-SP)
- AMD EPYC 7xx2(P)
- AMD EPYC 7xx3 Zen3 (Milan)

The following legacy processors are no longer supported:

- 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
- Xeon E3/5/7 family - Sandy Bridge
- Xeon E3/5/7 v2 family - Ivy Bridge
- Xeon E-23xx and E-23xxG processors - Rocket Lake

For more information, see the Hardware Compatibility List.

Changes to guest support

Citrix Hypervisor no longer supports guests that run in PV mode. For more information, see Deprecations and removals.

For the full list of supported guest operating systems in Citrix Hypervisor 8.2, see Guest operating system support.

Interoperation

Citrix Hypervisor Entitlement for Citrix Virtual Apps and Desktops Service Subscribers

If you have a Citrix Virtual Apps and Desktops Service cloud subscription that enables the use of on-premises Citrix Virtual Apps and Desktops, you are entitled to use Citrix Hypervisor for hosting these apps and desktops.

With this license you can use all of the same premium features as with an on-premises Citrix Virtual Apps and Desktops entitlement. Download a license through the licensing management tool. Install this license on your License Server to use an on-premises Citrix Hypervisor environment with your Citrix Virtual Apps and Desktops subscription.

Enablement for Citrix Virtual Desktops Tablet Mode (Premium Edition)

Citrix Hypervisor and Citrix Virtual Desktops are the only desktop virtualization solution to enable Windows 10 Continuum experience in a virtualized environment. Citrix Hypervisor, with XenDesktop 7.14 or later, allows you to experience tablet mode.

For information on how to enable Citrix Virtual Desktops tablet mode, see the Citrix Virtual Apps and Desktops documentation.

Citrix Director Integration

You can now use Citrix Director version 7.16 and later to access consoles of Server and Desktop OS machines hosted on your Citrix Hypervisor. This way, Citrix Virtual Apps and Desktops users don't require XenCenter to troubleshoot issues on Citrix Hypervisor-hosted VDAs.

For more information, see the Director documentation.

XenCenter

Authenticated download of updates

To provide a more secure service for hotfix downloads, XenCenter now requires that you authenticate it with Citrix to automatically download and apply hotfixes.

To receive these hotfixes through XenCenter, you must also install the latest version of XenCenter and obtain a client ID JSON file. For more information, see Authenticating your XenCenter to receive updates.

Citrix Hypervisor Conversion Manager console capabilities are now included in XenCenter

In Citrix Hypervisor 8.0 and earlier, a separate Conversion Manager console was provided. This capability is integrated into XenCenter. The legacy Citrix Hypervisor Conversion Manager console has been retired.

The conversion plug-in that was previously included in the Citrix Hypervisor server installation has also been removed. The removal of this plug-in means that you must use the latest version of XenCenter, which includes the conversion capability, with Citrix Hypervisor 8.2. (You cannot use older versions of the Conversion Manager console with Citrix Hypervisor 8.2.)

However, the Conversion Manager virtual appliance is still required for converting VMware VMs to Citrix Hypervisor VMs. This component is provided on the Citrix Hypervisor Product Download page.

For more information, see Convert VMware workloads.

Automatic application of hotfixes during upgrade or update (Premium Edition)

Citrix Hypervisor simplifies the hotfix application mechanism when upgrading your Citrix Hypervisor hosts or pools to a newer version. The enhanced Rolling Pool Upgrade and the Install Update wizards in XenCenter allow you to install available hotfixes when upgrading to a newer version of Citrix Hypervisor. This enables you to bring your standalone hosts or pools up-to-date with a minimum number of reboots at the end.

You must be connected to the internet during the upgrade process for this feature to work. You can benefit from the automatic application of hotfixes feature when you use the latest XenCenter to upgrade between any supported versions of Citrix Hypervisor or XenServer.

XenCenter: Host Status Visibility

Improvements in XenCenter make it easier to see the licensing status and patching status of your Citrix Hypervisor hosts and pools.

You can now see the licensing status of your hosts and pools in the title bar for the host or pool. Unlicensed pools also show an icon in the tree view. The **Updates** tab can now show the available updates for your hosts sorted by server. This makes it simpler to see the patching status of all your hosts and pools.

XenCenter alerts for end of life or end of support

XenCenter now alerts you when the version of your managed Citrix Hypervisor servers is approaching end of life or reaches end of life. For more information, see XenCenter Alerts.

XenCenter also alerts you when a Current Release or Cumulative Update is approaching or has passed a date when there will be no further hotfixes issued for that release. Act upon this information and update your environment to a later supported release, to ensure that updates to address any future functional and security related issues can be applied.

Enable and disable read caching from within XenCenter

The read caching feature improves performance on NFS, EXT3/EXT4, or SMB SRs that host multiple VMs cloned from the same source. This feature can now be enabled and disabled for each individual SR from the XenCenter console. You might want to disable read caching in the following cases:

- You have no file-based SRs
- You do not have any cloned VMs
- You have insufficient memory available to allocate to dom0 to derive any performance benefits

For more information, see Changing SR Properties.

XenCenter Scalability Improvements

The latest XenCenter offers significant improvements in UI responsiveness for customers with large-scale Citrix Hypervisor deployments. This enables customers to better manage their environments when dealing

with many pools and VMs.

XenCenter Proxy Authentication

XenCenter already allows the configuration of a proxy server to access the Internet. The latest version of XenCenter adds the ability to specify a user name and password to connect to the proxy server, if the proxy server requires authentication.

Localization for Email Performance Alerts

XenCenter adds the ability to receive performance alert emails in your preferred language. The languages available are English, Simplified Chinese, and Japanese.

VMs

Guest UEFI boot and Secure Boot

Citrix Hypervisor enables VMs running Windows 10 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit), or Windows Server 2022 (64-bit) to boot in UEFI mode. UEFI boot provides a richer interface for the guest operating systems to interact with the hardware, which can significantly reduce Windows VM boot times.

For these Windows operating systems, Citrix Hypervisor also supports Windows Secure Boot. Secure Boot prevents unsigned, incorrectly signed or modified binaries from being run during boot. Secure Boot also reduces the risk that malware in the guest can manipulate the boot files or run during the boot process.

For more information, see Windows VMs.

Scheduled Snapshots

The scheduled snapshots feature provides an easy-to-use backup and restore utility for critical VMs. This enables customers to configure their environment to automatically create VM snapshots at specified intervals. This helps guard against unforeseen data corruption issues, system crashes, or user errors, by providing a last-known working version of the VM.

BIOS Asset Tags

You can now use the xe CLI or the API to specify BIOS asset tags on a per VM basis. This enables you to track assets more easily and leads to smoother management and licensing.

Support for kdump and kexec in Linux VMs

The `kdump` utility and `kexec` command are now supported on Linux VMs running on Citrix Hypervisor.

Graphics

Multiple vGPU (Premium Edition)

For NVIDIA GPUs and drivers that support multiple vGPU, you can configure a single VM to use multiple virtual GPUs concurrently. These additional vGPUs can be used to perform computational processing. Only certain vGPU profiles can be used and all vGPUs attached to a single VM must be of the same type.

For more information, see Graphics Overview.

Support for disk and memory snapshots for vGPU-enabled VMs (Premium Edition)

When a disk and memory snapshot of a vGPU-enabled VM is taken the state of the VM includes the vGPU state. This vGPU state is restored when the VM is resumed from the snapshot.

vGPU live migration (Premium Edition)

You can migrate VMs with vGPUs between hosts without shutting the VMs down, allowing administrators to take advantage of live migration with vGPUs attached. vGPU live migration is available for supported software and graphics cards from GPU vendors. For more information, see the Hardware Compatibility List.

In addition to live migration, storage live migration and VM suspend with vGPUs attached have also been enabled in this release for VMs using supported software and graphics cards.

AMD MxGPU (Premium Edition)

With the addition of support for AMD's virtualized graphics solution, Citrix Hypervisor continues its leadership in the virtualized graphics domain.

Building on our first-to-market partnerships with NVIDIA vGPU and Intel GVT-g, Citrix Hypervisor becomes the only hypervisor platform to support the virtualization solutions of all three graphics vendors. Citrix Hypervisor customers can use AMD MxGPU on 64-bit versions of Windows 10, Windows Server 2016, and Windows Server 2019 VMs.

With the addition of support for AMD's virtualized graphics solution, Citrix Hypervisor continues its leadership in the virtualized graphics domain. Citrix Hypervisor customers can use AMD MxGPU on provided by the AMD FirePro S7100-series GPUs. See the list of supported hosts on the Hardware Compatibility List.

Storage

Changed Block Tracking (Premium Edition)

Changed block tracking provides a set of features and APIs that enable third-party software vendors to develop fast and space-efficient incremental backup solutions.

With changed block tracking, you need less disk space because, instead of handling and storing large VDIs, you can store space-efficient metadata-only snapshot files.

For more information, see Changed Block Tracking.

Thin provisioning for shared block storage - GFS2 (Premium Edition)

Citrix Hypervisor makes thin provisioning available to customers using block-based storage accessed through an iSCSI software initiator or Hardware HBA. Thin provisioning is implemented by using GFS2.

Thin provisioning makes better use of the available storage by allocating disk storage space to VDIs because data is written to the virtual disk, rather than allocating the full virtual size of the VDI in advance. Thin provisioning enables you to significantly reduce the amount of space required on a shared storage array, and with that your Total Cost of Ownership (TCO).

The following use cases can benefit from thin provisioning:

- Server virtualization
- Citrix Virtual Apps and Desktops (both persistent and non-persistent)
- Large-scale Cloud deployments

Thin provisioning for shared block storage is of particular interest in the following cases:

- If you want increased space efficiency, because images are sparsely and not thickly allocated.
- If you want to reduce the number of I/O operations per second on your storage array. The GFS2 SR is the first SR type to support storage read caching on shared block storage.
- If you use a common base image for multiple virtual machines, because the images of individual VMs then typically use even less space.
- If you use snapshots, because each snapshot is an image and each image is now sparse.

For more information, see GFS2.

Create VDIs greater than 2 TiB (Premium Edition)

You can also create virtual disk images on GFS2 SRs that are larger than the previous 2 TiB limit.

Primary disks for Windows VMs are in Master Boot Record (MBR) format. MBR limits the maximum addressable storage space of a disk to 2 TiB. To use a greater than 2 TiB disk for a Windows VM, create it as the secondary disk for the VM and select GUID Partition Table (GPT) format

Support for SMB version 3 for ISO SRs

Citrix Hypervisor now supports SMB version 3 as the default method of connecting to ISO SRs. SMB version 3 is more secure and robust than SMB version 1.0.

SMB version 1.0 is still supported and Citrix Hypervisor can fall back to using this protocol version if version 3 is not available. You can mount ISO SR using SMB version 1.0 using the CLI. However, we recommend that you use SMB version 3 where it is available.

Performance improvements

Increased configuration limits

The following configuration limits have been increased:

- The maximum host RAM is now 6 TB
- The maximum number of logical processors per host is now 448 CPUs

For more information, see Configuration limits.

Supported Pool Size Increased to 64

Citrix Hypervisor now supports up to a maximum of 64 hosts in a pool. Increased pool size helps in a more efficient management of VMs and provides greater flexibility when using High Availability.

Note:

> This feature is not available to users of the Express Edition.

Improved performance for VM imports and exports that use the XVA format

Changes to the checksum used in XVA files in Citrix Hypervisor 8.1 provided significant performance improvements when importing or exporting VMs using this new checksum algorithm.

The reduction in the time it takes to import or export a VM depends on the specific hardware of the machine. The larger the VM the larger the performance improvement seen.

Use the latest XenCenter to manage exported VMs that use XVA files with the new checksum algorithm.

If you have a custom application that relies on the format of the checksum included in the XVA file, update your application to use the new format. The checksum has changed to use the xxHash algorithm. The checksum file name now ends with the extension `.xxhash`.

Storage performance improvements

Storage performance is significantly improved when I/O is performed in block sizes larger than 64 KiB on an NFS SR.

Multipage support is now available in non-GFS2 SRs for better storage performance. If your Windows VM has the Citrix VM Tools installed, the VM uses multipage support automatically.

To enable multipage support on a Linux VM complete the following steps:

1. First, verify that your kernel supports the max_ring_page_order parameter. Run the following command:

   ```
   modinfo xen_blkfront | grep max_ring_page_order
   ```

   If this command returns an empty response, your kernel does not support this feature. Do not proceed with these steps.

2. Take a snapshot of your VM.

3. On the VM, run the following command:

   ```
   echo 'options xen_blkfront max_ring_page_order=3'
   >/etc/modprobe.d/xen_blkfront.conf
   ```

4. Depending on your Linux distribution, run one of the following commands:

   - For RHEL, CentOS, or Oracle Enterprise Linux: `dracut -f -v`
   - For Debian-based distributions: `update-initramfs -u -k all`

5. Reboot your VM.

New Windows I/O drivers with improved performance

Updated Windows I/O drivers with the major version 9 (9.x.x.x) include several performance improvements. For more information, see Updates to Citrix VM Tools for Windows.

XenCenter, C# SDK, and PowerShell module performance improvements

XenCenter, the C# SDK, and the PowerShell module now use JSON-RPC instead of XML-RPC to communicate with the Citrix Hypervisor host. This change improves the performance when interacting with Citrix Hypervisor, especially when connecting to a pool.

Security improvements

Install a TLS certificate on your Citrix Hypervisor server

Citrix Hypervisor now enables easy installation of server TLS certificates.

The Citrix Hypervisor server comes installed with a default TLS certificate. However, to use HTTPS to secure communication between Citrix Hypervisor and Citrix Virtual Apps and Desktops, you must install a new certificate. The certificate authority issuing the certificate must be trusted by the Citrix Virtual Apps and Desktop installation.

This feature provides a mechanism to update host certificates that does not require the user to have access to the Citrix Hypervisor server file system. It also verifies that the certificate and key files are valid and in the correct format.

You can install a TLS certificate on the Citrix Hypervisor server by using one of the following methods:

- XenCenter. For more information, see Install a TLS certificate on your server in the XenCenter documentation.
- xe CLI. For more information, see Install a TLS certificate on your server.
- API. For more information, see the Management API guide.

This feature also provides XenCenter alerts when a server TLS certificate is about to expire. For more information, see System Alerts in the XenCenter documentation.

Enforcing use of the TLS 1.2 protocol

Citrix Hypervisor now enforces the use of the TLS 1.2 protocol for any HTTPS traffic between Citrix Hypervisor and an external network. All Citrix Hypervisor components use the TLS 1.2 protocol when communicating with each other.

As part of this feature the legacy SSL mode and support for the TLS 1.0/1.1 protocol have been removed. Ensure you disable legacy SSL mode in your pools before upgrading or updating them to Citrix Hypervisor 8.2. If you have any custom scripts or clients that rely on a different protocol, update these components to use TLS 1.2.

Bromium Enhanced Security (Premium Edition)

You can use Bromium Secure Platform (now HP Sure Click Enterprise) on Windows VMs running on Citrix Hypervisor.

Bromium Secure Platform provides protection at the endpoint against all advanced malware. This protection is transparent to the end user and has no impact on user experience or system performance. For more information about the advantages of Bromium Enhanced Security, see the Bromium website.

Ciphersuite changes

To improve security, weaker ciphersuites have been removed from the list of ciphersuites that are supported for SSH communication. For information about the ciphersuites that are now supported, see .

General

Disaggregation of the Citrix VM Tools

The Citrix VM Tools are now provided as two separate components on the Citrix Hypervisor download page:

- Citrix VM Tools for Windows
- Citrix VM Tools for Linux

As a result, the `guest-tools.iso` file has been removed from the Citrix Hypervisor installation.

Providing the tools as a separate component removes the need for hotfixes to apply updates to a tools ISO stored on the Citrix Hypervisor server.

For more information, see Linux VMs and Windows VMs.

Networking SR-IOV: Passthrough of Virtual Functions (Premium Edition)

Citrix Hypervisor can now use Single Root I/O Virtualization (SR-IOV) that allows a single PCI device to appear as multiple PCI devices on the physical system.

You can assign one or more NIC Virtual Functions to a VM, allowing its network traffic to bypass the virtual switch. When configured, each VM behaves as though it is using the NIC directly, reducing processing overhead, and improving performance. For more information, see Using SR-IOV enabled NICs.

USB Passthrough (Premium Edition)

Citrix Hypervisor now supports passing through individual, physical USB devices to a VM. The VM's OS can use the physical USB device as a local USB device.

IGMP Snooping for IPv4 Multicast Support (Premium Edition)

You can now use IPv4 multicast to send data to VMs that are members of a multicast group built by using the IGMP protocol.

When enabled, this feature prevents multicast traffic being sent to all VMs and causing unnecessary load on host devices by requiring them to process packets they have not solicited. Instead, when multicast traffic comes into the Citrix Hypervisor host, Citrix Hypervisor detects the group of this traffic and forwards the traffic to guest VMs that subscribe to this group. This feature improves the performance of multicast and is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

VLAN Tagging

Citrix Hypervisor supports VLAN tagging on management and storage interfaces. You can create a pool of Citrix Hypervisor hosts to communicate on a VLAN network.

Additionally, you can upgrade or perform a fresh installation of the Citrix Hypervisor host to your management interface on a tagged VLAN. This enables you to provision your Citrix Hypervisor host management interface on a tagged VLAN network and access the host on the same VLAN network.

New structure for the product documentation

The Citrix Hypervisor product documentation is now provided as an HTML documentation set instead of PDFs.

- Use the table of contents on the left to navigate to the information that you need
- Use the search box in the top-right to search for specific information
- See an outline of the information in each article in the ‘In this article' box
- Download all content as a PDF for offline viewing by using the ‘View PDF' button

All information from the PDF guides is included in the new documentation structure. For example, content from the *Installation Guide* is available in the **Install** section and content from the *VM User's Guide* is available in the **VMs** section. The main subjects in the *Administrator's Guide* are not included in a separate ‘Administer' section and are instead listed in the table of contents.

Web-based help for XenCenter

Documentation for XenCenter is now available online at the Citrix Product Documentation website.

This online documentation replaces the in-product help. Now, when you press F1 in the UI or choose to access contextual help, the relevant article opens in your default browser. These articles are also available as a PDF for offline viewing. Use the **View PDF** button to download the PDF.

These web-based articles offer you the most accurate and up-to-date content.

Fixed issues

Rolled up Hotfixes in CU1

Citrix Hypervisor 8.2 Cumulative Update 1 includes the following Citrix Hypervisor 8.2 hotfixes:

- XS82E001 - https://support.citrix.com/article/CTX277444
- XS82E002 - https://support.citrix.com/article/CTX285938
- XS82E003 - https://support.citrix.com/article/CTX280214
- XS82E004 - https://support.citrix.com/article/CTX284749
- XS82E005 - https://support.citrix.com/article/CTX281575
- XS82E006 - https://support.citrix.com/article/CTX285536
- XS82E007 - https://support.citrix.com/article/CTX283446
- XS82E008 - https://support.citrix.com/article/CTX283510
- XS82E009 - https://support.citrix.com/article/CTX283516
- XS82E010 - https://support.citrix.com/article/CTX285172
- XS82E011 - https://support.citrix.com/article/CTX286459
- XS82E012 - https://support.citrix.com/article/CTX286796
- XS82E013 - https://support.citrix.com/article/CTX286800
- XS82E014 - https://support.citrix.com/article/CTX286804
- XS82E015 - https://support.citrix.com/article/CTX292897
- XS82E016 - https://support.citrix.com/article/CTX292625
- XS82E017 - https://support.citrix.com/article/CTX294145
- XS82E018 - Limited Availability
- XS82E019 - Limited Availability
- XS82E020 - https://support.citrix.com/article/CTX313808
- XS82E021 - https://support.citrix.com/article/CTX306540
- XS82E022 - https://support.citrix.com/article/CTX306423
- XS82E023 - https://support.citrix.com/article/CTX312232
- XS82E024 - https://support.citrix.com/article/CTX306481
- XS82E025 - https://support.citrix.com/article/CTX310674
- XS82E026 - https://support.citrix.com/article/CTX313807
- XS82E028 - https://support.citrix.com/article/CTX318325
- XS82E029 - https://support.citrix.com/article/CTX319717
- XS82E030 - https://support.citrix.com/article/CTX322578
- XS82E031 - https://support.citrix.com/article/CTX327907
- XS82E032 - https://support.citrix.com/article/CTX324257
- XS82E033 - https://support.citrix.com/article/CTX328166
- XS82E034 - https://support.citrix.com/article/CTX330706

Additional issues fixed in CU1

General

- When multiple VMs start at the same time, Workload Balancing recommends balancing the VMs placement on all servers in the pool evenly. However, sometimes Workload Balancing might

recommend putting many VMs on the same Citrix Hypervisor server. This issue occurs when Workload Balancing gets late feedback from XAPI about VM placement. (CA-337867)

- A runaway process that logs excessively can fill the log partition and prevent log rotation. This issue is resolved by rotating the log files before they exceed 100MB. (CA-356624)
- When installing Citrix Hypervisor on a system with the HBA355i Adapter Card the system hangs on the install screen. (CA-357134)
- The DNS settings in xsconsole are not retained after host reboot. (CA-355872)
- If an SR scan reports errors during SR attach, the attach process can fail. (CA-355401)
- You cannot use snapshots for VMs located on an NFS SR provided by a Tintri VMstore file system. (CA-359453)
- Under certain conditions the tapdisk process for a VM can crash when updating performance statistics. (CA-355145)

Guests

- On some servers, VMs with GPU/PCI passthrough configured can fail to boot and log the error; "Operation not permitted." (CA-356386)
- [Fixed in the latest Citrix VM Tools for Linux] If you attempt to install the Citrix VM Tools for Linux on a fully up-to-date CentOS 8 system, you see the error: `Fatal Error: Failed to determine Linux distribution and version`. This is caused by changes in that CentOS 8 updates release on Dec 08, 2020. To work around this issue, specify the OS when installing the Citrix VM Tools for Linux: `./install.sh -d centos -m 8`. However, if you use this workaround, the operating system information is not reported back to the Citrix Hypervisor server and does not appear in XenCenter. (CA-349929)
- The `kdump` utility and `kexec` command are now supported on Linux VMs running on Citrix Hypervisor. (CP-24801)

XenCenter

- If you have FIPS compliance enabled on the system where XenCenter is installed, you cannot import or export VMs in OVF/OVA format or import Virtual Hard Disk images. (CA-340581)
- When using XenCenter to upgrade pools in parallel and apply all released hotfixes after the upgrade, the hotfix files can be downloaded multiple times. This can cause a delay in hotfix application and increase the amount of downloaded data. (CA-359700)

8.2 LTSR (Initial release)

About this release

Citrix Hypervisor is a high-performance hypervisor optimized for virtual app and desktop workloads and based on the Xen Project hypervisor.

Citrix Hypervisor 8.2 is a Long Term Service Release which seeks to maximize stability in terms of the feature set.

Citrix Hypervisor 8.2 is available in the following editions:

- Premium Edition
- Standard Edition

For information about the features available in each edition, see the Citrix Hypervisor Feature Matrix.

New features and improvements in Citrix Hypervisor 8.2

Citrix Hypervisor 8.2 introduces enhanced features and functionality for application, desktop, and server virtualization use cases. All Citrix Hypervisor 8.2 features are available to all licensed Citrix Virtual Apps and Desktops customers.

Increased configuration limits

The following configuration limits have been increased:

- The maximum host RAM is now 6 TB
- The maximum number of logical processors per host is now 448 CPUs

For more information, see Configuration limits.

Enable and disable read caching from within XenCenter

The read caching feature improves performance on NFS, EXT3/EXT4, or SMB SRs that host multiple VMs cloned from the same source. This feature can now be enabled and disabled for each individual SR from the XenCenter console. You might want to disable read caching in the following cases:

- You have no file-based SRs
- You do not have any cloned VMs
- You have insufficient memory available to allocate to dom0 to derive any performance benefits

For more information, see Changing SR Properties.

Changes to guest operating system support

The set of guest operating systems that Citrix Hypervisor supports has been updated. For more information, see Guest operating system support.

Added

Citrix Hypervisor now supports the following additional guest operating systems:

- SUSE Linux Enterprise Server 12 SP5 (64-bit)
- Ubuntu 20.04 (64-bit)
- Gooroom 2 (64-bit) - requires Hotfix XS82E021 - For Citrix Hypervisor 8.2

Removed

- Windows 7
- Windows Server 2008 SP2
- Windows Server 2008 R2 SP1

Changes to processor support

The following processors are now supported:

- Xeon 83xxH(L)/63xxH(L)/53xxH (Cooper Lake SP)
- Xeon 83xx/63xx/53xx/43xx (Ice Lake SP)
- AMD EPYC 7xx3 Zen3 (Milan)

To get the full benefits of these processors, ensure that you install the latest hotfixes for Citrix Hypervisor 8.2.

For more information, see the Hardware Compatibility List.

Security improvements

Install a TLS certificate on your Citrix Hypervisor server

Citrix Hypervisor now enables easy installation of server TLS certificates.

The Citrix Hypervisor server comes installed with a default TLS certificate. However, to use HTTPS to secure communication between Citrix Hypervisor and Citrix Virtual Apps and Desktops, you must install a new certificate. The certificate authority issuing the certificate must be trusted by the Citrix Virtual Apps and Desktop installation.

This feature provides a mechanism to update host certificates that does not require the user to have access to the Citrix Hypervisor server file system. It also verifies that the certificate and key files are valid and in the correct format.

You can install a TLS certificate on the Citrix Hypervisor server by using one of the following methods:

- XenCenter. For more information, see Install a TLS certificate on your server in the XenCenter documentation.
- xe CLI. For more information, see Install a TLS certificate on your server.
- API. For more information, see the Management API guide.

This feature also provides XenCenter alerts when a server TLS certificate is about to expire. For more information, see System Alerts in the XenCenter documentation.

Enforcing use of the TLS 1.2 protocol

Citrix Hypervisor now enforces the use of the TLS 1.2 protocol for any HTTPS traffic between Citrix Hypervisor and an external network. All Citrix Hypervisor components use the TLS 1.2 protocol when communicating with each other.

As part of this feature the legacy SSL mode and support for the TLS 1.0/1.1 protocol have been removed. Ensure you disable legacy SSL mode in your pools before upgrading or updating them to Citrix Hypervisor 8.2. If you have any custom scripts or clients that rely on a different protocol, update these components to use TLS 1.2.

Disaggregation of the Citrix VM Tools

The Citrix VM Tools are now provided as two separate components on the Citrix Hypervisor download page:

- Citrix VM Tools for Windows
- Citrix VM Tools for Linux

As a result, the `guest-tools.iso` file has been removed from the Citrix Hypervisor installation.

Providing the tools as a separate component removes the need for hotfixes to apply updates to a tools ISO stored on the Citrix Hypervisor server.

For more information, see Linux VMs and Windows VMs.

Updates to the Workload Balancing appliance and Conversion Manager appliance

Both of these additional components now include the following improvements:

- Platform updated to CentOS 7.7
- Performance gains from using JSON-RPC to communicate with Citrix Hypervisor
- OpenSSL updated to version 1.1.1
- Other third-party libraries updated for security and performance improvements
- TLS 1.2 is now enforced to ensure security

Installation options

Citrix Hypervisor 8.2 is available to download from the Citrix Hypervisor Product Download page in the following packages:

- Citrix Hypervisor 8.2 Update ISO. Use this file to apply Citrix Hypervisor 8.2 as an update to Citrix Hypervisor 8.1 or 8.0.
- Citrix Hypervisor 8.2 Base Installation ISO. Use this file to create a fresh installation of Citrix Hypervisor 8.2 or to upgrade from XenServer 7.1 CU2 or 7.0.

Important:

- If you use XenCenter to upgrade your hosts, update your XenCenter installation to the latest version supplied on the Citrix Hypervisor 8.2 download page before beginning.
- Always upgrade the pool master before upgrading any other hosts in a pool.

- Ensure that you update your XenServer 7.1 to Cumulative Update 2 before attempting to upgrade to Citrix Hypervisor 8.2.
- Legacy SSL mode is no longer supported. Disable this mode on all hosts in your pool before attempting to upgrade to the latest version of Citrix Hypervisor. To disable legacy SSL mode, run the following command on your pool master before you begin the upgrade: `xe pool-disable-ssl-legacy uuid=<pool_uuid>`
- The Container Management supplemental pack is no longer supported. After you update or upgrade to the latest version of Citrix Hypervisor, you can no longer use the features of this supplemental pack.
- The vSwitch Controller is no longer supported. Disconnect the vSwitch Controller from your pool before attempting to update or upgrade to the latest version of Citrix Hypervisor.

  1. In the vSwitch controller user interface, go to the **Visibility & Control** tab.
  2. Locate the pool to disconnect in the **All Resource Pools** table. The pools in the table are listed using the IP address of the pool master.
  3. Click the cog icon and select **Remove Pool**.
  4. Click **Remove** to confirm.

  After the update or upgrade, the following configuration changes take place:

  - Cross-server private networks revert to single-server private networks.
  - Any Quality of Service settings made through the DVSC console are no longer applied. Network rate limits are no longer enforced.
  - ACL rules are removed. All traffic from VMs is allowed.
  - Port mirroring (RSPAN) is disabled.

  After update or upgrade, if you find any leftover state about the vSwitch Controller in your pool, clear the state with the following CLI command: `xe pool-set-vswitch-controller address=`

Before you start

Before beginning installation or migrating from an older version, review the following articles:

- System requirements
- Known issues
- Deprecations and removals

For information about the installation, upgrade, or update process, see Install

Licensing

Customers must upgrade their Citrix License Server to version 11.16 or higher to use all Citrix Hypervisor 8.2 licensed features.

For more information about Citrix Hypervisor 8.2 licensing, see Licensing.

Hardware compatibility

For the most recent additions and advice for all hardware compatibility questions, see the Citrix Hypervisor Hardware Compatibility List.

If you have VMs with attached virtual GPUs, ensure that supported drivers are available before upgrading to the latest release of Citrix Hypervisor. For more information, see both the Hardware Compatibility List and the GPU vendor documentation.

Interoperability with Citrix products

Citrix Hypervisor 8.2 is interoperable with Citrix Virtual Apps and Desktops 7.15 LTSR, 1912 LTSR, and 2006.

Citrix Hypervisor 8.2 is interoperable with Citrix Provisioning 7.15 LTSR, 1912 LTSR, and 2006.

Citrix Hypervisor 8.2 is interoperable with Citrix Cloud.

For more information about interoperability with other Citrix products, see the Citrix Upgrade Guide.

Localization support

The localized version of XenCenter (Simplified Chinese and Japanese) is also available in this release. In previous releases, the localized version of XenCenter was provided as a separate component. In Citrix Hypervisor 8.2 and later, all localized version of XenCenter are contained in the same `.msi` installation file as the English version.

Product documentation

To access Citrix Hypervisor 8.2 product documentation, see Citrix Hypervisor 8.2 Product Documentation.

To access the latest XenCenter product documentation, see XenCenter Product Documentation.

Documentation can be updated or changed after the initial release. We suggest that you subscribe to the Document History RSS feed to learn about updates.

Fixed issues

This article lists issues present in previous releases that are fixed in this release.

General

- On Citrix Hypervisor 8.1 systems that were updated from Citrix Hypervisor 8.0, after XAPI restart you might see errors from the following services:

  - `usb-scan.service`
  - `storage-init.service`
  - `xapi-domains.service`
  - `mpathcount.service`
  - `create-guest-templates.service`

  The errors in these services can present various different issues, for example, VMs that have been configured to start automatically might not start. The cause of this issue is `xapi-wait-init-complete.service` not being enabled. (CA-333953)

- Improvements to boot time, memory accounting, and stability of Citrix Hypervisor on systems with large amount of RAM. (CP-33195)

- A system with a software FCoE connection might experience a persistent memory leak in the Dom0 kernel. This memory leak eventually results in a host crash, sudden loss of connectivity, or other issue. (CA-332618)

- Some of the methods that take a DateTime parameter in the C# SDK and the corresponding PowerShell module cmdlets fail with an internal error. (CA-333871)

- USB passthrough does not work with version 2.00 devices with a speed less than or equal to 12 Mbps. (CA-328130)

- In rare error conditions, the XAPI process on the pool master can leak file descriptors for stunnel connections. This issue can cause the pool to become non-operational. (CA-337546)

- If there is malformed or unexpected content in the `/etc/passwd` or `/etc/group` file on your server, an upgrade from an earlier version of XenServer to Citrix Hypervisor 8.1 can fail. (CA-336696)

- When shutting down the system, a crash might occur and the system is rebooted instead. (CA-334114)

- If you have previously attempted to install the incorrect version of a driver disk, subsequent driver disk installations can fail because of data remaining in the yum cache. (CA-330961)

- Sometimes the RRD metrics related to VBDs that Workload Balancing collects from the Citrix Hypervisor control domain can be in an incorrect format. Workload Balancing now ignores incorrectly formatted metrics, collects the metrics again, and sends a WARNING log. (CA-335950)

Guests

- When installing Citrix VM Tools on a Windows VM, the installation might fail with the following error message: `Service 'Citrix XenServer Windows Management Agent' (XenSvc) could not be installed. Verify that you have sufficient privileges to install system services.` Work around this issue by uninstalling the Citrix VM Tools, rebooting the VM, and then installing the new tools.
- On CentOS 8 VMs with the Citrix VM Tools installed, boot times can be slow. (CA-333687)
- A VM migration from a pool member that takes more than 12 hours can fail with a connection reset error. This failure is a caused by an idle connection between the pool master and the pool member timing out. (CA-333610)
- If the Management Agent is installed on your Windows VM, attempting to copy more than 1 MB of text to the clipboard can cause your VM to become unresponsive. (CA-326354)
- When objects such as SRs are destroyed, their RRDs are not removed from memory, which can cause memory usage to grow over time. (CA-325582)

Storage

- When running Reclaim Space on a thinly provisioned LUN with more than 2 TB of free space, the operation fails with an `ioctl not supported` error. (CA-332782)
- Creating a VDI with Unicode characters in either the name or description causes the database backup script to fail with an error on a GFS2 SR. (CA-335367)
- The `xcp-rrdd-iostat` daemon does not recognize VDIs associated with IntelliCache as valid, causing spam in its log file: `Could not file device with physical path...` (CA-144246)

XenCenter

- When creating an LVM SR from XenCenter and passing CHAP credentials, the operation might fail with an authentication error. (CA-337280)

Improvements

- Greater tolerance for I/O during the leaf coalesces. This change benefits to customers who are taking regular snapshots on active VMs. (CP-32204)
- Greater tolerance for coalescing large leaves. This change benefits customers who have fast storage. (CP-32204)
- The xe CLI client that can be installed on a remote Windows or Linux system contains the following improvements:
    - The xe CLI client can now only upload configuration files that are less than 32 MiB
    - The xe CLI client only uploads or downloads files listed in the original command line arguments
    - Diagnostics xe CLI commands are limited to users with the Pool Admin or Pool Operator role

  Update the version of the xe CLI on your remote systems to the latest version provided with Citrix Hypervisor 8.2.

- The read and write latency per device metrics give us the average latency per operation. Previously, this average was taken over all operations ever performed. The average is now taken over the preceding five seconds. This change fixes an issue where the metrics showed constant read or write latencies when no disk operations were in progress. (CA-336067)

Known issues

This article contains advisories and minor issues in the Citrix Hypervisor 8.2 release and any workarounds that you can apply.

General

- If you host the Citrix License Server virtual appliance version 11.14 or earlier on your Citrix Hypervisor server, you see a warning when upgrading or updating to Citrix Hypervisor 8.2 Cumulative Update 1. The warning states that this virtual appliance is a PV VM that is no longer supported. You must uninstall this version of the Citrix License Server virtual appliance and instead install the latest version before upgrading or updating.

  The latest version of the Citrix License Server virtual appliance is available from the

- If your Citrix Hypervisor servers run on hardware containing Intel Sandy Bridge family CPUs, shut down and restart your VMs as part of updating or upgrading to Citrix Hypervisor 8.2 from Citrix Hypervisor 8.0 or earlier. For more information, see https://support.citrix.com/article/CTX231947. (CP-32460)

- A pool's CPU feature set can change while a VM is running. (For example, when a new host is added to an existing pool, or when the VM is migrated to a host in another pool.) When a pool's CPU feature set changes, the VM continues to use the feature set which was applied when it was started. To update the VM to use the pool's new feature set, you must power off and then start the VM. Rebooting the VM, for example, by clicking 'Reboot' in XenCenter, does not update the VM's feature set. (CA-188042)

- The increase in the amount memory allocated to dom0 in Citrix Hypervisor 8.0 can mean there is slightly less memory available for running VMs. On some hardware, you cannot run the same number of VMs with Citrix Hypervisor 8.2 as you can on the same hardware with XenServer 7.6 and earlier. (CP-29627)

- When attempting to use the serial console to connect to a Citrix Hypervisor server, the serial console might refuse to accept keyboard input. If you wait until after the console refreshes twice, the console then accepts keyboard input. (CA-311613)

- When read caching is enabled, it is slower to read from the parent snapshot than from the leaf. (CP-32853)

- After upgrading to Citrix Hypervisor 8.2, when there is a lot of VM activity on a server in a pool that uses NFS storage, connections through ENIC to external storage can become temporarily blocked (5–35 minutes). VMs on that server can freeze and their consoles can become unresponsive. Attempts to ping in or out of the affected server subnet fail during these times. To fix this issue, install version 4.0.0.8-802.24 or later of the enic driver. For more information, see Driver Disk for Cisco enic 4.0.0.11 - For Citrix Hypervisor 8.x CR. (XSI-916)

- When attempting to log in to the dom0 console with an incorrect password, you receive the following error message: `When trying to update a password, this return status indicates that the value provided as the current password is not correct.` This error message is

expected even though it relates to a password change, not a login. Try to log in with the correct password.

Graphics

- When you start in parallel many VMs with AMD MxGPU devices attached, some VMs might fail with a VIDEO_TDR_FAILURE. This behavior might be due to a hardware limitation. (CA-305555)
- When NVIDIA T4 added in passthrough mode to a VM on some specific server hardware, that VM might not power on. (CA-360450)

Guests

- Citrix Hypervisor no longer supports VMs that run in PV mode. In previous releases, after upgrading your Citrix Hypervisor server to the latest version, these unsupported VMs might still run. However, in Citrix Hypervisor 8.2 CU1, PV mode VMs no longer start-up. Ensure that you remove any PV VMs from your pool or convert these VMs to HVM mode before upgrading to your pool to Citrix Hypervisor 8.2 CU1. (CP-38086)
- If you install Debian 10 (Buster) by using PXE network boot, do not add `console=tty0` to the boot parameters. This parameter can cause issues with the installation process. Use only `console=hvc0` in the boot parameters. (CA-329015)
- After a CentOS 8 VM with only one CPU is migrated to a new Citrix Hypervisor server, the first time a CPU-bound command runs on the VM, it times out. To work around this issue, you can assign more than one CPU to the VM and restart it. (XSI-864)
- Some minor versions of Ubuntu 18.04 (for example 18.04.2 and 18.04.3) use an HWE kernel by default that can experience issues when running the graphical console. To work around these issues, you can choose to run these minor versions of Ubuntu 18.04 with the GA kernel or to change some of the graphics settings. For more information, see CTX265663 - Ubuntu 18.04.2 VMs can fail to boot on Citrix Hypervisor. (XSI-527)
- If you attempt to revert a VM to a scheduled VSS snapshot that was created with Citrix Hypervisor 8.0 or earlier, the VM does not boot. The boot fails with the following error: `This operation cannot be performed because the specified virtual disk could not be found`. This failure is because the VSS snapshot capability has been removed from Citrix Hypervisor 8.1 and later. (CA-329469)
- For domain-joined Windows 10 VMs (1903 and later) with FireEye Agent installed, repeated successful RDP connections can cause the VM to freeze with 100% CPU usage in `ntoskrnl.exe`. Perform a hard reboot on the VM to recover from this state. (CA-323760)
- The guest UEFI boot capability provided in Citrix Hypervisor 8.0 was an experimental feature. Citrix Hypervisor 8.2 does not support migrating UEFI boot VMs created in Citrix Hypervisor 8.0 to Citrix Hypervisor 8.2. Shut down UEFI boot VMs before upgrading to Citrix Hypervisor 8.2 from Citrix Hypervisor 8.0. (CA-330871)
- When UEFI-boot VMs start, they show a TianoCore logo. (CP-30146)

- On Windows VMs, when updating the `xenbus` driver to version 9.1.0.4, ensure that you complete both of the requested VM restarts. If both restarts are not completed, the VM might revert to emulated network adapters and use different settings, such as DHCP or different static IP addressing.

  To complete the second restart, you might be required to use a local account to log into the Windows VM. When you log in, you are prompted to restart.

  If you are unable to log in to the Windows VM after the first restart, you can use XenCenter to restart the VM and complete the `xenbus` driver installation. (CP-34181)

- When you create a UEFI VM, the Windows installation requires a key press to start. If you do not press a key during the required period, the VM console switches to the UEFI shell.

  To work around this issue, you can restart the installation process in one of the following ways:

  - In the UEFI console, type the following commands.

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

  - Reboot the VM

  When the installation process restarts, watch the VM console for the installation prompt. When the prompt appears, press any key. (CA-333694)

- On a Windows VM, after you have installed the version 9.x Citrix VM Tools for Windows, you might see both the previous and the latest version of the tools or management agent listed in your **Installed Programs**:

  - (PREVIOUS) Citrix XenServer Windows Management Agent
  - (LATEST) Citrix Hypervisor PV Tools

  The previous version of the management agent is not active and does not interfere with the operation of the latest version. We advise that you do not manually uninstall **Citrix XenServer Windows Management Agent** because this can disable the `xenbus` driver and cause the VM to revert to emulated devices.

- On Windows 10 20H2 and later, Windows Update treats the latest xennet driver as a Manual Update and does not install it automatically. You can check the status of your driver installations by going to **Windows Settings > Update & Security > View Update History > Driver Updates**. If this occurs, you can install the driver by downloading the Citrix VM Tools for Windows from the Citrix Hypervisor download page, and installing manually the driver inside the MSI file. (CA-350838)

- On a Windows VM, sometimes the IP address of an SR-IOV VIF is not visible in XenCenter. To fix the issue, restart the management agent from within the VMs Service Manager. (CA-340227)

- On a Windows VM with more than 8 vCPUs, Receive Side Scaling might not work because the xenvif driver fails to set up the indirection table. (CA-355277)

Installation

- If you are using a legacy disk layout, the control domain has less space available to it than the current layout (4 GB vs 18 GB).

  In this case, when attempting to apply the Citrix Hypervisor 8.2 or Citrix Hypervisor 8.2 Cumulative Update 1 update to an earlier, you might receive the error message "the server does not have enough space". This error happens because installation of the Citrix Hypervisor update requires sufficient free space to avoid filling the disk, which is not possible with the legacy layout.

  If you receive this error, you cannot update to Citrix Hypervisor 8.2 or Citrix Hypervisor 8.2 Cumulative Update 1. Do a fresh installation instead. (CA-268846)

- When updating from Citrix Hypervisor 8.0 to Citrix Hypervisor 8.2, you might see the following error: `Internal error: xenopsd internal error: Xenops_migrate.Remote_failed("unmarshalling error message from remote")`. This error is seen if `viridian` flags were modified for a Windows VM existing when applying the hotfix XS80E003, but the VM was not shut down and restarted.

  To avoid this issue, before you try to update to Citrix Hypervisor 8.2, complete all steps in the "After installing this hotfix" section of the hotfix article for all Windows VMs hosted on a Citrix Hypervisor 8.0 server that has XS80E003 applied. (XSI-571)

- If any vSwitch Controller state remains in your pool after an update or upgrade, clear the state with the following CLI commands:

  ```
  xe pool-set-vswitch-controller address=
  xe pool-param-set uuid=<uuid> vswitch-controller=
  ```

  (CA-339411)

- When upgrading to or installing Citrix Hypervisor 8.2 from an ISO located on an IIS server, the install or upgrade can fail and leave your servers unable to restart. The remote console shows the GRUB error: "File '/boot/grub/i3860pc/normal.mod' not found. Entering rescue mode". This issue is caused by the IIS configuration causing package files to be missing. To work around this issue, ensure that double escaping is allowed on IIS before extracting the installation ISO on it. (XSI-1063)

Internationalization

- Non-ASCII characters, for example, characters with accents, cannot be used in the host console. (CA-40845)

- In a Windows VM with Citrix VM Tools for Windows installed, copy and paste of double-byte characters can fail if using the default desktop console in XenCenter. The pasted characters appear as question marks (?).

  To work around this issue, you can use the remote desktop console instead. (CA-281807)

Storage

- If you use GFS2 SRs and have two servers in your clustered pool, your cluster can lose quorum and fence during an upgrade. To avoid this situation, either add a server to or remove a server from your

cluster. Ensure that you have either one or three servers in your pool during the upgrade process. (CA-313222)

- If you are using a GFS2 SR, ensure that you enable storage multipathing for maximum resiliency. If storage multipathing is not enabled, file system block writes might not fully complete in a timely manner. (CA-312678)
- If you use HPE 3PAR hardware for your storage repository and, with a previous release of XenServer, you use ALUA1 for your host persona, when you upgrade to Citrix Hypervisor 8.2 multipathing no longer works. To work around this issue, migrate your host persona to ALUA2. For more information, see https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02663749&docLocale=en_US.
- After removing an HBA LUN from a SAN, you might see log messages and I/O failures when querying Logical Volume information. To work around this issue, reboot the Citrix Hypervisor server. (XSI-984)
- You cannot set or change the name of the tmpfs SR used by the PVS Accelerator Supplemental Pack. When the `type` is `tmpfs`, the command `xe sr-create` disregards the value set for `name-label` and instead uses a fixed value. If you attempt to run the command `xe sr-param-set` to change the name of the tmpfs SR, you receive the error SCRIPT_MISSING.

Workload Balancing

- During the Workload Balancing maintenance window, Workload Balancing is unable to provide placement recommendations. When this situation occurs, you see the error: "4010 Pool discovery has not been completed. Using original algorithm." The Workload Balancing maintenance window is less than 20 minutes long and by default is scheduled at midnight. (CA-359926)
- In XenCenter, the date range showed on the Workload Balancing Pool Audit Report is incorrect. (CA-357115)
- For a Workload Balancing virtual appliance version 8.2.2 and later that uses LVM, you cannot extend the available disk space. (CA-358817)

XenCenter

- Changing the font size or dpi on the computer on which XenCenter is running can result in the user interface appearing incorrectly. The default font size is 96 dpi; Windows 8 and Windows 10 refer to this font size as 100%. (CA-45514) (CAR-1940)
- On Windows 10 (1903 and later) VMs, there can be a delay of a few minutes after installing the Citrix VM Tools before the **Switch to Remote Desktop** option is available in XenCenter. You can restart the toolstack to make this option appear immediately. (CA-322672)
- It is not advisable to update the same pool from concurrent instances of XenCenter because this might disrupt the update process.

  If more than one instance of XenCenter is attempting to install multiple hotfixes on a pool, a server might fail to install a hotfix with the error: "The update has already been applied to this server. The server will be skipped." This error causes the whole update process to stop. (CA-359814)

  To workaround this issue:

1. Ensure that no other XenCenter instance is in the process of updating the pool
2. Refresh the update list in the **Notifications > Updates** panel
3. Start the update from the beginning

- In XenCenter 8.2.3, importing an OVF or OVA file can be significantly slower than in earlier versions of XenCenter. (CP-38523)

Deprecation

The announcements in this article give you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

- For details about product lifecycle support, see the Product Lifecycle Support Policy article.
- For information about the Long Term Service Release (LTSR) servicing option, see https://support.citrix.com/article/CTX205549.

Deprecations and removals

The following table shows the platforms, Citrix products, and features that are deprecated or removed.

Deprecated items are not removed immediately. Citrix continues to support them in the current release, but they will be removed in a future release.

Removed items are either removed, or are no longer supported, in Citrix Hypervisor.

Dates in **bold** face indicate changes at this release.

Item	Deprecation announced in	Removed in	Alternative
Support for Windows Server 2012, Windows Server 2012 R2, and Windows 8.1	**8.2 CU1**	**8.2 CU1**	Upgrade your VMs to a later version of their operating system.

Item	Deprecation announced in	Removed in	Alternative
Transfer VM	**8.2 CU1**	**8.2 CU1**	Use the latest release of XenCenter. Since XenCenter 8.2.3, the mechanism used for OVF/OVA import/export and single disk image import has been simplified and these operations are now performed without using the Transfer VM.
Container Management Supplemental Pack	**8.2**	**8.2**	
Support for Hewlett-Packard Integrated Lights-Out (iLO)	**8.2**	**8.2**	
Support for the following legacy processors: `Xeon E3/5/7 family - Sandy Bridge`, `Xeon E3/5/7 v2 family - Ivy Bridge`	**8.2**	**8.2**	
The `guest-tools.iso` file included in the Citrix Hypervisor installation ISO	**8.2**	**8.2**	Download the Citrix VM Tools for Windows or for Linux from the Citrix Hypervisor downloads page.

Item	Deprecation announced in	Removed in	Alternative
Support for Windows 7, Windows Server 2008 SP2, and Windows Server 2008 R2 SP1	**8.2**	**8.2**	Upgrade your VMs to a later version of their operating system. For more information, see Upgrade from PV to HVM guests.
Legacy SSL mode and support for the TLS 1.0/1.1 protocol	**8.2**	**8.2**	
Cross-server private networks	**8.2**	**8.2**	
The following xe CLI log commands: `diagnostic-db-log`, `log-set-output`, `log-get-keys`, `log-get`, `log-reopen`	**8.2**		
The vSwitch Controller (see Notes)	8.1	**8.2**	
Dynamic Memory Control	8.1		
Legacy partition layouts: DOS partition layout, Old GPT partition layout. Note, this change also removes support for servers with less than 46 GB of primary disk space.	8.1		
VSS and quiesced snapshots	8.1	8.1	
Support for Ubuntu 14.04	8.1	8.1	
Support for all paravirtualized (PV) VMs, including the following: Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, CentOS 5, CentOS 6, Oracle Enterprise Linux 5, Oracle Enterprise Linux 6, Scientific Linux 6, NeoKylin Linux Advanced Server 6.2, Debian Wheezy 7, SUSE Linux Enterprise Server 11 SP3, SUSE Linux Enterprise Server 11 SP4, SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 12 SP1, SUSE Linux Enterprise Server 12 SP2, SUSE Linux Enterprise Desktop 11 SP3, SUSE Linux Enterprise Desktop 12, SUSE Linux Enterprise Desktop 12 SP1, SUSE Linux Enterprise Desktop 12 SP2	8.1	8.1	Upgrade your VMs to a later version of their operating system.
Legacy drivers: `qla4xxx`, `qla3xxx`, `netxen_nic`, `qlge`, `qlcnic`	8.0		

Item	Deprecation announced in	Removed in	Alternative
XenCenter installer bundled with the Citrix Hypervisor installation media.	8.0	8.0	Download the XenCenter installer from the Downloads page instead.
XenCenter connections to XenServer hosts that are version 6.x and earlier.	8.0	8.0	Upgrade your out-of-support XenServer hosts.
Support for Nutanix integration.	8.0	8.0	
Support for the following legacy processors: `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`	8.0	8.0	For information about supported processors, see the Hardware Compatibility List
Support for `qemu-trad`. It is no longer possible to use `qemu-trad` by setting `platform-devicemodel=qemu-trad`. All VMs created with `qemu-trad` device profile get automatically upgraded to `qemu-upstream-compat` profile.	8.0	8.0	
Support for the following guest templates: Debian 6 Squeeze, Ubuntu 12.04, Legacy Windows, Asianux Server 4.2, 4.4, and 4.5, NeoKylin Linux Security OS 5, Linx Linux 6, Linx Linux 8, GreatTurbo Enterprise Server 12, Yinhe Kylin 4	8.0	8.0	
Legacy Windows drivers from the Citrix VM Tools ISO	8.0	8.0	

Notes

Disconnecting the vSwitch controller

The vSwitch Controller is no longer supported. Disconnect the vSwitch Controller from your pool before attempting to update or upgrade to the latest version of Citrix Hypervisor.

1. In the vSwitch controller user interface, go to the **Visibility & Control** tab.
2. Locate the pool to disconnect in the **All Resource Pools** table. The pools in the table are listed using the IP address of the pool master.
3. Click the cog icon and select **Remove Pool**.
4. Click **Remove** to confirm.

After the update or upgrade, the following configuration changes take place:

- Cross-server private networks revert to single-server private networks.
- Any Quality of Service settings made through the DVSC console are no longer applied. Network rate limits are no longer enforced.
- ACL rules are removed. All traffic from VMs is allowed.
- Port mirroring (RSPAN) is disabled.

After update or upgrade, if you find any leftover state about the vSwitch Controller in your pool, clear the state with the following CLI command: `xe pool-set-vswitch-controller address=`

System requirements

Citrix Hypervisor requires at least two separate physical x86 computers: one to be the Citrix Hypervisor server and the other to run the XenCenter application or the Citrix Hypervisor Command-Line Interface (CLI). The Citrix Hypervisor server computer is dedicated entirely to the task of running Citrix Hypervisor and hosting VMs, and is not used for other applications.

> **Warning:**
>
> Installing third-party software directly in the control domain of the Citrix Hypervisor is not supported. The exception is for software supplied as a supplemental pack and explicitly endorsed by Citrix.

To run XenCenter use any general-purpose Windows system that satisfies the hardware requirements. This Windows system can be used to run other applications.

When you install XenCenter on this system, the Citrix Hypervisor CLI is also installed. A standalone remote Citrix Hypervisor CLI can be installed on any RPM-based Linux distribution. For more information, see Command-line interface.

Citrix Hypervisor server system requirements

Although Citrix Hypervisor is usually deployed on server-class hardware, Citrix Hypervisor is also compatible with many models of workstations and laptops. For more information, see the Hardware Compatibility List (HCL).

The following section describes the recommended Citrix Hypervisor hardware specifications.

The Citrix Hypervisor server must be a 64-bit x86 server-class machine devoted to hosting VMs. Citrix Hypervisor creates an optimized and hardened Linux partition with a Xen-enabled kernel. This kernel controls the interaction between the virtualized devices seen by VMs and the physical hardware.

Citrix Hypervisor can use:

- Up to 6 TB of RAM
- Up to 16 physical NICs
- Up to 448 logical processors per host.

> **Note:**
>
> The maximum number of logical processors supported differs by CPU. For more information, see the Hardware Compatibility List (HCL).

The system requirements for the Citrix Hypervisor server are:

CPUs

One or more 64-bit x86 CPUs, 1.5 GHz minimum, 2 GHz or faster multicore CPU recommended.

To support VMs running Windows or more recent versions of Linux, you require an Intel VT or AMD-V 64-bit x86-based system with one or more CPUs.

> **Note:**
>
> To run Windows VMs or more recent versions of Linux, enable hardware support for virtualization on the Citrix Hypervisor server. Virtualization support is an option in the BIOS. It is possible that your BIOS might have virtualization support disabled. For more information, see your BIOS documentation.

To support VMs running supported paravirtualized Linux, you require a standard 64-bit x86-based system with one or more CPUs.

RAM

2 GB minimum, 4 GB or more recommended

Disk space

- Locally attached storage with 46 GB of disk space minimum, 70 GB of disk space recommended
- SAN via HBA (not through software) when installing with multipath boot from SAN.

For a detailed list of compatible storage solutions, see the Hardware Compatibility List (HCL).

Network

100 Mbit/s or faster NIC. One or more Gb, or 10 Gb NICs is recommended for faster export/import data transfers and VM live migration.

We recommend that you use multiple NICs for redundancy. The configuration of NICs differs depending on the storage type. For more information, see the vendor documentation.

Citrix Hypervisor requires an IPv4 network for management and storage traffic.

> **Notes:**
>
> - Ensure that the time setting in the BIOS of your server is set to the current time in UTC.
> - In some support cases, serial console access is required for debug purposes. When setting up the Citrix Hypervisor configuration, we recommend that you configure serial console access. For hosts that do not have physical serial port or where suitable physical infrastructure is not available, investigate whether you can configure an embedded management device. For example, Dell DRAC. For more information about setting up serial console access, see CTX228930 - How to Configure Serial Console Access on XenServer 7.0 and later.

XenCenter system requirements

XenCenter has the following system requirements:

- **Operating System:**
  - Windows 10
  - Windows 8.1
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2016
  - Windows Server 2019
- **.NET Framework:** Version 4.8
- **CPU Speed:** 750 MHz minimum, 1 GHz or faster recommended
- **RAM:** 1 GB minimum, 2 GB or more recommended
- **Disk Space:** 100 MB minimum
- **Network:** 100 Mbit/s or faster NIC
- **Screen Resolution:** 1024x768 pixels, minimum

XenCenter is compatible with all supported versions of Citrix Hypervisor.

Supported guest operating systems

For a list of supported VM operating systems, see Guest operating system support.

Pool requirements

A resource pool is a homogeneous or heterogeneous aggregate of one or more servers, up to a maximum of 64. Before you create a pool or join a server to an existing pool, ensure that all servers in the pool meet the following requirements.

Hardware requirements

All of the servers in a Citrix Hypervisor resource pool must have broadly compatible CPUs, that is:

- The CPU vendor (Intel, AMD) must be the same on all CPUs on all servers.
- To run HVM virtual machines, all CPUs must have virtualization enabled.

Other requirements

In addition to the hardware prerequisites identified previously, there are some other configuration prerequisites for a server joining a pool:

- It must have a consistent IP address (a static IP address on the server or a static DHCP lease). This requirement also applies to the servers providing shared NFS or iSCSI storage.
- Its system clock must be synchronized to the pool master (for example, through NTP).
- It cannot be a member of an existing resource pool.
- It cannot have any running or suspended VMs or any active operations in progress on its VMs, such as shutting down or exporting. Shut down all VMs on the server before adding it to a pool.

- It cannot have any shared storage already configured.
- It cannot have a bonded management interface. Reconfigure the management interface and move it on to a physical NIC before adding the server to the pool. After the server has joined the pool, you can reconfigure the management interface again.
- It must be running the same version of Citrix Hypervisor, at the same patch level, as servers already in the pool.
- It must be configured with the same supplemental packs as the servers already in the pool. Supplemental packs are used to install add-on software into the Citrix Hypervisor control domain, dom0. To prevent an inconsistent user experience across a pool, all servers in the pool must have the same supplemental packs at the same revision installed.
- It must have the same Citrix Hypervisor license as the servers already in the pool. You can change the license of any pool members after joining the pool. The server with the lowest license determines the features available to all members in the pool.

Citrix Hypervisor servers in resource pools can contain different numbers of physical network interfaces and have local storage repositories of varying size.

> **Note:**
>
> Servers providing shared NFS or iSCSI storage for the pool must have a static IP address or be DNS addressable.

Homogeneous pools

A homogeneous resource pool is an aggregate of servers with identical CPUs. CPUs on a server joining a homogeneous resource pool must have the same vendor, model, and features as the CPUs on servers already in the pool.

Heterogeneous pools

Heterogeneous pool creation is made possible by using technologies in Intel (FlexMigration) and AMD (Extended Migration) CPUs that provide CPU *masking* or *leveling*. These features allow a CPU to be configured to *appear* as providing a different make, model, or feature set than it actually does. These capabilities enable you to create pools of hosts with different CPUs but still safely support live migrations.

For information about creating heterogeneous pools, see Hosts and resource pools.

Configuration limits

Use the following configuration limits as a guideline when selecting and configuring your virtual and physical environment for Citrix Hypervisor. The following tested and recommended configuration limits are fully supported for Citrix Hypervisor.

- Virtual machine limits
- Citrix Hypervisor server limits
- Resource pool limits

Factors such as hardware and environment can affect the limitations listed below. More information about supported hardware can be found on the Hardware Compatibility List. Consult your hardware manufacturers' documented limits to ensure that you do not exceed the supported configuration limits for your environment.

Virtual machine (VM) limits

Item	Limit
Compute	
Virtual CPUs per VM (Linux)	32 (see note 1)
Virtual CPUs per VM (Windows)	32
Memory	
RAM per VM	1.5 TiB (see note 2)
Storage	
Virtual Disk Images (VDI) (including CD-ROM) per VM	255 (see note 3)
Virtual CD-ROM drives per VM	1
Virtual Disk Size (NFS)	2040 GiB
Virtual Disk Size (LVM)	2040 GiB
Virtual Disk Size (GFS2)	16 TiB
Networking	
Virtual NICs per VM	7 (see note 4)
Graphics Capability	
vGPUs per VM	8
Passed through GPUs per VM	1

Item	Limit
Devices	
Passthrough USB devices	6

Notes:

1. Consult your guest OS documentation to ensure that you do not exceed the supported limits.
2. The maximum amount of physical memory addressable by your operating system varies. Setting the memory to a level greater than the operating system supported limit may lead to performance issues within your guest. Some 32-bit Windows operating systems can support more than 4 GiB of RAM through use of the physical address extension (PAE) mode. For more information, see your guest operating system documentation and Guest operating system support.
3. The maximum number of VDIs supported depends on the guest operating system. Consult your guest operating system documentation to ensure that you do not exceed the supported limits.
4. Several guest operating systems have a lower limit, other guests require installation of the Citrix VM Tools to achieve this limit.

Citrix Hypervisor server limits

Item	Limit
Compute	
Logical processors per host	448 (see note 1)
Concurrent VMs per host	1000 (see note 2)
Concurrent protected VMs per host with HA enabled	500
Virtual GPU VMs per host	128 (see note 3)
Memory	
RAM per host	6 TB
Storage	
Concurrent active virtual disks per host	2048
Storage repositories per host (NFS)	400
Networking	
Physical NICs per host	16
Physical NICs per network bond	4

Item	Limit
Virtual NICs per host	512
VLANs per host	800
Network Bonds per host	4
Graphics Capability	
GPUs per host	8 (See note 4)

Notes:

1. The maximum number of logical physical processors supported differs by CPU. For more information, see the Hardware Compatibility List.
2. The maximum number of VMs per host supported depends on VM workload, system load, network configuration, and certain environmental factors. We reserve the right to determine what specific environmental factors affect the maximum limit at which a system can function. For larger pools (over 32 hosts), we recommend allocating at least 8GB RAM to the Control Domain (Dom0). For systems running over 500 VMs or when using the PVS Accelerator, we recommend allocating at least 16 GB RAM to the Control Domain. For information about configuring Dom0 memory, see CTX134951 - How to Configure dom0 Memory.
3. For NVIDIA vGPU, 128 vGPU accelerated VMs per host with 4xM60 cards (4x32=128 VMs), or 2xM10 cards (2x64=128 VMs). For Intel GVT-g, 7 VMs per host with a 1,024 MB aperture size. Smaller aperture sizes can further restrict the number of GVT-g VMs supported per host. This figure might change. For the current supported limits, see the Hardware Compatibility List.
4. This figure might change. For the current supported limits, see the Hardware Compatibility List.

Resource pool limits

Item	Limit
Compute	
VMs per resource pool	2400
Hosts per resource pool	64 (See note 1)
Networking	
VLANs per resource pool	800
Disaster recovery	
Integrated site recovery storage repositories per resource pool	8

Item	Limit
Storage	
Paths to a LUN	8
Multipathed LUNs per host	150 (See note 2)
Multipathed LUNs per host (used by storage repositories)	150 (See note 2)
VDIs per SR (NFS, SMB, EXT, GFS2)	20000
VDIs per SR (LVM)	1000
Attached VDIs per SR (all types)	600
Storage repositories per pool (NFS)	400
Storage live migration	
(non-CDROM) VDIs per VM	6
Snapshots per VM	1
Concurrent transfers	3
XenCenter	
Concurrent operations per pool	25

Notes:

1. Clustered pools that use GFS2 storage support a maximum of 16 hosts in the resource pool.
2. When HA is enabled, we recommend increasing the default timeout to at least 120 seconds when more than 30 multipathed LUNs are present on a host. For information about increasing the HA timeout, see CTX139166 - How to Change High Availability Timeout Settings.

Guest operating system support

When installing VMs and allocating resources such as memory and disk space, follow the guidelines of the operating system and any relevant applications.

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Windows 10 (32-bit) [Latest tested version is 21H1]	1 GB	4 GB	24 GB (40 GB or more recommended)
Windows 10 (64-bit) [Latest tested version is 21H1]	2 GB	1.5 TB	32 GB (40 GB or more recommended)
Windows Server 2016, Windows Server Core 2016 (64-bit)	1 GB	1.5 TB	32 GB (40 GB or more recommended)
Windows Server 2019, Windows Server Core 2019 (64-bit)	1 GB	1.5 TB	32 GB (40 GB or more recommended)
Windows Server 2022, Windows Server Core 2022 (64-bit)	1 GB	1.5 TB	32 GB (40 GB or more recommended)
CentOS 7 (64-bit)	2 GB	1.5 TB	10 GB
CentOS 8 (64-bit)	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 7 (64-bit)	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 8 (64-bit)	2 GB	1.5 TB	10 GB
SUSE Linux Enterprise Server 12 SP3, 12 SP4, 12 SP5 (64-bit)	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Server 15, 15 SP1, 15 SP2, 15 SP3 (64-bit)	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 12 SP3, 12 SP4 (64-bit)	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 15, 15 SP1, 15 SP2, 15 SP3 (64-bit)	1 GB	1.5 TB	8 GB
Oracle Linux 7 (64-bit)	2 GB	1.5 TB	10 GB
Oracle Linux 8 (64-bit)	2 GB	1.5 TB	10 GB
Scientific Linux 7 (64-bit)	2 GB	1.5 TB	10 GB
Debian Jessie 8 (32-bit)	128 MB	64 GB	8 GB
Debian Jessie 8 (64-bit)	128 MB	1.5 TB	8 GB
Debian Stretch 9 (32-bit)	256 MB	64 GB	10 GB

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Debian Stretch 9 (64-bit)	256 MB	1.5 TB	10 GB
Debian Buster 10 (64-bit)	1 GB	1.5 TB	10 GB
Ubuntu 16.04 (32-bit)	512 MB	64 GB	10 GB
Ubuntu 16.04 (64-bit)	512 MB	1.5 TB	10 GB
Ubuntu 18.04 (64-bit)	512 MB	1.5 TB	10 GB
Ubuntu 20.04 (64-bit)	512 MB	1.5 TB	10 GB
NeoKylin Linux Advanced Server 7.2 (64-bit)	1 GB	1.5 TB	10 GB
Gooroom 2 (64-bit)	1 GB	1.5 TB	10 GB
Rocky Linux 8.4 (64-bit)	1 GB	1.5 TB	10 GB

- All supported operating systems run in HVM mode.

  Support for paravirtualized (PV) VMs is removed in Citrix Hypervisor 8.1. You can import existing VMs that use these operating systems into your Citrix Hypervisor 8.1 or later installation. However, Citrix does not provide support for VMs with these operating systems. Upgrade your VMs to a more recent and supported version of the OS as soon as possible.

- Individual versions of the operating systems can also impose their own maximum limits on the amount of memory supported (for example, for licensing reasons).

- When configuring guest memory, do not to exceed the maximum amount of physical memory that your operating system can address. Setting a memory maximum that is greater than the operating system supported limit might lead to stability problems within your guest.

- To create a VM of a newer minor version of RHEL than is listed in the preceding table, use the following method:

  - Install the VM from the latest supported media for the major version
  - Use `yum update` to update the VM to the newer minor version

  This approach also applies to RHEL-based operating systems such as CentOS and Oracle Linux.

- Some 32-bit Windows operating systems can support more than 4 GB of RAM by using physical address extension (PAE) mode. To reconfigure a VM with greater than 4 GB of RAM, use the xe CLI, not XenCenter, as the CLI doesn't impose upper bounds for `memory-static-max`.

Long-term guest support

Citrix Hypervisor includes a long-term guest support (LTS) policy for Linux VMs. The LTS policy enables you to consume minor version updates by one of the following methods:

- Installing from new guest media
- Upgrading from an existing supported guest

Out-of-support operating systems

The list of supported guest operating systems can contain operating systems that were supported by their vendors at the time this version of Citrix Hypervisor was released, but are now no longer supported by their vendors.

Citrix no longer offers support for these operating systems (even if they remain listed in the table of supported guests or their templates remain available on your Citrix Hypervisor hosts). While attempting to address and resolve a reported issue, Citrix assesses if the issue directly relates to an out-of-support operating system on a VM. To assist in making that determination, Citrix might ask you to attempt to reproduce an issue using a supported version of the guest operating system. If the issue seems to be related to the out-of-support operating system, Citrix will not investigate the issue further.

Install

This section contains procedures to guide you through the installation, configuration, and initial operation of Citrix Hypervisor. It also contains information about troubleshooting problems that might occur during installation and points you to extra resources.

This information is primarily aimed at system administrators who want to set up Citrix Hypervisor servers on physical servers.

Citrix Hypervisor installs directly on bare-metal hardware avoiding the complexity, overhead, and performance bottlenecks of an underlying operating system. It uses the device drivers available from the Linux kernel. As a result, Citrix Hypervisor can run on a wide variety of hardware and storage devices. However, ensure that you use certified device drivers.

For more information, see the Hardware Compatibility List (HCL).

Important:

The Citrix Hypervisor server must be installed on a dedicated 64-bit x86 server. Do not install any other operating system in a dual-boot configuration with the Citrix Hypervisor server. This configuration is not supported.

Before you start

Before installing Citrix Hypervisor 8.2 Cumulative Update 1, consider the following factors:

- What is the appropriate installation method?
- What are the system requirements?

Installation methods

Citrix Hypervisor 8.2 Cumulative Update 1 can be installed in one of the following ways:

- As a fresh installation
- As an update to Citrix Hypervisor 8.2
- As an upgrade to an earlier supported version of XenServer

Existing version of Citrix Hypervisor or XenServer	How to get Citrix Hypervisor 8.2 Cumulative Update 1	ISO file to use
None	Fresh installation	Base Installation ISO
8.2 initial release	Update	Update ISO
7.1 Cumulative Update 2	Upgrade	Base Installation ISO

> **Note:**
>
> Upgrade is only supported from the latest Cumulative Update of the LTSR. If your existing XenServer version is 7.1 or 7.1 Cumulative Update 1, first apply 7.1 Cumulative Update 2 before upgrading to Citrix Hypervisor 8.2 or Citrix Hypervisor 8.2 Cumulative Update 1.

Upgrade paths and compatibility information is also available in the Citrix Upgrade Guide.

There is no supported direct upgrade path from out-of-support versions of XenServer to Citrix Hypervisor 8.2 or Citrix Hypervisor 8.2 Cumulative Update 1. Instead, perform a fresh installation.

Fresh installation

If you are creating a fresh installation of Citrix Hypervisor 8.2 Cumulative Update 1:

- Use the **Citrix Hypervisor 8.2 Cumulative Update 1 Base Installation ISO** file. You can download this file from the Citrix download site
- Review the information in System Requirements, Licensing Citrix Hypervisor, and Installing Citrix Hypervisor and XenCenter before installing Citrix Hypervisor.

Update

If you are updating from Citrix Hypervisor 8.2 to Citrix Hypervisor 8.2 Cumulative Update 1:

- Use the **Citrix Hypervisor 8.2 Cumulative Update 1 ISO** file. You can download this file from the Citrix download site
- Review the information in System Requirements and Updating before updating Citrix Hypervisor.

Upgrade

If you are upgrading from XenServer 7.1 Cumulative Update 2 to Citrix Hypervisor 8.2 Cumulative Update 1:

- Use the **Citrix Hypervisor 8.2 Cumulative Update 1 Base Installation ISO** file. You can download this file from the Citrix download site.
- Review the information in System Requirements and Upgrading from an existing version before upgrading Citrix Hypervisor.

The installer presents the option to upgrade when it detects a previously installed version of Citrix Hypervisor. The upgrade process follows the first-time installation process, but several setup steps are bypassed. The existing settings are retained, including networking configuration, system time and so on.

Supplemental packs

You can install any required supplemental pack after installing Citrix Hypervisor. Download the supplemental pack to a known location on your computer and install the supplemental pack in the same way as an update.

For more information, see Supplemental Packs and the DDK Guide.

Install the Citrix Hypervisor server

> **Tip:**
>
> Throughout the installation, quickly advance to the next screen by pressing F12. Use Tab to move between elements and Space or Enter to select. Press F1 for general help.

To install or upgrade the Citrix Hypervisor server:

1. Back up data you want to preserve. Installing Citrix Hypervisor overwrites data on any hard drives that you select to use for the installation.
2. Boot the computer from the installation media or by using network boot:
   - To install Citrix Hypervisor server from a bootable USB:
     1. Use a tool like `rufus` or `diskpart` to create a bootable USB by using the Citrix Hypervisor installation ISO. Ensure that the tool does not alter the contents of the ISO file.
     2. Insert the bootable USB drive into the target system.
     3. Restart the system.
     4. In the BIOS, change the settings to boot the system from the USB.

        (If necessary, see your hardware vendor documentation for information on changing the boot order)
   - To install Citrix Hypervisor server from a CD:
     1. Burn the Citrix Hypervisor installation ISO file to a CD.
     2. Insert the bootable CD into the CD/DVD drive on the target system.
     3. Restart the system.
     4. In the BIOS, change the settings to boot the system from the CD.

        (If necessary, see your hardware vendor documentation for information on changing the boot order)
   - To install Citrix Hypervisor server from virtual media:
     1. Go to the virtual console of your system.
     2. Insert the Citrix Hypervisor installation ISO file as virtual media.
     3. Restart the system.
     4. In the BIOS, change the settings to boot the system from the virtual media.

        (If necessary, see your hardware vendor documentation for information on changing the boot order)

- To set up a network-accessible TFTP server to boot:

  For details about setting up a TFTP server to boot the installer using network, see Network Boot Installation.

- To install Citrix Hypervisor to a remote disk on a SAN to enable boot from SAN:

  For details, see Boot From SAN.

3. Following the initial boot messages and the Welcome to Citrix Hypervisor screen, select your key map (keyboard layout) for the installation.

   Note:

   If a System Hardware warning screen is displayed and hardware virtualization assist support is available on your system, see your hardware manufacturer for BIOS upgrades.

4. The Welcome to Citrix Hypervisor Setup screen is displayed.

   Citrix Hypervisor ships with a broad driver set that supports most modern server hardware configurations. However, if you have been provided with any additional essential device drivers, press F9. The installer steps you through installing the necessary drivers.

   Warning:

   Only update packages containing driver disks can be installed at this point in the installation process. However, you are prompted later in the installation process to install any update packages containing supplemental packs.

   After you have installed all of the required drivers, select **OK** to proceed.

   Citrix Hypervisor enables customers to configure the Citrix Hypervisor installation to boot from FCoE. Press F10 and follow the instructions displayed on the screen to set up FCoE.

   Notes:

   Before enabling your Citrix Hypervisor server to boot from FCoE, manually complete the configuration required to expose a LUN to the host. This manual configuration includes configuring the storage fabric and allocating LUNs to the public world wide name (PWWN) of your SAN. After you complete this configuration, the available LUN is mounted to the CNA of the host as a SCSI device. The SCSI device can then be used to access the LUN as if it were a locally attached SCSI device. For information about configuring the physical switch and the array to support FCoE, see the documentation provided by the vendor.

   When you configure the FCoE fabric, do not use VLAN 0. The Citrix Hypervisor server cannot find traffic that is on VLAN 0.

   Occasionally, booting a Citrix Hypervisor server from FCoE SAN using software FCoE stack can cause the host to stop responding. This issue is caused by a temporary link disruption in

> the host initialization phase. If the host fails to respond for a long time, you can restart the host to work around this issue.

5. The Citrix Hypervisor EULA is displayed. Use the Page Up and Page Down keys to scroll through and read the agreement. Select **Accept EULA** to proceed.

6. Select the appropriate action. You might see any of the following options:

   - *Perform clean installation*
   - *Upgrade*: If the installer detects a previously installed version of Citrix Hypervisor or XenServer, it offers the option to upgrade. For information about upgrading your Citrix Hypervisor server, see Upgrading from an existing version.
   - *Restore*: If the installer detects a previously created backup installation, it offers the option to restore Citrix Hypervisor from the backup.

   Make your selection, and choose **OK** to proceed.

7. If you have multiple local hard disks, choose a Primary Disk for the installation. Select **OK**.

8. Choose which disks you want to use for virtual machine storage. Information about a specific disk can be viewed by pressing **F5**.

   If you want to use thin provisioning to optimize the use of available storage, select Enable thin provisioning. This option selects the local SR of the host to be the one to be used for the local caching of VM VDIs. Citrix Virtual Desktops users are recommended to select this option for local caching to work properly. For more information, see Storage.

   Choose **OK**.

9. Select your installation media source.

   - To install from a USB or CD, choose **Local media**.
   - To install by using network, select **HTTP** or **FTP** or **NFS**.

     > **Note:**
     >
     > If you are using IIS to host the installation media, ensure that double escaping is enabled on IIS before extracting the installation ISO on it.

   Choose **OK** to proceed.

   If you select **HTTP** or **FTP** or **NFS**, set up networking so that the installer can connect to the Citrix Hypervisor installation media files:

   1. If the computer has multiple NICs, select one of them to be used to access the Citrix Hypervisor installation media files. Choose **OK** to proceed.

2. Choose **Automatic configuration (DHCP)** to configure the NIC using DHCP, or Static configuration to configure the NIC manually. If you choose **Static configuration**, enter details as appropriate.

3. Provide VLAN ID if you have your installation media present in a VLAN network.

4. If you choose **HTTP** or **FTP**, provide the URL for your HTTP or FTP repository, and a user name and password, if appropriate.

   If you choose **NFS**, provide the server and path of your NFS share.

   Select **OK** to proceed.

10. Indicate if you want to verify the integrity of the installation media. If you select **Verify installation source**, the SHA256 checksum of the packages is calculated and checked against the known value. Verification can take some time. Make your selection and choose **OK** to proceed.

11. Set and confirm a root password, which XenCenter uses to connect to the Citrix Hypervisor server. You also use this password (with user name "root") to log into **xsconsole**, the system configuration console.

    > **Note:**
    >
    > Citrix Hypervisor root passwords must contain only ASCII characters.

12. Set up the primary management interface that is used to connect to XenCenter.

    If your computer has multiple NICs, select the NIC which you want to use for management. Choose **OK** to proceed.

13. Configure the Management NIC IP address by choosing **Automatic configuration (DHCP)** to configure the NIC using DHCP, or **Static configuration** to configure the NIC manually. To have the management interface on a VLAN network, provide the VLAN ID.

    > **Note:**
    >
    > To be part of a pool, Citrix Hypervisor servers must have static IP addresses or be DNS addressable. When using DHCP, ensure that a static DHCP reservation policy is in place.

14. Specify the hostname and the DNS configuration, manually or automatically via DHCP.

    In the **Hostname Configuration** section, select **Automatically set via DHCP** to have the DHCP server provide the hostname along with the IP address. If you select **Manually specify**, enter the hostname for the server in the field provided.

    > **Note:**
    >
    > If you manually specify the hostname, enter a short hostname and *not the fully qualified domain name (FQDN)*. Entering an FQDN can cause external authentication to fail, or the

> Citrix Hypervisor server might be added to AD with a different name.

In the **DNS Configuration** section, choose **Automatically set via DHCP** to get name service configuration using DHCP. If you select **Manually specify**, enter the IP addresses of your primary (required), secondary (optional), and tertiary (optional) DNS servers in the fields provided.

Select **OK** to proceed.

15. Select your time zone by geographical area and city. You can type the first letter of the desired locale to jump to the first entry that begins with this letter. Choose **OK** to proceed.

16. Specify how you want the server to determine local time: using NTP or manual time entry. Make your selection, and choose **OK** to proceed.

    - If using NTP, select **NTP is configured by my DHCP server** or enter at least one NTP server name or IP address in the fields below. Choose **OK** to proceed.
    - If you elected to set the date and time manually, you are prompted to do so. Choose **OK** to proceed.

> **Note:**
>
> Citrix Hypervisor assumes that the time setting in the BIOS of the server is the current time in UTC.

17. Select **Install Citrix Hypervisor**.

    The installation process starts. This might take some minutes.

18. The next screen asks if you want to install any supplemental packs. If you plan to install any supplemental packs provided by your hardware supplier, choose **Yes**.

    If you choose to install supplemental packs, you are prompted to insert them. Eject the Citrix Hypervisor installation media, and insert the supplemental pack media. Choose **OK**.

    Select **Use media** to proceed with the installation.

    Repeat for each pack to be installed.

19. From the **Installation Complete** screen, eject the installation media (if installing from USB or CD) and select **OK** to reboot the server.

    After the server reboots, Citrix Hypervisor displays **xsconsole**, a system configuration console. To access a local shell from **xsconsole**, press **Alt+F3**; to return to **xsconsole**, press **Alt+F1**.

> **Note:**
>
> Make note of the IP address displayed. Use this IP address when you connect XenCenter to the Citrix Hypervisor server.

Install XenCenter

XenCenter must be installed on a Windows machine that can connect to the Citrix Hypervisor server through your network. Ensure that .NET framework version 4.6 or above is installed on this system.

To install XenCenter:

1. Download the installer for the latest version of XenCenter from the Citrix Hypervisor Download page.
2. Launch the installer `.msi` file.
3. Follow the Setup wizard, which allows you to modify the default destination folder and then to install XenCenter.

For more information about using XenCenter, see XenCenter documentation.

Connect XenCenter to the Citrix Hypervisor server

To connect XenCenter to the Citrix Hypervisor server:

1. Launch XenCenter. The program opens to the **Home** tab.
2. Click the **Add New Server** icon.
3. Enter the IP address of the Citrix Hypervisor server in the **Server** field. Type the root user name and password that you set during Citrix Hypervisor installation. Click **Add**.
4. The first time you add a host, the **Save and Restore Connection State** dialog box appears. This dialog enables you to set your preferences for storing your host connection information and automatically restoring host connections.

   If you later want to change your preferences, you can do so using XenCenter or the Windows Registry Editor.

   To do so in XenCenter: from the main menu, select **Tools** and then **Options**. The **Options** dialog box opens. Select the **Save and Restore** tab and set your preferences. Click **OK** to save your changes.

   To do so using the Windows Registry Editor, navigate to the key `HKEY_LOCAL_MACHINE\Software\Citrix\XenCenter` and add a key named `AllowCredentialSave` with the string value `true` or `false`.

Installation and deployment scenarios

This section steps through the following common installation and deployment scenarios:

- One or more Citrix Hypervisor servers with local storage
- Pools of Citrix Hypervisor servers with shared storage:
    - Multiple Citrix Hypervisor servers with shared NFS storage
    - Multiple Citrix Hypervisor servers with shared iSCSI storage

Citrix Hypervisor servers with local storage

The simplest deployment of Citrix Hypervisor is to run VMs on one or more Citrix Hypervisor servers with local storage.

> **Note:**
>
> Live migration of VMs between Citrix Hypervisor servers is only available when they share storage. However, storage live migration is still available.

Basic hardware requirements

- One or more 64-bit x86 servers with local storage
- One or more Windows systems, on the same network as the Citrix Hypervisor servers

High-level procedure

1. Install the Citrix Hypervisor server software on the servers.
2. Install XenCenter on the Windows systems.
3. Connect XenCenter to the Citrix Hypervisor servers.

After you connect XenCenter to the Citrix Hypervisor servers, storage is automatically configured on the local disk of the hosts.

Pools of Citrix Hypervisor servers with shared storage

A *pool* comprises multiple Citrix Hypervisor server installations, bound together as a single managed entity. When combined with shared storage, a pool enables VMs to be started on *any* Citrix Hypervisor server in the pool that has sufficient memory. The VMs can then dynamically be moved between hosts while running (live migration) with minimal downtime. If an individual Citrix Hypervisor server suffers a hardware failure, you can restart the failed VMs on another host in the same pool.

If the High Availability (HA) feature is enabled, protected VMs are automatically moved if there is a host failure.

To set up *shared storage* between hosts in a pool, create a storage repository. Citrix Hypervisor storage repositories (SR) are storage containers in which virtual disks are stored. SRs, like virtual disks, are persistent, on-disk objects that exist independently of Citrix Hypervisor. SRs can exist on different types of physical storage devices, both internal and external, including local disk devices and shared network storage. Several different types of storage are available when you create an SR, including:

- NFS VHD storage
- Software iSCSI storage
- Hardware HBA storage
- GFS2 storage

This following sections step through setting up two common shared storage solutions – NFS and iSCSI – for a pool of Citrix Hypervisor servers. Before you create an SR, configure your NFS or iSCSI storage. Setup differs depending on the type of storage solution that you use. For details, see your vendor documentation. In all cases, to be part of a pool, the servers providing shared storage must have static IP addresses or be DNS addressable. For further information on setting up shared storage, see Storage.

We recommend that you create a pool before you add shared storage. For pool requirements and setup procedures, see Pool Requirements in the XenCenter documentation or Hosts and Resource Pools.

Citrix Hypervisor servers with shared NFS storage

Basic hardware requirements

- Two or more 64-bit x86 servers with local storage
- One or more Windows systems, on the same network as the Citrix Hypervisor servers
- A server exporting a shared directory over NFS

High-level procedure

1. Install the Citrix Hypervisor server software on the servers.
2. Install XenCenter on the Windows systems.
3. Connect XenCenter to the Citrix Hypervisor servers.
4. Create your pool of Citrix Hypervisor servers.
5. Configure the NFS server.
6. Create an SR on the NFS share at the pool level.

Configuring your NFS storage

Before you create an SR, configure the NFS storage. To be part of a pool, the NFS share must have a static IP address or be DNS addressable. Configure the NFS server to have one or more targets that can be mounted by NFS clients (for example, Citrix Hypervisor servers in a pool). Setup differs depending on your storage solution, so it is best to see your vendor documentation for details.

To create an SR on the NFS share at the pool level in XenCenter:

1. On the **Resources** pane, select the pool. On the toolbar, click the **New Storage** button. The **New Storage Repository** wizard opens.
2. Under **Virtual disk storage**, choose NFS VHD as the storage type. Choose **Next** to continue.
3. Enter a name for the new SR and the name of the share where it is located. Click **Scan** to have the wizard scan for existing NFS SRs in the specified location.

   > **Note:**
   >
   > The NFS server must be configured to export the specified path to all Citrix Hypervisor servers in the pool.

4. Click **Finish**.

   The new SR appears in the **Resources** pane, at the pool level.

Creating an SR on the NFS share at the pool level using the xe CLI

1. Open a console on any Citrix Hypervisor server in the pool.
2. Create the storage repository on *server:/path* by entering the following:

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

   The `device-config-server` argument refers to the name of the NFS server and the `device-config-serverpath` argument refers to the path on the server. Since `shared` is set to true, the shared storage is automatically connected to every host in the pool. Any hosts that later join are also connected to the storage. The UUID of the created storage repository is printed to the console.
3. Find the UUID of the pool by using the `pool-list` command.
4. Set the new SR as the pool-wide default by entering the following:

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

   As shared storage has been set as the pool-wide default, all future VMs have their disks created on this SR.

Citrix Hypervisor servers with shared iSCSI storage

Basic hardware requirements

- Two or more 64-bit x86 servers with local storage
- One or more Windows systems, on the same network as the Citrix Hypervisor servers
- A server providing a shared directory over iSCSI

High-level procedure

1. Install the Citrix Hypervisor server software on the servers.
2. Install XenCenter on the Windows systems.
3. Connect XenCenter to the Citrix Hypervisor servers.
4. Create your pool of Citrix Hypervisor servers.
5. Configure the iSCSI storage.
6. If necessary, enable multiple initiators on your iSCSI device.
7. If necessary, configure the iSCSI Qualified Name (IQN) for each Citrix Hypervisor server.
8. Create an SR on the iSCSI share at the pool level.

Configuring your iSCSI storage

Before you create an SR, configure the iSCSI storage. To be part of a pool, the iSCSI storage must have a static IP address or be DNS addressable. Provide an iSCSI target LUN on the SAN for the VM storage. Configure Citrix Hypervisor servers to be able to see and access the iSCSI target LUN. Both the iSCSI target and each iSCSI initiator on each Citrix Hypervisor server must have a valid and **unique** IQN. For configuration details, it is best to see your vendor documentation.

Configuring an iSCSI IQN for each Citrix Hypervisor server

Upon installation, Citrix Hypervisor automatically attributes a unique IQN to each host. If you must adhere to a local administrative naming policy, you can change the IQN by using the following xe CLI command:

```
xe host-param-set uuid=<host_uuid> iscsi_iqn=<iscsi_iqn>
```

To create an SR on the iSCSI share at the pool level using XenCenter:

> **Warning:**
>
> When you create Citrix Hypervisor SRs on iSCSI or HBA storage, any existing contents of the volume are destroyed.

1. On the **Resources** pane, select the pool. On the toolbar, click the **New Storage** button. The **New Storage Repository** wizard opens.
2. Under **Virtual disk storage**, choose Software iSCSI as the storage type. Choose **Next** to continue.

3. Enter a name for the new SR and then the IP address or DNS name of the iSCSI target.

   > **Note:**
   >
   > The iSCSI storage target must be configured to enable every Citrix Hypervisor server in the pool to have access to one or more LUNs.

4. If you have configured the iSCSI target to use CHAP authentication, enter the User and Password.

5. Click the **Discover IQNs** button, and then choose the iSCSI target IQN from the Target IQN list.

   > **Warning:**
   >
   > The iSCSI target and all servers in the pool must have *unique* IQNs.

6. Click the **Discover LUNs** button, and then choose the LUN on which to create the SR from the Target LUN list.

   > **Warning:**
   >
   > Each individual iSCSI storage repository must be contained entirely on a single LUN and cannot span more than one LUN. Any data present on the chosen LUN is destroyed.

7. Click **Finish**.

   The new SR appears in the **Resources** pane, at the pool level.

To create an SR on the iSCSI share at the pool level by using the xe CLI:

> **Warning:**
>
> When you create Citrix Hypervisor SRs on iSCSI or HBA storage, any existing contents of the volume are destroyed.

1. On the console of any server in the pool, run the command:

   ```
   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
   ```

   The `device-config:target` argument refers to the name or IP address of the iSCSI server. Since the `shared` argument is set to `true`, the shared storage is automatically connected to every host in the pool. Any hosts that later join are also connected to the storage.

   The command returns the UUID of the created storage repository.

2. Find the UUID of the pool by running the `pool-list` command.

3. Set the new SR as the pool-wide default by entering the following:

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

   As shared storage has been set as the pool-wide default, all future VMs have their disks created on this SR.

Upgrade from an existing version

This article describes how to upgrade Citrix Hypervisor by using XenCenter or the xe CLI. It guides you through upgrading your Citrix Hypervisor servers – both pooled and standalone – automatically (using the XenCenter Rolling Pool Upgrade wizard) and manually.

We provide both upgrade and update capabilities that you can use to move from some earlier versions of Citrix Hypervisor to Citrix Hypervisor 8.2 Cumulative Update 1. Using the upgrade or update capability enables you to apply Citrix Hypervisor 8.2 Cumulative Update 1 without having to complete a full installation process. When you upgrade or update, Citrix Hypervisor 8.2 Cumulative Update 1 retains your VMs, SRs, and configuration.

- You can upgrade from XenServer 7.1 Cumulative Update 2 (LTSR) to Citrix Hypervisor 8.2 Cumulative Update 1 by using the **Base Installation ISO**. This section describes how to upgrade to Citrix Hypervisor 8.2 Cumulative Update 1.

  > **Note:**
  >
  > Upgrading from XenServer 7.1 or 7.1 Cumulative Update 1 to Citrix Hypervisor 8.2 Cumulative Update 1 is not supported. Ensure that the latest Cumulative Update is applied to Citrix Hypervisor 7.1 before attempting to upgrade.

- You can apply Citrix Hypervisor 8.2 Cumulative Update 1 as an update to Citrix Hypervisor 8.2 by using the **Update Installation ISO**. For more information, see Update your hosts.
- For all other versions of XenServer and Citrix Hypervisor you cannot upgrade to Citrix Hypervisor 8.2 Cumulative Update 1 directly. Perform a clean installation using the **Base Installation ISO**. For more information, see Install.

> **Note:**
>
> To retain VMs from your previous installation of Citrix Hypervisor or XenServer, export the VMs and import them into your clean installation of Citrix Hypervisor 8.2 Cumulative Update 1. VMs exported from any supported version of Citrix Hypervisor or XenServer can be imported into Citrix Hypervisor 8.2 Cumulative Update 1. For more information, see Import and export VMs.

Upgrade paths and compatibility information is also available in the Citrix Upgrade Guide.

Before you start

Review the following information before starting your upgrade. Take the necessary steps to ensure that your upgrade process is successful.

- Upgrading Citrix Hypervisor servers, and particularly a pool of Citrix Hypervisor servers, requires careful planning and attention. To avoid losing any existing data, either:

    - Map your upgrade path carefully.
    - Use the XenCenter Rolling Pool Upgrade wizard, and ensure that you select the option to *upgrade* when you are stepping through the installer.

- If you are using XenCenter to upgrade your hosts, download and install the latest version of XenCenter from the Citrix Hypervisor download site.

  For example, when upgrading to Citrix Hypervisor 8.2, use the latest version of XenCenter issued for Citrix Hypervisor 8.2. Using earlier versions of XenCenter to upgrade to a newer version of Citrix Hypervisor is not supported.

- If you have Windows VMs running in your pool that will be migrated as part of your upgrade, take the following steps for each VM:

    - Set the value of the following registry key to a REG_DWORD value of '3': `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`
    - Ensure that the latest version of the Citrix VM Tools for Windows is installed
    - Take a snapshot of the VM

- Boot-from-SAN settings are *not* inherited during the manual upgrade process. When upgrading using the ISO or PXE process, follow the same instructions as used in the installation process below to ensure that `multipathd` is correctly configured. For more information, see Boot from SAN.

- Paravirtualized (PV) VMs are not supported in Citrix Hypervisor 8.2. Ensure that before upgrading you remove any PV VMs from your pool or upgrade your VMs to a supported version of their operating system. For more information, see Upgrade from PV to HVM guests.

  Earlier versions of the Citrix License Server virtual appliance run in PV mode. Ensure that you update your Citrix License Server virtual appliance to the latest version before upgrading to Citrix Hypervisor 8.2.

- Quiesced snapshots are no longer supported. If you have existing snapshot schedules that create quiesced snapshots, these snapshot schedules fail after the upgrade. To ensure that snapshots continue to be created, delete the existing schedule and create a new one that creates non-quiesced snapshots before performing the upgrade.

- Legacy SSL mode is no longer supported. Disable this mode on all hosts in your pool before attempting to upgrade to the latest version on Citrix Hypervisor. To disable legacy SSL mode, run the following command on your pool master before you begin the upgrade: `xe pool-disable-ssl-legacy uuid=<pool_uuid>`

- The Container Management supplemental pack is no longer supported. After you update or upgrade to the latest version of Citrix Hypervisor, you can no longer use the features of this supplemental pack.

- When you upgrade Citrix Hypervisor, previously applied supplemental packs are removed and so they must be reapplied during or after the upgrade.

- The vSwitch Controller is no longer supported. Disconnect the vSwitch Controller from your pool before attempting to upgrade to the latest version on Citrix Hypervisor. After the upgrade, the following configuration changes take place:

- Cross-server private networks revert to single-server private networks.
- Any Quality of Service settings made through the DVSC console are no longer applied. Network rate limits are no longer enforced.
- ACL rules are removed. All traffic from VMs is allowed.
- Port mirroring (RSPAN) is disabled.

If, after update or upgrade, you find leftover state about the vSwitch Controller in your pool, clear the state with the following CLI command: `xe pool-set-vswitch-controller address=`

Rolling pool upgrades

Citrix Hypervisor enables you to perform a rolling pool upgrade. A rolling pool upgrade keeps all the services and resources offered by the pool available while upgrading all of the hosts in a pool. This upgrade method takes only one Citrix Hypervisor server offline at a time. Critical VMs are kept running during the upgrade process by live migrating the VMs to other hosts in the pool.

> **Note:**
>
> The pool must have shared storage to keep your VMs running during a rolling pool upgrade. If your pool does not have shared storage, you must stop your VMs before upgrading because the VMs cannot be live migrated.
>
> Storage live migration is not supported with rolling pool upgrades.

You can perform a rolling pool upgrade using XenCenter or the xe CLI. When using XenCenter, we recommend using the Rolling Pool Upgrade wizard. This wizard organizes the upgrade path automatically and guides you through the upgrade procedure. If you are using the xe CLI, first plan your upgrade path and then live migrate running VMs between Citrix Hypervisor servers as you perform the rolling pool upgrade manually.

The Rolling Pool Upgrade wizard is available for licensed Citrix Hypervisor customers or those customers who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement. For more information about Citrix Hypervisor licensing, see Licensing. To upgrade, or to buy a Citrix Hypervisor license, visit the Citrix website.

> **Important:**
>
> Do not use Rolling Pool Upgrade with Boot from SAN environments. For more information on upgrading boot from SAN environments, see Boot from SAN.

Upgrade Citrix Hypervisor servers by using the XenCenter Rolling Pool Upgrade wizard

The Rolling Pool Upgrade wizard enables you to upgrade Citrix Hypervisor servers, hosts in a pool or standalone hosts, to the current version of Citrix Hypervisor.

The Rolling Pool Upgrade wizard guides you through the upgrade procedure and organizes the upgrade path automatically. For pools, each of the hosts in the pool is upgraded in turn, starting with the pool master.

Before starting an upgrade, the wizard conducts a series of prechecks. These prechecks ensure certain pool-wide features, such as high availability are temporarily disabled and that each host in the pool is prepared for upgrade. Only one host is offline at a time. Any running VMs are automatically migrated off each host before the upgrade is installed on that host.

The Rolling Pool Upgrade wizard also allows you to automatically apply the available hotfixes when upgrading to a newer version of Citrix Hypervisor. This enables you to bring your standalone hosts or pools up-to-date with a minimum number of reboots at the end. You must be connected to the Internet during the upgrade process for this feature to work.

You can benefit from the automatic application of hotfixes feature when you use XenCenter issued with Citrix Hypervisor 8.2 Cumulative Update 1 to upgrade from any supported version of Citrix Hypervisor or XenServer.

> **Note:**
>
> Rolling Pool Upgrade using XenCenter is only available for licensed Citrix Hypervisor customers or those customers who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement.

The wizard can operate in **Manual** or **Automatic** mode:

- In **Manual Mode**, you must manually run the Citrix Hypervisor installer on each host in turn and follow the on-screen instructions on the serial console of the host. When the upgrade begins, XenCenter prompts you to insert the XenCenter installation media or specify a network boot server for each host that you upgrade.
- In **Automatic Mode**, the wizard uses network installation files on an HTTP, NFS, or FTP server to upgrade each host in turn. This mode doesn't require you to insert installation media, manually reboot, or step through the installer on each host. If you perform a rolling pool upgrade in this manner, you must unpack the installation media onto your HTTP, NFS, or FTP server before starting the upgrade.

  > **Note:**
  >
  > If you are using IIS to host the installation media, ensure that double escaping is enabled on IIS before extracting the installation ISO on it.

Before you upgrade

Before you begin your upgrade, be sure to make the following preparations:

- Download and install the latest version of XenCenter provided for Citrix Hypervisor 8.2 Cumulative Update 1 from the Citrix Hypervisor Product Download page. Using earlier versions of XenCenter to upgrade to a newer version of Citrix Hypervisor is not supported.
- We strongly recommend that you take a backup of the state of your existing pool using the `pool-dump-database` xe CLI command. For more information, see Command line interface. Taking a backup state

ensures that you can revert a partially complete rolling upgrade to its original state without losing VM data.

- Ensure that your hosts are not over-provisioned: check that hosts have sufficient memory to carry out the upgrade.

  As a general guideline, if N equals the total number of hosts in a pool, there must be sufficient memory across N-1 hosts to run all of the live VMs in the pool. It is best to suspend any non-critical VMs during the upgrade process.

- If you have vGPU-enabled VMs running on your pool, complete the following steps to migrate the pool while these VMs are running:

  - Ensure that the GPU you are using is supported on the version you plan to upgrade to.
  - Identify a version of the NVIDIA drivers that is available for both your current version of Citrix Hypervisor and the version of Citrix Hypervisor you are upgrading. If possible, choose the latest available drivers.
  - Install the new NVIDIA drivers on your Citrix Hypervisor servers and the matching guest drivers on any of your vGPU-enabled VMs.
  - Ensure that you also have the version of the NVIDIA driver that matches the version of Citrix Hypervisor that you are upgrading to. You are prompted to install these drivers as a supplemental pack as part of the Rolling Pool Upgrade process.

Rolling Pool Upgrade wizard checks that the following actions have been taken. Perform these actions before you begin the upgrade process:

- Empty the CD/DVD drives of the VMs in the pools.
- Disable high availability.

Upgrade process

To upgrade Citrix Hypervisor hosts by using the XenCenter Rolling Pool Upgrade wizard:

1. Open the Rolling Pool Upgrade wizard: on the **Tools** menu, select **Rolling Pool Upgrade**.
2. Read the **Before You Start** information, and then click **Next** to continue.
3. Select the pools and any individual hosts that you want to upgrade, and then click **Next**.
4. Choose one of the following modes:

   - **Automatic Mode** for an automated upgrade from network installation files on an HTTP, NFS, or FTP server
   - **Manual Mode** for a manual upgrade from either a USB/CD/DVD or using network boot (using existing infrastructure)

   Notes:

   If you choose **Automatic Mode** and are using IIS to host the installation media, ensure that double escaping is enabled on IIS before extracting the installation ISO on it.

> If you choose **Manual Mode**, you must run the Citrix Hypervisor installer on each host in turn. Follow the on-screen instructions on the serial console of the host. When the upgrade begins, XenCenter prompts you to insert the Citrix Hypervisor installation media or specify a network boot server for each host that you upgrade.

5. Choose whether you want XenCenter to automatically download and install the minimal set of updates (hotfixes) after upgrading the servers to a newer version. The apply updates option is selected by default. However, you must have internet connection to download and install the updates.

6. After you have selected your Upgrade Mode, click **Run Prechecks**.

7. Follow the recommendations to resolve any upgrade prechecks that have failed. If you want XenCenter to resolve all failed prechecks automatically, click **Resolve All**.

   When all prechecks have been resolved, click **Next** to continue.

8. Prepare the Citrix Hypervisor installation media.

   If you chose **Automatic Mode**, enter the installation media details. Choose **HTTP**, **NFS**, or **FTP** and then specify the URL, user name, and password, as appropriate.

   > **Notes:**
   >
   > - If you choose FTP, ensure that you escape any leading slashes that are in the file path section of the URL.
   > - Enter the user name and password associated with your HTTP or FTP server, if you have configured security credentials. Do not enter the user name and password associated with your Citrix Hypervisor pool.
   > - Citrix Hypervisor supports FTP in passive mode only.

   If you chose **Manual Mode**, note the upgrade plan and instructions.

   Click **Start Upgrade**.

9. When the upgrade begins, the Rolling Pool Upgrade wizard guides you through any actions you must take to upgrade each host. Follow the instructions until you have upgraded and updated all hosts in the pools.

   If you have vGPU-enabled VMs, when you reach the step that gives you the option to supply a supplemental pack, upload the NVIDIA driver that matches the one on your vGPU-enabled VMs. Ensure you upload the version of the driver for the Citrix Hypervisor version you are upgrading to.

   > **Note:**
   >
   > If the upgrade or the update process fails for any reason, the Rolling Pool Upgrade wizard halts the process. This allows you to fix the issue and resume the upgrade or update process by clicking the **Retry** button.

10. The Rolling Pool Upgrade wizard prints a summary when the upgrade is complete. Click **Finish** to close the wizard.

Upgrade Citrix Hypervisor servers by using the xe CLI

Performing a rolling pool upgrade using the xe CLI requires careful planning. Be sure to read the following section with care before you begin.

Plan an upgrade path

As you plan your upgrade, it is important to be aware of the following:

- You can only migrate VMs from Citrix Hypervisor servers running an older version of Citrix Hypervisor to one running the same version or higher. For example, from version 7.0 to version 7.1 Cumulative Update 2 or from version 7.1 Cumulative Update 2 to version 8.2 Cumulative Update 1.

  You **cannot** migrate VMs from an upgraded host to one running an older version of Citrix Hypervisor. For example, from version 8.2 Cumulative Update 1 to version 7.1 Cumulative Update 2. Be sure to allow for space on your Citrix Hypervisor servers accordingly.

- We strongly advise against running a mixed-mode pool (one with multiple versions of Citrix Hypervisor co-existing) for longer than necessary, as the pool operates in a degraded state during upgrade.

- Key control operations are not available during upgrade. Do not attempt to perform any control operations. Though VMs continue to function as normal, VM actions other than migrate are not available (for example, shut down, copy and export). In particular, it is not safe to perform storage-related operations such as adding, removing, or resizing virtual disks.

- Always upgrade the master host first. Do not place the host into maintenance mode using XenCenter before performing the upgrade. If you put the master in maintenance mode, a new master is designated.

- After upgrading a host, apply any hotfixes that have been released for the upgraded version of Citrix Hypervisor before migrating VMs onto the host.

- We strongly recommend that you take a backup of the state of your existing pool using the `pool-dump-database` xe CLI command. For more information, see Command Line interface. This allows you to revert a partially complete rolling upgrade back to its original state without losing any VM data. If you have to revert the rolling upgrade for any reason, you might have to shut down VMs. This action is required because it is not possible to migrate a VM from an upgraded Citrix Hypervisor server to a host running an older version of Citrix Hypervisor.

Before you begin your rolling pool upgrade

- If you are using XenCenter, upgrade XenCenter to the latest version provided on the Citrix download site. The newer version of XenCenter correctly controls older versions of Citrix Hypervisor servers.

- Empty the CD/DVD drives of the VMs in the pool. For details and instructions, see *Before Upgrading a Single Citrix Hypervisor server*.

- Disable high availability.

Perform rolling pool upgrades by using the xe CLI

1. **Start with the pool master**. Disable the master by using the `host-disable` command. This prevents any new VMs from starting on the specified host.
2. Ensure that no VMs are running on the master. Shut down, suspend or migrate VMs to other hosts in the pool.

   To migrate specified VMs to specified hosts, use the `vm-migrate` command. By using the `vm-migrate` command, you have full control over the distribution of migrated VMs to other hosts in the pool.

   To live migrate all VMs to other hosts in the pool, use the `host-evacuate` command. By using the `host-evacuate` command, you leave the distribution of migrated VMs to Citrix Hypervisor.
3. Shut down the pool master.

   > **Important:**
   >
   > You are unable to contact the pool master until the upgrade of the master is complete. Shutting down the pool master causes the other hosts in the pool to enter *emergency mode*. Hosts can enter emergency mode when they in a pool whose master has disappeared from the network and cannot be contacted after several attempts. VMs continue to run on hosts in emergency mode, but control operations are not available.
4. Boot the pool master using the Citrix Hypervisor installation media and method of your choice (such as, USB or network). Follow the Citrix Hypervisor installation procedure until the installer offers you the option to upgrade. **Choose to upgrade.** For more information, see Install.

   > **Warnings:**
   >
   > - Ensure you select the upgrade option to avoid losing any existing data.
   > - If anything interrupts the upgrade of the pool master or if the upgrade fails for any reason, do not attempt to proceed with the upgrade. Reboot the pool master and restore to a working version of the master.

   When your pool master restarts, the other hosts in the pool leave emergency mode and normal service is restored after a few minutes.
5. Apply any hotfixes that have been released for the new version of Citrix Hypervisor to the pool master.
6. On the pool master, start or resume any shutdown or suspended VMs. Migrate any VMs that you want back to the pool master.
7. Select the next Citrix Hypervisor server in your upgrade path. Disable the host.
8. Ensure that no VMs are running on the host. Shut down, suspend or migrate VMs to other hosts in the pool.
9. Shut down the host.

10. Follow the upgrade procedure for the host, as described for the master in Step 4.

    Note:

    If the upgrade of a host that is not the master fails or is interrupted, you do not have to revert. Use the `host-forget` command to forget the host. Reinstall Citrix Hypervisor on the host, and then join it, as a new host, to the pool using the `pool-join` command.

11. Apply any hotfixes that have been released for the new version of Citrix Hypervisor to the host.
12. On the host, start or resume any shutdown or suspended VMs. Migrate any VMs that you want back to the host.
13. Repeat Steps 6–10 for the rest of the hosts in the pool.

Upgrade a single Citrix Hypervisor server by using the xe CLI

Before you upgrade a single Citrix Hypervisor server

Before upgrading a standalone Citrix Hypervisor server, shut down or suspend any VMs running on that host. It is important to eject and empty CD/DVD drives of any VMs you plan to suspend. If you do not empty the CD/DVD drives, you may not be able to resume the suspended VMs after upgrade.

An *empty* VM CD/DVD drive means the VM is not attached to an ISO image or a physical CD/DVD mounted through the Citrix Hypervisor server. In addition, you must ensure that the VM is not attached to any physical CD/DVD drive on the Citrix Hypervisor server at all.

To empty the CD/DVD drive of a VM by using the xe CLI:

1. Identify which VMs do not have empty CD/DVD drives by typing the following:

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

   This returns a list of all the VM CD/DVD drives that are not empty, for example:

   ```
   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
   ```

Note the `uuid`, which is the first item in the list.

2. To empty the CD/DVD drives of the VMs listed, type the following:

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

Upgrade a single Citrix Hypervisor server by using the xe CLI

To upgrade a single Citrix Hypervisor server by using the xe CLI:

1. Disable the Citrix Hypervisor server that you want to upgrade by typing the following:

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

When the Citrix Hypervisor server is disabled, VMs cannot be created or started on that host. VMs also cannot be migrated to a disabled host.

2. Shut down or suspend any VMs running on the host that you want to upgrade by using the `xe vm-shutdown` or `xe vm-suspend` commands.

3. Shut down the host by using the `xe host-shutdown` command.

4. Follow the Citrix Hypervisor installation procedure until the installer offers you the option to upgrade. **Choose to upgrade.** For more information, see Install.

> **Warning:**
>
> Be sure to select the upgrade option to avoid losing any existing data.

You don't have to configure any settings again during the setup procedure. The upgrade process follows the first-time installation process but several setup steps are bypassed. The existing settings for networking configuration, system time, and so on, are retained.

When your host restarts, normal service is restored after a few minutes.

5. Apply any hotfixes that have been released for the new version of Citrix Hypervisor.

6. Restart any shutdown VMs, and resume any suspended VMs.

Update your hosts

Updates can often be applied with minimal service interruption. We recommend that customers use XenCenter to apply all updates. If you are updating a Citrix Hypervisor pool, you can avoid VM downtime by using the **Install Update** wizard in XenCenter. The **Install Update** wizard applies updates, updating one host at a time, automatically migrating VMs away from each host as the hotfix or update is applied.

You can configure XenCenter to check periodically for available Citrix Hypervisor and XenCenter updates and new versions. Any Alerts are displayed in the **Notifications** pane.

> **Note:**
>
> Ensure that you use the latest version of XenCenter to apply updates to your Citrix Hypervisor hosts and pools. The latest version of XenCenter is provided on the Citrix download site.

Upgrade paths and compatibility information is also available in the Citrix Upgrade Guide.

Types of update

The following types of updates are available for Citrix Hypervisor:

- **Releases**, which are full releases of Citrix Hypervisor that can be applied as updates to the supported versions of Citrix Hypervisor.
- **Hotfixes**, which generally supply bug fixes to one or more specific issues. Hotfixes are provided for supported Citrix Hypervisor or XenServer releases.
- **Cumulative Updates**, which contain previously released hotfixes and can contain support for new guests and hardware. Cumulative updates are applied to Citrix Hypervisor releases from the Long Term Service Release (LTSR) stream.

Supplemental packs provided by our partners can also be applied as updates to Citrix Hypervisor.

Releases

Citrix Hypervisor 8.2 Cumulative Update 1 is an update for Citrix Hypervisor 8.2. The following table shows which previous supported versions of Citrix Hypervisor or XenServer you can apply Citrix Hypervisor 8.2 Cumulative Update 1 to as an update:

Version	Apply Citrix Hypervisor 8.2 Cumulative Update 1 as an update?
Citrix Hypervisor 8.2	Yes
XenServer 7.1 Cumulative Update 2	No

For those versions of XenServer that cannot have Citrix Hypervisor 8.2 applied as an update, instead use the Base Installation ISO and upgrade your existing installation. For more information, see Upgrade from an existing version.

Notes:

- If you use XenCenter to update your hosts, you must update your XenCenter installation to the latest version before beginning.
- Always update the pool master before updating any other hosts in a pool.
- When applying Citrix Hypervisor 8.2 Cumulative Update 1 as an update to an existing Citrix Hypervisor installation that uses the legacy disk partition layout, the update might fail with insufficient space. If this failure occurs, create a fresh installation of Citrix Hypervisor 8.2 Cumulative Update 1 instead.

Hotfixes

We might release hotfixes for Citrix Hypervisor 8.2 Cumulative Update 1 that provide fixes for specific issues.

Hotfixes for Citrix Hypervisor 8.2 Cumulative Update 1 are made available from the Citrix Knowledge Center. We recommend that customers regularly check the Knowledge Center for new updates. Alternatively, you can subscribe to email alerts for updates to Citrix Hypervisor by registering for an account at http://www.citrix.com/support/.

Hotfixes on the latest release are available to all Citrix Hypervisor customers. However, hotfixes on previous releases that are still in support are only available for customers with an active Citrix Customer Success Services (CSS) account.

Hotfixes on the LTSR stream are available to customers with an active CSS account. For more information, See Licensing.

Cumulative Updates

Cumulative Updates are provided for LTSRs of Citrix Hypervisor. These updates provide fixes for issues, and may contain support for new guests and hardware.

Cumulative Updates are available to customers with an active CSS account.

Configure XenCenter to download updates

Downloading updates from https://support.citrix.com is restricted to customers with a Citrix account. Some updates are only available to customers who are part of Citrix Success Services. These restrictions are now enforced by XenCenter.

To receive updates through XenCenter, you must first install the latest version of XenCenter and obtain a client ID JSON file. For more information, see Authenticating your XenCenter to receive updates.

Prepare a pool for an update

Updates to Citrix Hypervisor can be delivered as a hotfix or a Cumulative Update or a Current Release. Pay careful attention to the release notes published with each update. Each update can have unique installation instructions, particularly regarding preparatory and post-update operations. The following sections offer general guidance and instructions for applying updates to your Citrix Hypervisor systems.

Before you apply an update to the Citrix Hypervisor pool, pay careful attention to the following:

- All hosts in the pool must be running Citrix Hypervisor 8.2 before you apply the hotfix.
- Back up your data before applying an update. For backup procedures, see Disaster recovery and backup.
- If you have Windows VMs running in your pool that will be migrated as part of the update, take the following steps for each VM:
  - Set the value of the following registry key to a REG_DWORD value of '3': `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`
  - Ensure that the latest version of the Citrix VM Tools for Windows is installed
  - Take a snapshot of the VM
- Update all servers in a pool within a short period: running a mixed-mode pool (a pool that includes updated and non-updated servers) is not a supported configuration. Scheduled your updates to minimize the amount of time that a pool runs in a mixed state.
- Update all servers within a pool sequentially, always starting with the pool master. XenCenter's **Install Update** wizard manages this process automatically.
- After applying an update to all hosts in a pool, update any required driver disks before restarting Citrix Hypervisor servers.
- After applying a Cumulative Update or Current Release to a host, apply any hotfixes released for that Cumulative Update or Current Release before migrating VMs onto the host.
- Legacy SSL mode is no longer supported. Disable this mode on all hosts in your pool before attempting to update to the latest version on Citrix Hypervisor. To disable legacy SSL mode, run the following command on your pool master before you begin the update: `xe pool-disable-ssl-legacy uuid=<pool_uuid>`
- The Container Management supplemental pack is no longer supported. After you update or upgrade to the latest version of Citrix Hypervisor, you can no longer use the features of this supplemental pack.
- The vSwitch Controller is no longer supported. Disconnect the vSwitch Controller from your pool before attempting to update to the latest version on Citrix Hypervisor. After the update, the following configuration changes take place:
  - Cross-server private networks revert to single-server private networks.
  - Any Quality of Service settings made through the DVSC console are no longer applied. Network rate limits are no longer enforced.
  - ACL rules are removed. All traffic from VMs is allowed.
  - Port mirroring (RSPAN) is disabled.

If, after update or upgrade, you find leftover state about the vSwitch Controller in your pool, clear the state with the following CLI command: `xe pool-set-vswitch-controller address=`

Before you begin updating

- Log into a user account with full access permissions (for example, as a Pool Administrator or using a local root account).
- Empty the CD/DVD drives of any VMs you plan to suspend. For details and instructions, see Before Upgrading a Single Citrix Hypervisor server.
- If applicable, disable high availability.

Apply updates to a pool

The update installation mechanism in XenCenter allows you to download and extract the selected update from the Support website. You can apply an update to multiple hosts and pools simultaneously using the **Install Update** wizard. During the process, the **Install Update** wizard completes the following steps for each server:

- Migrates VMs off the server
- Places the server in maintenance mode
- Applies the update to the server
- Reboots the host if necessary
- Migrates the VMs back to the updated host.

Any actions taken at the precheck stage to enable the updates to be applied, such as turning off HA, are reverted.

The **Install Update** wizard carries out a series of checks known as Prechecks before starting the update process. These checks ensure that the pool is in a valid configuration state. It then manages the update path and VM migration automatically. If you prefer to control the update path and VM migration manually, you can update each host individually.

Apply updates automatically

XenCenter allows you to apply automated updates that are required to bring your servers up-to-date. You can apply these updates to one or more pools. When you apply automated updates, XenCenter applies the minimum set of updates that are required to bring the selected pool or the standalone server up-to-date. XenCenter minimizes the number of reboots required to bring the pool or the standalone server pool up-to-date. Where possible, XenCenter limits it to a single reboot at the end. For more information, see Apply Automated Updates.

View available updates

The **Updates** section of the **Notifications** view lists the updates that are available for all connected servers and pools.

Notes:

- By default, XenCenter periodically checks for Citrix Hypervisor and XenCenter updates. Click **Refresh** to check manually for available updates.
- If you have disabled automatic check for updates, a message appears on the **Updates** tab. Click **Check for Updates Now** to check for updates manually.

You can select from the **View** list whether to view the list of updates **By Update** or **By Server**.

When you view the list of updates by update, XenCenter displays the list of updates. You can order these updates by server/pool or by date.

- Cumulative Updates and new releases are displayed at the top of this list. Not all new releases can be applied as an update.
- To export this information as a .csv file, click **Export All**. The .csv file lists the following information:
  - Update name
  - Description of the update
  - Servers that this update can be applied to
  - Timestamp of the update
  - A reference to the webpage that the update is downloaded from
- To apply an update to a server, from the **Actions** list for that update select **Download and Install**. This option extracts the update and opens the **Install Update** wizard on the **Select Servers** page with the relevant servers selected. For more information, see Apply an update to a pool.
- To open the release note of an update in your browser, click the **Actions** list and select **Go to Web Page**.

When you view the list of updates by server, XenCenter displays the list of servers connected to XenCenter. This list shows both the updates that you can apply to the servers and the updates that are already installed on the servers.

- To export this information as a .csv file, click Export All. The .csv file lists the following information:
  - Pool that the server belongs to
  - Server name
  - Status of the installed Citrix Hypervisor
  - Update status of the server
  - Required updates for this server
  - Installed updates for this server.
- To apply the updates, click **Install Updates**. This choice opens the **Install Update** wizard on the **Select Update** page. For more information, see Apply an update to a pool.

Apply an update to a pool

To apply an update to a pool by using XenCenter:

1. From the XenCenter menu, select **Tools** and then **Install Update**.

2. Read the information displayed on the **Before You Start** page and then click **Next**.

3. The Install Update wizard lists available updates on the **Select Update** page. Select the required update from the list and then click **Next**.

4. On the **Select Servers** page, select the pool and servers that you want to update.

   When applying a Cumulative Update or a Current Release, you can also select whether to apply the minimal set of hotfixes for the CU or CR.

   Click **Next**.

5. The **Install Update** wizard performs several prechecks to ensure that the pool is in a valid configuration state.

   The wizard also checks the following conditions:

   - Whether the hosts must be rebooted after the update is applied and displays the result.
   - Whether a live patch is available for the hotfix and whether the live patch can be applied to the hosts. For information about live patching, see Live Patching.

6. Follow the on-screen recommendations to resolve any update prechecks that have failed. If you want XenCenter to resolve all failed prechecks automatically, click **Resolve All**. When the prechecks have been resolved, click **Next**.

7. If you are installing a CU or a CR, XenCenter downloads the updates, uploads them to the default SR of the pool, and installs the updates. The **Upload and Install** page displays the progress.

   Notes:

   - If the default SR in a pool is not shared or does not have enough space, XenCenter tries to upload the update to another shared SR. If none of the shared SRs have sufficient space, the update is uploaded to local storage of the pool master.
   - If the update process cannot complete for any reason, XenCenter halts the process. This action allows you to fix the issue and resume the update process by clicking the **Retry** button.

   See Step 10. to complete the installation process.

8. If you are installing a hotfix, choose an **Update Mode**. Review the information displayed on the screen and select an appropriate mode. If the hotfix contains a live patch that can be successfully applied to the hosts, it displays `No action required` on the **Tasks to be performed** screen.

   Note:

   If you click **Cancel** at this stage, the Install Update wizard reverts the changes and removes the update file from the server.

9. Click **Install update** to proceed with the installation. The Install Update wizard shows the progress of the update, displaying the major operations that XenCenter performs while updating each server in the

pool.

10. When the update is applied, click **Finish** to close Install Update wizard. If you chose to perform post-update tasks manually, do so now.

Update a pool of Citrix Hypervisor servers by using the xe CLI

To update a pool of Citrix Hypervisor hosts by using the xe CLI:

1. Download the update file to a known location on the computer running the xe CLI. Note the path to the file.

2. Upload the update file to the pool you want to update by running the following:

```
xe -s server -u username -pw password update-upload file-name=filename [sr-uuid=storage_repository_uuid]
```

   Here, `-s` refers to the name of the pool master. Citrix Hypervisor assigns the update file a UUID, which this command prints. Note the UUID.

   > **Tip:**
   >
   > After an update file has been uploaded to the Citrix Hypervisor server, you can use the `update-list` and `update-param-list` commands to view information about the file.

3. If Citrix Hypervisor detects any errors or preparatory steps that have not been taken, it alerts you. Be sure to follow any guidance before continuing with the update.

   If necessary, you can shut down or suspend any VMs on the hosts that you want to update by using the `vm-shutdown` or `vm-suspend` commands.

   To migrate specified VMs to specified hosts, use the `vm-migrate` command. By using the `vm-migrate` command, you have full control over the distribution of migrated VMs to other hosts in the pool.

   To live migrate all VMs to other hosts in the pool automatically, use the `host-evacuate` command. By using the `host-evacuate` command, you leave the distribution of migrated VMs to Citrix Hypervisor.

4. Update the pool, specifying the UUID of the update file, by running the following:

```
xe update-pool-apply uuid=UUID_of_file
```

   This command applies the update or hotfix to all hosts in the pool, starting with the pool master.

   Or, to update and restart hosts in a rolling manner, you can apply the update file to an individual host by running the following command:

```
xe update-apply host=host uuid=UUID_of_file
```

Ensure that you update the pool master before you update any other pool member.

5. Verify that the update was applied by using the `update-list` command. If the update has been successful, the `hosts` field contains the host UUID.

6. Perform any post-update operations that are required, such as restarting the XAPI toolstack or rebooting the hosts. Perform these operations on the pool master first.

Update individual hosts by using the xe CLI

To update individual hosts by using the xe CLI:

1. Download the update file to a known location on the computer running the xe CLI. Note the path to the file.

2. Shut down or suspend any VMs on the hosts that you want to update by using the `vm-shutdown` or `vm-suspend` commands.

3. Upload the update file to the host you want to update by running the following:

```
xe -s server -u username -pw password update-upload file-name=filename [sr-uuid=storage_repository_uuid]
```

Here, `-s` refers to the host name. Citrix Hypervisor assigns the update file a UUID, which this command prints. Note the UUID.

> **Tip:**
>
> After an update file has been uploaded to the Citrix Hypervisor server, you can use the `update-list` and `update-param-list` commands to view information about the update file.

4. If Citrix Hypervisor detects any errors or preparatory steps that have not been taken, it alerts you. Be sure to follow any guidance before continuing with the update.

5. Update the host, specifying the UUIDs of the host and the update file, by running the following:

```
xe update-apply host-uuid=UUID_of_host uuid=UUID_of_file
```

If the host is a member of a pool, ensure that you update the pool master before you update any other pool member.

6. Verify that the update has been successfully applied by using the `update-list` command. If the update has been successful, the `hosts` field contains the host UUID.

7. Perform any post-update operations, as necessary (such as, restarting the XAPI toolstack, or rebooting the host).

Apply Automated Updates

Automated Updates mode applies any hotfixes and Cumulative Updates that are available for a host. This mode minimizes the number of reboots required to bring the pool or the standalone server pool up-to-date. Where possible, **Automated Updates** mode limits it to a single reboot at the end.

If a new Current Release version is available as an update, **Automated Updates** mode does not apply this update. Instead, you must select manually to update to the new Current Release.

XenCenter requires internet access to fetch the required updates.

To view the list of required updates, perform the following steps:

1. Select the host on the **Resources** pane in XenCenter.
2. Navigate to the **General** tab.
3. Expand the **Updates** section.

   You can see:

   - **Applied** – lists already-applied updates.
   - **Required Updates** – lists the set of updates required to bring the server up-to-date.

     > **Note:**
     >
     > If there are no updates required, the **Required Updates** section is not displayed.

   - **Installed supplemental packs** – lists supplemental packs that are installed on the server (if any).

     > **Note:**
     >
     > If you select a pool instead of a server, the **Updates** section lists updates that are already applied as **Fully Applied**.

If you want to choose and install a particular update, see Apply an update to a pool.

> **Note:**
>
> The Automated Updates feature is available for Citrix Hypervisor Premium Edition customers, or those customers who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement. To learn more about Citrix Hypervisor editions, and to find out how to upgrade, visit the Citrix website. For more information, see Licensing.
>
> The Automated Updates feature is available for Citrix Hypervisor Premium Edition customers.

Apply Automated Updates by using the Install Update wizard

The following section provides step-by-step instructions on how to apply the set of required updates automatically to bring your pool or standalone host up-to-date.

1. From the XenCenter menu, select **Tools** and then select **Install Update**.
2. Read the information displayed on the **Before You Start** page and then click **Next**.
3. On the **Select Update** page, select the mechanism to use to install the updates. You can see the following options:
   - **Automated Updates** – (default) this option is visible only if XenCenter is connected to at least one licensed pool or a licensed standalone server. Select this option to download and install all the current updates automatically to bring the pool or a standalone server up-to-date.
   - **Download update from Citrix** – the Install Update wizard lists available updates from the Support site. To apply the updates, see Apply an update to a pool.
   - **Select update or Supplemental pack from disk** – to install an update you have already downloaded, see Apply an update to a pool. To install supplemental pack updates, see the Installing Supplemental Packs article in XenCenter documentation.
4. To continue with the automatic application of hotfixes, select **Automated Updates** and then click **Next**.
5. Select one or more pools or standalone servers that you want to update and click **Next**. Any server or pool that cannot be updated appears unavailable.
6. The **Install Update** wizard performs several update prechecks, to ensure that the pool is in a valid configuration state.

   Follow the on-screen recommendations to resolve any update prechecks that have failed. If you want XenCenter to resolve all failed prechecks automatically, click **Resolve All**. When the prechecks have been resolved, click **Next**.
7. The Install Update wizard automatically downloads and installs the recommended updates. The wizard also shows the overall progress of the update, displaying the major operations that XenCenter performs while updating each server in the pool.

   Notes:
   - The updates are uploaded to the default SR of the pool. If the default SR is not shared or does not have enough space, XenCenter tries to upload the update to another shared SR with sufficient space. If none of the shared SRs have sufficient space, the update is uploaded to local storage on each host.
   - The update process cannot complete for any reason, XenCenter halts the process. This allows you to fix the issue and resume the update process by clicking the **Retry** button.
8. When all the updates have been applied, click **Finish** to close Install Update wizard.

Live patching in Citrix Hypervisor

The live patching feature applies to hotfixes only. Current Releases and Cumulative Updates cannot be applied as live patches.

Citrix Hypervisor customers who deploy Citrix Hypervisor servers can often be required to reboot their hosts after applying hotfixes. This rebooting results in unwanted downtime for the hosts while customers have to wait until the system is restarted. This unwanted downtime can impact business. Live patching enables customers to install some Linux kernel and Xen hypervisor hotfixes without having to reboot the hosts. Such hotfixes include both a live patch, which is applied to the memory of the host, and a hotfix that updates the files on disk. Using live patching can reduce maintenance costs and downtime.

When applying an update by using XenCenter, the **Install Update** wizard checks whether the hosts must be rebooted after the update is applied. XenCenter displays the result on the **Prechecks** page. This check enables customers to know the post-update tasks well in advance and schedule the application of hotfixes accordingly.

> **Note:**
>
> Citrix Hypervisor Live Patching is available for Citrix Hypervisor Premium Edition customers, or those customers who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement. To learn more about Citrix Hypervisor editions, and to find out how to upgrade, visit the Citrix website. For detailed information about Licensing, see Licensing.

Live patching scenarios

Hotfixes can be live patched across pools, hosts, or on a standalone server. Some require a reboot, some require the XAPI toolstack to be restarted, and some hotfixes do not have any post-update tasks. The following scenarios describe the behavior when a Live Patch is and is not available for an update.

- **Updates with a live patch** — Some hotfixes that update the Linux kernel and the Xen hypervisor usually do not require a reboot after applying the hotfix. However, in some rare cases, when the live patch cannot be applied, a reboot might be required.
- **Updates without a live patch** — No change in the behavior here. It works as usual.

  > **Note:**
  >
  > If a host does not require a reboot, or if the hotfix contains live patches, XenCenter displays `No action required` on the **Update Mode** page.

Apply Automated Updates and live patching

Automated Updates mode in XenCenter enables you to download and apply the minimum set of hotfixes required to bring your pool or standalone host up-to-date automatically. **Automated Updates** mode does apply any Cumulative Updates that are available for a host. However, if a new Current Release version is available as an update, **Automated Updates** mode does not apply this update. You must manually select to update to the new Current Release.

You can benefit from the live patching feature when you apply hotfixes using the Automated Updates mode in XenCenter. You can avoid rebooting hosts if live patches are available and are successfully applied to the hosts that are updated using **Automated Updates** mode. For more information about the Automated Updates, see Apply Automated Updates.

Enable live patching by using XenCenter and the xe CLI

Live patching feature is enabled by default. Customers can enable or disable live patching using XenCenter or xe CLI command.

Using XenCenter

1. Select the pool or the standalone host on the **Resource** pane.
2. From the **Pool** menu (**Server** in case on standalone hosts) menu, select **Properties** and then click **Live Patching**.
3. On the **Live Patching** page:
    - Select **Use live Patching when possible** to enable live patching.
    - Select **Don't use Live Patching** to disable live patching.

Using the xe CLI

- To enable live patching, run the following command:

```
xe pool-param-set live-patching-disabled=false uuid="pool_uuid"
```

- To disable live patching, run the following command:

```
xe pool-param-set live-patching-disabled=true uuid="pool_uuid"
```

Troubleshoot the installation

Citrix provides two forms of support: free, self-help support from www.citrix.com/support and paid-for Support Services, which you can purchase from the Support site. With Citrix Technical Support, you can open a Support Case online or contact the support center by phone.

The Citrix support site, www.citrix.com/support, hosts various resources. These resources might be helpful to you if you experience odd behavior, crashes, or other problems during installation. Resources include: forums, knowledge base articles, software updates, security bulletins, tools, and product documentation.

Using a keyboard connected directly to the host machine (not connected over a serial port), you can access three virtual terminals during installation:

- Press **Alt+F1** to access the main Citrix Hypervisor Installer
- Press **Alt+F2** to access a local shell
- Press **Alt+F3** to access the event log

If you experience an unknown error during installation, capture the log file from your host and provide it to Technical Support. To capture the log file, complete the following procedure.

To capture and save the log files:

1. Press **Alt+F2** to access the local shell.
2. Enter the following:

   ```
   /opt/xensource/installer/report.py
   ```

3. You are prompted to choose where you want to save the log file: **NFS**, **FTP**, or **Local media**.

   Select **NFS** or **FTP** to copy the log file to another machine on your network. To do so, networking must be working properly, and you must have write access to a remote machine.

   Select **Local media** to save the file to a removable storage device, such as a USB flash drive, on the local machine.

   Once you have made your selections, the program writes the log file to your chosen location. The file name is `support.tar.bz2`.

Send the captured log file to the Support team for them to inspect.

Hosts and resource pools

This section describes how resource pools can be created through a series of examples using the xe command line interface (CLI). A simple NFS-based shared storage configuration is presented and several simple VM management examples are discussed. It also contains procedures for dealing with physical node failures.

Citrix Hypervisor servers and resource pools overview

A *resource pool* comprises multiple Citrix Hypervisor server installations, bound together to a single managed entity which can host Virtual Machines. If combined with shared storage, a resource pool enables VMs to be started on *any* Citrix Hypervisor server which has sufficient memory. The VMs can then be dynamically moved among Citrix Hypervisor servers while running with a minimal downtime (live migration). If an individual Citrix Hypervisor server suffers a hardware failure, the administrator can restart failed VMs on another Citrix Hypervisor server in the same resource pool. When high availability is enabled on the resource pool, VMs automatically move to another host when their host fails. Up to 64 hosts are supported per resource pool, although this restriction is not enforced.

A pool always has at least one physical node, known as the *master*. Only the master node exposes an administration interface (used by XenCenter and the Citrix Hypervisor Command Line Interface, known as the xe CLI). The master forwards commands to individual members as necessary.

> **Note:**
>
> When the pool master fails, master re-election takes place only if high availability is enabled.

Requirements for creating resource pools

A resource pool is a homogeneous (or heterogeneous with restrictions) aggregate of one or more Citrix Hypervisor servers, up to a maximum of 64. The definition of homogeneous is:

- CPUs on the server joining the pool are the same (in terms of the vendor, model, and features) as the CPUs on servers already in the pool.
- The server joining the pool is running the same version of Citrix Hypervisor software, at the same patch level, as servers already in the pool.

The software enforces extra constraints when joining a server to a pool. In particular, Citrix Hypervisor checks that the following conditions are true for the server joining the pool:

- The server is not a member of an existing resource pool.
- The server has no shared storage configured.
- The server is not hosting any running or suspended VMs.
- No active operations are in progress on the VMs on the server, such as a VM shutting down.

- The clock on the server is synchronized to the same time as the pool master (for example, by using NTP).
- The management interface of the server is not bonded. You can configure the management interface when the server successfully joins the pool.
- The management IP address is static, either configured on the server itself or by using an appropriate configuration on your DHCP server.

Citrix Hypervisor servers in resource pools can contain different numbers of physical network interfaces and have local storage repositories of varying size. In practice, it is often difficult to obtain multiple servers with the exact same CPUs, and so minor variations are permitted. If it is acceptable to have hosts with varying CPUs as part of the same pool, you can force the pool joining operation by passing `--force` parameter.

All hosts in the pool must be in the same site and connected by a low latency network.

> **Note:**
>
> Servers providing shared NFS or iSCSI storage for the pool must have a static IP address.

A pool must contain shared storage repositories to select on which Citrix Hypervisor server to run a VM and to move a VM between Citrix Hypervisor servers dynamically. If possible create a pool after shared storage is available. We recommend that you move existing VMs with disks located in local storage to shared storage after adding shared storage. You can use the `xe vm-copy` command or use XenCenter to move VMs.

Create a resource pool

Resource pools can be created using XenCenter or the CLI. When a new host joins a resource pool, the joining host synchronizes its local database with the pool-wide one, and inherits some settings from the pool:

- VM, local, and remote storage configuration is added to the pool-wide database. This configuration is applied to the joining host in the pool unless you explicitly make the resources shared after the host joins the pool.
- The joining host inherits existing shared storage repositories in the pool. Appropriate PBD records are created so that the new host can access existing shared storage automatically.
- Networking information is partially inherited to the joining host: the *structural* details of NICs, VLANs, and bonded interfaces are all inherited, but *policy* information is not. This policy information, which must be reconfigured, includes:
    - The IP addresses of management NICs, which are preserved from the original configuration.
    - The location of the management interface, which remains the same as the original configuration. For example, if the other pool hosts have management interfaces on a bonded interface, the joining host must be migrated to the bond after joining.
    - Dedicated storage NICs, which must be reassigned to the joining host from XenCenter or the CLI, and the PBDs replugged to route the traffic accordingly. This is because IP addresses are not assigned as part of the pool join operation, and the storage NIC works only when this is

correctly configured. For more information on how to dedicate a storage NIC from the CLI, see Manage networking.

Note:

You can only join a new host to a resource pool when the host's management interface is on the same tagged VLAN as that of the resource pool.

To join Citrix Hypervisor servers host1 and host2 into a resource pool by using the CLI

1. Open a console on Citrix Hypervisor server *host2*.
2. Command Citrix Hypervisor server *host2* to join the pool on Citrix Hypervisor server *host1* by issuing the command:

   ```
   xe pool-join master-address=host1 master-username=administrators_username
   master-password=password
   ```

   The `master-address` must be set to the fully qualified domain name of Citrix Hypervisor server *host1*. The `password` must be the administrator password set when Citrix Hypervisor server *host1* was installed.

Citrix Hypervisor servers belong to an unnamed pool by default. To create your first resource pool, rename the existing nameless pool. Use tab-complete to find the `pool_uuid`:

```
xe pool-param-set name-label="New Pool" uuid=pool_uuid
```

Create heterogeneous resource pools

Citrix Hypervisor simplifies expanding deployments over time by allowing disparate host hardware to be joined in to a resource pool, known as heterogeneous resource pools. Heterogeneous resource pools are made possible by using technologies in Intel (FlexMigration) and AMD (Extended Migration) CPUs that provide CPU "masking" or "leveling". The CPU masking and leveling features allow a CPU to be configured to *appear* as providing a different make, model, or functionality than it actually does. This feature enables you to create pools of hosts with disparate CPUs but still safely support live migration.

Note:

The CPUs of Citrix Hypervisor servers joining heterogeneous pools must be of the same vendor (that is, AMD, Intel) as CPUs on hosts in the pool. However, the specific type (family, model, and stepping numbers) need not be.

Citrix Hypervisor simplifies the support of heterogeneous pools. Hosts can now be added to existing resource pools, irrespective of the underlying CPU type (as long as the CPU is from the same vendor family). The pool feature set is dynamically calculated every time:

- A new host joins the pool
- A pool member leaves the pool
- A pool member reconnects following a reboot

Any change in the pool feature set does not affect VMs that are currently running in the pool. A Running VM continues to use the feature set which was applied when it was started. This feature set is fixed at boot and persists across migrate, suspend, and resume operations. If the pool level drops when a less-capable host joins the pool, a running VM can be migrated to any host in the pool, except the newly added host. When you move or migrate a VM to a different host within or across pools, Citrix Hypervisor compares the VM's feature set against the feature set of the destination host. If the feature sets are found to be compatible, the VM is allowed to migrate. This enables the VM to move freely within and across pools, regardless of the CPU features the VM is using. If you use Workload Balancing to select an optimal destination host to migrate your VM, a host with incompatible feature set will not be recommended as the destination host.

Add shared storage

For a complete list of supported shared storage types, see Storage repository formats. This section shows how shared storage (represented as a storage repository) can be created on an existing NFS server.

To add NFS shared storage to a resource pool by using the CLI

1. Open a console on any Citrix Hypervisor server in the pool.
2. Create the storage repository on server:/path by issuing the command

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

   `device-config:server` Is the host name of the NFS server and `device-config:serverpath` is the path on the NFS server. As `shared` is set to true, shared storage is automatically connected to every Citrix Hypervisor server in the pool. Any Citrix Hypervisor servers that join later are also connected to the storage. The Universally Unique Identifier (UUID) of the storage repository is printed on the screen.
3. Find the UUID of the pool by running the following command:

   ```
   xe pool-list
   ```
4. Set the shared storage as the pool-wide default with the command

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

As the shared storage has been set as the pool-wide default, all future VMs have their disks created on shared storage by default. For information about creating other types of shared storage, see Storage repository formats.

Remove Citrix Hypervisor servers from a resource pool

> **Note:**
>
> Before removing any Citrix Hypervisor server from a pool, ensure that you shut down all the VMs running on that host. Otherwise, you can see a warning stating that the host cannot be removed.

When you remove (*eject*) a host from a pool, the machine is rebooted, reinitialized, and left in a state similar to a fresh installation. Do not eject Citrix Hypervisor servers from a pool if there is important data on the local disks.

To remove a host from a resource pool by using the CLI

1. Open a console on any host in the pool.
2. Find the UUID of the host by running the command

   ```
   xe host-list
   ```

3. Eject the required host from the pool:

   ```
   xe pool-eject host-uuid=host_uuid
   ```

   The Citrix Hypervisor server is ejected and left in a freshly installed state.

   > **Warning:**
   >
   > Do *not* eject a host from a resource pool if it contains important data stored on its local disks. All of the data is erased when a host is ejected from the pool. If you want to preserve this data, copy the VM to shared storage on the pool using XenCenter, or the `xe vm-copy` CLI command.

When Citrix Hypervisor servers containing locally stored VMs are ejected from a pool, the VMs will be present in the pool database. The locally stored VMs are also visible to the other Citrix Hypervisor servers. The VMs do not start until the virtual disks associated with them have been changed to point at shared storage seen by other Citrix Hypervisor servers in the pool, or removed. Therefore, we recommend that you move any local storage to shared storage when joining a pool. Moving to shared storage allows individual Citrix Hypervisor servers to be ejected (or physically fail) without loss of data.

Note:

When a host is removed from a pool that has its management interface on a tagged VLAN network, the machine is rebooted and its management interface will be available on the same network.

Prepare a pool of Citrix Hypervisor servers for maintenance

Before performing maintenance operations on a host that is part of a resource pool, you must disable it. Disabling the host prevents any VMs from being started on it. You must then migrate its VMs to another Citrix Hypervisor server in the pool. You can do this by placing the Citrix Hypervisor server in to Maintenance mode using XenCenter. For more information, see Run in maintenance mode in the XenCenter documentation.

Backup synchronization occurs every 24 hrs. Placing the master host in to maintenance mode results in the loss of the last 24 hrs of RRD updates for offline VMs.

Warning:

We highly recommend rebooting all Citrix Hypervisor servers before installing an update and then verifying their configuration. Some configuration changes only take effect when Citrix Hypervisor is rebooted, so the reboot may uncover configuration problems that can cause the update to fail.

To prepare a host in a pool for maintenance operations by using the CLI

1. Run the following command:

   ```
   xe host-disable uuid=Citrix Hypervisor_host_uuid
   xe host-evacuate uuid=Citrix Hypervisor_host_uuid
   ```

   This command disables the Citrix Hypervisor server and then migrate any running VMs to other Citrix Hypervisor servers in the pool.

2. Perform the desired maintenance operation.

3. Enable the Citrix Hypervisor server when the maintenance operation is complete:

   ```
   xe host-enable
   ```

4. Restart any halted VMs and resume any suspended VMs.

Export resource pool data

The Export Resource Data option allows you to generate a resource data report for your pool and export the report into a .xls or .csv file. This report provides detailed information about various resources in the pool such as, servers, networks, storage, virtual machines, VDIs, and GPUs. This feature enables administrators to track, plan, and assign resources based on various workloads such as CPU, storage, and Network.

Note:

Export Resource Pool Data is available for Citrix Hypervisor Premium Edition customers, or those who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement.

The list of resources and various types of resource data that are included in the report:

Server:

- Name
- Pool Master
- UUID
- Address
- CPU Usage
- Network (avg/max KBs)
- Used Memory
- Storage
- Uptime
- Description

Networks:

- Name
- Link Status
- MAC
- MTU
- VLAN
- Type
- Location

VDI:

- Name
- Type
- UUID
- Size
- Storage
- Description

Storage:

- Name
- Type
- UUID
- Size
- Location
- Description

VMs:

- Name
- Power State
- Running on
- Address
- MAC
- NIC
- Operating System
- Storage
- Used Memory
- CPU Usage
- UUID
- Uptime
- Template
- Description

GPU:

- Name
- Servers
- PCI Bus Path
- UUID
- Power Usage
- Temperature
- Used Memory
- Computer Utilization

> **Note:**
>
> Information about GPUs is available only if there are GPUs attached to your Citrix Hypervisor server.

To export resource data

1. In the XenCenter Navigation pane, select **Infrastructure** and then select the pool.
2. Select the **Pool** menu and then **Export Resource Data**.
3. Browse to a location where you would like to save report and then click **Save**.

Host power on

Powering on hosts remotely

You can use the Citrix Hypervisor server Power On feature to turn a server on and off remotely, either from XenCenter or by using the CLI.

To enable host power, the host must have one of the following power-control solutions:

- **Wake on LAN enabled network card**.

- **Dell Remote Access Cards (DRAC)**. To use Citrix Hypervisor with DRAC, you must install the Dell supplemental pack to get DRAC support. DRAC support requires installing RACADM command-line utility on the server with the remote access controller and enabling DRAC and its interface. RACADM is often included in the DRAC management software. For more information, see Dell's DRAC documentation.
- A custom script based on the management API that enables you to turn the power on and off through Citrix Hypervisor. For more information, see *Configuring a custom script for the Host Power On feature* in the following section.

Using the Host Power On feature requires two tasks:

1. Ensure the hosts in the pool support controlling the power remotely. For example, they have Wake on LAN functionality or a DRAC card, or you have created a custom script).
2. Enable the Host Power On functionality using the CLI or XenCenter.

Use the CLI to manage host power on

You can manage the Host Power On feature using either the CLI or XenCenter. This section provides information about managing it with the CLI.

Host Power On is enabled at the host level (that is, on each Citrix Hypervisor).

After you enable Host Power On, you can turn on hosts using either the CLI or XenCenter.

To enable host power on by using the CLI

Run the command:

```
xe host-set-power-on-mode host=<host uuid> \
    power-on-mode="" , "wake-on-lan", "DRAC","custom") \
    power-on-config=key:value
```

For DRAC the keys are `power_on_ip` to specify the password if you are using the secret feature. For more information, see Secrets.

To turn on hosts remotely by using the CLI

Run the command:

```
xe host-power-on host=<host uuid>
```

Configure a custom script for the Host Power On feature

If your server's remote-power solution uses a protocol that is not supported by default (such as Wake-On-Ring or Intel Active Management Technology), you can create a custom Linux Python script to turn on your

Citrix Hypervisor computers remotely. However, you can also create custom scripts for DRAC and Wake on LAN remote-power solutions.

This section provides information about configuring a custom script for Host Power On using the key/value pairs associated with the Citrix Hypervisor API call `host.power_on`.

When you create a custom script, run it from the command line each time you want to control power remotely on Citrix Hypervisor. Alternatively, you can specify it in XenCenter and use the XenCenter UI features to interact with it.

The Citrix Hypervisor API is documented in the document, the Citrix Hypervisor Management API, which is available from the developer documentation website.

> **Warning:**
>
> Do not change the scripts provided by default in the `/etc/xapi.d/plugins/` directory. You can include new scripts in this directory, but you must never change the scripts contained in that directory after installation.

Key/Value Pairs

To use Host Power On, configure the `host.power_on_mode` and `host.power_on_config` keys. See the following section for information about the values.

There is also an API call that lets you set these fields simultaneously:

```
void host.set_host_power_on_mode(string mode, Dictionary<string,string> config)
```

host.power_on_mode

- **Definition**: Contains key/value pairs to specify the type of remote-power solution (for example, Dell DRAC).
- **Possible values**:
  - An empty string, representing power-control disabled
  - "DRAC": Lets you specify Dell DRAC. To use DRAC, you must have already installed the Dell supplemental pack.
  - "wake-on-lan": Lets you specify Wake on LAN.
  - Any other name (used to specify a custom power-on script). This option is used to specify a custom script for power management.
- **Type**: string

host.power_on_config

- **Definition**: Contains key/value pairs for mode configuration. Provides additional information for DRAC.
- **Possible values:**
  - If you configured DRAC as the type of remote-power solution, you must also specify one of the following keys:
    - "power_on_ip": The IP address you specified configured to communicate with the power-control card. Alternatively, you can type the domain name for the network interface where DRAC is configured.
    - "power_on_user": The DRAC user name associated with the management processor, which you may have changed from its factory default settings.
    - "power_on_password_secret": Specifies using the secrets feature to secure your password.
  - To use the secrets feature to store your password, specify the key "power_on_password_secret". For more information, see Secrets.
- **Type**: Map (string,string)

Sample script

The sample script imports the Citrix Hypervisor API, defines itself as a custom script, and then passes parameters specific to the host you want to control remotely. You must define the parameters `session` in all custom scripts.

The result appears when the script is unsuccessful.

```
import XenAPI
def custom(session,remote_host,
power_on_config):
result="Power On Not Successful"
for key in power_on_config.keys():
result=result+''
key=''+key+''
value=''+power_on_config[key]
return result
```

> **Note:**
>
> After creating the script, save it in /etc/xapi.d/plugins with a .py extension.

Communicate with Citrix Hypervisor servers and resource pools

TLS

Citrix Hypervisor uses the TLS 1.2 protocol to encrypt management API traffic. Any communication between Citrix Hypervisor and management API clients (or appliances) uses the TLS 1.2 protocol.

> **Important:**
>
> We do not support customer modifications to the cryptographic functionality of the product.

Citrix Hypervisor uses the following cipher suite:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

In addition, the following cipher suites are also supported for backwards compatibility with some versions of Citrix Virtual Apps and Desktops:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

SSH

When using an SSH client to connect directly to the Citrix Hypervisor server the following algorithms can be used:

Ciphers:

- aes128-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com
- aes128-cbc
- aes256-cbc

MACs:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1

KexAlgorithms:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1

HostKeyAlgorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

- ssh-ed25519
- ssh-rsa

> **Note:**
>
> To restrict the available ciphersuites to only those in the preceding list, ensure that you install Hotfix XS82E015 - For Citrix Hypervisor 8.2.

If you want to disable SSH access to your Citrix Hypervisor server, you can do this in `xsconsole`.

1. From XenCenter, open the server console and log in as `root`.
2. Type `xsconsole`.
3. In `xsconsole`, go to **Remote Service Configuration** > **Enable/Disable Remote Shell**.

   The console displays whether remote shell is enabled.
4. To change whether remote shell is enabled or disabled, press **Enter**.

> **Important:**
>
> We do not support customer modifications to the cryptographic functionality of the product.

Install a TLS certificate on your server

The Citrix Hypervisor server comes installed with a default TLS certificate. However, to use HTTPS to secure communication between Citrix Hypervisor and Citrix Virtual Apps and Desktops, install a certificate provided by a trusted certificate authority.

This section describes how to install certificates by using the xe CLI. For information about working with certificates by using XenCenter, see the XenCenter documentation.

Ensure that your TLS certificate and its key meet the following requirements:

- The certificate and key pair are an RSA key
- The key matches the certificate
- The key is provided in a separate file to the certificate
- The certificate is provided in a separate file to any intermediate certificates
- The key file must be one of the following types: `.pem` or `.key`
- Any certificate files must be one of the following types: `.pem`, `.cer`, or `.crt`
- The key is greater than or equal to 2048 bits and less than or equal to 4096 bits in length
- The key is an unencrypted PKCS #8 key and does not have a passkey
- The key and certificate are in base-64 encoded 'PEM' format
- The certificate is valid and has not expired
- The signature algorithm is SHA-2 (SHA256)

The xe CLI warns you when the certificate and key you choose do not meet these requirements.

You might already have a trusted certificate that you want to install on your Citrix Hypervisor server. However, you can instead create a certificate on your server and send it to a certificate authority to be signed. This method is more secure as the private key can remain on the Citrix Hypervisor server and not be copied between systems.

First, generate a private key and certificate signing request. On the Citrix Hypervisor server, complete the following steps:

1. To create a private key file, run the following command:

   ```
   openssl genrsa -des3 -out privatekey.pem 2048
   ```

2. Remove the password from the key:

   ```
   openssl rsa -in privatekey.pem -out privatekey.nop.pem
   ```

3. Create the certificate signing request by using the private key:

   ```
   openssl req -new -key privatekey.nop.pem -out csr
   ```

4. Follow the prompts to provide the information necessary to generate the certificate signing request.

   - **Country Name**. Enter the TLS Certificate country codes for your country. For example, CA for Canada or JM for Jamaica. You can find a list of TLS Certificate country codes on the web.
   - **State or Province Name (full name)**. Enter the state or province where the pool is located. For example, Massachusetts or Alberta.
   - **Locality Name**. The name of the city where the pool is located.
   - **Organization Name**. The name of your company or organization.
   - **Organizational Unit Name**. Enter the department name. This field is optional.
   - **Common Name**. Enter the FQDN of your Citrix Hypervisor server. Citrix recommends specifying either an FQDN or an IP address that does not expire.
   - **Email Address**. This email address is included in the certificate when you generate it.

   The certificate signing request is saved in the current directory and is named `csr`.

5. Display the certificate signing request in the console window by running the following command:

   ```
   cat csr
   ```

6. Copy the entire certificate signing request and use this information to request the certificate from the certificate authority.

After the certificate authority reponds to the certificate signing request, complete the following steps to install the certificate on your Citrix Hypervisor server:

1. Download the signed certificate, root certificate and, if the certificate authority has one, the intermediate certificate from the certificate authority.
2. Copy the key and certificates to the Citrix Hypervisor server.
3. Run the following command on the server:

   ```
   xe host-server-certificate-install certificate=<path_to_certificate_file>
   private-key=<path_to_private_key> certificate-chain=<path_to_chain_file>
   ```

   The `certificate-chain` parameter is optional.

For additional security, you can delete the private key file after the certificate is installed.

Rotate the pool secret

The pool secret is a secret shared among the servers in a pool that enables the server to prove its membership to a pool. Users with the Pool Admin role can view this secret when connecting to the server over SSH. Rotate the pool secret if one of these users leaves your organization or loses their Pool Admin role.

You can rotate the pool secret by using XenCenter. For more information, see Pool security

You can also rotate the pool secret by using the xe CLI. Run the following command on a server in the pool:

```
xe pool-secret-rotate
```

Enable IGMP snooping on your Citrix Hypervisor pool

Citrix Hypervisor sends multicast traffic to all guest VMs leading to unnecessary load on host devices by requiring them to process packets they have not solicited. Enabling IGMP snooping prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined, and improves the performance of multicast. IGMP snooping is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

You can enable IGMP snooping on a pool using either XenCenter or the command-line interface. To enable IGMP snooping using XenCenter, navigate to **Pool Properties** and select **Network Options**. For xe commands, see `pool-igmp-snooping`.

Notes:

- IGMP snooping is available only when network back-end uses Open vSwitch.
- When enabling this feature on a pool, it may also be necessary to enable IGMP querier on one of the physical switches. Or else, multicast in the sub network will fallback to broadcast and may decrease Citrix Hypervisor performance.

- When enabling this feature on a pool running IGMP v3, VM migration or network bond failover results in IGMP version switching to v2.
- To enable this feature with GRE network, users must set up an IGMP Querier in the GRE network. Alternatively, you can forward the IGMP query message from the physical network into the GRE network. Or else, multicast traffic in the GRE network can be blocked.

Manage users

Defining users, groups, roles and permissions allows you to control who has access to your Citrix Hypervisor servers and pools and what actions they can perform.

When you first install Citrix Hypervisor, a user account is added to Citrix Hypervisor automatically. This account is the local super user (LSU), or root, which Citrix Hypervisor authenticates locally.

The LSU, or root, is a special user account intended for system administration and has all permissions. In Citrix Hypervisor, the LSU is the default account at installation. Citrix Hypervisor authenticates the LSU account. LSU does not require any external authentication service. If an external authentication service fails, the LSU can still log in and manage the system. The LSU can always access the Citrix Hypervisor physical server through SSH.

You can create more users by adding the Active Directory accounts through either XenCenter's Users tab or the xe CLI. If your environment does not use Active Directory, you are limited to the LSU account.

> **Note:**
>
> When you create users, Citrix Hypervisor does not assign newly created user accounts RBAC roles automatically. Therefore, these accounts do not have any access to the Citrix Hypervisor pool until you assign them a role.

These permissions are granted through roles, as discussed in the *Authenticating users with Active Directory (AD)* section.

Authenticate users with Active Directory (AD)

If you want to have multiple user accounts on a server or a pool, you must use Active Directory user accounts for authentication. AD accounts let Citrix Hypervisor users log on to a pool using their Windows domain credentials.

> **Note:**
>
> You can enable LDAP channel binding and LDAP signing on your AD domain controllers. For more information, see Microsoft Security Advisory.

You can configure varying levels of access for specific users by enabling Active Directory authentication, adding user accounts, and assign roles to those accounts.

Active Directory users can use the xe CLI (passing appropriate `-u` and `-pw` arguments) and also connect to the host using XenCenter. Authentication is done on a per-resource pool basis.

Subjects control access to user accounts. A subject in Citrix Hypervisor maps to an entity on your directory server (either a user or a group). When you enable external authentication, Citrix Hypervisor checks the credentials used to create a session against the local root credentials and then against the subject list. To

permit access, create a subject entry for the person or group you want to grant access to. You can use XenCenter or the xe CLI to create a subject entry.

If you are familiar with XenCenter, note that the Citrix Hypervisor CLI uses slightly different terminology to refer to Active Directory and user account features: XenCenter Term Citrix Hypervisor CLI Term Users Subjects Add users Add subjects

Even though Citrix Hypervisor is Linux-based, Citrix Hypervisor lets you use Active Directory accounts for Citrix Hypervisor user accounts. To do so, it passes Active Directory credentials to the Active Directory domain controller.

When you add Active Directory to Citrix Hypervisor, Active Directory users and groups become Citrix Hypervisor subjects. The subjects are referred to as users in XenCenter. Users/groups are authenticated by using Active Directory on logon when you register a subject with Citrix Hypervisor. Users and groups do not need to qualify their user name by using a domain name.

To qualify a user name, you must type the user name in Down-Level log on Name format, for example, `mydomain\myuser`.

> **Note:**
>
> By default, if you did not qualify the user name, XenCenter attempts to log in users to AD authentication servers using the domain to which it is joined. The exception to this is the LSU account, which XenCenter always authenticates locally (that is, on the Citrix Hypervisor) first.

The external authentication process works as follows:

1. The credentials supplied when connecting to a server are passed to the Active Directory domain controller for authentication.
2. The domain controller checks the credentials. If they are invalid, the authentication fails immediately.
3. If the credentials are valid, the Active Directory controller is queried to get the subject identifier and group membership associated with the credentials.
4. If the subject identifier matches the one stored in the Citrix Hypervisor, authentication succeeds.

When you join a domain, you enable Active Directory authentication for the pool. However, when a pool joins a domain, only users in that domain (or a domain with which it has trust relationships) can connect to the pool.

> **Note:**
>
> Manually updating the DNS configuration of a DHCP-configured network PIF is unsupported and can cause AD integration, and therefore user authentication, to fail or stop working.

Configure Active Directory authentication

Citrix Hypervisor supports use of Active Directory servers using Windows 2008 or later.

To authenticate Active Directory for Citrix Hypervisor servers, you must use the same DNS server for both the Active Directory server (configured to allow interoperability) and the Citrix Hypervisor server. In some configurations, the active directory server can provide the DNS itself. This can be achieved either using DHCP to provide the IP address and a list of DNS servers to the Citrix Hypervisor server. Alternatively, you can set the values in the PIF objects or use the installer when a manual static configuration is used.

We recommend enabling DHCP to assign host names. Do not assign the hostnames `localhost` or `linux` to hosts.

> **Warning:**
>
> Citrix Hypervisor server names must be unique throughout the Citrix Hypervisor deployment.

Note the following:

- Citrix Hypervisor labels its AD entry on the AD database using its hostname. If two Citrix Hypervisor servers with the same hostname are joined to the same AD domain, the second Citrix Hypervisor overwrites the AD entry of the first Citrix Hypervisor. The overwriting occurs regardless of whether the hosts belong to the same or different pools. This can cause the AD authentication on the first Citrix Hypervisor to stop working.

  You can use the same host name in two Citrix Hypervisor servers, as long as they join different AD domains.

- The Citrix Hypervisor servers can be in different time-zones, because it is the UTC time that is compared. To ensure that synchronization is correct, you can use the same NTP servers for your Citrix Hypervisor pool and the Active Directory server.

- Mixed-authentication pools are not supported. You cannot have a pool where some servers in the pool are configured to use Active Directory and some are not).

- The Citrix Hypervisor Active Directory integration uses the Kerberos protocol to communicate with the Active Directory servers. Therefore, Citrix Hypervisor does not support communicating with Active Directory servers that do not use Kerberos.

- For external authentication using Active Directory to be successful, clocks on your Citrix Hypervisor servers must be synchronized with the clocks on your Active Directory server. When Citrix Hypervisor joins the Active Directory domain, the synchronization is checked and authentication fails if there is too much skew between the servers.

> **Warning:**
>
> Host names must consist solely of no more than 63 alphanumeric characters, and must not be purely numeric.

When you add a server to a pool after enabling Active Directory authentication, you are prompted to configure Active Directory on the server joining the pool. When prompted for credentials on the joining server, type Active Directory credentials with sufficient privileges to add servers to that domain.

Active Directory integration

Ensure that the following firewall ports are open for outbound traffic in order for Citrix Hypervisor to access the domain controllers.

Port	Protocol	Use
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes
3268	TCP	Global Catalog Search

Notes:

- To view the firewall rules on a Linux computer using *iptables*, run the following command: `iptables -nL`.
- Citrix Hypervisor uses PowerBroker Identity Services (PBIS) to authenticate the AD user in the AD server, and to encrypt communications with the AD server.

How does Citrix Hypervisor manage the machine account password for AD integration?

Similarly to Windows client machines, PBIS automatically updates the machine account password. PBIS renews the password every 30 days, or as specified in the machine account password renewal policy in the AD server.

Enable external authentication on a pool

External authentication using Active Directory can be configured using either XenCenter or the CLI using the following command.

```
xe pool-enable-external-auth auth-type=AD \
  service-name=full-qualified-domain \
  config:user=username \
  config:pass=password
```

The user specified must have `Add/remove computer objects or workstations` privilege, which is the default for domain administrators.

If you are not using DHCP on the network used by Active Directory and your Citrix Hypervisor servers, use the following approaches to set up your DNS:

1. Set up your domain DNS suffix search order for resolving non-FQDN entries:

```
xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \
   "other-config:domain=suffix1.com suffix2.com suffix3.com"
```

2. Configure the DNS server to use on your Citrix Hypervisor servers:

```
xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \
  gateway=gateway netmask=netmask uuid=uuid
```

3. Manually set the management interface to use a PIF that is on the same network as your DNS server:

```
xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
```

Note:

External authentication is a per-host property. However, we recommend that you enable and disable external authentication on a per-pool basis. A per-pool setting allows Citrix Hypervisor to deal with failures that occur when enabling authentication on a particular host. Citrix Hypervisor also rolls back any changes that may be required, ensuring a consistent configuration across the pool. Use the `host-param-list` command to inspect properties of a host and to determine the status of external authentication by checking the values of the relevant fields.

Use XenCenter to disable Active Directory authentication, or the following xe command:

```
xe pool-disable-external-auth
```

User authentication

To allow a user access to your Citrix Hypervisor server, you must add a subject for that user or a group that they are in. (Transitive group memberships are also checked in the normal way. For example, adding a subject for group `A`, where group `A` contains group `B` and `user 1` is a member of group `B` would permit access to `user 1`.) If you want to manage user permissions in Active Directory, you can create a single group that you then add and delete users to/from. Alternatively, you can add and delete individual users from Citrix Hypervisor, or a combination of users and groups as appropriate for your authentication requirements. You can manage the subject list from XenCenter or using the CLI as described in the following section.

When authenticating a user, the credentials are first checked against the local root account, allowing you to recover a system whose AD server has failed. If the credentials (user name and password) do not match,

then an authentication request is made to the AD server. If the authentication is successful, the user's information is retrieved and validated against the local subject list. Access is denied if the authentication fails. Validation against the subject list succeeds if the user or a group in the transitive group membership of the user is in the subject list.

> **Note:**
>
> When using Active Directory groups to grant access for Pool Administrator users who require host ssh access, the size of the AD group must not exceed 500 users.

To add an AD subject to Citrix Hypervisor:

```
xe subject-add subject-name=entity_name
```

The entity_name is the name of the user or group to which you want to grant access. You can include the domain of the entity (for example, 'xendt\user1' as opposed to 'user1') although the behavior is the same unless disambiguation is required.

Find the user's subject identifier. The identifier is the user or the group containing the user. Removing a group removes access to all users in that group, provided they are not also specified in the subject list. Use the `subject list` command to find the user's subject identifier. :

```
xe subject-list
```

This command returns a list of all users.

To apply a filter to the list, for example to find the subject identifier for a user `user1` in the `testad` domain, use the following command:

```
xe subject-list other-config:subject-name='testad\user1'
```

Remove the user using the `subject-remove` command, passing in the subject identifier you learned in the previous step:

```
xe subject-remove subject-uuid=subject_uuid
```

You can end any current session this user has already authenticated. For more information, see *Terminating all authenticated sessions using xe* and *Terminating individual user sessions using xe* in the following section. If you do not end sessions, users with revoked permissions may continue to access the system until they log out.

Run the following command to identify the list of users and groups with permission to access your Citrix Hypervisor server or pool:

```
xe subject-list
```

Remove access for a user

When a user is authenticated, they can access the server until they end their session, or another user ends their session. Removing a user from the subject list, or removing them from a group in the subject list, doesn't automatically revoke any already-authenticated sessions that the user has. Users can continue to access the pool using XenCenter or other API sessions that they have already created. XenCenter and the CLI provide facilities to end individual sessions, or all active sessions forcefully. See the XenCenter documentation for information on procedures using XenCenter, or the following section for procedures using the CLI.

Terminate all authenticated sessions using xe

Run the following CLI command to end all authenticated sessions using xe:

```
xe session-subject-identifier-logout-all
```

Terminate individual user sessions using xe

1. Determine the subject identifier whose session you want to log out. Use either the `session-subject-identifier-list` or `subject-list` xe commands to find the subject identifier. The first command shows users who have sessions. The second command shows all users but can be filtered. For example, by using a command like `xe subject-list other-config:subject-name=xendt\\user1`. You may need a double backslash as shown depending on your shell).

2. Use the `session-subject-logout` command, passing the subject identifier you have determined in the previous step as a parameter, for example:

   ```
   xe session-subject-identifier-logout subject-identifier=subject_id
   ```

Leave an AD domain

> **Warning:**
>
> When you leave the domain, any users who authenticated to the pool or server with Active Directory credentials are disconnected.

Use XenCenter to leave an AD domain. For more information, see the XenCenter documentation. Alternately run the `pool-disable-external-auth` command, specifying the pool UUID if necessary.

Note:

Leaving the domain does not delete the host objects from the AD database. Refer to the Active Directory documentation for information about how to detect and remove your disabled host entries.

Role-based access control

Role Based Access Control (RBAC) feature in Citrix Hypervisor allows you to assign users, roles, and permissions to control who has access to your Citrix Hypervisor and what actions they can perform. The Citrix Hypervisor RBAC system maps a user (or a group of users) to defined roles (a named set of permissions). The roles have associated Citrix Hypervisor permissions to perform certain operations.

Permissions are not assigned to users directly. Users acquire permissions through roles assigned to them. Therefore, managing individual user permissions becomes a matter of assigning the user to the appropriate role, which simplifies common operations. Citrix Hypervisor maintains a list of authorized users and their roles.

RBAC allows you to restrict which operations different groups of users can perform, reducing the probability of an accident by an inexperienced user.

RBAC also provides an Audit Log feature for compliance and auditing.

RBAC depends on Active Directory for authentication services. Specifically, Citrix Hypervisor keeps a list of authorized users based on Active Directory user and group accounts. As a result, you must join the pool to the domain and add Active Directory accounts before you can assign roles.

The local super user (LSU), or root, is a special user account used for system administration and has all rights or permissions. The local super user is the default account at installation in Citrix Hypervisor. The LSU is authenticated through Citrix Hypervisor and not through an external authentication service. If the external authentication service fails, the LSU can still log in and manage the system. The LSU can always access the Citrix Hypervisor physical host through SSH.

RBAC process

The following section describes the standard process for implementing RBAC and assigning a user or group a role:

1. Join the domain. For more information, see Enabling external authentication on a pool.
2. Add an Active Directory user or group to the pool. This becomes a subject. For more information, see To add a subject to RBAC.
3. Assign (or change) the subject's RBAC role. For more information, see To assign an RBAC role to a subject.

RBAC roles and permissions

Roles

Citrix Hypervisor is shipped with the following six, pre-established roles:

- *Pool Administrator* (Pool Admin) – the same as the local root. Can perform all operations.

  > **Note:**
  >
  > The local super user (root) has the "Pool Admin" role. The Pool Admin role has the same permissions as the local root.
  >
  > If you remove the Pool Admin role from a user, consider also changing the server root password and rotating the pool secret. For more information, see Pool Security.

- *Pool Operator* (Pool Operator) – can do everything apart from adding/removing users and changing their roles. This role is focused mainly on host and pool management (that is, creating storage, making pools, managing the hosts and so on.)
- *Virtual Machine Power Administrator* (VM Power Admin) – creates and manages Virtual Machines. This role is focused on provisioning VMs for use by a VM operator.
- *Virtual Machine Administrator* (VM Admin) – similar to a VM Power Admin, but cannot migrate VMs or perform snapshots.
- *Virtual Machine Operator* (VM Operator) – similar to VM Admin, but cannot create/destroy VMs – but can perform start/stop lifecycle operations.
- *Read-only* (Read Only) – can view resource pool and performance data.

> **Warning:**
>
> When using Active Directory groups to grant access for Pool Administrator users who require host ssh access, the number of users in the Active Directory group must not exceed 500.

For a summary of the permissions available for each role and for information on the operations available for each permission, see *Definitions of RBAC roles and permissions* in the following section.

When you create a user in Citrix Hypervisor, you must first assign a role to the newly created user before they can use the account. Citrix Hypervisor **does not** automatically assign a role to the newly created user. As a result, these accounts do not have any access to Citrix Hypervisor pool until you assign them a role.

1. Modify the subject to role mapping. This requires the assign/modify role permission, only available to a Pool Administrator.
2. Modify the user's containing group membership in Active Directory.

Definitions of RBAC roles and permissions

The following table summarizes which permissions are available for each role. For details on the operations available for each permission, see *Definitions of permissions*.

Role permissions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
Assign/modify roles	X					
Log in to (physical) server consoles (through SSH and XenCenter)	X					
Server backup/restore	X					
Import/export OVF/OVA packages and disk images	X					
Set cores per socket	X	X	X	X		
Convert virtual machines using Citrix Hypervisor Conversion Manager	X					
Switch-port locking	X	X				
Multipathing	X	X				
Log out active user connections	X	X				
Create and dismiss alerts	X	X				
Cancel task of any user	X	X				
Pool management	X	X				
Live migration	X	X	X			
Storage live migration	X	X	X			
VM advanced operations	X	X	X			
VM create/destroy operations	X	X	X	X		
VM change CD media	X	X	X	X	X	
VM change power state	X	X	X	X	X	
View VM consoles	X	X	X	X	X	
XenCenter view management operations	X	X	X	X	X	
Cancel own tasks	X	X	X	X	X	X
Read audit logs	X	X	X	X	X	X

Role permissions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
Connect to pool and read all pool metadata	X	X	X	X	X	X
Configure virtual GPU	X	X				
View virtual GPU configuration	X	X	X	X	X	X
Access the config drive (CoreOS VMs only)	X					
Scheduled Snapshots (Add/Remove VMs to existing Snapshots Schedules)	X	X	X			
Scheduled Snapshots (Add/Modify/Delete Snapshot Schedules)	X	X				
Gather diagnostic information	X	X				
Configure Health Check	X	X				
View Health Check results and settings	X	X	X	X	X	X
Configure changed block tracking	X	X	X	X		
List changed blocks	X	X	X	X	X	
Configure PVS-Accelerator	X	X				
View PVS-Accelerator configuration	X	X	X	X	X	X

Definitions of permissions

Assign/modify roles:

- Add/remove users
- Add/remove roles from users
- Enable and disable Active Directory integration (being joined to the domain)

This permission lets the user grant themselves any permission or perform any task.

Warning: This role lets the user disable the Active Directory integration and all subjects added from Active Directory.

Log in to server consoles:

- Server console access through ssh
- Server console access through XenCenter

Warning: With access to a root shell, the assignee can arbitrarily reconfigure the entire system, including RBAC.

Server backup/restore VM create/destroy operations:

- Back up and restore servers
- Back up and restore pool metadata

The capability to restore a backup lets the assignee revert RBAC configuration changes.

Import/export OVF/OVA packages and disk images:

- Import OVF and OVA packages
- Import disk images
- Export VMs as OVF/OVA packages

Set cores-per-socket:

- Set the number of cores per socket for the VM's virtual CPUs

This permission enables the user to specify the topology for the VM's virtual CPUs.

Convert VMs using Citrix Hypervisor Conversion Manager:

- Convert VMware VMs to Citrix Hypervisor VMs

This permission lets the user convert workloads from VMware to Citrix Hypervisor by copying batches of VMware VMs to Citrix Hypervisor environment.

Switch-port locking:

- Control traffic on a network

This permission lets the user block all traffic on a network by default, or define specific IP addresses from which a VM is allowed to send traffic.

Multipathing:

- Enable multipathing
- Disable multipathing

Log out active user connections:

- Ability to disconnect logged in users

Create/dismiss alerts:

- Configure XenCenter to generate alerts when resource usage crosses certain thresholds
- Remove alerts from the Alerts view

Warning: A user with this permission can dismiss alerts for the entire pool.

Note: The ability to view alerts is part of the Connect to Pool and read all pool metadata permission.

Cancel task of any user:

- Cancel any user's running task

This permission lets the user request Citrix Hypervisor cancel an in-progress task initiated by any user.

Pool management:

- Set pool properties (naming, default SRs)
- Create a clustered pool
- Enable, disable, and configure high availability
- Set per-VM high availability restart priorities
- Configure DR and perform DR failover, failback, and test failover operations
- Enable, disable, and configure Workload Balancing (WLB)
- Add and remove server from pool
- Emergency transition to master
- Emergency master address
- Emergency recover pool members
- Designate new master
- Manage pool and server certificates
- Patching
- Set server properties
- Configure server logging
- Enable and disable servers
- Shut down, reboot, and power-on servers
- Restart toolstack
- System status reports
- Apply license
- Live migration of all other VMs on a server to another server, because of maintenance mode, or high availability
- Configure server management interface and secondary interfaces
- Disable server management
- Delete crashdumps
- Add, edit, and remove networks
- Add, edit, and remove PBDs/PIFs/VLANs/Bonds/SRs
- Add, remove, and retrieve secrets

This permission includes all the actions required to maintain a pool.

Note: If the management interface is not functioning, no logins can authenticate except local root logins.

Live migration:

- Migrate VMs from one host to another host when the VMs are on storage shared by both hosts

Storage live migration:

- Migrate from one host to another host when the VMs are not on storage shared between the two hosts
- Move Virtual Disk (VDIs) from one SR to another SR

VM advanced operations:

- Adjust VM memory (through Dynamic Memory Control)
- Create a VM snapshot with memory, take VM snapshots, and roll-back VMs
- Migrate VMs
- Start VMs, including specifying physical server
- Resume VMs

This permission provides the assignee with enough privileges to start a VM on a different server if they are not satisfied with the server Citrix Hypervisor selected.

VM create/destroy operations:

- Install or delete
- Clone/copy VMs
- Add, remove, and configure virtual disk/CD devices
- Add, remove, and configure virtual network devices
- Import/export XVA files
- VM configuration change
- Server backup/restore

> **Note:**
>
> The VM Admin role can import XVA files only into a pool with a shared SR. The VM Admin role has insufficient permissions to import an XVA file into a host or into a pool without shared storage.

VM change CD media:

- Eject current CD
- Insert new CD

Import/export OVF/OVA packages; import disk images

VM change power state:

- Start VMs (automatic placement)
- Shut down VMs
- Reboot VMs
- Suspend VMs
- Resume VMs (automatic placement)

This permission does not include start_on, resume_on, and migrate, which are part of the VM advanced operations permission.

View VM consoles:

- See and interact with VM consoles

This permission does not let the user view server consoles.

XenCenter view management operations:

- Create and modify global XenCenter folders

- Create and modify global XenCenter custom fields
- Create and modify global XenCenter searches

Folders, custom fields, and searches are shared between all users accessing the pool

Cancel own tasks:

- Lets a user cancel their own tasks

Read audit log:

- Download the Citrix Hypervisor audit log

Connect to pool and read all pool metadata:

- Log in to pool
- View pool metadata
- View historical performance data
- View logged in users
- View users and roles
- View messages
- Register for and receive events

Configure virtual GPU:

- Specify a pool-wide placement policy
- Assign a virtual GPU to a VM
- Remove a virtual GPU from a VM
- Modify allowed virtual GPU types
- Create, destroy, or assign a GPU group

View virtual GPU configuration:

- View GPUs, GPU placement policies, and virtual GPU assignments

Access the config drive (CoreOS VMs only):

- Access the config driver of the VM
- Modify the cloud-config parameters

Scheduled Snapshots:

- Add VMs to existing snapshot schedules
- Remove VMs from existing snapshot schedules
- Add snapshot schedules
- Modify snapshot schedules
- Delete snapshot schedules

Gather diagnostic information from Citrix Hypervisor:

- Initiate GC collection and heap compaction
- Gather garbage collection statistics

- Gather database statistics
- Gather network statistics

Configure Health Check:

- Enable Health Check
- Disable Health Check
- Update Health Check settings
- Manually upload a server status report

View Health Check results and settings:

- View the results of a Health Check upload
- View Health Check enrollment settings

Configure changed block tracking:

- Enable changed block tracking
- Disable changed block tracking
- Destroy the data associated with a snapshot and retain the metadata
- Get the NBD connection information for a VDI

Changed block tracking can be enabled only for licensed instances of Citrix Hypervisor Premium Edition.

List changed blocks:

- Compare two VDI snapshots and list the blocks that have changed between them

Configure PVS-Accelerator:

- Enable PVS-Accelerator
- Disable PVS-Accelerator
- Update (PVS-Accelerator) cache configuration
- Add/Remove (PVS-Accelerator) cache configuration

View PVS-Accelerator configuration:

- View the status of PVS-Accelerator

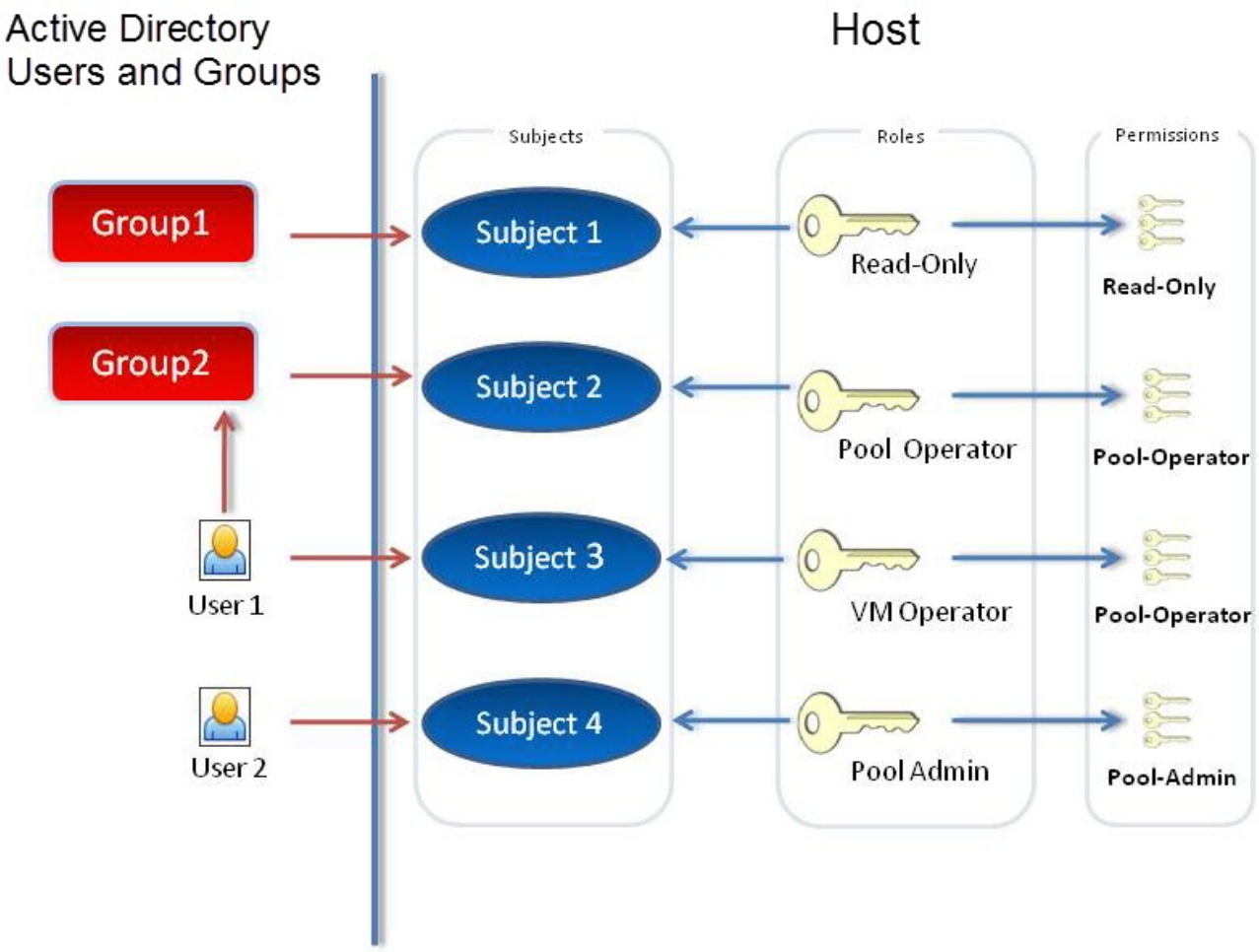
> **Note:**
>
> Sometimes, a Read Only user cannot move a resource into a folder in XenCenter, even after receiving an elevation prompt and supplying the credentials of a more privileged user. In this case, log on to XenCenter as the more privileged user and retry the action.

How does Citrix Hypervisor compute the roles for the session?

1. The subject is authenticated through the Active Directory server to verify which containing groups the subject may also belong to.

2. Citrix Hypervisor then verifies which roles have been assigned both to the subject, and to its containing groups.

3. As subjects can be members of multiple Active Directory groups, they inherit all of the permissions of the associated roles.



Use RBAC with the CLI

RBAC xe CLI commands

Use the following commands to work with roles and subjects.

To list all the available defined roles

Run the command: `xe role-list`

This command returns a list of the currently defined roles, for example:

```
    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
```

Note:

This list of roles is static. You cannot add, remove, or modify roles.

To display a list of current subjects

Run the following command:

```
xe subject-list
```

This command returns a list of Citrix Hypervisor users, their uuid, and the roles they are associated with:

```
    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:
      S-1-5-21-1539997073-1618981536-2562117463-2242; \
      subject-gecos: user_pool_op; subject-displayname: user_pool_op; \
      subject-is-group: false; subject-account-disabled: false; \
      subject-account-expired: false; subject-account-locked: \
      false; subject-password-expired: false
      roles (SRO): pool-operator
```

To add a subject to RBAC

To enable existing AD users to use RBAC, create a subject instance within Citrix Hypervisor, either for the AD user directly, or for the containing groups:

Run the following command to add a new subject instance:

```
xe subject-add subject-name=AD user/group
```

To assign an RBAC role to a subject

After adding a subject, you can assign it to an RBAC role. You can refer to the role by either by its uuid or name:

Run the command:

```
xe subject-role-add uuid=subject uuid role-uuid=role_uuid
```

Or

```
xe subject-role-add uuid=subject uuid role-name=role_name
```

For example, the following command adds a subject with the uuid `b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4` to the Pool Administrator role:

```
xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name=pool-admin
```

To change the RBAC role of a subject

To change the role of a user, it is necessary to remove them from their existing role and add them to a new role:

Run the following commands:

```
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
```

The user must log out and log back in to ensure that the new role takes effect. This requires the "Logout Active User Connections" permission available to a Pool Administrator or Pool Operator).

If you remove the Pool Admin role from a user, consider also changing the server root password and rotating the pool secret. For more information, see Pool Security.

> **Warning:**
>
> When you add or remove a pool-admin subject, it can take a few seconds for all hosts in the pool to accept ssh sessions associated with this subject.

Auditing

The RBAC audit log records any operation taken by a logged-in user.

- The message records the Subject ID and user name associated with the session that invoked the operation.
- If a subject invokes an operation that is not authorized, the operation is logged.
- Any successful operation is also recorded. If the operation failed then the error code is logged.

Audit log xe CLI commands

The following command downloads all the available records of the RBAC audit file in the pool to a file. If the optional parameter 'since' is present, then it only downloads the records from that specific point in time.

```
xe audit-log-get \[since=timestamp\] filename=output filename
```

To obtain all audit records from the pool

Run the following command:

```
xe audit-log-get filename=/tmp/auditlog-pool-actions.out
```

To obtain audit records of the pool since a precise millisecond timestamp

Run the following command:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z \
    filename=/tmp/auditlog-pool-actions.out
```

To obtain audit records of the pool since a precise minute timestamp

Run the following command:

```
xe audit-log-get since=2009-09-24T17:56Z \
    filename=/tmp/auditlog-pool-actions.out
```

Networking

This section provides an overview of Citrix Hypervisor networking, including networks, VLANs, and NIC bonds. It also discusses how to manage your networking configuration and troubleshoot it.

> **Important:**
>
> vSwitch is the default network stack of Citrix Hypervisor. Follow the instructions in vSwitch networks to configure the Linux network stack.

If you are already familiar with Citrix Hypervisor networking concepts, you can skip ahead to Manage networking for information about the following sections:

- Create networks for standalone Citrix Hypervisor servers
- Create private networks across Citrix Hypervisor servers
- Create networks for Citrix Hypervisor servers that are configured in a resource pool
- Create VLANs for Citrix Hypervisor servers, either standalone or part of a resource pool
- Create bonds for standalone Citrix Hypervisor servers
- Create bonds for Citrix Hypervisor servers that are configured in a resource pool

> **Note:**
>
> The term 'management interface' is used to indicate the IP-enabled NIC that carries the management traffic. The term 'secondary interface' is used to indicate an IP-enabled NIC configured for storage traffic.

Networking support

Citrix Hypervisor supports up to 16 physical network interfaces (or up to 4 bonded network interfaces) per host and up to 7 virtual network interfaces per VM.

> **Note:**
>
> Citrix Hypervisor provides automated configuration and management of NICs using the xe command line interface (CLI). Do not edit the host networking configuration files directly.

vSwitch networks

vSwitch networks support open flow.

- Supports fine-grained security policies to control the flow of traffic sent to and from a VM.

- Provides detailed visibility about the behavior and performance of all traffic sent in the virtual network environment.

A vSwitch greatly simplifies IT administration in virtualized networking environments. All VM configuration and statistics remain bound to the VM even when the VM migrates from one physical host in the resource pool to another.

To determine what networking stack is configured, run the following command:

```
xe host-list params=software-version
```

In the command output, look for `network_backend`. When the vSwitch is configured as the network stack, the output appears as follows:

```
network_backend: openvswitch
```

When the Linux bridge is configured as the network stack, the output appears as follows:

```
network_backend: bridge
```

To revert to the Linux network stack, run the following command:

```
xe-switch-network-backend bridge
```

Restart your host after running this command.

Citrix Hypervisor networking overview

This section describes the general concepts of networking in the Citrix Hypervisor environment.

Citrix Hypervisor creates a network for each physical NIC during installation. When you add a server to a pool, the default networks are merged. This is to ensure all physical NICs with the same device name are attached to the same network.

Typically, you add a network to create an internal network, set up a new VLAN using an existing NIC, or create a NIC bond.

You can configure four different types of networks in Citrix Hypervisor:

- **External networks** have an association with a physical network interface. External networks provide a bridge between a virtual machine and the physical network interface connected to the network. External networks enable a virtual machine to connect to resources available through the server's physical NIC.

- **Bonded networks** create a bond between two or more NICs to create a single, high-performing channel between the virtual machine and the network.
- **Single-Server Private networks** have no association to a physical network interface. Single-server private networks can be used to provide connectivity between the virtual machines on a given host, with no connection to the outside world.

> **Note:**
>
> Some networking options have different behaviors when used with standalone Citrix Hypervisor servers compared to resource pools. This section contains sections on general information that applies to both standalone hosts and pools, followed by specific information and procedures for each.

Network objects

This section uses three types of server-side software objects to represent networking entities. These objects are:

- A *PIF*, which represents a physical NIC on a host. PIF objects have a name and description, a UUID, the parameters of the NIC they represent, and the network and server they are connected to.
- A *VIF*, which represents a virtual NIC on a virtual machine. VIF objects have a name and description, a UUID, and the network and VM they are connected to.
- A *network*, which is a virtual Ethernet switch on a host. Network objects have a name and description, a UUID, and the collection of VIFs and PIFs connected to them.

XenCenter and the xe CLI allow you to configure networking options. You can control the NIC used for management operations, and create advanced networking features such as VLANs and NIC bonds.

Networks

Each Citrix Hypervisor server has one or more networks, which are virtual Ethernet switches. Networks that are not associated with a PIF are considered *internal*. Internal networks can be used to provide connectivity only between VMs on a given Citrix Hypervisor server, with no connection to the outside world. Networks associated with a PIF are considered *external*. External networks provide a bridge between VIFs and the PIF connected to the network, enabling connectivity to resources available through the PIF's NIC.

VLANs

VLANs, as defined by the IEEE 802.1Q standard, allow a single physical network to support multiple logical networks. Citrix Hypervisor servers support VLANs in multiple ways.

> **Note:**
>
> All supported VLAN configurations are equally applicable to pools and standalone hosts, and bonded and non-bonded configurations.

Using VLANs with virtual machines

Switch ports configured as 802.1Q VLAN trunk ports can be used with the Citrix Hypervisor VLAN features to connect guest virtual network interfaces (VIFs) to specific VLANs. In this case, the Citrix Hypervisor server performs the VLAN tagging/untagging functions for the guest, which is unaware of any VLAN configuration.

Citrix Hypervisor VLANs are represented by additional PIF objects representing VLAN interfaces corresponding to a specified VLAN tag. You can connect Citrix Hypervisor networks to the PIF representing the physical NIC to see all traffic on the NIC. Alternatively, connect networks to a PIF representing a VLAN to see only the traffic with the specified VLAN tag. You can also connect a network such that it only sees the native VLAN traffic, by attaching it to VLAN 0.

For procedures on how to create VLANs for Citrix Hypervisor servers, either standalone or part of a resource pool, see Creating VLANs.

If you want the guest to perform the VLAN tagging and untagging functions, the guest must be aware of the VLANs. When configuring the network for your VMs, configure the switch ports as VLAN trunk ports, but do not create VLANs for the Citrix Hypervisor server. Instead, use VIFs on a normal, non-VLAN network.

Using VLANs with management interfaces

Management interface can be configured on a VLAN using a switch port configured as trunk port or access mode port. Use XenCenter or xe CLI to set up a VLAN and make it the management interface. For more information, see Management interface.

Using VLANs with dedicated storage NICs

Dedicated storage NICs can be configured to use native VLAN or access mode ports as described in the previous section for management interfaces. Dedicated storage NICs are also known as IP-enabled NICs or secondary interfaces. You can configure dedicated storage NICs to use trunk ports and Citrix Hypervisor VLANs as described in the previous section for virtual machines. For more information, see Configuring a dedicated storage NIC.

Combining management interfaces and guest VLANs on a single host NIC

A single switch port can be configured with both trunk and native VLANs, allowing one host NIC to be used for a management interface (on the native VLAN) and for connecting guest VIFs to specific VLAN IDs.

Jumbo frames

Jumbo frames can be used to optimize the performance of storage traffic. Jumbo frames are Ethernet frames containing more than 1,500 bytes of payload. Jumbo frames are typically used to achieve better throughput, reducing the load on system bus memory, and reducing the CPU overhead.

> **Note:**
>
> Citrix Hypervisor supports jumbo frames only when using vSwitch as the network stack on all hosts in the pool.

Requirements for using jumbo frames

Customers must note the following when using jumbo frames:

- Jumbo frames are configured at a pool level
- vSwitch must be configured as the network back-end on all hosts in the pool
- Every device on the subnet must be configured to use jumbo frames
- Enable jumbo frames on a dedicated storage network (recommended)
- Enabling jumbo frames on the Management network is not a supported configuration
- Jumbo frames are not supported for use on VMs

To use jumbo frames, set the Maximum Transmission Unit (MTU) to a value between 1500 and 9216. You can use XenCenter or the xe CLI to set the MTU.

NIC Bonds

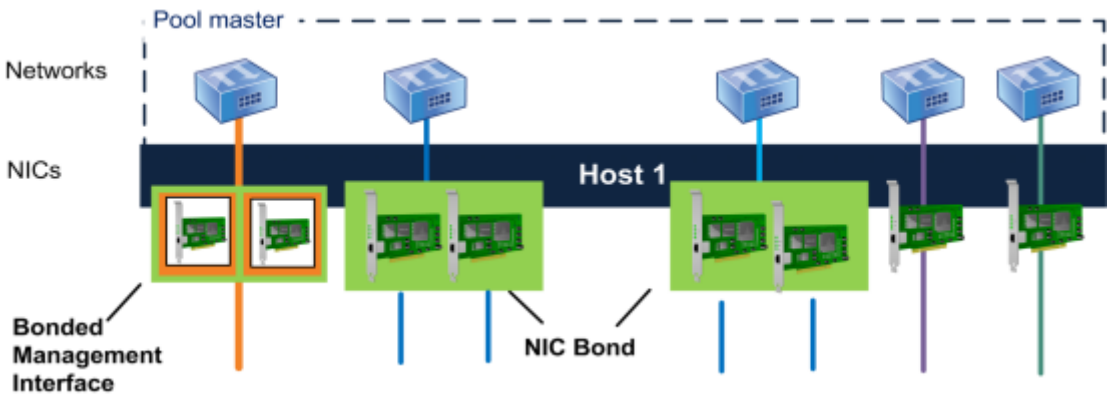
NIC bonds, sometimes also known as NIC teaming, improve Citrix Hypervisor server resiliency and bandwidth by enabling administrators to configure two or more NICs together. NIC bonds logically function as one network card and all bonded NICs share MAC address.

If one NIC in the bond fails, the host's network traffic is automatically redirected through the second NIC. Citrix Hypervisor supports up to eight bonded networks.

Citrix Hypervisor supports active-active, active-passive, and LACP bonding modes. The number of NICs supported and the bonding mode supported varies according to network stack:

- LACP bonding is only available for the vSwitch whereas active-active and active-passive are available for both the vSwitch and Linux bridge.
- When the vSwitch is the network stack, you can bond either two, three, or four NICs.
- When the Linux bridge is the network stack, you can only bond two NICs.

In the illustration that follows, the management interface is on a bonded pair of NICs. Citrix Hypervisor uses this bond for management traffic.



All bonding modes support failover. However, not all modes allow all links to be active for all traffic types. Citrix Hypervisor supports bonding the following types of NICs together:

- **NICs (non-management)**. You can bond NICs that Citrix Hypervisor is using solely for VM traffic. Bonding these NICs not only provides resiliency, but doing so also balances the traffic from multiple VMs between the NICs.
- **Management interfaces**. You can bond a management interface to another NIC so that the second NIC provides failover for management traffic. Although configuring a LACP link aggregation bond provides load balancing for management traffic, active-active NIC bonding does not. You can create a VLAN on bonded NICs and host management interface can be assigned to that VLAN.
- **Secondary interfaces**. You can bond NICs that you have configured as secondary interfaces (for example, for storage). However, for most iSCSI software initiator storage, we recommend configuring multipathing instead of NIC bonding as described in the Designing Citrix Hypervisor Network Configurations.

  Throughout this section, the term IP-based storage traffic is used to describe iSCSI and NFS traffic collectively.

You can create a bond if a VIF is already using one of the interfaces that will be bonded: the VM traffic migrates automatically to the new bonded interface.

In Citrix Hypervisor, An additional PIF represents a NIC bond. Citrix Hypervisor NIC bonds completely subsume the underlying physical devices (PIFs).

Notes:

- Creating a bond that contains only one NIC is not supported.
- The bonded NICs can be different models to each other.
- NIC bonds are not supported on NICs that carry FCoE traffic.

Key points about IP addressing

Bonded NICs either have one IP address or no IP addresses, as follows:

- **Management and storage networks**.
  - If you bond a management interface or secondary interface, a single IP address is assigned to the bond. That is, each NIC does not have its own IP address. Citrix Hypervisor treats the two NICs as one logical connection.
  - When bonds are used for non-VM traffic, for example, to connect to shared network storage or XenCenter for management, configure an IP address for the bond. However, if you have already assigned an IP address to one of the NICs (that is, created a management interface or secondary interface), that IP address is assigned to the entire bond automatically.
  - If you bond a management interface or secondary interface to a NIC without an IP address, the bond assumes the IP address of the respective interface.

    - If you bond a tagged VLAN management interface and a secondary interface, the management VLAN is created on that bonded NIC.

- **VM networks**. When bonded NICs are used for VM traffic, you do not need to configure an IP address for the bond. This is because the bond operates at Layer 2 of the OSI model, the data link layer, and no IP addressing is used at this layer. IP addresses for virtual machines are associated with VIFs.

Bonding types

Citrix Hypervisor provides three different types of bonds, all of which can be configured using either the CLI or XenCenter:

- Active-Active mode, with VM traffic balanced between the bonded NICs. See Active-active bonding.
- Active-Passive mode, where only one NIC actively carries traffic. See Active-passive bonding.
- LACP Link Aggregation, in which active and stand-by NICs are negotiated between the switch and the server. See LACP Link Aggregation Control Protocol bonding.

> **Note:**
>
> Bonding is set up with an Up Delay of 31,000 ms and a Down Delay of 200 ms. The seemingly long Up Delay is deliberate because of the time some switches take to enable the port. Without a delay, when a link comes back after failing, the bond can rebalance traffic onto it before the switch is ready to pass traffic. To move both connections to a different switch, move one, then wait 31 seconds for it to be used again before moving the other. For information about changing the delay, see Changing the up delay for bonds.

Bond status

Citrix Hypervisor provides status for bonds in the event logs for each host. If one or more links in a bond fails or is restored, it is noted in the event log. Likewise, you can query the status of a bond's links by using the `links-up` parameter as shown in the following example:

```
xe bond-param-get uuid=bond_uuid param-name=links-up
```

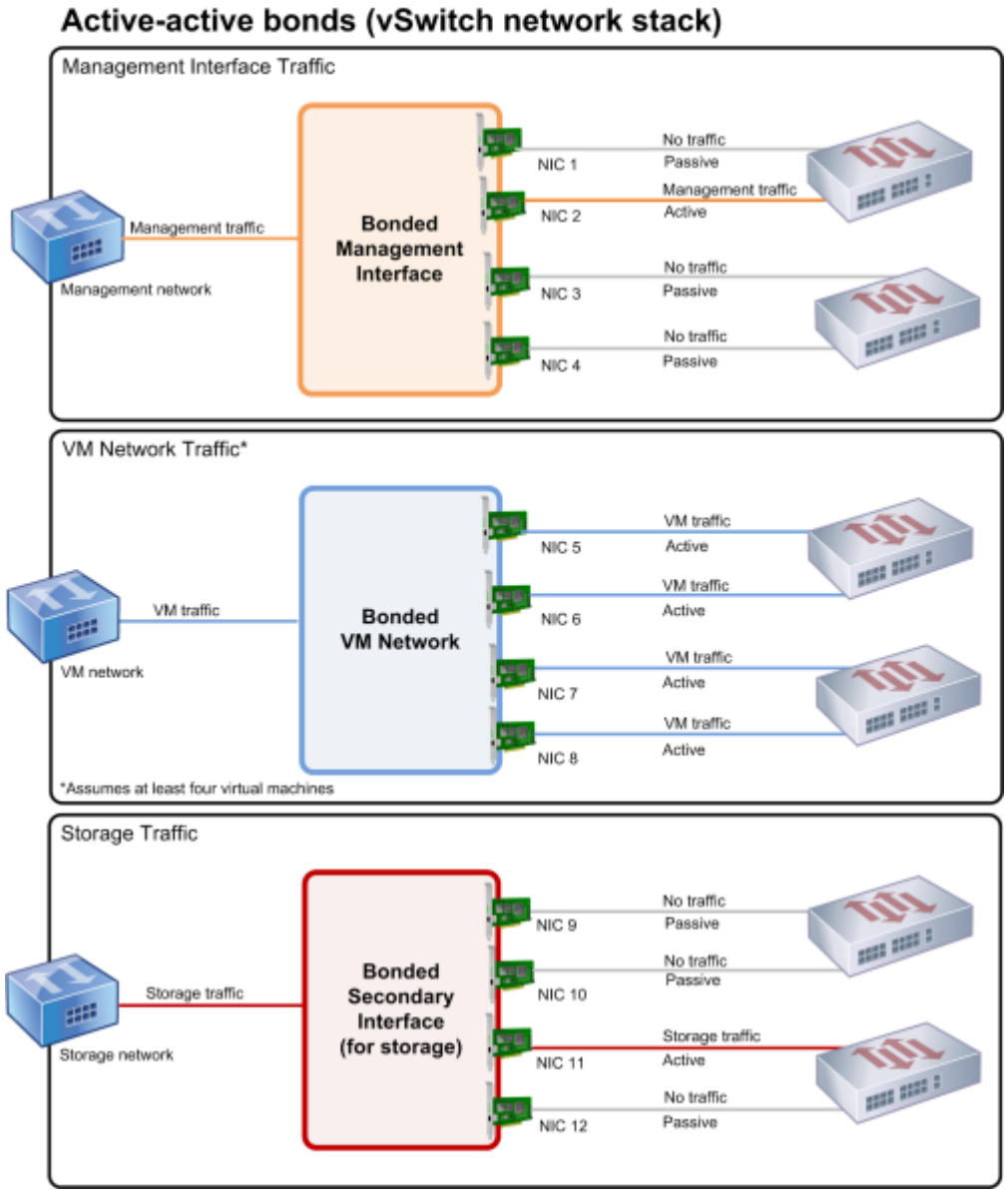
Citrix Hypervisor checks the status of links in bonds approximately every five seconds. Therefore, if more links in the bond fail in the five-second window, the failure is not logged until the next status check.

Bonding event logs appear in the XenCenter Logs tab. For users not running XenCenter, event logs also appear in `/var/log/xensource.log` on each host.

Active-active bonding

Active-active is an active/active configuration for guest traffic: both NICs can route VM traffic simultaneously. When bonds are used for management traffic, only one NIC in the bond can route traffic: the other NIC remains unused and provides failover support. Active-active mode is the default bonding mode when either the Linux bridge or vSwitch network stack is enabled.

When active-active bonding is used with the Linux bridge, you can only bond two NICs. When using the vSwitch as the network stack, you can bond either two, three, or four NICs in active-active mode. However, in active-active mode, bonding three, or four NICs is only beneficial for VM traffic, as shown in the illustration that follows.



Citrix Hypervisor can only send traffic over two or more NICs when there is more than one MAC address associated with the bond. Citrix Hypervisor can use the virtual MAC addresses in the VIF to send traffic across multiple links. Specifically:

- **VM traffic**. Provided you enable bonding on NICs carrying only VM (guest) traffic, all links are active and NIC bonding can balance spread VM traffic across NICs. An individual VIF's traffic is never split between NICs.
- **Management or storage traffic**. Only one of the links (NICs) in the bond is active and the other NICs remain unused unless traffic fails over to them. Configuring a management interface or secondary interface on a bonded network provides resilience.
- **Mixed traffic**. If the bonded NIC carries a mixture of IP-based storage traffic and guest traffic, only the guest and control domain traffic are load balanced. The control domain is essentially a virtual machine

so it uses a NIC like the other guests. Citrix Hypervisor balances the control domain's traffic the same way as it balances VM traffic.

Traffic balancing

Citrix Hypervisor balances the traffic between NICs by using the source MAC address of the packet. Because, for management traffic, only one source MAC address is present, active-active mode can only use one NIC, and traffic is not balanced. Traffic balancing is based on two factors:

- The virtual machine and its associated VIF sending or receiving the traffic
- The quantity of data (in kilobytes) being sent.

Citrix Hypervisor evaluates the quantity of data (in kilobytes) each NIC is sending and receiving. If the quantity of data sent across one NIC exceeds the quantity of data sent across the other NIC, Citrix Hypervisor rebalances which VIFs use which NICs. The VIF's entire load is transferred. One VIF's load is never split between two NICs.

Though active-active NIC bonding can provide load balancing for traffic from multiple VMs, it cannot provide a single VM with the throughput of two NICs. Any given VIF only uses one of the links in a bond at a time. As Citrix Hypervisor periodically rebalances traffic, VIFs are not permanently assigned to a specific NIC in the bond.

Active-active mode is sometimes described as Source Load Balancing (SLB) bonding as Citrix Hypervisor uses SLB to share load across bonded network interfaces. SLB is derived from the open-source Adaptive Load Balancing (ALB) mode and reuses the ALB functionality to rebalance load across NICs dynamically.

When rebalancing, the number of bytes going over each secondary (interface) is tracked over a given period. If a packet to be sent contains a new source MAC address, it is assigned to the secondary interface with the lowest utilization. Traffic is rebalanced at regular intervals.

Each MAC address has a corresponding load and Citrix Hypervisor can shift entire loads between NICs depending on the quantity of data a VM sends and receives. For active-active traffic, all the traffic from one VM can be sent on only one NIC.

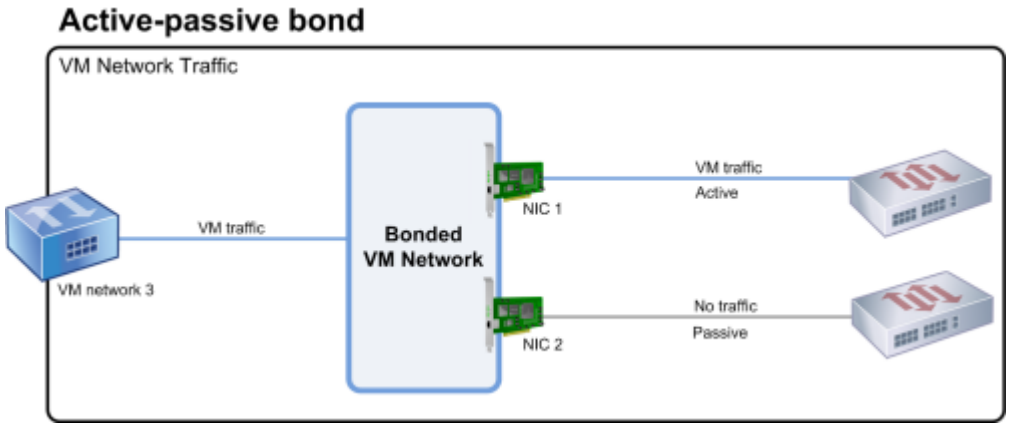
> **Note:**
>
> Active-active bonding does not require switch support for EtherChannel or 802.3ad (LACP).

Active-passive bonding

An active-passive bond routes traffic over only one of the NICs. If the active NIC loses network connectivity, traffic fails over to the other NIC in the bond. Active-passive bonds route traffic over the active NIC. The traffic shifts to the passive NIC if the active NIC fails.

Active-passive bonding is available in the Linux bridge and the vSwitch network stack. When used with the Linux bridge, you can bond two NICs together. When used with the vSwitch, you can only bond two, three, or four NICs together. However, regardless of the traffic type, when you bond NICs in active-passive mode, only one link is active and there is no load balancing between links.

The illustration that follows shows two bonded NICs configured in active-passive mode.



Active-active mode is the default bonding configuration in Citrix Hypervisor. If you are configuring bonds using the CLI, you must specify a parameter for the active-passive mode. Otherwise, an active-active bond is created. You do not need to configure active-passive mode because a network is carrying management traffic or storage traffic.

Active-passive can be a good choice for resiliency as it offers several benefits. With active-passive bonds, traffic does not move around between NICs. Similarly, active-passive bonding lets you configure two switches for redundancy but does not require stacking. If the management switch dies, stacked switches can be a single point of failure.

Active-passive mode does not require switch support for EtherChannel or 802.3ad (LACP).

Consider configuring active-passive mode in situations when you do not need load balancing or when you only intend to send traffic on one NIC.

> **Important:**
>
> After you have created VIFs or your pool is in production, be careful about changing bonds or creating bonds.

LACP Link Aggregation Control Protocol bonding

LACP Link Aggregation Control Protocol is a type of bonding that bundles a group of ports together and treats it like a single logical channel. LACP bonding provides failover and can increase the total amount of bandwidth available.

Unlike other bonding modes, LACP bonding requires configuring both sides of the links: creating a bond on the host, and creating a Link Aggregation Group (LAG) for each bond on the switch. See Switch configuration for LACP bonds. You must configure the vSwitch as the network stack to use LACP bonding. Also, your switches must support the IEEE 802.3ad standard.

A comparison of active-active SLB bonding and LACP bonding:

Active-active SLB bonding

Benefits:

- Can be used with any switch on the Hardware Compatibility List.
- Does not require switches that support stacking.
- Supports four NICs.

Considerations:

- Optimal load balancing requires at least one NIC per VIF.
- Storage or management traffic cannot be split on multiple NICs.
- Load balancing occurs only if multiple MAC addresses are present.

LACP bonding

Benefits:

- All links can be active regardless of traffic type.
- Traffic balancing does not depend on source MAC addresses, so all traffic types can be balanced.

Considerations:

- Switches must support the IEEE 802.3ad standard.
- Requires switch-side configuration.
- Supported only for the vSwitch.
- Requires a single switch or stacked switch.

Traffic balancing

Citrix Hypervisor supports two LACP bonding hashing types. The term hashing describes how the NICs and the switch distribute the traffic— (1) load balancing based on IP and port of source and destination addresses and (2) load balancing based on source MAC address.

Depending on the hashing type and traffic pattern, LACP bonding can potentially distribute traffic more evenly than active-active NIC bonding.

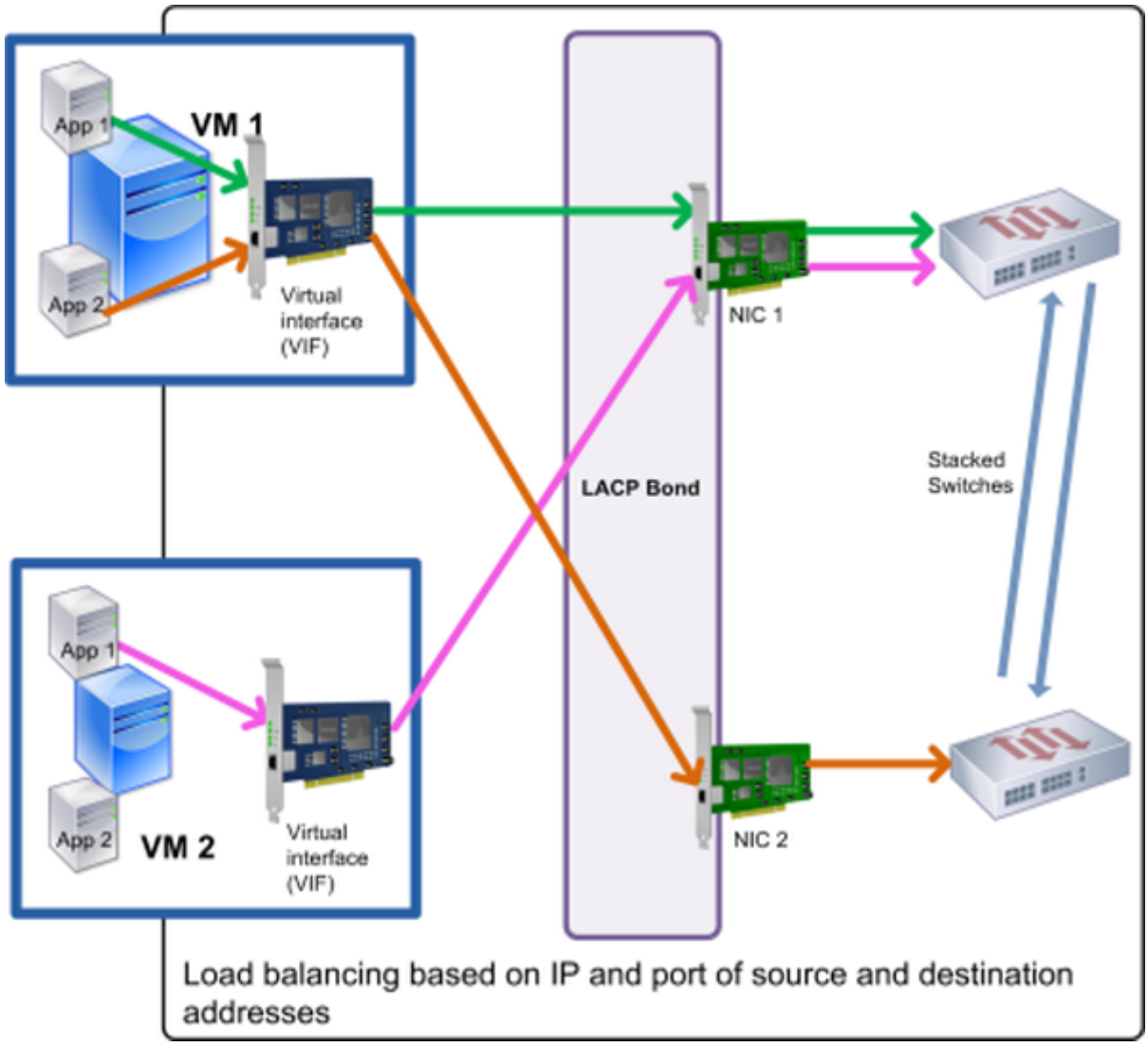
> **Note:**
>
> You configure settings for outgoing and incoming traffic separately on the host and the switch: the configuration does not have to match on both sides.

Load balancing based on IP and port of source and destination addresses.

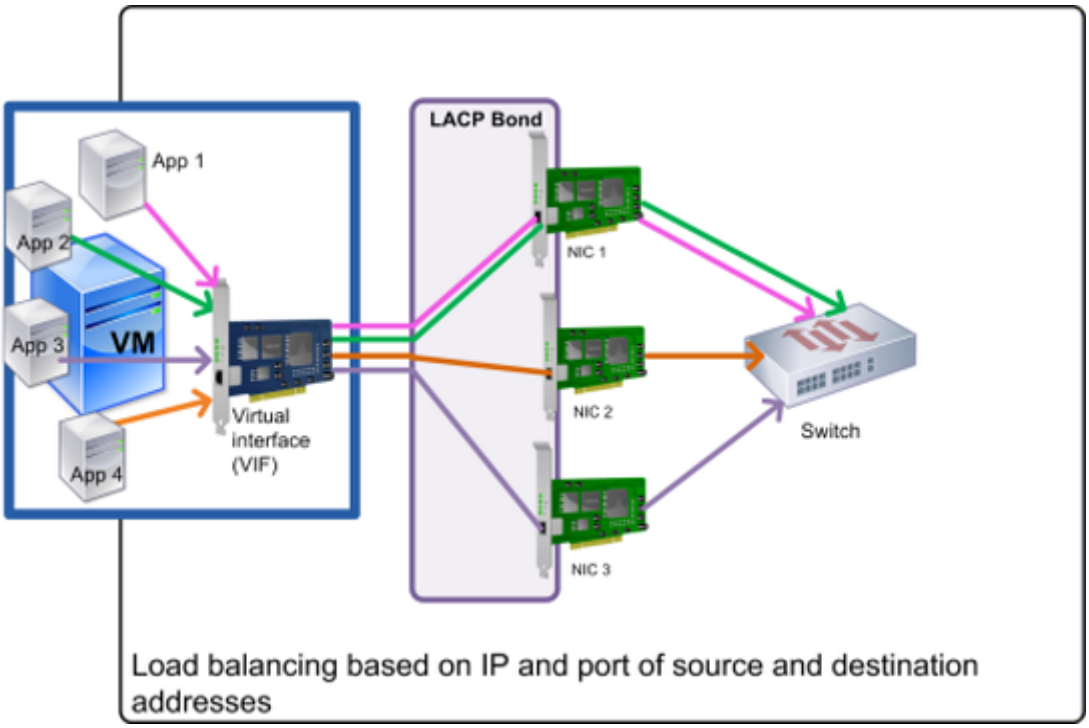
This hashing type is the default LACP bonding hashing algorithm. If there is a variation in the source or destination IP or port numbers, traffic from one guest can be distributed over two links.

If a virtual machine is running several applications which use different IP or port numbers, this hashing type distributes traffic over several links. Distributing the traffic gives the guest the possibility of using the aggregate throughput. This hashing type lets one guest use the whole throughput of multiple NICs.

As shown in the illustration that follows, this hashing type can distribute the traffic of two different applications on a virtual machine to two different NICs.



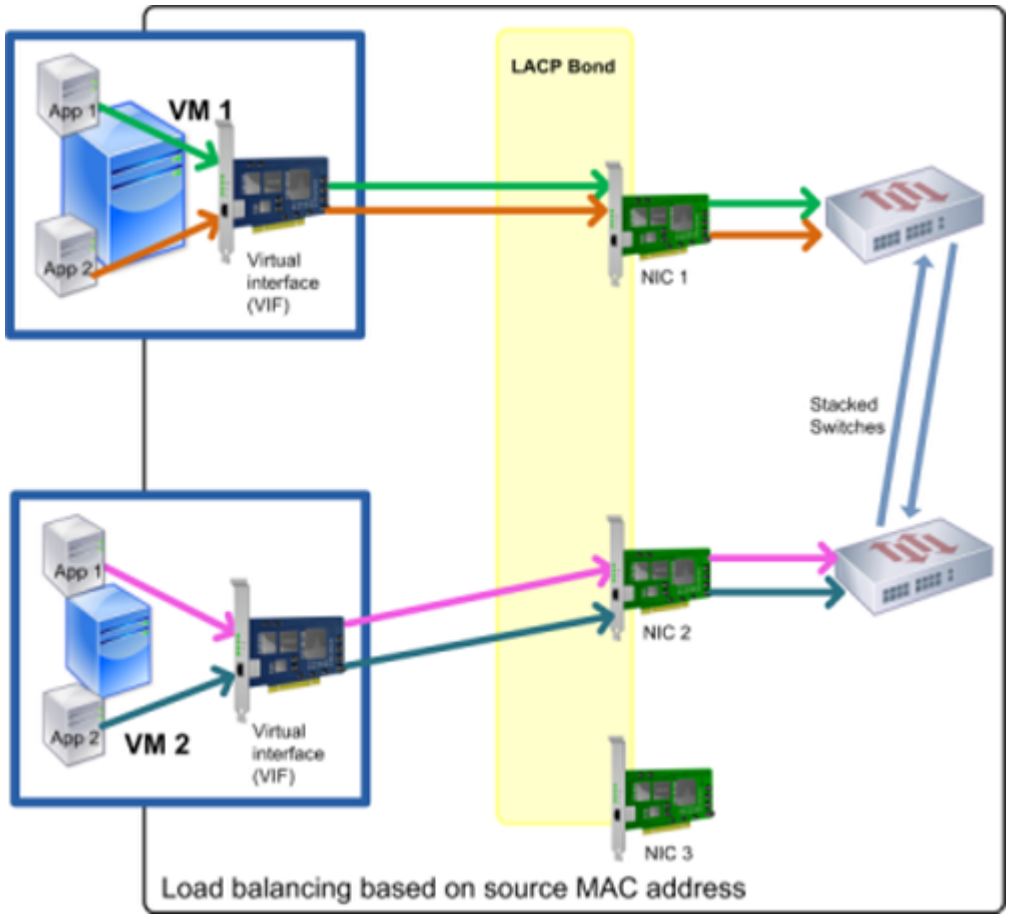
Configuring LACP bonding based on IP and port of source and destination address is beneficial when you want to balance the traffic of two different applications on the same VM. For example, when only one virtual machine is configured to use a bond of three NICs.



The balancing algorithm for this hashing type uses five factors to spread traffic across the NICs: the source IP address, source port number, destination IP address, destination port number, and source MAC address.

Load balancing based on source MAC address.

This type of load balancing works well when there are multiple virtual machines on the same host. Traffic is balanced based on the virtual MAC address of the VM from which the traffic originated. Citrix Hypervisor sends outgoing traffic using the same algorithm as it does in active-active bonding. Traffic coming from the same guest is not split over multiple NICs. As a result, this hashing type is not suitable if there are fewer VIFs than NICs: load balancing is not optimal because the traffic cannot be split across NICs.



Switch configuration

Depending on your redundancy requirements, you can connect the NICs in the bond to either the same or separate stacked switches. If you connect one of the NICs to a second, redundant switch and a NIC or switch fails, traffic fails over to the other NIC. Adding a second switch prevents a single point-of-failure in your configuration in the following ways:

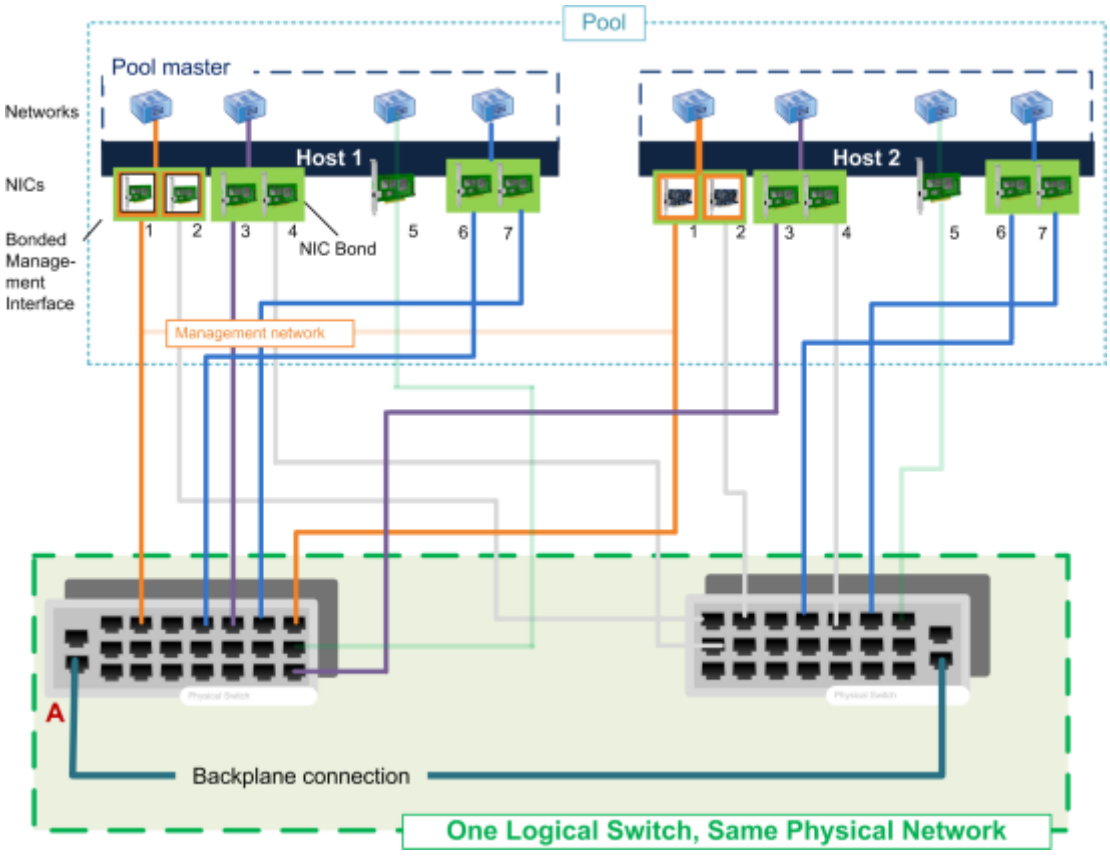
- When you connect one of the links in a bonded management interface to a second switch, if the switch fails, the management network remains online and the hosts can still communicate with each other.
- If you connect a link (for any traffic type) to a second switch and the NIC or switch fails, the virtual machines remain on the network as their traffic fails over to the other NIC/switch.

Use stacked switches when you want to connect bonded NICs to multiple switches and you configured the LACP bonding mode. The term 'stacked switches' is used to describe configuring multiple physical switches to function as a single logical switch. You must join the switches together physically and through the switch-

management software so the switches function as a single logical switching unit, as per the switch manufacturer's guidelines. Typically, switch stacking is only available through proprietary extensions and switch vendors may market this functionality under different terms.

> **Note:**
>
> If you experience issues with active-active bonds, the use of stacked switches may be necessary. Active-passive bonds do not require stacked switches.

The illustration that follows shows how the cables and network configuration for the bonded NICs have to match.



Switch configuration for LACP bonds

Because the specific details of switch configuration vary by manufacturer, there are a few key points to remember when configuring switches for use with LACP bonds:

- The switch must support LACP and the IEEE 802.3ad standard.
- When you create the LAG group on the switch, you must create one LAG group for each LACP bond on the host. For example, if you have a five-host pool and you created a LACP bond on NICs 4 and 5 on each host, you must create five LAG groups on the switch. One group for each set of ports corresponding with the NICs on the host.

  You may also need to add your VLAN ID to your LAG group.
- Citrix Hypervisor LACP bonds require setting the Static Mode setting in the LAG group to be set to Disabled.

As previously mentioned in *Switch configuration*, stacking switches are required to connect LACP bonds to multiple switches.

Initial networking configuration after setup

The Citrix Hypervisor server networking configuration is specified during initial host installation. Options such as IP address configuration (DHCP/static), the NIC used as the management interface, and hostname are set based on the values provided during installation.

When a host has multiple NICs, the configuration present after installation depends on which NIC is selected for management operations during installation:

- PIFs are created for each NIC in the host
- The PIF of the NIC selected for use as the management interface is configured with the IP addressing options specified during installation
- A network is created for each PIF ("network 0", "network 1", and so on)
- Each network is connected to one PIF
- The IP addressing options are left unconfigured for all PIFs other than the PIF used as the management interface

When a host has a single NIC, the follow configuration is present after installation:

- A single PIF is created corresponding to the host's single NIC
- The PIF is configured with the IP addressing options specified during installation and to enable management of the host
- The PIF is set for use in host management operations
- A single network, network 0, is created
- Network 0 is connected to the PIF to enable external connectivity to VMs

When an installation of Citrix Hypervisor is done on a tagged VLAN network, the following configuration is present after installation:

- PIFs are created for each NIC in the host
- The PIF for the tagged VLAN on the NIC selected for use as management interface is configured with the IP address configuration specified during installation
- A network is created for each PIF (for example: network 1, network 2, and so on). Additional VLAN network is created (for example, for Pool-wide network associated with eth0 on VLAN<TAG>)
- Each network is connected to one PIF. The VLAN PIF is set for use in host management operations

In both cases, the resulting networking configuration allows connection to the Citrix Hypervisor server by XenCenter, the xe CLI, and any other management software running on separate machines through the IP

address of the management interface. The configuration also provides external networking for VMs created on the host.

The PIF used for management operations is the only PIF ever configured with an IP address during Citrix Hypervisor installation. External networking for VMs is achieved by bridging PIFs to VIFs using the network object which acts as a virtual Ethernet switch.

The steps required for networking features such as VLANs, NIC bonds, and dedicating a NIC to storage traffic are covered in the sections that follow.

Changing networking configuration

You can change your networking configuration by modifying the network object. To do so, you run a command that affects either the network object or the VIF.

Modifying the network object

You can change aspects of a network, such as the frame size (MTU), name-label, name-description, purpose, and other values. Use the xe `network-param-set` command and its associated parameters to change the values.

When you run the xe `network-param-set` command, the only required parameter is `uuid`.

Optional parameters include:

- `default_locking_mode`. See Simplifying VIF locking mode configuration in the Cloud.
- `name-label`
- `name-description`
- `MTU`
- `purpose`. See Adding a purpose to a network.
- `other-config`

If a value for a parameter is not given, the parameter is set to a null value. To set a (key, value) pair in a map parameter, use the syntax `map-param:key=value`.

Changing the up delay for bonds

Bonding is set up with an Up Delay of 31,000 ms by default to prevent traffic from being rebalanced onto a NIC after it fails. While seemingly long, the up delay is important for all bonding modes and not just active-active.

However, if you understand the appropriate settings to select for your environment, you can change the up delay for bonds by using the procedure that follows.

Set the up delay in milliseconds:

```
xe pif-param-set uuid=<uuid of bond master PIF> other-config:bond-updelay=<delay
in ms>
```

To make the change take effect, you must unplug and then replug the physical interface:

```
xe pif-unplug uuid=<uuid of bond master PIF>
```

```
xe pif-plug uuid=<uuid of bond master PIF>
```

Manage networking

Network configuration procedures in this section differ depending on whether you are configuring a stand-alone server or a server that is part of a resource pool.

Create networks in a standalone server

Because external networks are created for each PIF during host installation, creating extra networks is typically only required to:

- Use a private network
- Support advanced operations such as VLANs or NIC bonding

For information about how to add or delete networks using XenCenter, see Add a New Network in the XenCenter documentation.

Open the Citrix Hypervisor server text console.

Create the network by using the network-create command, which returns the UUID of the newly created network:

```
xe network-create name-label=mynetwork
```

At this point, the network is not connected to a PIF and therefore is internal.

Create networks in resource pools

All Citrix Hypervisor servers in a resource pool must have the same number of physical NICs (NICs). This requirement is not strictly enforced when a host is joined to a pool.

As all hosts in a pool share a common set of network. It is important to have the same physical networking configuration for Citrix Hypervisor servers in a pool. PIFs on the individual hosts are connected to pool-wide networks based on device name. For example, all Citrix Hypervisor servers in a pool with eth0 NIC have a corresponding PIF plugged to the pool-wide `Network 0` network. The same is true for hosts with eth1 NICs and `Network 1`, and other NICs present in at least one Citrix Hypervisor server in the pool.

If one Citrix Hypervisor server has a different number of NICs than other hosts in the pool, complications can arise. The complications can arise because not all pool networks are valid for all pool hosts. For example, if hosts *host1* and *host2* are in the same pool and *host1* has four NICs and *host2* only has two, only the networks connected to PIFs corresponding to eth0 and eth1 are valid on *host2*. VMs on *host1* with VIFs connected to networks corresponding to eth2 and eth3 cannot migrate to host *host2*.

Create VLANs

For servers in a resource pool, you can use the `pool-vlan-create` command. This command creates the VLAN and automatically creates and plug-ins the required PIFs on the hosts in the pool. For more

information, see `pool-vlan-create`.

Open the Citrix Hypervisor server console.

Create a network for use with the VLAN. The UUID of the new network is returned:

```
xe network-create name-label=network5
```

Use the `pif-list` command to find the UUID of the PIF corresponding to the physical NIC supporting the desired VLAN tag. The UUIDs and device names of all PIFs are returned, including any existing VLANs:

```
xe pif-list
```

Create a VLAN object specifying the desired physical PIF and VLAN tag on all VMs to be connected to the new VLAN. A new PIF is created and plugged to the specified network. The UUID of the new PIF object is returned.

```
xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
```

Attach VM VIFs to the new network. For more information, see Creating networks in a standalone server.

Create NIC bonds on a standalone host

We recommend using XenCenter to create NIC bonds. For more information, see Configuring NICs.

This section describes how to use the xe CLI to bond NIC interfaces on Citrix Hypervisor servers that are not in a pool. For information on using the xe CLI to create NIC bonds on Citrix Hypervisor servers that comprise a resource pool, see *Creating NIC bonds in resource pools*.

Create a NIC bond

When you bond a NIC, the bond absorbs the PIF/NIC in use as the management interface. The management interface is automatically moved to the bond PIF.

1. Use the `network-create` command to create a network for use with the bonded NIC. The UUID of the new network is returned:

   ```
   xe network-create name-label=bond0
   ```

2. Use the `pif-list` command to determine the UUIDs of the PIFs to use in the bond:

   ```
   xe pif-list
   ```

3. Do one of the following:

   - To configure the bond in active-active mode (default), use the `bond-create` command to create the bond. Using commas to separate the parameters, specify the newly created network UUID and the UUIDs of the PIFs to be bonded:

     ```
     xe bond-create network-uuid=network_uuid /
          pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
     ```

     Type two UUIDs when you are bonding two NICs and four UUIDs when you are bonding four NICs. The UUID for the bond is returned after running the command.

   - To configure the bond in active-passive or LACP bond mode, use the same syntax, add the optional `mode` parameter, and specify `lacp` or `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
     ```

Control the MAC address of the bond

When you bond the management interface, it subsumes the PIF/NIC in use as the management interface. If the host uses DHCP, the bond's MAC address is the same as the PIF/NIC in use. The management interface's IP address can remain unchanged.

You can change the bond's MAC address so that it is different from the MAC address for the (current) management-interface NIC. However, as the bond is enabled and the MAC/IP address in use changes, existing network sessions to the host are dropped.

You can control the MAC address for a bond in two ways:

- An optional `mac` parameter can be specified in the `bond-create` command. You can use this parameter to set the bond MAC address to any arbitrary address.
- If the `mac` parameter is not specified, Citrix Hypervisor uses the MAC address of the management interface if it is one of the interfaces in the bond. If the management interface is not part of the bond, but another management interface is, the bond uses the MAC address (and also the IP address) of that management interface. If none of the NICs in the bond is a management interface, the bond uses the MAC of the first named NIC.

Revert NIC bonds

When reverting the Citrix Hypervisor server to a non-bonded configuration, the `bond-destroy` command automatically configures the primary NIC as the interface for the management interface. Therefore, all VIFs are moved to the management interface. If management interface of a host is on tagged VLAN bonded interface, on performing `bond-destroy`, management VLAN is moved to primary NIC.

The term primary NIC refers to the PIF that the MAC and IP configuration was copied from when creating the bond. When bonding two NICs, the primary NIC is:

1. The management interface NIC (if the management interface is one of the bonded NICs).
2. Any other NIC with an IP address (if the management interface was not part of the bond).
3. The first named NIC. You can find out which one it is by running the following:

```
xe bond-list params=all
```

Create NIC bonds in resource pools

Whenever possible, create NIC bonds as part of initial resource pool creation, before joining more hosts to the pool or creating VMs. Doing so allows the bond configuration to be automatically replicated to hosts as they are joined to the pool and reduces the number of steps required.

Adding a NIC bond to an existing pool requires one of the following:

- Using the CLI to configure the bonds on the master and then each member of the pool.
- Using the CLI to configure bonds on the master and then restarting each pool member so that it inherits its settings from the master.
- Using XenCenter to configure the bonds on the master. XenCenter automatically synchronizes the networking settings on the member servers with the master, so you do not need to restart the member servers.

For simplicity and to prevent misconfiguration, we recommend using XenCenter to create NIC bonds. For more information, see Configuring NICs.

This section describes using the xe CLI to create bonded NIC interfaces on Citrix Hypervisor servers that comprise a resource pool. For information on using the xe CLI to create NIC bonds on a standalone host, see *Creating NIC bonds on a standalone host*.

> **Warning:**
>
> Do not attempt to create network bonds when high availability is enabled. The process of bond creation disturbs the in-progress high availability heartbeat and causes hosts to self-fence (shut themselves down). The hosts can fail to restart properly and may need the `host-emergency-ha-disable` command to recover.

Select the host you want to be the master. The master host belongs to an unnamed pool by default. To create a resource pool with the CLI, rename the existing nameless pool:

```
xe pool-param-set name-label="New Pool" uuid=pool_uuid
```

Create the NIC bond as described in Create a NIC bond.

Open a console on a host that you want to join to the pool and run the command:

```
xe pool-join master-address=host1 master-username=root master-password=password
```

The network and bond information is automatically replicated to the new host. The management interface is automatically moved from the host NIC where it was originally configured to the bonded PIF. That is, the management interface is now absorbed into the bond so that the entire bond functions as the management interface.

Use the `host-list` command to find the UUID of the host being configured:

```
xe host-list
```

Warning:

Do not attempt to create network bonds while high availability is enabled. The process of bond creation disturbs the in-progress high availability heartbeat and causes hosts to self-fence (shut themselves down). The hosts can fail to restart properly and you may need to run the `host-emergency-ha-disable` command to recover.

Configure a dedicated storage NIC

You can use XenCenter or the xe CLI to assign a NIC an IP address and dedicate it to a specific function, such as storage traffic. When you configure a NIC with an IP address, you do so by creating a secondary interface. (The IP-enabled NIC Citrix Hypervisor used for management is known as the management interface.)

When you want to dedicate a secondary interface for a specific purpose, ensure that the appropriate network configuration is in place. This is to ensure that the NIC is used only for the desired traffic. To dedicate a NIC to storage traffic, configure the NIC, storage target, switch, and VLAN such that the target is only accessible over the assigned NIC. If your physical and IP configuration does not limit the traffic sent across the storage NIC, you can send traffic, such as management traffic across the secondary interface.

When you create a new secondary interface for storage traffic, you must assign it an IP address that is:

- On the same subnet as the storage controller, if applicable, and
- Not on the same subnet as any other secondary interfaces or the management interface.

When you are configuring secondary interfaces, each secondary interface must be on a separate subnet. For example, if you want to configure two more secondary interfaces for storage, you require IP addresses on three different subnets – one subnet for the management interface, one subnet for Secondary Interface 1, and one subnet for Secondary Interface 2.

If you are using bonding for resiliency for your storage traffic, you may want to consider using LACP instead of the Linux bridge bonding. To use LACP bonding, you must configure the vSwitch as your networking stack. For more information, see vSwitch networks.

> **Note:**
>
> When selecting a NIC to configure as a secondary interface for use with iSCSI or NFS SRs, ensure that the dedicated NIC uses a separate IP subnet that is not routable from the management interface. If this is not enforced, then storage traffic may be directed over the main management interface after a host restart, because of the order in which network interfaces are initialized.

Ensure that the PIF is on a separate subnet, or routing is configured to suit your network topology to force desired traffic over the selected PIF.

Set up an IP configuration for the PIF, adding appropriate values for the mode parameter. If using static IP addressing, add the IP, netmask, gateway, and DNS parameters:

```
xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
```

Set the PIF's disallow-unplug parameter to true:

```
xe pif-param-set disallow-unplug=true uuid=pif-uuid
```

```
xe pif-param-set other-config:management_purpose="Storage" uuid=pif-uuid
```

If you want to use a secondary interface for storage that can be routed from the management interface also (bearing in mind that this configuration is not the best practice), you have two options:

- After a host restart, ensure that the secondary interface is correctly configured. Use the `xe pbd-unplug` and `xe pbd-plug` commands to reinitialize the storage connections on the host. This command restarts the storage connection and routes it over the correct interface.
- Alternatively, you can use `xe pif-forget` to delete the interface from the Citrix Hypervisor database and manually configure it in the control domain. `xe pif-forget` is an advanced option and requires you to be familiar with how to configure Linux networking manually.

Use SR-IOV enabled NICs

Single Root I/O Virtualization (SR-IOV) is a virtualization technology that allows a single PCI device to appear as multiple PCI devices on the physical system. The actual physical device is known as a Physical Function (PF) while the others are known as Virtual Functions (VF). The hypervisor can assign one or more VFs to a Virtual Machine (VM): the guest can then use the device as if it were directly assigned.

Assigning one or more NIC VFs to a VM allows its network traffic to bypass the virtual switch. When configured, each VM behaves as though it is using the NIC directly, reducing processing overhead, and improving performance.

Benefits of SR-IOV

An SR-IOV VF has a better performance than VIF. It can ensure the hardware-based segregation between traffic from different VMs through the same NIC (bypassing the Citrix Hypervisor network stack).

Using this feature, you can:

- Enable SR-IOV on NICs that support SR-IOV.
- Disable SR-IOV on NICs that support SR-IOV.
- Manage SR-IOV VFs as a VF resource pool.
- Assign SR-IOV VFs to a VM.
- Configure SR-IOV VFs (For example, MAC address, VLAN, rate).
- Run tests to confirm if SR-IOV is supported as part of the Automated Certification Kit.

System configuration

Configure the hardware platform correctly to support SR-IOV. The following technologies are required:

- I/O MMU virtualization (AMD-Vi and Intel VT-d)
- Alternative Routing-ID Interpretation (ARI)
- Address Translation Services (ATS)
- Access Control Services (ACS)

Check the documentation that comes with your system for information on how to configure the BIOS to enable the mentioned technologies.

Enable an SR-IOV network on a NIC

In XenCenter, use the **New Network** wizard in the **Networking** tab to create and enable an SR-IOV network on a NIC.

Assign an SR-IOV network to the virtual interface (VM level)

In XenCenter, at the VM level, use the **Add Virtual Interface** wizard in the **Networking** tab to add an SR-IOV enabled network as a virtual interface for that VM. For more information, see Add a New Network.

Supported NICs and guests

For a list of supported hardware platforms and NICs, see Hardware Compatibility List. See the documentation provided by the vendor for a particular guest to determine whether it supports SR-IOV.

Limitations

- For certain NICs using legacy drivers (for example, Intel I350 family) the host must be rebooted to enable or disable SR-IOV on these devices.
- Only HVM guests are supported with SR-IOV.
- A pool level SR-IOV network having different types of NICs are not supported.
- An SR-IOV VF and a normal VIF from the same NIC may not be able to communicate with each other because of the NIC hardware limitations. To enable these hosts to communicate, ensure that communication uses the pattern VF to VF or VIF to VIF, and not VF to VIF.
- Quality of Service settings for some SR-IOV VFs do not take effect because they do not support network speed rate limiting.
- Performing live migration, suspend, and checkpoint is not supported on VMs using an SR-IOV VF.
- SR-IOV VFs do not support hot-plugging.
- For some NICs with legacy NIC drivers, rebooting may be required even after host restart which indicates that the NIC is not able to enable SR-IOV.
- VMs created in previous releases cannot use this feature from XenCenter.
- If your VM has an SR-IOV VF, functions that require Live Migration are not possible. This is because the VM is directly tied to the physical SR-IOV enabled NIC VF.
- Hardware restriction: The SR-IOV feature relies on the Controller to reset device functions to a pristine state within 100ms, when requested by the hypervisor using Function Level Reset (FLR).
- SR-IOV can be used in an environment that makes use of high availability. However, SR-IOV is not considered in the capacity planning. VMs that have SR-IOV VFs assigned are restarted on a best-effort basis when there is a host in the pool that has appropriate resources. These resources include SR-IOV enabled on the right network and a free VF.

Configure SR-IOV VFs for legacy drivers

Usually the maximum number of VFs that a NIC can support can be determined automatically. For NICs using legacy drivers (for example, Intel I350 family), the limit is defined within the driver module configuration file. The limit may need to be adjusted manually. To set it to the maximum, open the file using an editor and change the line starting:

```
## VFs-maxvfs-by-user:
```

For example, to set the maximum VFs to 4 for the `igb` driver edit `/etc/modprobe.d/igb.conf` to read:

```
## VFs-param: max_vfs
## VFs-maxvfs-by-default: 7
```

```
## VFs-maxvfs-by-user: 4
options igb max_vfs=0
```

Notes:

- The value must be less than or equal to the value in the line `VFs-maxvfs-by-default`.
- Do not change any other line in these files.
- Make the changes before enabling SR-IOV.

CLI

See SR-IOV commands for CLI instructions on creating, deleting, displaying SR-IOV networks and assigning an SR-IOV VF to a VM.

Control the rate of outgoing data (QoS)

To limit the amount of *outgoing* data a VM can send per second, set an optional Quality of Service (QoS) value on VM virtual interfaces (VIFs). The setting lets you specify a maximum transmit rate for outgoing packets in *kilobytes* per second.

The Quality of Service value limits the rate of transmission *from* the VM. The Quality of Service setting does not limit the amount of data the VM can receive. If such a limit is desired, we recommend limiting the rate of incoming packets higher up in the network (for example, at the switch level).

Depending on networking stack configured in the pool, you can set the Quality of Service value on VM virtual interfaces (VIFs) in one of two places. Either by using the xe CLI or in XenCenter).

- **XenCenter** You can set the Quality of Service transmit rate limit value in the properties dialog for the virtual interface.
- **xe commands** You can set the Quality of Service transmit rate using the CLI using the commands in the section that follow.

Example of CLI command for QoS

To limit a VIF to a maximum transmit rate of 100 kilobytes per second using the CLI, use the `vif-param-set` command:

```
xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
```

Change networking configuration options

This section discusses how to change the networking configuration of your Citrix Hypervisor server. It includes:

- Changing the hostname (that is, the Domain Name System (DNS) name)
- Adding or deleting DNS servers
- Changing IP addresses
- Changing which NIC is used as the management interface
- Adding a new physical NIC to the server
- Adding a purpose to a network
- Enabling ARP filtering (switch-port locking)

Hostname

The system hostname, also known as the domain or DNS name, is defined in the pool-wide database and changed using the `xe host-set-hostname-live` CLI command as follows:

```
xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
```

The underlying control domain hostname changes dynamically to reflect the new hostname.

DNS servers

To add or delete DNS servers in the IP addressing configuration of the Citrix Hypervisor server, use the `pif-reconfigure-ip` command. For example, for a PIF with a static IP:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip
```

Change IP address configuration for a standalone host

You can use the xe CLI to change the network interface configuration. Do not change the underlying network configuration scripts directly.

To change the IP address configuration of a PIF, use the `pif-reconfigure-ip` CLI command. See `pif-reconfigure-ip` for details on the parameters of the `pif-reconfigure-ip` command. See the following section for information on changing host IP addresses in resource pools.

Change IP address configuration in resource pools

Citrix Hypervisor servers in resource pools have a single management IP address used for management and communication to and from other hosts in the pool. The steps required to change the IP address of a host's management interface are different for master and other hosts.

Note:

> You must be careful when changing the IP address of a server, and other networking parameters. Depending upon the network topology and the change being made, connections to network storage can be lost. When this happens, the storage must be replugged using the **Repair Storage** function in XenCenter, or by using the `pbd-plug` CLI command. For this reason, we recommend that you migrate VMs away from the server before changing its IP configuration.

Use the `pif-reconfigure-ip` CLI command to set the IP address as desired. See `pif-reconfigure-ip` for details on the parameters of the `pif-reconfigure-ip` command. :

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

Use the `host-list` CLI command to confirm that the member host has successfully reconnected to the master host by checking that all the other Citrix Hypervisor servers in the pool are visible:

```
xe host-list
```

Changing the IP address of the master Citrix Hypervisor server requires extra steps. This is because each pool member uses the advertised IP address of the pool master for communication. The pool members do not know how to contact the master when its IP address changes.

Whenever possible, use a dedicated IP address that is not likely to change for the lifetime of the pool for pool masters.

Use the `pif-reconfigure-ip` CLI command to set the IP address as desired:

```
xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

When the IP address of the pool master changes, all member hosts enter into an emergency mode when they fail to contact the master host.

On the pool master, use the `pool-recover-slaves` command to force the master to contact each pool member and inform them of the new master IP address:

```
xe pool-recover-slaves
```

Management interface

When Citrix Hypervisor is installed on a host with multiple NICs, one NIC is selected for use as the management interface. The management interface is used for XenCenter connections to the host and for host-to-host communication.

Use the `pif-list` command to determine which PIF corresponds to the NIC to be used as the management interface. The UUID of each PIF is returned.

```
xe pif-list
```

Use the `pif-param-list` command to verify the IP addressing configuration for the PIF used for the management interface. If necessary, use the `pif-reconfigure-ip` command to configure IP addressing for the PIF to be used.

```
xe pif-param-list uuid=pif_uuid
```

Use the `host-management-reconfigure` CLI command to change the PIF used for the management interface. If this host is part of a resource pool, *this command must be issued on the member host console*:

```
xe host-management-reconfigure pif-uuid=pif_uuid
```

Use the `network-list` command to determine which PIF corresponds to the NIC to be used as the management interface for all the hosts in the pool. The UUID of pool wide network is returned.

```
xe network-list
```

Use the `network-param-list` command to fetch the PIF UUIDs of all the hosts in the pool. Use the `pif-param-list` command to verify the IP addressing configuration for the PIF for the management interface. If necessary, use the `pif-reconfigure-ip` command to configure IP addressing for the PIF to be used.

```
xe pif-param-list uuid=pif_uuid
```

Use the `pool-management-reconfigure` CLI command to change the PIF used for the management interface listed in the Networks list.

```
xe pool-management-reconfigure network-uuid=network_uuid
```

Disable management access

To disable remote access to the management console entirely, use the `host-management-disable` CLI command.

> **Warning:**
>
> When the management interface is disabled, you must log in on the physical host console to perform management tasks. External interfaces such as XenCenter do not work when the management interface is disabled.

Add a new physical NIC

Install a new physical NIC on your Citrix Hypervisor server in the usual manner. After restarting the server, run the xe CLI command `pif-scan` to cause a new PIF object to be created for the new NIC.

Remove a physical NIC

Before removing the NIC, ensure that you know the UUID of the corresponding PIF. Remove the physical NIC from your Citrix Hypervisor server in the usual manner. After restarting the server, run the xe CLI command `pif-forget uuid=<UUID>` to destroy the PIF object.

Add a purpose to a network

The network purpose can be used to add extra functionalities to a network. For example, the ability to use the network to make NBD connections.

To add a network purpose, use the`xe network-param-add` command:

```
xe network-param-add param-name=purpose param-key=purpose uuid=network-uuid
```

To delete a network purpose, use the`xe network-param-remove` command:

```
xe network-param-remove param-name=purpose param-key=purpose uuid=network-uuid
```

Currently, the available values for the network purpose are `nbd` and `insecure_nbd`. For more information, see the Citrix Hypervisor Changed Block Tracking Guide.

Use switch port locking

The Citrix Hypervisor switch-port locking feature lets you control traffic sent from unknown, untrusted, or potentially hostile VMs by limiting their ability to pretend they have a MAC or IP address that was not assigned to them. You can use the port-locking commands to block all traffic on a network by default or define specific IP addresses from which an individual VM is allowed to send traffic.

Switch-port locking is a feature designed for public cloud-service providers in environments concerned about internal threats. This functionality assists public cloud-service providers who have a network architecture in which each VM has a public, internet-connected IP address. Because cloud tenants are untrusted, you can use security measures such as spoofing protection to ensure that tenants cannot attack other virtual machines in the cloud.

Using switch-port locking lets you simplify your network configuration by enabling all of your tenants or guests to use the same Layer 2 network.

One of the most important functions of the port-locking commands is they can restrict the traffic that an untrusted guest send. This restricts the guest's ability to pretend it has a MAC or IP address it does not actually possess. Specifically, you can use these commands to prevent a guest from:

- Claiming an IP or MAC address other than the ones the Citrix Hypervisor administrator has specified it can use
- Intercepting, spoofing, or disrupting the traffic of other VMs

Requirements

- The Citrix Hypervisor switch-port locking feature is supported on the Linux bridge and vSwitch networking stacks.
- When you enable Role Based Access Control (RBAC) in your environment, the user configuring switch-port locking must be logged in with an account that has at least a Pool Operator or Pool Admin role. When RBAC is not enabled in your environment, the user must be logged in with the root account for the pool master.
- When you run the switch-port locking commands, networks can be online or offline.
- In Windows guests, the disconnected Network icon only appears when Citrix VM Tools are installed in the guest.

Notes

Without any switch-port locking configurations, VIFs are set to "network_default" and Networks are set to "unlocked."

Configuring switch-port locking is not supported when any third-party controllers are in use in the environment.

Switch port locking does not prevent cloud tenants from:

- Performing an IP-level attack on another tenant/user. However, switch-port locking prevents them performing the IP-level attack if they attempt to use the following means to do so and switch-port locking is configured: a) impersonating another tenant in the cloud or user or b) initiating an intercept of traffic intended for another user.
- Exhausting network resources.
- Receiving some traffic intended for other virtual machines through normal switch flooding behaviors (for broadcast MAC addresses or unknown destination MAC addresses).

Likewise, switch-port locking does not restrict where a VM can send traffic to.

Implementation notes

You can implement the switch-port locking functionality either by using the command line or the Citrix Hypervisor API. However, in large environments, where automation is a primary concern, the most typical implementation method might be by using the API.

Examples

This section provides examples of how switch-port locking can prevent certain types of attacks. In these examples, VM-c is a virtual machine that a hostile tenant (Tenant C) is leasing and using for attacks. VM-a and VM-b are virtual machines leased by non-attacking tenants.

Example 1: How switch port locking can prevent ARP spoofing prevention:

ARP spoofing is used to indicate an attacker's attempts to associate their MAC address with the IP address for another node. ARP spoofing can potentially result in the node's traffic being sent to the attacker instead. To achieve this goal the attacker sends fake (spoofed) ARP messages to an Ethernet LAN.

Scenario:

Virtual Machine A (VM-a) wants to send IP traffic from VM-a to Virtual Machine B (VM-b) by addressing it to VM-b's IP address. The owner of Virtual Machine C wants to use ARP spoofing to pretend their VM, VM-c, is actually VM-b.

1. VM-c sends a speculative stream of ARP replies to VM-a. The ARP replies claim that the MAC address in the reply (c_MAC) is associated with the IP address, b_IP

   Result: Because the administrator enabled switch-port locking, these packets are all dropped because enabling switch-port locking prevents impersonation.

2. VM-b sends an ARP reply to VM-a, claiming that the MAC address in the reply (b_MAC) is associated with the IP address, b_IP.

   Result: VM-a receives VM-b's ARP response.

Example 2: IP Spoofing prevention:

IP address spoofing is a process that conceals the identity of packets by creating Internet Protocol (IP) packets with a forged source IP address.

Scenario:

Tenant C is attempting to perform a Denial of Service attack using their host, Host-C, on a remote system to disguise their identity.

Attempt 1:

Tenant C sets Host-C's IP address and MAC address to VM-a's IP and MAC addresses (a_IP and a_MAC). Tenant C instructs Host-C to send IP traffic to a remote system.

Result: The Host-C packets are dropped. This is because the administrator enabled switch-port locking. The Host-C packets are dropped because enabling switch-port locking prevents impersonation.

Attempt 2:

Tenant C sets Host-C's IP address to VM-a's IP address (a_IP) and keeps their original c_MAC.

Tenant C instructs Host-C to send IP traffic to a remote system.

Result: The Host-C packets are dropped. This is because the administrator enabled switch-port locking, which prevents impersonation.

Example 3: Web hosting:

Scenario:

Alice is an infrastructure administrator.

One of her tenants, Tenant B, is hosting multiple websites from their VM, VM-b. Each website needs a distinct IP address hosted on the same virtual network interface (VIF).

Alice reconfigures Host-B's VIF to be locked to a single MAC but many IP addresses.

How switch-port locking works

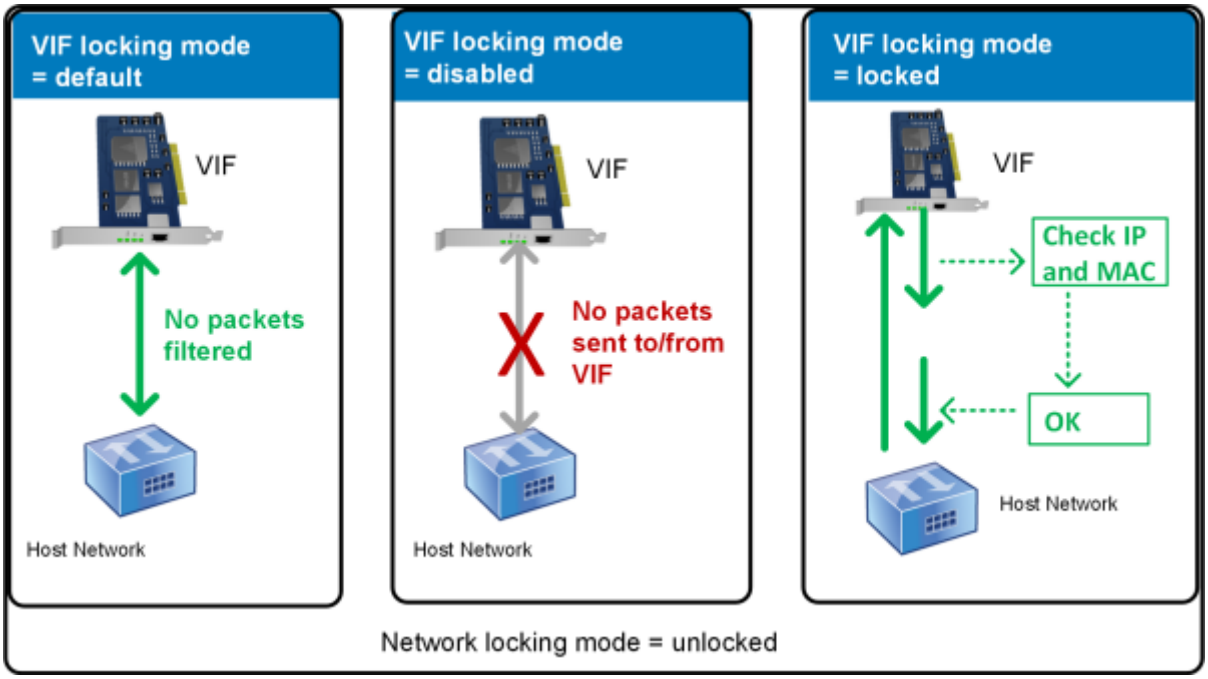
The switch-port locking feature lets you control packet filtering at one or more of two levels:

- **VIF level**. Settings you configure on the VIF determine how packets are filtered. You can set the VIF to prevent the VM from sending any traffic, restrict the VIF so it can only send traffic using its assigned IP address, or allow the VM to send traffic to any IP address on the network connected to the VIF.
- **Network level**. The Citrix Hypervisor network determines how packets are filtered. When a VIF's locking mode is set to `network_default`, it refers to the network-level locking setting to determine what traffic to allow.

Regardless of which networking stack you use, the feature operates the same way. However, as described in more detail in the sections that follow, the Linux bridge does not fully support switch-port locking in IPv6.

VIF locking-mode states

The Citrix Hypervisor switch-port locking feature provides a locking mode that lets you configure VIFs in four different states. These states only apply when the VIF is plugged into a running virtual machine.



- **Network_default**. When the VIF's state is set to `network_default`, Citrix Hypervisor uses the network's `default-locking-mode` parameter to determine if and how to filter packets traveling through

the VIF. The behavior varies according to if the associated network has the network default locking mode parameter set to disabled or unlocked:

`-default-locking-mode=disabled`, Citrix Hypervisor applies a filtering rule so that the VIF drops all traffic.

`-default-locking-mode`=unlocked, Citrix Hypervisor removes all the filtering rules associated with the VIF. By default, the default locking mode parameter is set to `unlocked`.

For information about the `default-locking-mode` parameter, see Network commands.

The default locking mode of the network has no effect on attached VIFs whose locking state is anything other than `network_default`.

> **Note:**
>
> You cannot change the `default-locking-mode` of a network that has active VIFs attached to it.

- **Locked**. Citrix Hypervisor applies filtering rules so that only traffic sent to/from the specified MAC and IP addresses is allowed to be sent out through the VIF. In this mode, if no IP addresses are specified, the VM cannot send any traffic through that VIF, on that network.

  To specify the IP addresses from which the VIF accepts traffic, use the IPv4 or IPv6 IP addresses by using the `ipv4_allowed` or `ipv6_allowed` parameters. However, if you have the Linux bridge configured, do not type IPv6 addresses.

  Citrix Hypervisor lets you type IPv6 addresses when the Linux bridge is active. However, Citrix Hypervisor cannot filter based on the IPv6 addresses typed. The reason is the Linux bridge does not have modules to filter Neighbor Discovery Protocol (NDP) packets. Therefore, complete protection cannot be implemented and guests would be able to impersonate another guest by forging NDP packets. As result, if you specify even one IPv6 address, Citrix Hypervisor lets all IPv6 traffic pass through the VIF. If you do not specify any IPv6 addresses, Citrix Hypervisor does not let any IPv6 traffic pass through to the VIF.

- **Unlocked**. All network traffic can pass through the VIF. That is, no filters are applied to any traffic going to or from the VIF.

- **Disabled**. No traffic is allowed to pass through the VIF. (That is, Citrix Hypervisor applies a filtering rule so that the VIF drops all traffic.)

Configure switch port locking

This section provides three different procedures:

- Restrict VIFs to use a specific IP address

- Add an IP address to an existing restricted list. For example, to add an IP address to a VIF when the VM is running and connected to the network (for example, if you are taking a network offline temporarily).

- Remove an IP address from an existing restricted list

If a VIF's locking-mode is set to `locked`, it can only use the addresses specified in the `ipv4-allowed` or `ipv6-allowed` parameters.

Because, in some relatively rare cases, VIFs may have more than one IP address, it is possible to specify multiple IP addresses for a VIF.

You can perform these procedures before or after the VIF is plugged in (or the VM is started).

Change the default-locking mode to locked, if it is not using that mode already, by running the following command:

```
xe vif-param-set uuid=vif-uuid locking-mode=locked
```

The `vif-uuid` represents the UUID of the VIF you want to allow to send traffic. To obtain the UUID, run the xe `vif-list` command on the host. `vm-uuid` Indicates the virtual machine for which the information appears. The device ID indicates the device number of the VIF.

Run the `vif-param-set` command to specify the IP addresses from which the virtual machine can send traffic. Do one or more of the following:

- Specify one or more IPv4 IP addresses destinations. For example:

  ```
  xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list of ipv4-
  addresses
  ```

- Specify one or more IPv6 IP addresses destinations. For example:

  ```
  xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list of ipv6-
  addresses
  ```

You can specify multiple IP addresses by separating them with a comma, as shown in the preceding example.

After performing the procedure to restrict a VIF to using a specific IP address, you can add one or more IP addresses the VIF can use.

Run the `vif-param-add` command to add the IP addresses to the existing list. Do one or more of the following:

- Specify the IPv4 IP address. For example:

  ```
  xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list of ipv4-
  addresses
  ```

- Specify the IPv6 IP address. For example:

```
xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list of ipv6-
addresses
```

If you restrict a VIF to use two or more IP addresses, you can delete one of those IP addresses from the list.

Run the `vif-param-remove` command to delete the IP addresses from the existing list. Do one or more of the following:

- Specify the IPv4 IP address to delete. For example:

```
xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated list of ipv4-
addresses
```

- Specify the IPv6 IP address to delete. For example:

```
xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated list of ipv6-
addresses
```

Prevent a virtual machine from sending or receiving traffic from a specific network

The following procedure prevents a virtual machine from communicating through a specific VIF. As a VIF connects to a specific Citrix Hypervisor network, you can use this procedure to prevent a virtual machine from sending or receiving any traffic from a specific network. This provides a more granular level of control than disabling an entire network.

If you use the CLI command, you do not need to unplug the VIF to set the VIF's locking mode. The command changes the filtering rules while the VIF is running. In this case, the network connection still appears to be present, however, the VIF drops any packets the VM attempts to send.

> **Tip:**
>
> To find the UUID of a VIF, run the xe `vif-list` command on the host. The device ID indicates the device number of the VIF.

To prevent a VIF from receiving traffic, disable the VIF connected to the network from which you want to stop the VM from receiving traffic:

```
xe vif-param-set uuid=vif-uuid locking-mode=disabled
```

You can also disable the VIF in XenCenter by selecting the virtual network interface in the VM's Networking tab and clicking Deactivate.

Remove a VIF's restriction to an IP address

To revert to the default (original) locking mode state, use the following procedure. By default, when you create a VIF, Citrix Hypervisor configures it so that it is not restricted to using a specific IP address.

To revert a VIF to an unlocked state, change the VIF default-locking mode to unlocked. If it is not using that mode already, run the following command:

```
xe vif-param-set uuid=vif_uuid locking-mode=unlocked
```

Simplify VIF locking mode configuration in the Cloud

Rather than running the VIF locking mode commands for each VIF, you can ensure all VIFs are disabled by default. To do so, you must change the packet filtering at the network level. Changing the packet filtering causes the Citrix Hypervisor network to determine how packets are filtered, as described in the previous section *How switch-port locking works*.

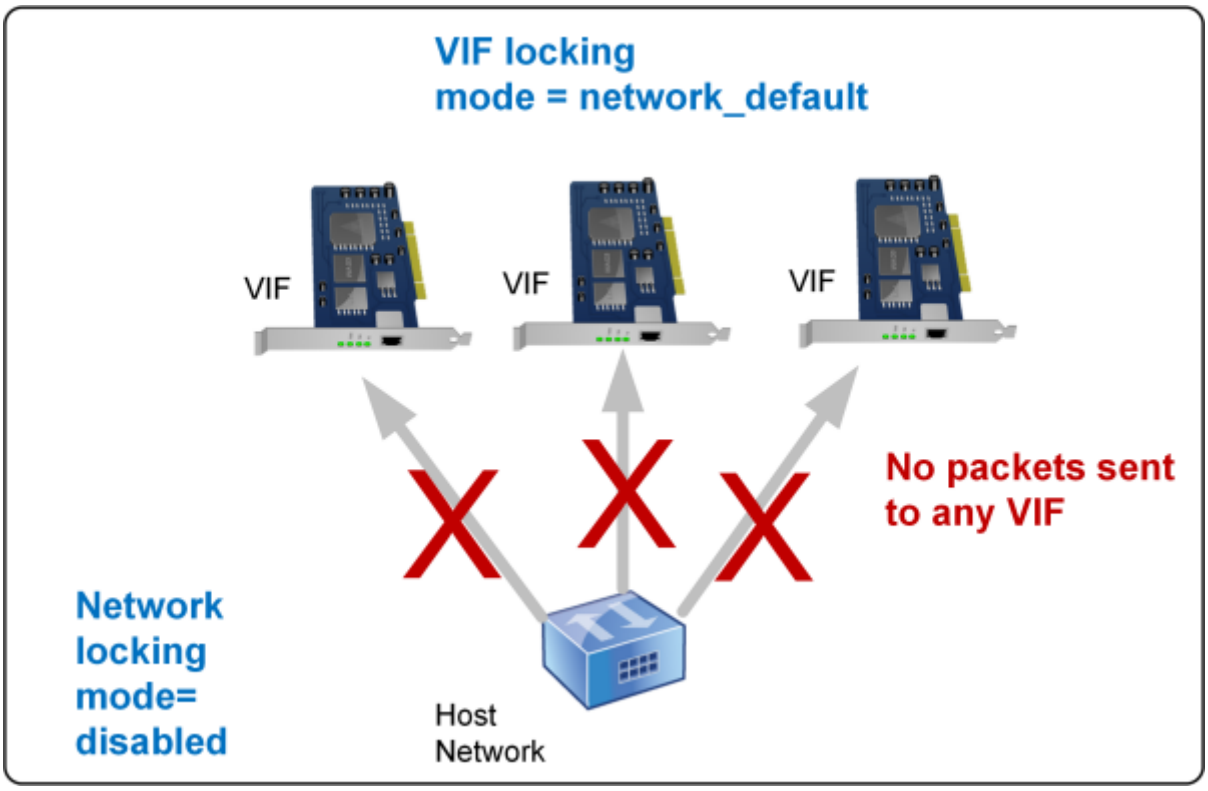
Specifically, a network's `default-locking-mode` setting determines how new VIFs with default settings behave. Whenever a VIF's `locking-mode` is set to `default`, the VIF refers to the network-locking mode (`default-locking-mode`) to determine if and how to filter packets traveling through the VIF:

- **Unlocked**. When the network `default-locking-mode` parameter is set to `unlocked`, Citrix Hypervisor lets the VM send traffic to any IP address on the network the VIF connects to.
- **Disabled**. When the `default-locking-mode` parameter is set to `disabled`, Citrix Hypervisor applies a filtering rule so that the VIF drops all traffic.

By default, the `default-locking-mode` for all networks created in XenCenter and using the CLI are set to `unlocked`.

By setting the VIF's locking mode to its default (`network_default`), you can create a basic default configuration (at the network level) for all newly created VIFs that connect to a specific network.

This illustration shows how, when a VIF's `locking-mode` is set to its default setting (`network_default`), the VIF uses the network `default-locking-mode` to determine its behavior.



For example, by default, VIFs are created with their `locking-mode` set to `network_default`. If you set a network's `default-locking-mode=disabled`, any new VIFs for which you have not configured the locking mode are disabled. The VIFs remain disabled until you either (a) change the individual VIF's `locking-mode` parameter or (b) explicitly set the VIF's `locking-mode` to `unlocked. This is helpful when you trust a specific VM enough so you do not want to filter its traffic at all.

To change a network's default locking mode setting:

After creating the network, change the default-locking mode by running the following command:

```
xe network-param-set uuid=network-uuid default-locking-mode=[unlocked|disabled]
```

> **Note:**
>
> To get the UUID for a network, run the xe `network-list` command. This command displays the UUIDs for all the networks on the host on which you ran the command.

To check a network's default locking mode setting:

Run one of the following commands:

```
xe network-param-get uuid=network-uuid param-name=default-locking-mode
```

OR

```
xe network-list uuid=network-uuid params=default-locking-mode
```

Use network settings for VIF traffic filtering

The following procedure instructs a VIF on a virtual machine to use the Citrix Hypervisor network `default-locking-mode` settings on the network itself to determine how to filter traffic.

1. Change the VIF locking state to `network_default`, if it is not using that mode already, by running the following command:

   ```
   xe vif-param-set uuid=vif_uuid locking-mode=network_default
   ```

2. Change the default-locking mode to `unlocked`, if it is not using that mode already, by running the following command:

   ```
   xe network-param-set uuid=network-uuid default-locking-mode=unlocked
   ```

Troubleshoot networking

If you are experiencing problems with configuring networking, first ensure that you have not directly changed any of the control domain `ifcfg-*` files. The control domain host agent manages the `ifcfg` files directly, and any changes are overwritten.

Diagnosing network corruption

Some network card models require firmware upgrades from the vendor to work reliably under load, or when certain optimizations are turned on. If you see corrupted traffic to VMs, try to obtain the latest firmware from your vendor and then apply a BIOS update.

If the problem still persists, then you can use the CLI to disable receive or transmit offload optimizations on the physical interface.

> **Warning:**
>
> Disabling receive or transmit offload optimizations can result in a performance loss and increased CPU usage.

First, determine the UUID of the physical interface. You can filter on the `device` field as follows:

```
xe pif-list device=eth0
```

Next, set the following parameter on the PIF to disable TX offload:

```
xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
```

Finally, replug the PIF or restart the host for the change to take effect.

Emergency network reset

Incorrect networking settings can cause loss of network connectivity. When there is no network connectivity, Citrix Hypervisor server can become inaccessible through XenCenter or remote SSH. Emergency Network Reset provides a simple mechanism to recover and reset a host's networking.

The Emergency network reset feature is available from the CLI using the `xe-reset-networking` command, and within the **Network and Management Interface** section of `xsconsole`.

Incorrect settings that cause a loss of network connectivity include renaming network interfaces, creating bonds or VLANs, or mistakes when changing the management interface. For example, typing the wrong IP address. You may also want to run this utility in the following scenarios:

- When a rolling pool upgrade, manual upgrade, hotfix installation, or driver installation causes a lack of network connectivity, or
- If a Pool master or host in a resource pool is unable to contact with other hosts.

Use the `xe-reset-networking` utility only in an emergency because it deletes the configuration for all PIFs, bonds, VLANs, and tunnels associated with the host. Guest Networks and VIFs are preserved. As part of this utility, VMs are shut down forcefully. Before running this command, cleanly shut down the VMs where possible. Before you apply a reset, you can change the management interface and specify which IP configuration, DHCP, or Static can be used.

If the pool master requires a network reset, reset the network on the pool master first before applying a network reset on pool members. Apply the network reset on all remaining hosts in the pool to ensure that the pool's networking configuration is homogeneous. Network homogeneity is an important factor for live migration.

> **Note:**
>
> If the pool master's IP address (the management interface) changes as a result of a network reset or `xe host-management-reconfigure`, apply the network reset command to other hosts in the pool. This is to ensure that the pool members can reconnect to the Pool Master on its new IP address. In this situation, the IP address of the Pool Master must be specified.
>
> Network reset is NOT supported when High Availability is enabled. To reset network configuration in this scenario, you must first manually disable high availability, and then run the network reset command.

Verifying the network reset

After you specify the configuration mode to be used after the network reset, `xsconsole` and the CLI display settings that will be applied after host reboot. It is a final chance to modify before applying the emergency network reset command. After restart, the new network configuration can be verified in XenCenter and `xsconsole`. In XenCenter, with the host selected, select the **Networking** tab to see the new network configuration. The Network and Management Interface section in **xsconsole** display this information.

> **Note:**
>
> Run emergency network reset on other pool members to replicate bonds, VLANs, or tunnels from the Pool Master's new configuration.

Using the CLI for network reset

The following table shows the available optional parameters which can be used by running the `xe-reset-networking` command.

> **Warning:**

Users are responsible to ensure the validity of parameters for the `xe-reset-networking` command, and to check the parameters carefully. If you specify invalid parameters, network connectivity and configuration can be lost. In this situation, we advise that you rerun the command `xe-reset-networking` without using any parameters.

Resetting the networking configuration of a whole pool **must** begin on the pool master, followed by network reset on all remaining hosts in the pool.

Parameter	Required/Optional	Description
`-m`, `--master`	Optional	IP address of the Pool Master's management interface. Defaults to the last known Pool Master's IP address.
`--device`	Optional	Device name of the management interface. Defaults to the device name specified during installation.
`--mode=static`	Optional	Enables the following four networking parameters for static IP configuration for the management interface. If not specified, networking is configured using DHCP.
`--ip`	Required, if `mode=static`	IP address for the host's management interface. Only valid if `mode=static`.
`--netmask`	Required, if `mode=static`	Netmask for the management interface. Only valid if `mode=static`.
`--gateway`	Optional	Gateway for the management interface. Only valid if `mode=static`.
`--dns`	Optional	DNS Server for the management interface. Only valid if `mode=static`.
`--vlan`	Optional	VLAN tag for the management interface. Defaults to the VLAN tag specified during installation.

Pool master command-line examples

Examples of commands that can be applied on a Pool Master:

To reset networking for DHCP configuration:

```
xe-reset-networking
```

To reset networking for Static IP configuration:

```
xe-reset-networking --mode= static --ip=ip-address \
    --netmask=netmask --gateway=gateway \
    --dns=dns
```

To reset networking for DHCP configuration if another interface became the management interface after initial setup:

```
xe-reset-networking --device=device-name
```

To reset networking for Static IP configuration if another interface became the management interface after initial setup:

```
xe-reset-networking --device=device-name --mode=static \
    --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
```

To reset networking for management interface on VLAN:

```
xe-reset-networking --vlan=VLAN TAG
```

Note:

The `reset-network` command can also be used along with the IP configuration settings.

Pool member command-line examples

All previous examples also apply to pool members. Additionally, the Pool Master's IP address can be specified (which is necessary if it has changed.)

To reset networking for DHCP configuration:

```
xe-reset-networking
```

To reset networking for DHCP if the Pool Master's IP address was changed:

```
xe-reset-networking --master=master-ip-address
```

To reset networking for Static IP configuration, assuming the Pool Master's IP address didn't change:

```
xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \
    --gateway=gateway --dns=dns
```

To reset networking for DHCP configuration if the management interface and the Pool Master's IP address was changed after initial setup:

```
xe-reset-networking --device=device-name --master=master-ip-address
```

Storage

This section describes how physical storage hardware maps to virtual machines (VMs), and the software objects used by the management API to perform storage-related tasks. Detailed sections on each of the supported storage types include the following information:

- Procedures for creating storage for VMs using the CLI, with type-specific device configuration options
- Generating snapshots for backup purposes
- Best practices for managing storage
- Virtual disk QoS (Quality of Service) settings

Storage repositories (SRs)

A Storage Repository (SR) is a particular storage target, in which Virtual Machine (VM) Virtual Disk Images (VDIs) are stored. A VDI is a storage abstraction that represents a virtual hard disk drive (HDD).

SRs are flexible, with built-in support for the following drives:

Locally connected:

- SATA
- SCSI
- SAS
- NVMe

The local physical storage hardware can be a hard disk drive (HDD) or a solid state drive (SSD).

Remotely connected:

- iSCSI
- NFS
- SAS
- SMB (version 3 only)
- Fibre Channel

> **Note:**
>
> NVMe over Fibre Channel and NVMe over TCP are not supported.

The SR and VDI abstractions allow for advanced storage features to be exposed on storage targets that support them. For example, advanced features such as *thin provisioning*, VDI snapshots, and fast cloning. For storage subsystems that don't support advanced operations directly, a software stack that implements these features is provided. This software stack is based on Microsoft's Virtual Hard Disk (VHD) specification.

A storage repository is a persistent, on-disk data structure. For SR types that use an underlying block device, the process of creating an SR involves erasing any existing data on the specified storage target. Other storage types such as NFS, create a container on the storage array in parallel to existing SRs.

Each Citrix Hypervisor server can use multiple SRs and different SR types simultaneously. These SRs can be shared between hosts or dedicated to particular hosts. Shared storage is pooled between multiple hosts within a defined resource pool. A shared SR must be network accessible to each host in the pool. All servers in a single resource pool must have at least one shared SR in common. Shared storage cannot be shared between multiple pools.

SR commands provide operations for creating, destroying, resizing, cloning, connecting and discovering the individual VDIs that they contain. CLI operations to manage storage repositories are described in SR commands.

> **Warning:**
>
> Citrix Hypervisor does not support snapshots at the external SAN-level of a LUN for any SR type.

Virtual disk image (VDI)

A virtual disk image (VDI) is a storage abstraction that represents a virtual hard disk drive (HDD). VDIs are the fundamental unit of virtualized storage in Citrix Hypervisor. VDIs are persistent, on-disk objects that exist independently of Citrix Hypervisor servers. CLI operations to manage VDIs are described in VDI commands. The on-disk representation of the data differs by SR type. A separate storage plug-in interface for each SR, called the SM API, manages the data.

Physical block devices (PBDs)

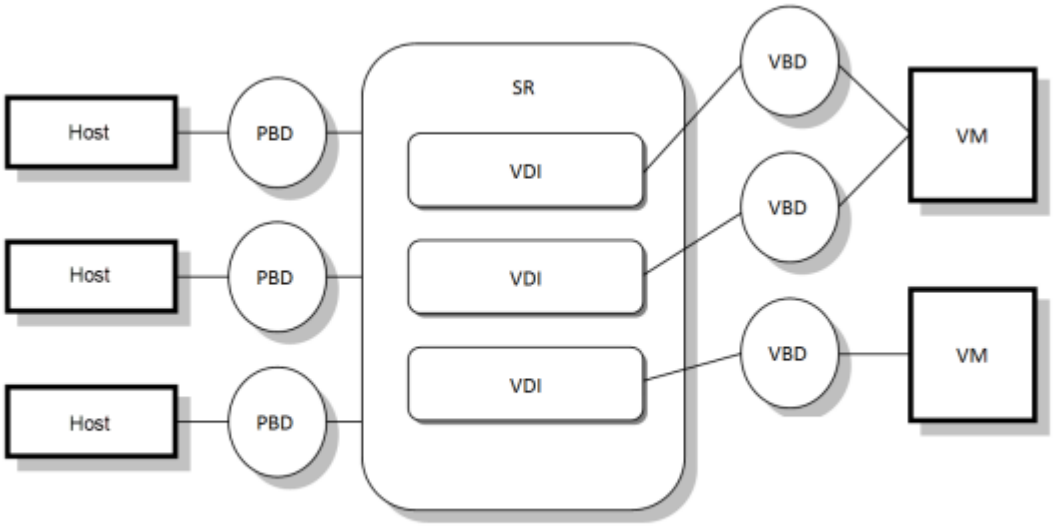
Physical block devices represent the interface between a physical server and an attached SR. PBDs are connector objects that allow a given SR to be mapped to a host. PBDs store the device configuration fields that are used to connect to and interact with a given storage target. For example, NFS device configuration includes the IP address of the NFS server and the associated path that the Citrix Hypervisor server mounts. PBD objects manage the run-time attachment of a given SR to a given Citrix Hypervisor server. CLI operations relating to PBDs are described in PBD commands.

Virtual block devices (VBDs)

Virtual Block Devices are connector objects (similar to the PBD described above) that allows mappings between VDIs and VMs. In addition to providing a mechanism for attaching a VDI into a VM, VBDs allow for the fine-tuning of parameters regarding QoS (Quality of Service) and statistics of a given VDI, and whether that VDI can be booted. CLI operations relating to VBDs are described in VBD commands.

Summary of storage objects

The following image is a summary of how the storage objects presented so far are related:



Virtual disk data formats

In general, there are the following types of mapping of physical storage to a VDI:

1. *Logical volume-based VHD on a LUN:* The default Citrix Hypervisor block-based storage inserts a logical volume manager on a disk. This disk is either a locally attached device (LVM) or a SAN attached LUN over either Fibre Channel, iSCSI, or SAS. VDIs are represented as volumes within the volume manager and stored in VHD format to allow thin provisioning of reference nodes on snapshot and clone.

2. *File-based QCOW2 on a LUN:* VM images are stored as thin-provisioned QCOW2 format files on a GFS2 shared-disk filesystem on a LUN attached over either iSCSI software initiator or Hardware HBA.

3. *File-based VHD on a filesystem:* VM images are stored as thin-provisioned VHD format files on either a local non-shared filesystem (EXT3/EXT4 type SR), a shared NFS target (NFS type SR), or a remote SMB target (SMB type SR).

VDI types

For GFS2 SRs, QCOW2 VDIs are created.

For other SR types, VHD format VDIs are created. You can opt to use raw at the time you create the VDI. This option can only be specified by using the xe CLI.

> **Note:**
>
> If you create a raw VDI on an LVM-based SR or HBA/LUN-per-VDI SR, it might allow the owning VM to access data that was part of a previously deleted VDI (of any format) belonging to any VM. We recommend that you consider your security requirements before using this option.
>
> Raw VDIs on a NFS, EXT, or SMB SR do not allow access to the data of previously deleted VDIs belonging to any VM.

To check if a VDI was created with `type=raw`, check its `sm-config` map. The `sr-param-list` and `vdi-param-list` xe commands can be used respectively for this purpose.

Create a raw virtual disk by using the xe CLI

1. Run the following command to create a VDI given the UUID of the SR you want to place the virtual disk in:

   ```
   xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size \
           name-label=VDI name sm-config:type=raw
   ```

2. Attach the new virtual disk to a VM. Use the disk tools within the VM to partition and format, or otherwise use the new disk. You can use the `vbd-create` command to create a VBD to map the virtual disk into your VM.

Convert between VDI formats

It is not possible to do a direct conversion between the raw and VHD formats. Instead, you can create a VDI (either raw, as described above, or VHD) and then copy data into it from an existing volume. Use the xe CLI to ensure that the new VDI has a virtual size at least as large as the VDI you are copying from. You can do this by checking its `virtual-size` field, for example by using the `vdi-param-list` command. You can then attach this new VDI to a VM and use your preferred tool within the VM to do a direct block-copy of the data. For example, standard disk management tools in Windows or the `dd` command in Linux. If the new volume is a VHD volume, use a tool that can avoid writing empty sectors to the disk. This action can ensure that space is used optimally in the underlying storage repository. A file-based copy approach may be more suitable.

VHD-based and QCOW2-based VDIs

VHD and QCOW2 images can be *chained*, allowing two VDIs to share common data. In cases where a VHD-backed or QCOW2-backed VM is cloned, the resulting VMs share the common on-disk data at the time of cloning. Each VM proceeds to make its own changes in an isolated copy-on-write version of the VDI. This feature allows such VMs to be quickly cloned from templates, facilitating very fast provisioning and deployment of new VMs.

As VMs and their associated VDIs get cloned over time this creates trees of chained VDIs. When one of the VDIs in a chain is deleted, Citrix Hypervisor rationalizes the other VDIs in the chain to remove unnecessary VDIs. This *coalescing* process runs asynchronously. The amount of disk space reclaimed and time taken to perform the process depends on the size of the VDI and amount of shared data.

Both the VHD and QCOW2 formats support *thin provisioning*. The image file is automatically extended in fine granular chunks as the VM writes data into the disk. For file-based VHD and GFS2-based QCOW2, this approach has the considerable benefit that VM image files take up only as much space on the physical storage as required. With LVM-based VHD, the underlying logical volume container must be sized to the virtual size of the VDI. However unused space on the underlying copy-on-write instance disk is reclaimed when a snapshot or clone occurs. The difference between the two behaviors can be described in the following way:

- For *LVM-based VHD images*, the difference disk nodes within the chain consume only as much data as has been written to disk. However, the leaf nodes (VDI clones) remain fully inflated to the virtual size of the disk. Snapshot leaf nodes (VDI snapshots) remain deflated when not in use and can be attached Read-only to preserve the deflated allocation. Snapshot nodes that are attached Read-Write are fully inflated on attach, and deflated on detach.
- For *file-based VHDs* and *GFS2-based QCOW2 images*, all nodes consume only as much data as has been written. The leaf node files grow to accommodate data as it is actively written. If a 100 GB VDI is allocated for a VM and an OS is installed, the VDI file is physically only the size of the OS data on the disk, plus some minor metadata overhead.

When cloning VMs based on a single VHD or QCOW2 template, each child VM forms a chain where new changes are written to the new VM. Old blocks are directly read from the parent template. If the new VM was converted into a further template and more VMs cloned, then the resulting chain results in degraded performance. Citrix Hypervisor supports a maximum chain length of 30. Do not approach this limit without good reason. If in doubt, "copy" the VM using XenCenter or use the `vm-copy` command, which resets the chain length back to 0.

VHD-specific notes on coalesce

Only one coalescing process is ever active for an SR. This process thread runs on the SR master host.

If you have critical VMs running on the master server of the pool, you can take the following steps to mitigate against occasional slow I/O:

- Migrate the VM to a host other than the SR master
- Set the disk I/O priority to a higher level, and adjust the scheduler. For more information, see Virtual disk QoS settings.

Storage repository formats

You can use the **New Storage Repository** wizard in XenCenter to create storage repositories. The wizard guides you through the configuration steps. Alternatively, use the CLI, and the `sr-create` command. The `sr-create` command creates an SR on the storage substrate (potentially destroying any existing data). It also creates the SR API object and a corresponding PBD record, enabling VMs to use the storage. On successful creation of the SR, the PBD is automatically plugged. If the SR `shared=true` flag is set, a PBD record is created and plugged for every Citrix Hypervisor in the resource pool.

If you are creating an SR for IP-based storage (iSCSI or NFS), you can configure one of the following as the storage network: the NIC that handles the management traffic or a new NIC for the storage traffic. To assign an IP address to a NIC, see Configure a dedicated storage NIC.

All Citrix Hypervisor SR types support VDI resize, fast cloning, and snapshot. SRs based on the LVM SR type (local, iSCSI, or HBA) provide thin provisioning for snapshot and hidden parent nodes. The other SR types (EXT3/EXT4, NFS, GFS2) support full thin provisioning, including for virtual disks that are active.

Warnings:

- When VHD VDIs are not attached to a VM, for example for a VDI snapshot, they are stored as thinly provisioned by default. If you attempt to reattach the VDI, ensure that there is sufficient disk-space available for the VDI to become thickly provisioned. VDI clones are thickly provisioned.
- Citrix Hypervisor does not support snapshots at the external SAN-level of a LUN for any SR type.
- If you use thin provisioning on a file-based SR, ensure that you monitor the free space on your SR. If the SR usage grows to 100%, further writes from VMs fail. These failed writes can cause the VM to freeze or crash.

The maximum supported VDI sizes are:

Storage Repository Format	Maximum VDI size
EXT3/EXT4	2 TiB
LVM	2 TiB
NFS	2 TiB
LVMoFCOE	2 TiB
LVMoiSCSI	2 TiB
LVMoHBA	2 TiB
GFS2 (with iSCSI or HBA)	16 TiB

Local LVM

The Local LVM type presents disks within a locally attached Volume Group.

By default, Citrix Hypervisor uses the local disk on the physical host on which it is installed. The Linux Logical Volume Manager (LVM) is used to manage VM storage. A VDI is implemented in VHD format in an LVM logical volume of the specified size.

> **Note:**
>
> The block size of an LVM LUN must be 512 bytes. To use storage with 4 KB native blocks, the storage must also support emulation of 512 byte allocation blocks.

LVM performance considerations

The snapshot and fast clone functionality for LVM-based SRs comes with an inherent performance overhead. When optimal performance is required, Citrix Hypervisor supports creation of VDIs in the *raw* format in addition to the default VHD format. The Citrix Hypervisor snapshot functionality is not supported on raw VDIs.

> **Warning:**
>
> Do not try to snapshot a VM that has `type=raw` disks attached. This action can result in a partial snapshot being created. In this situation, you can identify the orphan snapshot VDIs by checking the `snapshot-of` field and then deleting them.

Creating a local LVM SR

An LVM SR is created by default on host install.

Device-config parameters for LVM SRs are:

Parameter Name	Description	Required?
Device	Device name on the local host to use for the SR	Yes

To create a local LVM SR on `/dev/sdb`, use the following command.

```
xe sr-create host-uuid=valid_uuid content-type=user \
name-label="Example Local LVM SR" shared=false \
device-config:device=/dev/sdb type=lvm
```

Local EXT3/EXT4

Using EXT3/EXT4 enables thin provisioning on local storage. However, the default storage repository type is LVM as it gives a consistent write performance and, prevents storage over-commit. If you use EXT3/EXT4, you might see reduced performance in the following cases:

- When carrying out VM lifecycle operations such as VM create and suspend/resume
- When creating large files from within the VM

Local disk EXT3/EXT4 SRs must be configured using the Citrix Hypervisor CLI.

Whether a local EXT SR uses EXT3 or EXT4 depends on what version of Citrix Hypervisor created it:

- If you created the local EXT SR on an earlier version of XenServer or Citrix Hypervisor and then upgraded to Citrix Hypervisor 8.2, it uses EXT3.
- If you created the local EXT SR on Citrix Hypervisor 8.2, it uses EXT4.

> **Note:**
>
> The block size of an EXT3/EXT4 disk must be 512 bytes. To use storage with 4 KB native blocks, the storage must also support emulation of 512 byte allocation blocks.

Creating a local EXT4 SR (`ext`)

Device-config parameters for ext SRs:

Parameter Name	Description	Required?
Device	Device name on the local host to use for the SR	Yes

To create a local EXT4 SR on `/dev/sdb`, use the following command:

```
xe sr-create host-uuid=valid_uuid content-type=user \
   name-label="Example Local EXT4 SR" shared=false \
   device-config:device=/dev/sdb type=ext
```

udev

The `udev` type represents devices plugged in using the `udev` device manager as VDIs.

Citrix Hypervisor has two SRs of type `udev` that represent removable storage. One is for the CD or DVD disk in the physical CD or DVD-ROM drive of the Citrix Hypervisor server. The other is for a USB device plugged into a USB port of the Citrix Hypervisor server. VDIs that represent the media come and go as disks or USB sticks are inserted and removed.

ISO

The ISO type handles CD images stored as files in ISO format. This SR type is useful for creating shared ISO libraries. For storage repositories that store a library of ISOs, the `content-type` parameter must be set to `iso`.

For example:

```
    xe sr-create host-uuid=valid_uuid content-type=iso \
      type=iso name-label="Example ISO SR" \
      device-config:location=nfs server:path
```

We recommend that you use SMB version 3 to mount ISO SR on Windows file server. Version 3 is selected by default because it is more secure and robust than SMB version 1.0. However, you can mount ISO SR using SMB version 1 using the following command:

```
     xe sr-create content-type=iso type=iso shared=true device-
config:location=valid location
     device-config:username=username device-config:cifspassword=password
     device-config:type=cifs device-config:vers=<Choose either 1.0 or 3.0> name-
label="Example ISO SR"
```

Note:

When running the `sr-create` command you can use the `device-config:cifspassword_secret` argument instead of specifying the password on the command line. For more information, see Secrets.

Software iSCSI support

Citrix Hypervisor supports shared SRs on iSCSI LUNs. iSCSI is supported using the Open-iSCSI software iSCSI initiator or by using a supported iSCSI Host Bus Adapter (HBA). The steps for using iSCSI HBAs are identical to the steps for Fibre Channel HBAs. Both sets of steps are described in Create a Shared LVM over Fibre Channel / Fibre Channel over Ethernet / iSCSI HBA or SAS SR.

Shared iSCSI support using the software iSCSI initiator is implemented based on the Linux Volume Manager (LVM). This feature provides the same performance benefits provided by LVM VDIs in the local disk case. Shared iSCSI SRs using the software-based host initiator can support VM agility using live migration: VMs can be started on any Citrix Hypervisor server in a resource pool and migrated between them with no noticeable downtime.

iSCSI SRs use the entire LUN specified at creation time and may not span more than one LUN. CHAP support is provided for client authentication, during both the data path initialization and the LUN discovery phases.

Note:

The block size of an iSCSI LUN must be 512 bytes. To use storage with 4 KB native blocks, the storage must also support emulation of 512 byte allocation blocks.

Citrix Hypervisor server iSCSI configuration

All iSCSI initiators and targets must have a unique name to ensure they can be uniquely identified on the network. An initiator has an iSCSI initiator address, and a target has an iSCSI target address. Collectively these names are called iSCSI Qualified Names, or IQNs.

Citrix Hypervisor servers support a single iSCSI initiator which is automatically created and configured with a random IQN during host installation. The single initiator can be used to connect to multiple iSCSI targets concurrently.

iSCSI targets commonly provide access control using iSCSI initiator IQN lists. All iSCSI targets/LUNs that your Citrix Hypervisor server accesses must be configured to allow access by the host's initiator IQN. Similarly, targets/LUNs to be used as shared iSCSI SRs must be configured to allow access by all host IQNs in the resource pool.

Note:

iSCSI targets that do not provide access control typically default to restricting LUN access to a single initiator to ensure data integrity. If an iSCSI LUN is used as a shared SR across multiple servers in a pool, ensure that multi-initiator access is enabled for the specified LUN.

The Citrix Hypervisor server IQN value can be adjusted using XenCenter, or using the CLI with the following command when using the iSCSI software initiator:

```
xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=new_initiator_iqn
```

Warning:

- Each iSCSI target and initiator must have a unique IQN. If a non-unique IQN identifier is used, data corruption or denial of LUN access can occur.
- Do not change the Citrix Hypervisor server IQN with iSCSI SRs attached. Doing so can result in failures connecting to new targets or existing SRs.

Software FCoE storage

Software FCoE provides a standard framework to which hardware vendors can plug in their FCoE-capable NIC and get the same benefits of a hardware-based FCoE. This feature eliminates the need for using expensive HBAs.

Before you create a software FCoE storage, manually complete the configuration required to expose a LUN to the host. This configuration includes configuring the FCoE fabric and allocating LUNs to your SAN's public world wide name (PWWN). After you complete this configuration, the available LUN is mounted to the host's CNA as a SCSI device. The SCSI device can then be used to access the LUN as if it were a locally attached SCSI device. For information about configuring the physical switch and the array to support FCoE, see the documentation provided by the vendor.

Note:

Software FCoE can be used with Open vSwitch and Linux bridge as the network back-end.

Create a Software FCoE SR

Before creating a Software FCoE SR, customers must ensure that there are FCoE-capable NICs attached to the host.

Device-config parameters for FCoE SRs are:

Parameter Name	Description	Required?
`SCSIid`	The SCSI bus ID of the destination LUN	Yes

Run the following command to create a shared FCoE SR:

```
xe sr-create type=lvmofcoe \
name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
```

Hardware host bus adapters (HBAs)

This section covers various operations required to manage SAS, Fibre Channel, and iSCSI HBAs.

Sample QLogic iSCSI HBA setup

For details on configuring QLogic Fibre Channel and iSCSI HBAs, see the Cavium website.

Once the HBA is physically installed into the Citrix Hypervisor server, use the following steps to configure the HBA:

1. Set the IP networking configuration for the HBA. This example assumes DHCP and HBA port 0. Specify the appropriate values if using static IP addressing or a multi-port HBA.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
   ```

2. Add a persistent iSCSI target to port 0 of the HBA.

   ```
   /opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0 iscsi_target_ip_address
   ```

3. Use the xe `sr-probe` command to force a rescan of the HBA controller and display available LUNs. For more information, see Probe an SR and Create a Shared LVM over Fibre Channel / Fibre Channel over Ethernet / iSCSI HBA or SAS SR.

Remove HBA-based SAS, FC, or iSCSI device entries

Note:

This step is not required. We recommend that only power users perform this process if it is necessary.

Each HBA-based LUN has a corresponding global device path entry under `/dev/disk/by-scsibus` in the format `<SCSIid>-<adapter>:<bus>:<target>:<lun>` and a standard device path under `/dev`. To remove the device entries for LUNs no longer in use as SRs, use the following steps:

1. Use `sr-forget` or `sr-destroy` as appropriate to remove the SR from the Citrix Hypervisor server database. See Remove SRs for details.
2. Remove the zoning configuration within the SAN for the desired LUN to the desired host.
3. Use the `sr-probe` command to determine the ADAPTER, BUS, TARGET, and LUN values corresponding to the LUN to be removed. For more information, Probe an SR.
4. Remove the device entries with the following command:

```
echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/delete
```

Warning:

Make sure that you are certain which LUN you are removing. Accidentally removing a LUN required for host operation, such as the boot or root device, renders the host unusable.

Shared LVM storage

The Shared LVM type represents disks as Logical Volumes within a Volume Group created on an iSCSI (FC or SAS) LUN.

Note:

The block size of an iSCSI LUN must be 512 bytes. To use storage with 4 KB native blocks, the storage must also support emulation of 512 byte allocation blocks.

Create a shared LVM over iSCSI SR by using the Software iSCSI initiator

Device-config parameters for LVMoiSCSI SRs:

Parameter Name	Description	Required?
`target`	The IP address or host name of the iSCSI filer that hosts the SR. This can also be a comma-separated list of values.	Yes
`targetIQN`	The IQN target address of iSCSI filer that hosts the SR	Yes
`SCSIid`	The SCSI bus ID of the destination LUN	Yes

Parameter Name	Description	Required?
`chapuser`	The user name to be used for CHAP authentication	No
`chappassword`	The password to be used for CHAP authentication	No
`port`	The network port number on which to query the target	No
`usediscoverynumber`	The specific iSCSI record index to use	No
`incoming_chapuser`	The user name that the iSCSI filter uses to authenticate against the host	No
`incoming_chappassword`	The password that the iSCSI filter uses to authenticate against the host	No

To create a shared LVMoiSCSI SR on a specific LUN of an iSCSI target, use the following command.

```
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
```

Create a Shared LVM over Fibre Channel / Fibre Channel over Ethernet / iSCSI HBA or SAS SR

SRs of type LVMoHBA can be created and managed using the xe CLI or XenCenter.

Device-config parameters for LVMoHBA SRs:

Parameter name	Description	Required?
`SCSIid`	Device SCSI ID	Yes

To create a shared LVMoHBA SR, perform the following steps on each host in the pool:

1. Zone in one or more LUNs to each Citrix Hypervisor server in the pool. This process is highly specific to the SAN equipment in use. For more information, see your SAN documentation.
2. If necessary, use the HBA CLI included in the Citrix Hypervisor server to configure the HBA:
   - Emulex: `/bin/sbin/ocmanager`
   - QLogic FC: `/opt/QLogic_Corporation/SANsurferCLI`
   - QLogic iSCSI: `/opt/QLogic_Corporation/SANsurferiCLI`

   For an example of QLogic iSCSI HBA configuration, see *Hardware host bus adapters (HBAs)* in the previous section. For more information on Fibre Channel and iSCSI HBAs, see the Broadcom and Cavium websites.

3. Use the `sr-probe` command to determine the global device path of the HBA LUN. The `sr-probe` command forces a rescan of HBAs installed in the system to detect any new LUNs that have been zoned to the host. The command returns a list of properties for each LUN found. Specify the `host-uuid` parameter to ensure that the probe occurs on the desired host.

   The global device path returned as the `<path>` property is common across all hosts in the pool. Therefore, this path must be used as the value for the `device-config:device` parameter when creating the SR.

   If multiple LUNs are present use the vendor, LUN size, LUN serial number, or the SCSI ID from the `<path>` property to identify the desired LUN.

```
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-360a98000686669496734463876653 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. On the master host of the pool, create the SR. Specify the global device path returned in the `<path>` property from `sr-probe`. PBDs are created and plugged for each host in the pool automatically.

```
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
```

Note:

You can use the XenCenter Repair Storage Repository function to retry the PBD creation and plugging portions of the `sr-create` operation. This function can be valuable in cases where the LUN zoning was incorrect for one or more hosts in a pool when the SR was created. Correct the zoning for the affected hosts and use the Repair Storage Repository function instead of removing and re-creating the SR.

Thin provisioned shared GFS2 block storage

{% includeContent gfs2-intro.md %}

To use shared GFS2 storage, the Citrix Hypervisor resource pool must be a clustered pool. Enable clustering on your pool before creating a GFS2 SR. For more information, see Clustered pools.

Ensure that storage multipathing is set up between your clustered pool and your GFS2 SR. For more information, see Storage multipathing.

SRs of type GFS2 can be created and managed using the xe CLI or XenCenter.

Constraints

{% includeContent gfs2-constraints.md %}

Note:

Operations on GFS2 SRs can get stuck if you have an IP address conflict (multiple hosts having the same IP address) on your clustering network involving at least one host with clustering enabled. In

this case, the hosts do not fence. To fix this issue, resolve the IP address conflict.

Create a shared GFS2 over iSCSI SR by using the Software iSCSI initiator

{% includeContent gfs2-iscsi.md %}

Create a shared GFS2 over HBA SR

{% includeContent gfs2-hba.md %}

NFS and SMB

Shares on NFS servers (that support NFSv4 or NFSv3) or on SMB servers (that support SMB 3) can be used immediately as an SR for virtual disks. VDIs are stored in the Microsoft VHD format only. Additionally, as these SRs can be shared, VDIs stored on shared SRs allow:

- VMs to be started on any Citrix Hypervisor servers in a resource pool
- VM migrate between Citrix Hypervisor servers in a resource pool using live migration (without noticeable downtime)

Important:

- Support for SMB3 is limited to the ability to connect to a share using the 3 protocol. Extra features like Transparent Failover depend on feature availability in the upstream Linux kernel and are not supported in Citrix Hypervisor 8.2.
- For NFSv4, only the authentication type `AUTH_SYS` is supported.
- SMB storage is available for Citrix Hypervisor Premium Edition customers, or those customers who have access to Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement.

VDIs stored on file-based SRs are *thinly provisioned*. The image file is allocated as the VM writes data into the disk. This approach has the considerable benefit that the VM image files take up only as much space on the storage as is required. For example, if a 100 GB VDI is allocated for a VM and an OS is installed, the VDI file only reflects the size of the OS data written to the disk rather than the entire 100 GB.

VHD files may also be chained, allowing two VDIs to share common data. In cases where a file-based VM is cloned, the resulting VMs share the common on-disk data at the time of cloning. Each VM proceeds to make its own changes in an isolated copy-on-write version of the VDI. This feature allows file-based VMs to be quickly cloned from templates, facilitating very fast provisioning and deployment of new VMs.

Note:

The maximum supported length of VHD chains is 30.

File-based SRs and VHD implementations in Citrix Hypervisor assume that they have full control over the SR directory on the file server. Administrators must not modify the contents of the SR directory, as this action can risk corrupting the contents of VDIs.

Citrix Hypervisor has been tuned for enterprise-class storage that uses non-volatile RAM to provide fast acknowledgments of write requests while maintaining a high degree of data protection from failure. Citrix Hypervisor has been tested extensively against Network Appliance FAS2020 and FAS3210 storage, using Data OnTap 7.3 and 8.1

Warning:

As VDIs on file-based SRs are created as thin provisioned, administrators must ensure that the file-based SRs have enough disk space for all required VDIs. Citrix Hypervisor servers do not enforce that the space required for VDIs on file-based SRs is present.

Ensure that you monitor the free space on your SR. If the SR usage grows to 100%, further writes from VMs fail. These failed writes can cause the VM to freeze or crash.

Create a shared NFS SR (NFS)

To create an NFS SR, you must provide the hostname or IP address of the NFS server. You can create the SR on any valid destination path; use the `sr-probe` command to display a list of valid destination paths exported by the server.

In scenarios where Citrix Hypervisor is used with lower-end storage, it cautiously waits for all writes to be acknowledged before passing acknowledgments on to VMs. This approach incurs a noticeable performance cost, and might be solved by setting the storage to present the SR mount point as an asynchronous mode export. Asynchronous exports acknowledge writes that are not actually on disk. Consider the risks of failure carefully in these situations.

Note:

The NFS server must be configured to export the specified path to all servers in the pool. If this configuration is not done, the creation of the SR and the plugging of the PBD record fails.

The Citrix Hypervisor NFS implementation uses TCP by default. If your situation allows, you can configure the implementation to use UDP in scenarios where there may be a performance benefit. To do this configuration, when creating an SR, specify the `device-config` parameter `useUDP=true`.

Device-config parameters for NFS SRs:

Parameter Name	Description	Required?
`server`	IP address or hostname of the NFS server	Yes
`serverpath`	Path, including the NFS mount point, to the NFS server that hosts the SR	Yes

For example, to create a shared NFS SR on `192.168.1.10:/export1`, use the following command:

```
    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"
```

To create a non-shared NFS SR, run the following command:

```
    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"
```

Create a shared SMB SR (SMB)

To create an SMB SR, provide the hostname or IP address of the SMB server, the full path of the exported share, and appropriate credentials.

Device-config parameters for SMB SRs:

Parameter Name	Description	Required?
`server`	Full path to share on server	Yes
`username`	User account with RW access to share	Optional
`password`	Password for the user account	Optional

For example, to create a shared SMB SR on `192.168.1.10:/share1`, use the following command:

```
    xe sr-create content-type=user \
    name-label="Example shared SMB SR" shared=true \
    device-config:server=//192.168.1.10/share1 \
    device-config:username=valid_username device-config:password=valid_password
type=smb
```

To create a non-shared SMB SR, run the following command:

```
    xe sr-create host-uuid=host_uuid content-type=user \
    name-label="Non-shared SMB SR" \
    device-config:server=//192.168.1.10/share1 \
    device-config:username=valid_username device-config:password=valid_password
type=smb
```

Note:

When running the `sr-create` command you can use the `device-config:password_secret` argument instead of specifying the password on the command line. For more information, see Secrets.

LVM over Hardware HBA

The LVM over hardware HBA type represents disks as VHDs on Logical Volumes within a Volume Group created on an HBA LUN that provides, for example, hardware-based iSCSI or FC support.

Citrix Hypervisor servers support Fibre Channel SANs through Emulex or QLogic host bus adapters (HBAs). All Fibre Channel configuration required to expose a Fibre Channel LUN to the host must be completed manually. This configuration includes storage devices, network devices, and the HBA within the Citrix Hypervisor server. After all FC configuration is complete, the HBA exposes a SCSI device backed by the FC LUN to the host. The SCSI device can then be used to access the FC LUN as if it were a locally attached SCSI device.

Use the `sr-probe` command to list the LUN-backed SCSI devices present on the host. This command forces a scan for new LUN-backed SCSI devices. The path value returned by `sr-probe` for a LUN-backed SCSI device is consistent across all hosts with access to the LUN. Therefore, this value must be used when creating shared SRs accessible by all hosts in a resource pool.

The same features apply to QLogic iSCSI HBAs.

See Create storage repositories for details on creating shared HBA-based FC and iSCSI SRs.

Note:

Citrix Hypervisor support for Fibre Channel does not support direct mapping of a LUN to a VM. HBA-based LUNs must be mapped to the host and specified for use in an SR. VDIs within the SR are exposed to VMs as standard block devices.

The block size of an LVM over HBA LUN must be 512 bytes. To use storage with 4 KB native blocks, the storage must also support emulation of 512 byte allocation blocks.

Manage storage repositories

This section covers creating storage repository types and making them available to your Citrix Hypervisor server. It also covers various operations required in the ongoing management of Storage Repositories (SRs), including Live VDI Migration.

Create storage repositories

This section explains how to create Storage Repositories (SRs) of different types and make them available to your Citrix Hypervisor server. The examples provided cover creating SRs using the xe CLI. For details on using the **New Storage Repository** wizard to add SRs using XenCenter, see the XenCenter documentation.

> **Note:**
>
> Local SRs of type `lvm` and `ext` can only be created using the xe CLI. After creation, you can manage all SR types by either XenCenter or the xe CLI.

There are two basic steps to create a storage repository for use on a host by using the CLI:

1. Probe the SR type to determine values for any required parameters.
2. Create the SR to initialize the SR object and associated PBD objects, plug the PBDs, and activate the SR.

These steps differ in detail depending on the type of SR being created. In all examples, the `sr-create` command returns the UUID of the created SR if successful.

SRs can be *destroyed* when no longer in use to free up the physical device. SRs can also be *forgotten* to detach the SR from one Citrix Hypervisor server and attach it to another. For more information, see *Removing SRs* in the following section.

Probe an SR

The `sr-probe` command can be used in the following ways:

- To identify unknown parameters for use in creating an SR
- To return a list of existing SRs

In both cases `sr-probe` works by specifying an SR type and one or more `device-config` parameters for that SR type. If an incomplete set of parameters is supplied, the `sr-probe` command returns an error message indicating parameters are missing and the possible options for the missing parameters. When a complete set of parameters is supplied, a list of existing SRs is returned. All `sr-probe` output is returned as XML.

For example, a known iSCSI target can be probed by specifying its name or IP address. The set of IQNs available on the target is returned:

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10

    Error code: SR_BACKEND_FAILURE_96
    Error parameters: , The request is missing or has an incorrect target IQN
parameter, \
    <?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>
```

Probing the same target again and specifying both the name/IP address and desired IQN returns the set of `SCSIids` (LUNs) available on the target/IQN.

```
    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>
                14945540000000000000000002000000b70200000f000000
            </SCSIid>
        </LUN>
    </iscsi-target>
```

Probing the same target and supplying all three parameters returns a list of SRs that exist on the LUN, if any.

```
    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000b70200000f000000

    <?xml version="1.0" ?>
    <SRlist>
        <SR>
            <UUID>
                3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
            </UUID>
            <Devlist>
                /dev/disk/by-id/scsi-
149455400000000000000000002000000b70200000f000000
            </Devlist>
        </SR>
    </SRlist>
```

The following parameters can be probed for each SR type:

SR type	The parameters, in order of dependency	Can be probed?	Required for ?
lvmoiscsi	target	No	Yes
	chapuser	No	No
	chappassword	No	No
	targetIQN	Yes	Yes
	SCSIid	Yes	Yes
lvmohba	SCSIid	Yes	Yes
NetApp	target	No	Yes
	username	No	Yes
	password	No	Yes
	chapuser	No	No
	chappassword	No	No
	aggregate	No (see note 1)	Yes
	FlexVols	No	No
	allocation	No	No
	asis	No	No
nfs	server	No	Yes

SR type	The parameters, in order of dependency	Can be probed?	Required for ?
	`serverpath`	Yes	Yes
`lvm`	`device`	No	Yes
`ext`	`device`	No	Yes
`EqualLogic`	`target`	No	Yes
	`username`	No	Yes
	`password`	No	Yes
	`chapuser`	No	No
	`chappassword`	No	No
	`storagepool`	No (see note 2)	Yes

Notes:

- Aggregate probing is only possible at `sr-create` time.
- Storage pool probing is only possible at `sr-create` time.

Remove SRs

A Storage Repository (SR) can be removed either temporarily or permanently.

Detach: Breaks the association between the storage device and the pool or host (PBD Unplug). The SR (and its VDIs) becomes inaccessible. The contents of the VDIs and the meta-information used by VMs to access the VDIs are preserved. Detach can be used when you temporarily take an SR offline, for example, for maintenance. A detached SR can later be reattached.

Forget: Preserves the contents of the SR on the physical disk, but the information that connects a VM to its VDIs is permanently deleted. For example, allows you to reattach the SR, to another Citrix Hypervisor server, without removing any of the SR contents.

Destroy: Deletes the contents of the SR from the physical disk.

For Destroy or Forget, the PBD connected to the SR must be unplugged from the host.

1. Unplug the PBD to detach the SR from the corresponding Citrix Hypervisor server:

   ```
   xe pbd-unplug uuid=pbd_uuid
   ```

2. Use the `sr-destroy` command to remove an SR. The command destroys the SR, deletes the SR and corresponding PBD from the Citrix Hypervisor server database and deletes the SR contents from the physical disk:

```
xe sr-destroy uuid=sr_uuid
```

3. Use the `sr-forget` command to forget an SR. The command removes the SR and corresponding PBD from the Citrix Hypervisor server database but leaves the actual SR content intact on the physical media:

```
xe sr-forget uuid=sr_uuid
```

Note:

It can take some time for the software object corresponding to the SR to be garbage collected.

Introduce an SR

To reintroduce a previously *forgotten* SR, create a PBD. Manually plug the PBD to the appropriate Citrix Hypervisor servers to activate the SR.

The following example introduces an SR of type `lvmoiscsi`.

1. Probe the existing SR to determine its UUID:

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000b70200000f000000
```

2. Introduce the existing SR UUID returned from the `sr-probe` command. The UUID of the new SR is returned:

```
xe sr-introduce content-type=user name-label="Example Shared LVM over iSCSI
SR" \
    shared=true uuid=valid_sr_uuid type=lvmoiscsi
```

3. Create a PBD to accompany the SR. The UUID of the new PBD is returned:

```
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=149455400000000000000000002000000b70200000f000000
```

4. Plug the PBD to attach the SR:

```
xe pbd-plug uuid=pbd_uuid
```

5. Verify the status of the PBD plug. If successful, the `currently-attached` property is true:

```
xe pbd-list sr-uuid=sr_uuid
```

Note:

Perform steps 3 through 5 for each server in the resource pool. These steps can also be performed using the Repair Storage Repository function in XenCenter.

Live LUN expansion

To fulfill capacity requirements, you may need to add capacity to the storage array to increase the size of the LUN provisioned to the Citrix Hypervisor server. Live LUN Expansion allows to you to increase the size of the LUN without any VM downtime.

After adding more capacity to your storage array, enter,

```
xe sr-scan sr-uuid=sr_uuid
```

This command rescans the SR, and any extra capacity is added and made available.

This operation is also available in XenCenter. Select the SR to resize, and then click **Rescan**.

Warnings:

- It is not possible to shrink or truncate LUNs. Reducing the LUN size on the storage array can lead to data loss.

Live VDI migration

Live VDI migration allows the administrator to relocate the VMs Virtual Disk Image (VDI) without shutting down the VM. This feature enables administrative operations such as:

- Moving a VM from cheap local storage to fast, resilient, array-backed storage.
- Moving a VM from a development to production environment.
- Moving between tiers of storage when a VM is limited by storage capacity.
- Performing storage array upgrades.

Limitations and caveats

Live VDI Migration is subject to the following limitations and caveats

- There must be sufficient disk space available on the target repository.

To move virtual disks by using XenCenter

1. In the **Resources** pane, select the SR where the Virtual Disk is stored and then click the **Storage** tab.
2. In the **Virtual Disks** list, select the Virtual Disk that you would like to move, and then click **Move**.
3. In the **Move Virtual Disk** dialog box, select the target SR that you would like to move the VDI to.

   > **Note:**
   >
   > Ensure that the SR has sufficient space for another virtual disk: the available space is shown in the list of available SRs.

4. Click **Move** to move the virtual disk.

For xe CLI reference, see `vdi-pool-migrate`.

Cold VDI migration between SRs (offline migration)

VDIs associated with a VM can be copied from one SR to another to accommodate maintenance requirements or tiered storage configurations. XenCenter enables you to copy a VM and all of its VDIs to the same or a different SR. A combination of XenCenter and the xe CLI can be used to copy individual VDIs.

For xe CLI reference, see `vm-migrate`.

Copy all of a VM's VDIs to a different SR

The XenCenter Copy VM function creates copies of all VDIs for a selected VM on the same or a different SR. The source VM and VDIs are not affected by default. To move the VM to the selected SR rather than creating a copy, select the Remove original VM option in the Copy Virtual Machine dialog box.

1. Shut down the VM.
2. Within XenCenter, select the VM and then select the **VM** > **Copy VM** option.
3. Select the desired target SR.

Copy individual VDIs to a different SR

A combination of the xe CLI and XenCenter can be used to copy individual VDIs between SRs.

1. Shut down the VM.
2. Use the xe CLI to identify the UUIDs of the VDIs to be moved. If the VM has a DVD drive, its `vdi-uuid` is listed as `not in database` and can be ignored.

   ```
   xe vbd-list vm-uuid=valid_vm_uuid
   ```

   > **Note:**

> The `vbd-list` command displays both the VBD and VDI UUIDs. Be sure to record the VDI UUIDs rather than the VBD UUIDs.

3. In XenCenter, select the **VM Storage** tab. For each VDI to be moved, select the VDI and click the **Detach** button. This step can also be done using the `vbd-destroy` command.

   > **Note:**
   >
   > If you use the `vbd-destroy` command to detach the VDI UUIDs, first check if the VBD has the parameter `other-config:owner` set to `true`. Set this parameter to `false`. Issuing the `vbd-destroy` command with `other-config:owner=true` also destroys the associated VDI.

4. Use the `vdi-copy` command to copy each of the VM VDIs to be moved to the desired SR.

   ```
   xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
   ```

5. In XenCenter, select the **VM Storage** tab. Click the **Attach** button and select the VDIs from the new SR. This step can also be done use the `vbd-create` command.

6. To delete the original VDIs, select the **Storage** tab of the original SR in XenCenter. The original VDIs are listed with an empty value for the VM field. Use the **Delete** button to delete the VDI.

Convert local Fibre Channel SRs to shared SRs

Use the xe CLI and the XenCenter **Repair Storage Repository** feature to convert a local FC SR to a shared FC SR:

1. Upgrade all hosts in the resource pool to Citrix Hypervisor 8.2.

2. Ensure that all hosts in the pool have the SR's LUN zoned appropriately. See Probe an SR for details on using the `sr-probe` command to verify that the LUN is present on each host.

3. Convert the SR to shared:

   ```
   xe sr-param-set shared=true uuid=local_fc_sr
   ```

4. The SR is moved from the host level to the pool level in XenCenter, indicating that it is now shared. The SR is marked with a red exclamation mark to show that it is not currently plugged on all hosts in the pool.

5. Select the SR and then select the **Storage** > **Repair Storage Repository** option.

6. Click **Repair** to create and plug a PBD for each host in the pool.

Reclaim space for block-based storage on the backing array using discard

You can use space reclamation to free up unused blocks on a thinly provisioned LUN. After the space is released, the storage array can then reuse this reclaimed space.

> **Note:**
>
> Space reclamation is only available on some types of storage arrays. To determine whether your array supports this feature and whether it needs a specific configuration, see the Hardware Compatibility List and your storage vendor specific documentation.

To reclaim the space using XenCenter:

1. Select the **Infrastructure** view, and then choose the server or pool connected to the SR.
2. Click the **Storage** tab.
3. Select the SR from the list, and click **Reclaim freed space**.
4. Click **Yes** to confirm the operation.
5. Click **Notifications** and then **Events** to view the status of the operation.

For more information, press `F1`in XenCenter to access the Online Help.

> **Notes:**
>
> - This operation is available only in XenCenter.
> - The operation is only available for LVM-based SRs that are based on thinly provisioned LUNs on the array. Local SSDs can also benefit from space reclamation.
> - Space reclamation is not required for file-based SRs such as NFS and EXT3/EXT4. The **Reclaim Freed Space** button is not available in XenCenter for these SR types.
> - Space Reclamation is an intensive operation and can lead to a degradation in storage array performance. Therefore, only initiate this operation when space reclamation is required on the array. We recommend that you schedule this work outside of peak array demand hours.

Automatically reclaim space when deleting snapshots

When deleting snapshots with Citrix Hypervisor, space allocated on LVM-based SRs is reclaimed automatically and a VM reboot is not required. This operation is known as 'Online Coalescing'.

Online Coalescing only applies to LVM-based SRs (LVM, LVMoISCSI, and LVMoHBA). It does not apply to EXT3/EXT4 or NFS SRs, whose behavior remains unchanged. In certain cases, automated space reclamation might be unable to proceed. We recommend that you use the Off-Line Coalesce tool in these scenarios:

- Under conditions where a VM I/O throughput is considerable
- In conditions where space is not being reclaimed after a period

> **Notes:**

- Running the Off Line Coalesce tool incurs some downtime for the VM, due to the suspend/resume operations performed.
- Before running the tool, delete any snapshots and clones you no longer want. The tool reclaims as much space as possible given the remaining snapshots/clones. If you want to reclaim the entire space, delete all snapshots and clones.
- VM disks must be either on shared or local storage for a single host. VMs with disks in both types of storage cannot be coalesced.

Reclaim space by using the off line coalesce tool

Note:

Online Coalescing only applies to LVM-based SRs (LVM, LVMoISCSI, and LVMoHBA), it does not apply to EXT3/EXT4 or NFS SRs, whose behavior remains unchanged.

Enable the hidden objects using XenCenter. Click **View** > **Hidden** objects. In the Resource pane, select the VM for which you want to obtain the UUID. The UUID is displayed in the **General** tab.

In the Resource pane, select the resource pool master (the first host in the list. The **General** tab displays the UUID. If you are not using a resource pool, select the VM's host.

1. Open a console on the host and run the following command:

   ```
   xe host-call-plugin host-uuid=host-UUID \
       plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=VM-UUID
   ```

   For example, if the VM UUID is `9bad4022-2c2d-dee6-abf5-1b6195b1dad5` and the host UUID is `b8722062-de95-4d95-9baa-a5fe343898ea`, run the following command:

   ```
   xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea \
       plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2c2d-dee6-
   abf5-1b6195b1dad5
   ```

2. This command suspends the VM (unless it is already powered down), initiates the space reclamation process, and then resumes the VM.

Notes:

We recommend that you shut down or suspend the VM manually before executing the off-line coalesce tool. You can shut down or suspend the VM using either XenCenter or the Citrix Hypervisor CLI. If you execute the coalesce tool on a running VM, the tool automatically suspends the VM, performs the required VDI coalesce operations, and resumes the VM. Agile VMs might restart on a different host.

If the Virtual Disk Images (VDIs) to be coalesced are on shared storage, you must execute the off-line coalesce tool on the pool master.

If the VDIs to be coalesced are on local storage, execute the off-line coalesce tool on the server to which the local storage is attached.

Adjust the disk I/O scheduler

For general performance, the default disk scheduler `noop` is applied on all new SR types. The `noop` scheduler provides the fairest performance for competing VMs accessing the same device. To apply disk QoS, it is necessary to override the default setting and assign the `cfq` disk scheduler to the SR. The corresponding PBD must be unplugged and replugged for the scheduler parameter to take effect. The disk scheduler can be adjusted using the following command:

```
xe sr-param-set other-config:scheduler=noop|cfq|anticipatory|deadline \
    uuid=valid_sr_uuid
```

Note:

This command does not affect EqualLogic, NetApp, or NFS storage.

Virtual disk QoS settings

Virtual disks have an optional I/O priority Quality of Service (QoS) setting. This setting can be applied to existing virtual disks using the xe CLI as described in this section.

For shared SR, where multiple hosts are accessing the same LUN, the QoS setting is applied to VBDs accessing the LUN from the same host. QoS is not applied across hosts in the pool.

Before configuring any QoS parameters for a VBD, ensure that the disk scheduler for the SR has been set appropriately. See *Adjusting the disk I/O scheduler* in the previous section for details on how to adjust the scheduler. The scheduler parameter must be set to `cfq` on the SR for which the QoS is desired.

Note:

Remember to set the scheduler to `cfq` on the SR, and to ensure that the PBD has been replugged for the scheduler change to take effect.

The first parameter is `qos_algorithm_type`. This parameter must be set to the value `ionice`, which is the only type of QoS algorithm supported for virtual disks in this release.

The QoS parameters themselves are set with key/value pairs assigned to the `qos_algorithm_param` parameter. For virtual disks, `qos_algorithm_param` takes a `sched` key, and depending on the value, also requires a `class` key.

Possible values of `qos_algorithm_param:sched` are:

-`sched=rt` or `sched=real-time` sets the QoS scheduling parameter to real time priority, which requires a class parameter to set a value

-`sched=idle` sets the QoS scheduling parameter to idle priority, which requires no class parameter to set any value

-`sched=anything` sets the QoS scheduling parameter to best effort priority, which requires a class parameter to set a value

The possible values for `class` are:

- One of the following keywords: highest, high, normal, low, lowest
- An integer between 0 and 7, where 7 is the highest priority and 0 is the lowest. For example, I/O requests with a priority of 5, are given priority over I/O requests with a priority of 2.

To enable the disk QoS settings, you must also set the `other-config:scheduler` to `cfq` and replug PBDs for the storage in question.

For example, the following CLI commands set the virtual disk's VBD to use real time priority `5`:

```
xe vbd-param-set uuid=vbd_uuid qos_algorithm_type=ionice
xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:sched=rt
xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:class=5
xe sr-param-set uuid=sr_uuid other-config:scheduler=cfq
xe pbd-plug uuid=pbd_uuid
```

Storage multipathing

Dynamic multipathing support is available for Fibre Channel and iSCSI storage back-ends. You can enable multipathing in XenCenter or on the xe CLI.

{% includeContent multipathing-prereqs.md %}

{% includeContent multipathing-setup.md %}

To disable multipathing, first unplug your PBDs, set the host `other-config:multipathing` parameter to `false` and then replug your PBDs as described above. Do not modify the `other-config:multipathhandle` parameter as this action is done automatically.

Multipath support in Citrix Hypervisor is based on the device-mapper `multipathd components`. The Storage Manager API handles activating and deactivating multipath nodes automatically. Unlike the standard `dm-multipath` tools in Linux, device mapper nodes are not automatically created for all LUNs on the system. Device mapper nodes are only provisioned when LUNs are actively used by the storage management layer. Therefore, it is unnecessary to use any of the `dm-multipath` CLI tools to query or refresh DM table nodes in Citrix Hypervisor. If it is necessary to query the status of device-mapper tables manually, or list active device mapper multipath nodes on the system, use the `mpathutil` utility:

```
mpathutil list
```

```
mpathutil status
```

Notes:

- Due to incompatibilities with the integrated multipath management architecture, we recommend that you do not use the standard `dm-multipath` CLI utility with Citrix Hypervisor. Use the `mpathutil` CLI tool for querying the status of nodes on the host.
- Multipath support in EqualLogic arrays does not encompass Storage I/O multipathing in the traditional sense of the term. Multipathing must be handled at the network/NIC bond level. For information about configuring network failover for EqualLogic SRs/LVMoISCSI SRs, see the EqualLogic documentation.

Storage read caching

Read caching improves a VM's disk performance as, after the initial read from external disk, data is cached within the host's free memory. It improves performance in situations where many VMs are cloned off a single base VM, as it drastically reduces the number of blocks read from disk. For example, in Citrix Virtual Desktops environment Machine Creation Service (MCS) environments.

The performance improvement can be seen whenever data is read from disk more than once, as it gets cached in memory. This change is most noticeable in the degradation of service that occurs during heavy I/O situations. For example, in the following situations:

- When a significant number of end users boot up within a very narrow time frame (boot storm)
- When a significant number of VMs are scheduled to run malware scans at the same time (antivirus storms).

Read caching is enabled by default when you have the appropriate license type.

> **Note:**
>
> Storage Read Caching is available for Citrix Hypervisor Premium Edition customers.
>
> Storage Read Caching is also available for customers who access Citrix Hypervisor through their Citrix Virtual Apps and Desktops entitlement.

Enable and disable read caching

For file-based SRs, such as NFS and EXT3/EXT4 SR types, read-caching is enabled by default. Read-caching is disabled for all other SRs.

To disable read caching for a specific SR by using the xe CLI, run the following command:

```
xe sr-param-set uuid=sr-uuid other-config:o_direct=true
```

To disable read caching for a specific SR by using XenCenter, go to the **Properties** dialog for the SR. In the **Read Caching** tab, you can select to enable or disable read caching.

For more information, see Changing SR Properties.

Limitations

- Read caching is available only for NFS and EXT3/EXT4 SRs. It is not available for other SR Types.
- Read caching only applies to read-only VDIs and VDI parents. These VDIs exist where VMs are created from ‘Fast Clone’ or disk snapshots. The greatest performance improvements can be seen when many VMs are cloned from a single ‘golden’ image.

- Performance improvements depend on the amount of free memory available in the host's Control Domain (dom0). Increasing the amount of dom0 memory allows more memory to be allocated to the read-cache. For information on how to configure dom0 memory, see CTX134951.

Comparison with IntelliCache

IntelliCache and memory based read caching are to some regards complementary. IntelliCache not only caches on a different tier, but it also caches writes in addition to reads. IntelliCache caches reads from the network onto a local disk. In-memory read caching caches the reads from network or disk into host memory. The advantage of in-memory read caching, is that memory is still an order of magnitude faster than a solid-state disk (SSD). Performance in boot storms and other heavy I/O situations improves.

Both read-caching and IntelliCache can be enabled simultaneously. In this case, IntelliCache caches the reads from the network to a local disk. Reads from that local disk are cached in memory with read caching.

Set the read cache size

The read cache performance can be optimized, by giving more memory to Citrix Hypervisor's control domain (dom0).

> **Important:**
>
> Set the read cache size on ALL hosts in the pool individually for optimization. Any subsequent changes to the size of the read cache must also be set on all hosts in the pool.

On the Citrix Hypervisor server, open a local shell and log on as root.

To set the size of the read cache, run the following command:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
```

Set both the initial and maximum values to the same value. For example, to set dom0 memory to 2,048 MiB:

```
/opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
```

> **Important:**
>
> Reboot all hosts after changing the read cache size.

How to view the current dom0 memory allocation?

To view the current dom0 memory settings, enter:

```
free -m
```

The output of `free -m` shows the current dom0 memory settings. The value may be less than expected due to various overheads. The example table below shows the output from a host with dom0 set to 2.6 GiB

```
|                     | Total  | Used | Free  | Shared | Buffer/cache | Available
|
|---------------------|--------|------|-------|--------|--------------|-----------
|
| Mem:                | 2450   | 339  | 1556  | 9      | 554          | 2019
|
| Swap:               | 1023   | 0    | 1023  |        |              |
|
```

What Range of Values Can be Used?

As the Citrix Hypervisor Control Domain (dom0) is 64-bit, large values can be used, for example 32768 MiB. However, we recommend that you **do not reduce the dom0 memory below 1 GiB**.

XenCenter display notes

The entire host's memory can be considered to comprise the Xen hypervisor, dom0, VMs, and free memory. Even though dom0 and VM memory is usually of a fixed size, the Xen hypervisor uses a variable amount of memory. The amount of memory used depends on various factors. These factors include the number of VMs running on the host at any time and how those VMs are configured. It is not possible to limit the amount of memory that Xen uses. Limiting the amount of memory can cause Xen to run out of memory and prevent new VMs from starting, even when the host had free memory.

To view the memory allocated to a host, in XenCenter select the host, and then click the **Memory** tab.

The Citrix Hypervisor field displays the *sum* of the memory allocated to dom0 *and* Xen memory. Therefore, the amount of memory displayed might be higher than specified by the administrator. The memory size can vary when starting and stopping VMs, even when the administrator has set a fixed size for dom0.

Memory usage

Two components contribute to the memory footprint of the Citrix Hypervisor server. First, the memory consumed by the Xen hypervisor itself. Second, there is the memory consumed by the *Control Domain* of the host. Also known as 'Domain0', or 'dom0', the control domain is a secure, privileged Linux VM that runs the Citrix Hypervisor management toolstack (XAPI). Besides providing Citrix Hypervisor management functions, the control domain also runs the driver stack that provides user created VM access to physical devices.

Control domain memory

The amount of memory allocated to the control domain is adjusted automatically and is based on the amount of physical memory on the physical host. By default, Citrix Hypervisor allocates **1 GiB plus 5% of the total physical memory** to the control domain, up to an initial maximum of 8 GiB.

> **Note:**
>
> The amount reported in the Citrix Hypervisor section in XenCenter includes the memory used by the control domain (dom0), the Xen hypervisor itself, and the crash kernel. Therefore, the amount of memory reported in XenCenter can exceed these values. The amount of memory used by the hypervisor is larger for hosts using more memory.

Change the amount of memory allocated to the control domain

You can change the amount of memory allocated to dom0 by using XenCenter or by using the command line. If you increase the amount of memory allocated to the control domain beyond the amount allocated by default, this action results in less memory being available to VMs.

You might need to increase the amount of memory assigned to the control domain of a Citrix Hypervisor server in the following cases:

- You are running many VMs on the server
- You are using PVS-Accelerator
- You are using read caching

The amount of memory to allocate to the control domain depends on your environment and the requirements of your VMs.

You can monitor the following metrics to judge whether the amount of control domain memory is appropriate for your environment and what effects any changes you make have:

- **Swap activity:** If the control domain is swapping, increase the control domain memory.
- **Tapdisk mode:** You can monitor whether your tapdisks are in low-memory mode from within the XenCenter **Performance** tab for the server. Select **Actions** > **New Graph** and choose the **Tapdisks in low memory mode** graph. If a tapdisk is in low-memory mode, increase the control domain memory.
- **Pagecache pressure:** Use the `top` command to monitor the `buff/cache` metric. If this number becomes too low, you might want to increase the control domain memory.

Changing the dom0 memory by using XenCenter

For information about changing the dom0 memory by using XenCenter, see Changing the Control Domain Memory in the XenCenter documentation.

> **Note:**
>
> You cannot use XenCenter to reduce dom0 memory below the value that was initially set during Citrix Hypervisor installation. To make this change you must use the command line.

Changing the dom0 memory by using the command line

> **Note:**
>
> On hosts with smaller memory (less than 16 GiB), you might want to reduce the memory allocated to the Control Domain to lower than the installation default value. You can use the command line to make this change. However, we recommend that you **do not reduce the dom0 memory below 1 GiB** and that you do this operation under the guidance of the Support Team.

1. On the Citrix Hypervisor server, open a local shell and log on as root.
2. Type the following:

   ```
   /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<nn>M
   ```

   Where `<nn>` represents the amount of memory, in MiB, to be allocated to dom0.
3. Restart the Citrix Hypervisor server using XenCenter or the `reboot` command on the Citrix Hypervisor console.

   When the host restarts, on the Citrix Hypervisor console, run the `free` command to verify the new memory settings.

How much memory is available to VMs?

To find out how much host memory is available to be assigned to VMs, find the value of the free memory of the host by running `memory-free`. Then type the command `vm-compute-maximum-memory` to get the actual amount of free memory that can be allocated to the VM. For example:

```
xe host-list uuid=host_uuid params=memory-free
xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
```

Monitor and manage your deployment

Citrix Hypervisor provides detailed monitoring of performance metrics. These metrics include CPU, memory, disk, network, C-state/P-state information, and storage. Where appropriate, these metrics are available on a per host and a per VM basis. These metrics are available directly, or can be accessed and viewed graphically in XenCenter or other third-party applications.

Citrix Hypervisor also provides system and performance alerts. Alerts are notifications that occur in response to selected system events. These notifications also occur when one of the following values goes over a specified threshold on a managed host, VM, or storage repository: CPU usage, network usage, memory usage, control domain memory usage, storage throughput, or VM disk usage. You can configure the alerts by using the xe CLI or by using XenCenter. To create notifications based on any of the available Host or VM performance metrics see Performance alerts.

Monitor Citrix Hypervisor performance

Customers can monitor the performance of their Citrix Hypervisor servers and Virtual Machines (VMs) using the metrics exposed through Round Robin Databases (RRDs). These metrics can be queried over HTTP or through the RRD2CSV tool. In addition, XenCenter uses this data to produce system performance graphs. For more information, see Analyze and visualize metrics.

The following tables list all of the available Host and VM metrics.

Notes:

- Latency over a period is defined as the average latency of operations during that period.
- The availability and utility of certain metrics are SR and CPU dependent.
- Performance metrics are not available for GFS2 SRs and disks on those SRs.

Available host metrics

Metric Name	Description	Condition	XenCenter Name
`avgqu_sz_<sr-uuid-short>`	Average I/O queue size (requests).	At least one plugged VBD in SR `<sr-uuid-short>` on the host	`sr-uuid-short` Queue Size
`cpu<cpu>-C<cstate>`	Time CPU `cpu` spent in C-state `cstate` in milliseconds.	C-state exists on CPU	CPU `cpu` C-state `cstate`
`cpu<cpu>-P<pstate>`	Time CPU `cpu` spent in P-state `pstate` in milliseconds.	P-state exists on CPU	CPU `cpu` P-state `pstate`

Metric Name	Description	Condition	XenCenter Name
cpu<cpu>	Utilization of physical CPU cpu (fraction). Enabled by default.	CPU cpu exists	CPU cpu
cpu_avg	Mean utilization of physical CPUs (fraction). Enabled by default.	None	Average CPU
inflight_<sr-uuid-short>	Number of I/O requests currently in flight. Enabled by default.	At least one plugged VBD in SR sr on the host	sr Inflight Requests
io_throughput_read_<sr-uuidshort>	Data read from SR (MiB/s).	At least one plugged VBD in SR sr on the host	sr Read Throughput
io_throughput_write_<sr-uuidshort>	Data written to the SR (MiB/s).	At least one plugged VBD in SR sr on the host	sr Write Throughput
io_throughput_total_<sr-uuidshort>	All SR I/O (MiB/s).	At least one plugged VBD in SR sr on the host	sr Total Throughput
iops_read_<sr-uuid-short>	Read requests per second.	At least one plugged VBD in SR sr on the host	sr Read IOPS
iops_write_<sr-uuid-short>	Write requests per second.	At least one plugged VBD in SR sr on the host	sr Write IOPS
iops_total_<sr-uuid-short>	I/O requests per second.	At least one plugged VBD in SR sr on the host	sr Total IOPS
iowait_<sr-uuid-short>	Percentage of the time waiting for I/O.	At least one plugged VBD in SR sr on the host	sr IO Wait

Metric Name	Description	Condition	XenCenter Name
latency_<sr-uuid-short>	Average I/O latency (milliseconds).	At least one plugged VBD in SR sr on the host	sr Latency
loadavg	Domain0 load average. Enabled by default	None	Control Domain Load
memory_free_kib	Total amount of free memory (KiB). Enabled by default.	None	Free Memory
memory_reclaimed	Host memory reclaimed by squeeze (B).	None	Reclaimed Memory
memory_reclaimed_max	Host memory available to reclaim with squeeze (B).	None	Potential Reclaimed Memory
memory_total_kib	Total amount of memory (KiB) in the host. Enabled by default.	None	Total Memory
network/latency	Interval in seconds between the last two heartbeats transmitted from the local host to all Online hosts. Disabled by default.	HA Enabled	Network Latency
statefile/<t>/latency	Turn-around time in seconds of the latest State-File access from the local host. Disabled by default.	HA Enabled	HA State File Latency
pif_<pif>_rx	Bytes per second received on physical interface pif. Enabled by default.	PIF exists	XenCenter-pifname Receive (see note)
pif_<pif>_tx	Bytes per second sent on physical interface pif. Enabled by default.	PIF exists	XenCenter-pifname Send (see note)

Metric Name	Description	Condition	XenCenter Name
pif_<pif>_rx_errors	Receive errors per second on physical interface pif. Disabled by default.	PIF exists	XenCenter-pifname Receive Errors (see note)
pif_<pif>_tx_errors	Transmit errors per second on physical interface pif . Disabled by default	PIF exists	XenCenter-pifname Send Errors (see note)
pif_aggr_rx	Bytes per second received on all physical interfaces. Enabled by default.	None	Total NIC Receive
pif_aggr_tx	Bytes per second sent on all physical interfaces. Enabled by default.	None	Total NIC Send
pvsaccelerator_evicted	Bytes per second evicted from the cache	PVSAccelerator Enabled	PVS-Accelerator eviction rate
pvsaccelerator_read_hits	Reads per second served from the cache	PVSAccelerator Enabled	PVS-Accelerator hit rate
pvsaccelerator_read_misses	Reads per second that cannot be served from the cache	PVSAccelerator Enabled	PVS-Accelerator miss rate
pvsaccelerator_traffic_client_sent	Bytes per second sent by cached PVS clients	PVSAccelerator Enabled	PVS-Accelerator observed network traffic from clients
pvsaccelerator_traffic_server_sent	Bytes per second sent by cached PVS servers	PVSAccelerator Enabled	PVS-Accelerator observed network traffic from servers

Metric Name	Description	Condition	XenCenter Name
pvsaccelerator_read_total	Reads per second observed by the cache	PVSAccelerator Enabled	PVS-Accelerator observed read rate
pvsaccelerator_traffic_proxy_saved	Bytes per second sent by PVSAccelerator instead of the PVS server	PVSAccelerator Enabled	PVS-Accelerator saved network traffic
pvsaccelerator_space_utilization	Percentage of space used by PVSAccelerator on this host, compared to the total size of the cache storage	PVSAccelerator Enabled	PVS-Accelerator space utilization
sr_<sr>_cache_size	Size in bytes of the IntelliCache SR. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Size
sr_<sr>_cache_hits	Cache hits per second. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Hits
sr_<sr>_cache_misses	Cache misses per second. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Misses
xapi_allocation_kib	Memory (KiB) allocation done by the XAPI daemon. Enabled by default.	None	Agent Memory Allocation
xapi_free_memory_kib	Free memory (KiB) available to the XAPI daemon. Enabled by default.	None	Agent Memory Free
xapi_healthcheck/latency_health	Turn-around time in seconds of the latest XAPI status monitoring call on the local host. Disabled by default	High availability Enabled	Citrix Hypervisor Health Check Latency
xapi_live_memory_kib	Live memory (KiB) used by XAPI daemon. Enabled by default.	None	Agent Memory Live

Metric Name	Description	Condition	XenCenter Name
xapi_memory_usage_kib	Total memory (KiB) allocated used by XAPI daemon. Enabled by default.	None	Agent Memory Usage

Available VM metrics

Metric Name	Description	Condition	XenCenter Name
cpu<cpu>	Utilization of vCPU cpu (fraction). Enabled by default	vCPU cpu exists	CPU
memory	Memory currently allocated to VM (Bytes).Enabled by default	None	Total Memory
memory_target	Target of VM balloon driver (Bytes). Enabled by default	None	Memory target
memory_internal_free	Memory used as reported by the guest agent (KiB). Enabled by default	None	Free Memory
runstate_fullrun	Fraction of time that all vCPUs are running.	None	vCPUs full run
runstate_full_contention	Fraction of time that all vCPUs are runnable (that is, waiting for CPU)	None	vCPUs full contention
runstate_concurrency_hazard	Fraction of time that some vCPUs are running and some are runnable	None	vCPUs concurrency hazard
runstate_blocked	Fraction of time that all vCPUs are blocked or offline	None	vCPUs idle
runstate_partial_run	Fraction of time that some vCPUs are running, and some are blocked	None	vCPUs partial run
runstate_partial_contention	Fraction of time that some vCPUs are runnable and some are blocked	None	vCPUs partial contention
vbd_<vbd>_write	Writes to device vbd in bytes per second. Enabled by default	VBD vbd exists	Disk vbd Write

Metric Name	Description	Condition	XenCenter Name
vbd_<vbd>_read	Reads from device vbd in bytes per second. Enabled by default.	VBD vbd exists	Disk vbd Read
vbd_<vbd>_write_latency	Writes to device vbd in microseconds.	VBD vbd exists	Disk vbd Write Latency
vbd_<vbd>_read_latency	Reads from device vbd in microseconds.	VBD vbd exists	Disk vbd Read Latency
vbd <vbd>_iops_read	Read requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd Read IOPs
vbd <vbd>_iops_write	Write requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd Write IOPS
vbd <vbd>_iops_total	I/O requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd Total IOPS
vbd <vbd>_iowait	Percentage of time waiting for I/0.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd IO Wait
vbd <vbd>_inflight	Number of I/O requests currently in flight.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd Inflight Requests
vbd <vbd>_avgqu_sz	Average I/O queue size.	At least one plugged VBD for non-ISO VDI on the host	Disk vbd Queue Size
vif_<vif>_rx	Bytes per second received on virtual interface number vif. Enabled by default.	VIF vif exists	vif Receive

Metric Name	Description	Condition	XenCenter Name
vif_<vif>_tx	Bytes per second transmitted on virtual interface vif. Enabled by default.	VIF vif exists	vif Send
vif_<vif>_rx_errors	Receive errors per second on virtual interface vif. Enabled by default.	VIF vif exists	vif Receive Errors
vif_<vif>_tx_errors	Transmit errors per second on virtual interface vif Enabled by default.	VIF vif exists	vif Send Errors

Note:

The value of <XenCenter-pif-name> can be any of the following:

NIC <pif>	If <pif> contains pif_eth#, where ## is 0–9
<pif>	If <pif> contains pif_eth#.## or pif_xenbr## or pif_bond##
<Internal> Network <pif>	If <pif> contains pif_xapi##, (note that <Internal> appears as is)
TAP <tap>	If <pif> contains pif_tap##
xapi Loopback	If <pif> contains pif_lo

Analyze and visualize metrics

The Performance tab in XenCenter provides real time monitoring of performance statistics across resource pools in addition to graphical trending of virtual and physical machine performance. Graphs showing CPU, memory, network, and disk I/O are included on the Performance tab by default. You can add more metrics, change the appearance of the existing graphs or create extra ones. For more information, see *Configuring metrics* in the following section.

- You can view up to 12 months of performance data and zoom in to take a closer look at activity spikes.
- XenCenter can generate performance alerts when CPU, memory, network I/O, storage I/O, or disk I/O usage exceed a specified threshold on a server, VM, or SR. For more information, see *Alerts* in the following section.

Note:

Install the Citrix VM Tools to see full VM performance data.

Configure performance graphs

To add a graph:

1. On the **Performance** tab, click **Actions** and then **New Graph**. The New Graph dialog box is displayed.
2. In the **Name** field, enter a name for the graph.
3. From the list of **Datasources**, select the check boxes for the datasources you want to include in the graph.
4. Click **Save**.

To edit an existing graph:

1. Navigate to the **Performance** tab, and select the graph that you would like to modify.
2. Right-click on the graph and select **Actions**, or click the **Actions** button. Then select **Edit Graph**.
3. On the graph details window, make the necessary changes, and click **OK**.

Configure the graph type

Data on the performance graphs can be displayed as lines or as areas. To change the graph type:

1. On the **Tools** menu, click **Options** and select **Graphs**.
2. To view performance data as a line graph, click the **Line graph** option.
3. To view performance data as an area graph, click the **Area graph** option.
4. Click **OK** to save your changes.

Comprehensive details for configuring and viewing XenCenter performance graphs can be found in the XenCenter documentation in the section Monitoring System Performance.

Configure metrics

> **Note:**
>
> C-states and P-states are power management features of some processors. The range of states available depends on the physical capabilities of the host, as well power management configuration.

Both host and VM commands return the following:

- A full description of the data source
- The units applied to the metric
- The range of possible values that may be used

For example:

```
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
```

Enable a specific metric

Most metrics are enabled and collected by default, to enable those metrics that are not, enter the following:

```
xe host-data-source-record data-source=metric name host=hostname
```

Disable a specific metric

You may not want to collect certain metrics regularly. To disable a previously enabled metric, enter the following:

```
xe host-data-source-forget data-source=metric name host=hostname
```

Display a list of currently enabled host metrics

To list the host metrics currently being collected, enter the following:

```
xe host-data-source-list host=hostname
```

Display a list of currently enabled VM metrics

To host the VM metrics currently being collected, enter the following:

```
xe vm-data-source-list vm=vm_name
```

Use RRDs

Citrix Hypervisor uses RRDs to store performance metrics. These RRDs consist of multiple Round Robin Archives (RRAs) in a fixed size database.

Each archive in the database samples its particular metric on a specified granularity:

- Every 5 seconds for 10 minutes
- Every minute for the past two hours
- Every hour for the past week
- Every day for the past year

The sampling that takes place every five seconds records actual data points, however the following RRAs use Consolidation Functions instead. The consolidation functions supported by Citrix Hypervisor are:

- AVERAGE
- MIN
- MAX

RRDs exist for individual VMs (including dom0) and the Citrix Hypervisor server. VM RRDs are stored on the host on which they run, or the pool master when not running. Therefore the location of a VM must be known to retrieve the associated performance data.

For detailed information on how to use Citrix Hypervisor RRDs, see the Citrix Hypervisor Software Development Kit Guide.

Analyze RRDs using HTTP

You can download RRDs over HTTP from the Citrix Hypervisor server specified using the HTTP handler registered at `/host_rrd` or `/vm_rrd`. Both addresses require authentication either by HTTP authentication, or by providing a valid management API session references as a query argument. For example:

Download a Host RRD.

```
wget http://server/host_rrd?session_id=OpaqueRef:SESSION HANDLE>
```

Download a VM RRD.

```
wget http://server/vm_rrd?session_id=OpaqueRef:SESSION HANDLE>&uuid=VM UUID>
```

Both of these calls download XML in a format that can be imported into the `rrdtool` for analysis, or parsed directly.

Analyze RRDs using rrd2csv

In addition to viewing performance metrics in XenCenter, the rrd2csv tool logs RRDs to Comma Separated Value (CSV) format. Man and help pages are provided. To display the rrd2csv tool man or help pages, run the following command:

```
man rrd2csv
```

Or

```
rrd2csv --help
```

Note:

Where multiple options are used, supply them individually. For example: to return both the UUID and the name-label associated with a VM or a host, call rrd2csv as shown below:

```
rrd2csv -u -n
```

The UUID returned is unique and suitable as a primary key, however the name-label of an entity may not necessarily be unique.

The man page (`rrd2csv --help`) is the definitive help text of the tool.

Alerts

You can configure Citrix Hypervisor to generate alerts based on any of the available Host or VM Metrics. In addition, Citrix Hypervisor provides preconfigured alerts that trigger when hosts undergo certain conditions and states. You can view these alerts using XenCenter or the xe CLI.

View alerts using XenCenter

You can view different types of alerts in XenCenter by clicking **Notifications** and then **Alerts**. The Alerts view displays various types of alerts, including Performance alerts, System alerts, and Software update alerts.

Performance alerts

Performance alerts can be generated when one of the following values exceeds a specified threshold on a managed host, VM, or storage repository (SR): CPU usage, network usage, memory usage, control domain memory usage, storage throughput, or VM disk usage.

By default, the alert repeat interval is set to 60 minutes, it can be modified if necessary. Alerts are displayed on the Alerts page in the Notifications area in XenCenter. You can also configure XenCenter to send an email for any specified performance alerts along with other serious system alerts.

Any customized alerts that are configured using the xe CLI are also displayed on the Alerts page in XenCenter.

Each alert has a corresponding priority/severity level. You can modify these levels and optionally choose to receive an email when the alert is triggered. The default alert priority/severity is set at `3`.

Priority	Name	Description	Default Email Alert
1	Critical	Act now or data may be permanently lost/corrupted.	Yes
2	Major	Act now or some services may fail.	Yes
3	Warning	Act now or a service may suffer.	Yes
4	Minor	Notice that something just improved.	No

Priority	Name	Description	Default Email Alert
5	Information	Day-to-day information (VM Start, Stop, Resume and so on)	No
?	Unknown	Unknown error	No

Configure performance alerts

1. In the **Resources** pane, select the relevant host, VM, or SR, then click the **General** tab and then **Properties**.
2. Click the **Alerts** tab. You can configure the following alerts:
   - **CPU usage** alerts for a host or VM: Check the **Generate CPU** usage alerts check box, then set the CPU usage and time threshold that trigger the alert
   - **Network usage** alerts for a host or VM: Check the **Generate network usage alerts** check box, then set the network usage and time threshold that trigger the alert.
   - **Memory usage** alerts for a host: Check the **Generate memory usage alerts** check box, and then set the free memory and time threshold that trigger the alert.
   - **Control domain memory usage** alerts for a host: Check the **Generate control domain memory usage alerts** check box, and then set the control domain memory usage and time threshold that trigger the alert.
   - **Disk usage** alerts for a VM: Check the **Generate disk usage alerts** check box, then set the disk usage and time threshold that trigger the alert.
   - **Storage throughput** alerts for an SR: Check the **Generate storage throughput alerts** check box, then set the storage throughput and time threshold that trigger the alert.

     Note:

     Physical Block Devices (PBD) represent the interface between a specific Citrix Hypervisor server and an attached SR. When the total read/write SR throughput activity on a PBD exceeds the threshold you have specified, alerts are generated on the host connected to the PBD. Unlike other Citrix Hypervisor server alerts, this alert must be configured on the SR.
3. To change the alert repeat interval, enter the number of minutes in the **Alert repeat interval** box. When an alert threshold has been reached and an alert generated, another alert is not generated until after the alert repeat interval has elapsed.
4. Click **OK** to save your changes.

For comprehensive details on how to view, filter and configure severities for performance alerts, see Configuring Performance Alerts in the XenCenter documentation.

System alerts

The following table displays the system events/conditions that trigger an alert to be displayed on the Alerts page in XenCenter.

Name	Priority/Severity	Description
license_expires_soon	2	Citrix Hypervisor License agreement expires soon.
ha-statefile_lost	2	Lost contact with the high availability Storage Repository, act soon.
ha-heartbeat_approaching_timeout	5	High availability approaching timeout, host may reboot unless action is taken.
ha_statefile_approaching_timeout	5	High availability approaching timeout, host may reboot unless action is taken.
haxapi_healthcheck_approaching_timeout	5	High availability approaching timeout, host may reboot unless action is taken.
ha_network_bonding_error	3	Potential service loss. Loss of network that sends high availability heartbeat.
ha_pool_overcommited	3	Potential service loss. High availability is unable to guarantee protection for configured VMs.
ha_poor_drop_in_plan_exists_for	3	High availability coverage has dropped, more likely to fail, no loss present yet.
ha_protected_vm_restart_failed	2	Service Loss. High availability was unable to restart a protected VM.
ha_host_failed	3	High availability detected that a host failed.
ha_host_was_fenced	4	High availability rebooted a host to protect against VM corruption.
redo_log_healthy	4	The XAPI redo log has recovered from a previous error.
redo_log_broken	3	The XAPI redo log has encountered an error.
ip_configured_pif_can_unplug	3	An IP configured NIC can be unplugged by XAPI when using high availability, possibly leading to high availability failure.
host_sync_data_failed	3	Failed to synchronize Citrix Hypervisor performance statistics.

Name	Priority/Severity	Description
host_clock_skew_detected	3	The host clock is not synchronized with other hosts in the pool.
host_clock_went_backwards	1	The host clock is corrupted.
pool_master_transition	4	A new host has been specified as Pool Master.
pbd_plug_failed_on_server_start	3	The host failed to connect to Storage at boot time.
auth_external_init_failed	2	The host failed to enable external AD authentication.
auth_external_pool_non-homogeneous	2	Hosts in a pool have different AD authentication configuration.
multipath_period_alert	3	A path to an SR has failed or recovered.
bond-status-changed	3	A link in a bond has disconnected or reconnected.

Software update alerts

- **XenCenter old:** Citrix Hypervisor expects a newer version but can still connect to the current version
- **XenCenter out of date:** XenCenter is too old to connect to Citrix Hypervisor
- **Citrix Hypervisor out of date:** Citrix Hypervisor is an old version that the current XenCenter cannot connect to
- **License expired alert:** Citrix Hypervisor license has expired
- **Missing IQN alert:** Citrix Hypervisor uses iSCSI storage but the host IQN is blank
- **Duplicate IQN alert:** Citrix Hypervisor uses iSCSI storage, and there are duplicate host IQNs

Configure performance alerts by using the xe CLI

> **Note:**
>
> Triggers for alerts are checked at a minimum interval of five minutes. This interval avoids placing excessive load on the system to check for these conditions and reporting of false positives. Setting an alert repeat interval smaller than five minutes results in the alerts still being generated at the five minute minimum interval.

The performance monitoring `perfmon` tool runs once every five minutes and requests updates from Citrix Hypervisor which are averages over one minute. These defaults can be changed in `/etc/sysconfig/perfmon`.

The `perfmon` tool reads updates every five minutes of performance variables running on the same host. These variables are separated into one group relating to the host itself, and a group for each VM running on

that host. For each VM and host, `perfmon` reads the parameter `other-config:perfmon` and uses this string to determine which variables to monitor, and under which circumstances to generate a message.

For example, the following shows an example of configuring a VM "CPU usage" alert by writing an XML string into the parameter `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>'
```

Note:

You can use multiple variable nodes.

After setting the new configuration, use the following command to refresh `perfmon` for each host:

```
xe host-call-plugin host=host_uuid plugin=perfmon fn=refresh
```

If this refresh is not done, there is a delay before the new configuration takes effect, since by default, `perfmon` checks for new configuration every 30 minutes. This default can be changed in `/etc/sysconfig/perfmon`.

Valid VM elements

- `name`: The name of the variable (no default). If the name value is either `cpu_usage`, `network_usage`, or `disk_usage`, the `rrd_regex` and `alarm_trigger_sense` parameters are not required as defaults for these values are used.
- `alarm_priority`: The priority of the alerts generated (default `3`).
- `alarm_trigger_level`: The level of value that triggers an alert (no default).
- `alarm_trigger_sense`: The value is `high` if `alarm_trigger_level` is a maximum value otherwise `low` if the `alarm_trigger_level` is a minimum value (the default `high`).
- `alarm_trigger_period`: The number of seconds that values (above or below the alert threshold) can be received before an alert is sent (the default is `60`).
- `alarm_auto_inhibit_period`: The number of seconds this alert will be disabled after an alert is sent (the default is `3600`).
- `consolidation_fn`: Combines variables from rrd_updates into one value. For `cpu-usage` the default is `average`, for `fs_usage` the default is`get_percent_fs_usage` and for all others - `sum`.

- `rrd_regex`: Matches the names of variables from `xe vm-data-sources-list uuid=vm_uuid`, to compute performance values. This parameter has defaults for the named variables:
    - cpu_usage
    - network_usage
    - disk_usage

If specified, the values of all items returned by `xe vm-data-source-list` whose names match the specified regular expression are consolidated using the method specified as the `consolidation_fn`.

Valid host elements

- `name`: The name of the variable (no default).
- `alarm_priority`: The priority of the alerts generated (default `3`).
- `alarm_trigger_level`: The level of value that triggers an alert (no default).
- `alarm_trigger_sense`: The value is `high` when `alarm_trigger_level` is a maximum value otherwise `low` if the `alarm_trigger_level` is a minimum value. (default `high`)
- `alarm_trigger_period`: The number of seconds that values (above or below the alert threshold) can be received before an alert is sent (default `60`).
- `alarm_auto_inhibit_period`: The number of seconds that the alert is disabled for after an alert is sent. (default `3600`).
- `consolidation_fn`: Combines variables from `rrd_updates` into one value (default `sum` - or `average`)
- `rrd_regex`: A regular expression to match the names of variables returned by the `xe vm-data-source-list uuid=vm_uuid` command to use to compute the statistical value. This parameter has defaults for the following named variables:
    - cpu_usage
    - network_usage
    - memory_free_kib
    - sr_io_throughput_total_xxxxxxxx (where `xxxxxxxx`is the first eight characters of the SR-UUID).

SR Throughput: Storage throughput alerts must be configured on the SR rather than the host. For example:

```
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>'
```

Generic example configuration

The following example shows a generic configuration:

```
<config>
  <variable>
    <name value="NAME_CHOSEN_BY_USER"/>
```

```
        <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALERT"/>
        <alarm_trigger_period
value="RAISE_ALERT_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
        <alarm_priority value="PRIORITY_LEVEL"/>
        <alarm_trigger_sense value="HIGH_OR_LOW"/>
        <alarm_auto_inhibit_period
value="MINIMUM_TIME_BETWEEN_ALERT_FROM_THIS_MONITOR"/>
        <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
        <rrd_regex value="REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
      </variable>

      <variable>
        ...
      </variable>

      ...
    </config>
```

Configure email alerts

You can configure Citrix Hypervisor to send email notifications when Citrix Hypervisor servers generate alerts. This configuration can be done either by using XenCenter, or by using the xe Command Line Interface (CLI).

Enable email alerts by using XenCenter

1. In the Resources pane, right-click on a pool and select **Properties**.
2. In the Properties window, select **Email Options**.
3. Select the Send email alert notifications check box and enter the email address and SMTP server details.

   > **Note:**
   >
   > Enter the details of an SMTP server which does not require authentication

4. Choose the preferred language from the **Mail language** list to receive performance alert email. The three languages available are English, Chinese, and Japanese.

   The default language for configuring performance alert email language for XenCenter is English.

Enable email alerts by using the xe CLI

> **Important:**
>
> When using XenCenter or the xe CLI to enable email notifications, enter the details of an SMTP server, which does not require authentication. Emails sent through SMTP servers which require authentication are not delivered.

To configure email alerts, specify the email address and SMTP server:

```
    xe pool-param-set uuid=pool_uuid other-config:mail-
destination=joe.bloggs@domain.tld
    xe pool-param-set uuid=pool_uuid other-config:ssmtp-
mailhub=smtp.domain.tld[:port]
```

You can also specify the minimum value of the priority (known as 'severity' in XenCenter) field in the message before the email is sent:

```
    xe pool-param-set uuid=pool_uuid other-config:mail-min-priority=level
```

The default priority level is `3`.

> **Note:**
>
> Some SMTP servers only forward mails with addresses that use FQDNs. If you find that emails are not being forwarded it might be for this reason. In which case, you can set the server host name to the FQDN so this address is used when connecting to your mail server.

To configure performance alert mail language:

```
    xe pool-param-set uuid=pool_uuid other-config:mail-language=en-US | zh-CN |
ja-JP
```

Send email alerts through authenticated SMTP servers

The mail-alarm utility in Citrix Hypervisor uses sSMTP to send email notifications. Before sending email notifications, the mail-alarm utility looks for the configuration file, `mail-alarm.conf`. If the configuration file exists, the contents of the file are used to configure sSMTP. Otherwise the details available in the XAPI database (as configured using XenCenter or the xe CLI) are used to send email alerts. To send email notifications through authenticated SMTP servers, create a `mail-alarm.conf` file in `/etc/` with the following contents:

```
    root=postmaster
    authUser=<username>
    authPass=<password>
    mailhub=<server address>:<port>
```

> **Note:**
>
> This configuration file is used for all alerts generated by Citrix Hypervisor servers.

Extra configuration options

Each SMTP server can differ slightly in its setup and may require extra configuration. The following extract from the `ssmtp.conf` man page shows the correct syntax and available options:

```
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 TLS
        negotiation. See RFC 2487.

    TLSCert
        The file name of an RSA certificate to use for TLS, if required.

    AuthUser
        The user name to use for SMTP AUTH. The default is blank, in
        which case SMTP AUTH is not used.

    AuthPass
```

```
            The password to use for SMTP AUTH.

        AuthMethod
            The authorization method to use. If unset, plain text is used.
            May also be set to "cram-md5".
```

Custom fields and tags

XenCenter supports the creation of tags and custom fields, which allows for organization and quick searching of VMs, storage and so on. For more information, see Monitoring System Performance.

Custom searches

XenCenter supports the creation of customized searches. Searches can be exported and imported, and the results of a search can be displayed in the navigation pane. For more information, see Monitoring System Performance.

Determine throughput of physical bus adapters

For FC, SAS and iSCSI HBAs you can determine the network throughput of your PBDs using the following procedure.

1. List the PBDs on a host.
2. Determine which LUNs are routed over which PBDs.
3. For each PBD and SR, list the VBDs that reference VDIs on the SR.
4. For all active VBDs that are attached to VMs on the host, calculate the combined throughput.

For iSCSI and NFS storage, check your network statistics to determine if there is a throughput bottleneck at the array, or whether the PBD is saturated.

Manage virtual machines

This section provides an overview of how to create Virtual Machines (VMs) using templates. It also explains other preparation methods, including cloning templates and importing previously exported VMs.

What is a virtual machine?

A Virtual Machine (VM) is a software computer that, like a physical computer, runs an operating system and applications. The VM comprises a set of specification and configuration files backed by the physical resources of a host. Every VM has virtual devices that provide the same functions as physical hardware. VMs can give the benefits of being more portable, more manageable, and more secure. In addition, you can tailor the boot behavior of each VM to your specific requirements. For more information, see VM Boot Behavior.

Citrix Hypervisor supports guests with any combination of IPv4 or IPv6 configured addresses.

In Citrix Hypervisor VMs can operate in full virtualized (HVM) mode. Specific processor features are used to 'trap' privileged instructions that the virtual machine carries out. This capability enables you to use an unmodified operating system. For network and storage access, emulated devices are presented to the virtual machine. Alternatively, PV drivers can be used for performance and reliability reasons.

Create VMs

Use VM templates

VMs are prepared from templates. A template is a *gold image* that contains all the various configuration settings to create an instance of a specific VM. Citrix Hypervisor ships with a base set of templates, which are *raw* VMs, on which you can install an operating system. Different operating systems require different settings to run at their best. Citrix Hypervisor templates are tuned to maximize operating system performance.

There are two basic methods by which you can create VMs from templates:

- Using a complete pre-configured template, for example the Demo Linux Virtual Appliance.
- Installing an operating system from a CD, ISO image or network repository onto the appropriate provided template.

Windows VMs describes how to install Windows operating systems onto VMs.

Linux VMs describes how to install Linux operating systems onto VMs.

> **Note:**
>
> Templates created by older versions of Citrix Hypervisor can be used in newer versions of Citrix Hypervisor. However, templates created in newer versions of Citrix Hypervisor are not compatible with older versions of Citrix Hypervisor. If you created a VM template by using Citrix Hypervisor 8.2, to use it with an earlier version, export the VDIs separately and create the VM again.

Other methods of VM creation

In addition to creating VMs from the provided templates, you can use the following methods to create VMs.

Clone an existing VM

You can make a copy of an existing VM by *cloning* from a template. Templates are ordinary VMs which are intended to be used as master copies to create instances of VMs from. A VM can be customized and converted into a template. Ensure that you follow the appropriate preparation procedure for the VM. For more information, see Preparing for Cloning a Windows VM Using Sysprep and Preparing to Clone a Linux VM.

> **Note:**
>
> Templates cannot be used as normal VMs.

Citrix Hypervisor has two mechanisms for cloning VMs:

- A full copy
- Copy-on-Write

  The faster Copy-on-Write mode only writes *modified* blocks to disk. Copy-on-Write is designed to save disk space and allow fast clones, but slightly slows down normal disk performance. A template can be fast-cloned multiple times without slowdown.

  > **Note:**
  >
  > If you clone a template into a VM and then convert the clone into a template, disk performance can decrease. The amount of decrease has a linear relationship to the number of times this process has happened. In this event, the `vm-copy` CLI command can be used to perform a full copy of the disks and restore expected levels of disk performance.

Notes for resource pools

If you create a template from VM virtual disks on a shared SR, the template cloning operation is forwarded to any server in the pool that can access the shared SRs. However, if you create the template from a VM virtual disk that only has a local SR, the template clone operation is only able to run on the server that can access that SR.

Import an exported VM

You can create a VM by *importing* an existing exported VM. Like cloning, exporting and importing a VM is fast way to create more VMs of a certain configuration. Using this method enables you to increase the speed of your deployment. You might, for example, have a special-purpose server configuration that you use many times. After you set up a VM as required, export it and import it later to create another copy of your specially configured VM. You can also use export and import to move a VM to the Citrix Hypervisor server that is in another resource pool.

For details and procedures on importing and exporting VMs, see Importing and Exporting VMs.

Citrix VM Tools

Citrix VM Tools provide high performance I/O services without the overhead of traditional device emulation.

Citrix VM Tools for Windows

Citrix VM Tools for Windows consist of I/O drivers (also known as paravirtualized drivers or PV drivers) and the Management Agent.

The I/O drivers contain storage and network drivers, and low-level management interfaces. These drivers replace the emulated devices and provide high-speed transport between Windows and the Citrix Hypervisor product family software. While installing a Windows operating system, Citrix Hypervisor uses traditional device emulation to present a standard IDE controller and a standard network card to the VM. This emulation allows the Windows installation to use built-in drivers, but with reduced performance due to the overhead inherent in emulating the controller drivers.

The Management Agent, also known as the Guest Agent, is responsible for high-level virtual machine management features and provides a full set of functions to XenCenter.

Install Citrix VM Tools for Windows on each Windows VM for that VM to have a fully supported configuration, and to be able to use the xe CLI or XenCenter. A VM functions without the Citrix VM Tools for Windows, but performance is hampered when the I/O drivers (PV drivers) are not installed. You must install Citrix VM Tools for Windows on Windows VMs to be able to perform the following operations:

- Cleanly shut down, reboot, or suspend a VM
- View VM performance data in XenCenter
- Migrate a running VM (using live migration or storage live migration)
- Create snapshots with memory (checkpoints) or revert to snapshots

For more information, see Install Citrix VM Tools for Windows.

Citrix VM Tools for Linux

Citrix VM Tools for Linux contain a guest agent that provides extra information about the VM to the host.

You must install the Citrix VM Tools for Linux on Linux VMs to be able to perform the following operations:

- View VM performance data in XenCenter
- Adjust the number of vCPUs on a running Linux VM
- Enable dynamic memory control

For more information, see Install Citrix VM Tools for Linux.

Find out the virtualization state of a VM

XenCenter reports the virtualization state of a VM on the VM's **General** tab. You can find out whether or not Citrix VM Tools are installed. This tab also displays whether the VM can install and receive updates from Windows Update. The following section lists the messages displayed in XenCenter:

I/O optimized (not optimized): This field displays whether or not the I/O drivers are installed on the VM.

Management Agent installed (not installed): This field displays whether or not the Management Agent is installed on the VM.

Able to (Not able to) receive updates from Windows Update: specifies whether the VM can receive I/O drivers from Windows Update.

> **Note:**
>
> Windows Server Core 2016 does not support using Windows Update to install or update the I/O drivers. Instead use the Citrix VM Tools for Windows installer provided on the Citrix Hypervisor downloads page.

Install I/O drivers and Management Agent: this message is displayed when the VM does not have the I/O drivers or the Management Agent installed.

Supported guests and allocating resources

For a list of supported guest operating systems, see Supported Guests, Virtual Memory, and Disk Size Limits

This section describes the differences in virtual device support for the members of the Citrix Hypervisor product family.

Citrix Hypervisor product family virtual device support

The current version of the Citrix Hypervisor product family has some general limitations on virtual devices for VMs. Specific guest operating systems may have lower limits for certain features. The individual guest installation section notes the limitations. For detailed information on configuration limits, see Configuration Limits.

Factors such as hardware and environment can affect the limitations. For information about supported hardware, see the Citrix Hypervisor Hardware Compatibility List.

VM block devices

Citrix Hypervisor emulates an IDE bus in the form of an `hd*` device. When using Windows, installing the Citrix VM Tools installs a special I/O driver that works in a similar way to Linux, except in a fully virtualized environment.

Windows VMs

Installing Windows VMs on the Citrix Hypervisor server requires hardware virtualization support (Intel VT or AMD-V).

Basic procedure for creating a Windows VM

The process of installing a Windows on to a VM consists of the following steps:

1. Selecting the appropriate Windows template
2. Choosing the appropriate boot mode
3. Installing the Windows operating system
4. Installing the Citrix VM Tools for Windows (*I/O drivers* and the *Management Agent*)

> **Warning:**
>
> Windows VMs are supported only when the VMs have the Citrix VM Tools for Windows installed.

Windows VM templates

Windows operating systems are installed onto VMs by cloning an appropriate template using either XenCenter or the xe CLI, and then installing the operating system. The templates for individual guests have predefined platform flags set which define the configuration of the virtual hardware. For example, all Windows VMs are installed with the ACPI Hardware Abstraction Layer (HAL) mode enabled. If you later change one of these VMs to have multiple virtual CPUs, Windows automatically switches the HAL to multi-processor mode.

The available Windows templates are listed in the following table:

Template Name	Supported boot modes	Description
Windows 10 (32-bit)	BIOS	Used to install Windows 10.
Windows 10 (64-bit)	BIOS, UEFI, UEFI Secure Boot	Used to install Windows 10 (64-bit).
Windows Server 2016 (64-bit)	BIOS, UEFI, UEFI Secure Boot	Used to install Windows Server 2016 or Windows Server Core 2016 (64-bit)
Windows Server 2019 (64-bit)	BIOS, UEFI, UEFI Secure Boot	Used to install Windows Server 2019 or Windows Server Core 2019 (64-bit)
Windows Server 2022 (64-bit)	BIOS, UEFI, UEFI Secure Boot	Used to install Windows Server 2022 or Windows Server Core 2022 (64-bit)

Attach an ISO image library

The Windows operating system can be installed either from an install CD in a physical CD-ROM drive on the Citrix Hypervisor server, or from an ISO image. See Create ISO images for information on how to make an ISO image from a Windows install CD and make it available for use.

Guest UEFI boot and Secure Boot

Citrix Hypervisor enables recent versions of Windows guest operating systems to boot in UEFI mode. UEFI boot provides a richer interface for the guest operating systems to interact with the hardware, which can significantly reduce Windows VM boot times.

For these Windows operating systems, Citrix Hypervisor also supports Windows Secure Boot. Secure Boot prevents unsigned, incorrectly signed or modified binaries from being run during boot. On a UEFI-enabled VM that enforces Secure Boot, all drivers must be signed. This requirement might limit the range of uses for the VM, but provides the security of blocking unsigned/modified drivers. If you use an unsigned driver secure boot fails and an alert is shown in XenCenter.

Secure Boot also reduces the risk that malware in the guest can manipulate the boot files or run during the boot process.

> **Note:**
>
> Guest UEFI boot was provided as an experimental feature in Citrix Hypervisor 8.0. UEFI-enabled VMs that were created in Citrix Hypervisor 8.0 are not supported in Citrix Hypervisor 8.2. Delete these VMs and create new ones with Citrix Hypervisor 8.2.

Citrix Hypervisor supports UEFI boot and Secure Boot on newly created Windows 10 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit), and Windows Server 2022 (64-bit) VMs. You must specify the boot mode when creating a VM. It is not possible to change the boot mode of a VM between BIOS and UEFI (or UEFI Secure Boot) after booting the VM for the first time. However, you can change the boot mode between UEFI and UEFI Secure Boot at any time.

Consider the following when enabling UEFI boot on VMs:

- Ensure that the UEFI-enabled VM has at least two vCPUs.
- You can import or export a UEFI-enabled VM created on Citrix Hypervisor as an OVA, OVF, or an XVA file. Importing a UEFI-enabled VM from OVA or OVF packages created on other hypervisors is not supported.
- To use PVS-Accelerator with UEFI-enabled VMs, ensure that you are using Citrix Provisioning 1906 or later.
- Use the UEFI settings menu to change the screen resolution of the XenCenter console. For detailed instructions, see Troubleshooting.

Consider the following when enabling UEFI Secure Boot on VMs:

- The Citrix Hypervisor server must be booted in UEFI mode. For more information, see Network boot installations
- Your resource pool or standalone server must have access to Secure Boot certificates.

Only one Citrix Hypervisor server in the pool requires access to the certificates. When a server joins a pool the certificates on that server are made available to other servers in the pool.

> **Note**
>
> UEFI-enabled VMs use NVME and E1000 for emulated devices. The emulation information does not display these values until after you install Citrix VM Tools for Windows on the VM. UEFI-enabled VMs also show as only having 2 NICs until after you install Citrix VM Tools for Windows.

Enabling UEFI boot or UEFI Secure Boot

You can use XenCenter or the xe CLI to enable UEFI boot or UEFI Secure Boot for your VM.

For information about creating a UEFI-enabled VM in XenCenter, see Create a VM by using XenCenter.

Using the xe CLI to enable UEFI boot or UEFI Secure Boot

When you create a VM, run the following command before booting the VM for the first time:

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

Where, `UUID` is the VM's UUID, `MODE` is either `BIOS` or `uefi`, and `OPTION` is either 'true' or 'false'. If you do not specify the mode, it defaults to `uefi` if that option is supported for your VM operating system. Otherwise, the mode defaults to `BIOS`. If you do not specify the `secureboot` option, it defaults to 'auto'. For UEFI-enabled VMs created on a Citrix Hypervisor server that is booted in UEFI mode and has Secure Boot certificates available, the 'auto' behavior is to enable Secure Boot for the VM. Otherwise, Secure Boot is not enabled.

To create a UEFI-enabled VM from a template supplied with Citrix Hypervisor, run the following command:

```
    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>
platform:secureboot=<OPTION>
```

Do not run this command for templates that have something installed on them or templates that you created from a snapshot. The boot mode of these snapshots cannot be changed and, if you attempt to change the boot mode, the VM fails to boot.

When you boot the UEFI-enabled VM the first time you are prompted on the VM console to press any key to start the Windows installation. If you do not start the Windows installation, the VM console switches to the UEFI shell.

To restart the installation process, in the UEFI console, type the following commands.

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

When the installation process restarts, watch the VM console for the installation prompt. When the prompt appears, press any key.

Disabling Secure Boot

You might want to disable Secure Boot on occasion. For example, Windows debugging cannot be enabled on a VM that in Secure Boot user mode. To disable Secure Boot, change the VM into Secure Boot setup mode. On your Citrix Hypervisor server, run the following command:

```
varstore-sb-state <VM_UUID> setup
```

Keys

UEFI-enabled VMs are provisioned with a PK from an ephemeral private key, the Microsoft KEK, the Microsoft Windows Production PCA, and Microsoft third party keys. The VMs are also provided with an up-to-date revocation list from the UEFI forum. This configuration enables Windows VMs to boot with Secure Boot turned on and to receive automatic updates to the keys and revocation list from Microsoft.

Troubleshooting your UEFI and UEFI Secure Boot VMs

For information about troubleshooting your UEFI or UEFI Secure Boot VMs, see Troubleshoot UEFI and Secure Boot problems on Windows VMs.

Create a VM by using XenCenter

To create a Windows VM:

1. On the XenCenter toolbar, click the **New VM** button to open the New VM wizard.

   The New VM wizard allows you to configure the new VM, adjusting various parameters for CPU, storage, and networking resources.

2. Select a VM template and click **Next**.

   Each template contains the setup information that is required to create a VM with a specific guest operating system (OS), and with optimum storage. This list reflects the templates that Citrix Hypervisor currently supports.

   > **Note:**
   >
   > If the OS that you are installing on your VM is compatible only with the original hardware, check the **Copy host BIOS strings to VM** box. For example, you might use this option for an OS installation CD that was packaged with a specific computer.

> After you first start a VM, you cannot change its BIOS strings. Ensure that the BIOS strings are correct before starting the VM for the first time.

To copy BIOS strings using the CLI, see Install HVM VMs from Reseller Option Kit (BIOS-locked) Media. The option to set user-defined BIOS strings are not available for HVM VMs.

3. Enter a name and an optional description for the new VM.
4. Choose the source of the OS media to install on the new VM.

   Installing from a CD/DVD is the simplest option for getting started.

   1. Choose the default installation source option (DVD drive)
   2. Insert the disk into the DVD drive of the Citrix Hypervisor server

   Citrix Hypervisor also allows you to pull OS installation media from a range of sources, including a pre-existing ISO library. An ISO image is a file that contains all the information that an optical disc (CD, DVD, and so on) would contain. In this case, an ISO image would contain the same OS data as a Windows installation CD.

   To attach a pre-existing ISO library, click **New ISO library** and indicate the location and type of ISO library. You can then choose the specific operating system ISO media from the list.

5. Choose a boot mode for the VM. By default, XenCenter select the most secure boot mode available for the VM operating system version.

   > **Note:**
   >
   > - The **UEFI Boot** and **UEFI Secure Boot** options appear grayed out if the VM template you have chosen does not support UEFI boot.
   > - You cannot change the boot mode after you boot the VM for the first time.

6. Select a home server for the VM.

   A home server is the server which provides the resources for a VM in a pool. When you nominate a home server for a VM, Citrix Hypervisor attempts to start the VM on that server. If this action is not possible, an alternate server within the same pool is selected automatically. To choose a home server, click **Place the VM on this server** and select a server from the list.

   > **Notes:**
   >
   > - In WLB-enabled pools, the nominated home server isn't used for starting, restarting, resuming, or migrating the VM. Instead, Workload Balancing nominates the best server for the VM by analyzing Citrix Hypervisor resource pool metrics and by recommending optimizations.
   > - If a VM has one or more virtual GPUs assigned to it, the home server nomination doesn't take effect. Instead, the server nomination is based on the virtual GPU placement policy set by the user.

If you do not want to nominate a home server, click **Don't assign this VM a home server**. The VM is started on any server with the necessary resources.

Click **Next** to continue.

7. Allocate processor and memory resources for the VM. For a Windows 10 VM, the default is 1 virtual CPU and 2,048 MB of RAM. You can also choose to modify the defaults. Click **Next** to continue.

8. Assign a virtual GPU. The New VM wizard prompts you to assign a dedicated GPU or one or more virtual GPUs to the VM. This option enables the VM to use the processing power of the GPU. With this feature, you have better support for high-end 3D professional graphics applications such as CAD/CAM, GIS, and Medical Imaging applications.

9. Allocate and configure storage for the new VM.

   Click **Next** to select the default allocation (24 GB) and configuration, or you might want to do the following extra configuration:

   - Change the name, description, or size of your virtual disk by clicking **Properties**.
   - Add a new virtual disk by selecting **Add**.

10. Configure networking on the new VM.

    Click **Next** to select the default NIC and configurations, including an automatically created unique MAC address for each NIC. Alternatively, you might want to do the following extra configuration:

    - Change the physical network, MAC address, or Quality of Service (QoS) priority of the virtual disk by clicking **Properties**.
    - Add a new virtual NIC by selecting **Add**.

11. Review settings, and then click **Create Now** to create the VM and return to the **Search** tab.

    An icon for your new VM appears under the host in the **Resources** pane.

    On the **Resources** pane, select the VM, and then click the **Console** tab to see the VM console.

12. Follow the OS installation screens and make your selections.

13. After the OS installation completes and the VM reboots, install the Citrix VM Tools for Windows.

Install Citrix VM Tools for Windows

Citrix VM Tools for Windows provide high performance I/O services without the overhead of traditional device emulation. Citrix VM Tools for Windows consist of I/O drivers (also known as paravirtualized drivers or PV drivers) and the Management Agent. Citrix VM Tools for Windows must be installed on each Windows VM for the VM to have a fully supported configuration. A VM functions without them, but performance is significantly hampered.

> **Note:**
>
> To install Citrix VM Tools for Windows on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.

Before you install the Citrix VM Tools for Windows, ensure that your VM is configured to receive the I/O drivers from Windows Update. Windows Update is the recommended way to receive updates to the I/O drivers. However, if Windows Update is not an available option for your VM, you can also receive updates to the I/O drivers through the Management Agent or update the drivers manually. For more information, see Update the I/O drivers.

To install Citrix VM Tools for Windows:

1. Download the Citrix VM Tools for Windows file from the Citrix Hypervisor downloads page.

   The tools are available in a 32-bit and a 64-bit version.

2. Copy the file to your Windows VM or to a shared drive that the Windows VM can access.

3. Run the `managementagent.msi` file to begin Citrix VM Tools installation.

   ```
   Msiexec.exe /package managementagent.msi
   ```

4. Follow the prompts in the installer.

   - Follow the instructions on the wizard to accept the license agreement and choose a destination folder.

   - Customize the settings on the **Installation and Updates Settings** page. The **Citrix Hypervisor Windows Management Agent Setup** wizard displays the recommended settings. By default, the wizard displays the following settings:

     - Install I/O Drivers Now
     - Allow automatic management agent updates
     - Disallow automatic I/O drivers updates by the management agent
     - Send anonymous usage information to Citrix

     If you do not want to allow the automatic updating of the Management Agent, select **Disallow automatic management agent updates** from the list.

     If you would like to allow the Management Agent to update the I/O drivers automatically, select **Allow automatic I/O driver updates by the management agent**. However, we recommend that you use Windows Update to update the I/O drivers, not the Management Agent.

     > **Note:**
     >
     > If you have chosen to receive I/O driver updates through the Windows Update mechanism, do not allow the Management Agent to update the I/O drivers automatically.

     If you do not want to share anonymous usage information with Citrix, clear the **Send anonymous usage information to Citrix** check box. The information transmitted to Citrix

contains the UUID of the VM requesting the update. No other information relating to the VM is collected or transmitted to Citrix.

- Click **Next** and then **Install** to begin the Citrix VM Tools for Windows installation process.

5. Restart the VM when prompted to complete the installation process.

> **Note:**
>
> The Citrix VM Tools for Windows can request to restart with `/quiet /norestart` or `/quiet /forcerestart` specified after the VM has already been restarted once as part of the installation.
>
> I/O drivers are automatically installed on a Windows VM that can receive updates from Windows Update. However, we recommend that you install the Citrix VM Tools for Windows to install the Management Agent, and to maintain supported configuration.

Customers who install the Citrix VM Tools for Windows or the Management Agent through RDP might not see the restart prompt as it only appears on the Windows console session. To ensure that you restart your VM (if necessary) and to get your VM to an optimized state, specify the force restart option in RDP. The force restart option restarts the VM only if it is required to get the VM to an optimized state.

Silent installation

To install the Citrix VM Tools for Windows silently and to prevent the system from rebooting, run one of the following commands:

```
Msiexec.exe /package managementagentx86.msi /quiet /norestart
Msiexec.exe /package managementagentx64.msi /quiet /norestart
```

Or

```
Setup.exe /quiet /norestart
```

A non-interactive, but non-silent installation can be obtained by running:

```
Msiexec.exe managementagentx86.msi /passive
Msiexec.exe managementagentx64.msi /passive
```

Or

```
Setup.exe /passive
```

To customize the installation settings, use the following parameters with the silent installation commands:

Parameter	Allowed values	Default	Description
ALLOWAUTOUPDATE	YES or NO	YES	Allow automatic management agent updates
ALLOWDRIVERINSTALL	YES or NO	YES	Install the I/O Drivers now
ALLOWDRIVERUPDATE	YES or NO	NO	Allow the automatic management agent updates to install updated drivers
IDENTIFYAUTOUPDATE	YES or NO	YES	Send anonymous usage information to Citrix

For example, to do a silent install of the tools that does not allow future automatic management agent updates and does not send anonymous information to Citrix, run one of the following commands:

```
Msiexec.exe /package managementagentx86.msi ALLOWAUTOUPDATE=NO
IDENTIFYAUTOUPDATE=NO /quiet /norestart
Msiexec.exe /package managementagentx64.msi ALLOWAUTOUPDATE=NO
IDENTIFYAUTOUPDATE=NO /quiet /norestart
```

For interactive, silent, and passive installations, following the next system restart there might be several automated reboots before the Citrix VM Tools for Windows are fully installed. This behavior is also the case for installations with the `/norestart` flag specified. However, for installations where the `/norestart` flag is provided, the initial restart might be manually initiated.

The Citrix VM Tools for Windows are installed by default in the `C:\Program Files\Citrix\XenTools` directory on the VM.

Notes:

- To install Citrix VM Tools for Windows on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.
- The `/quiet` parameter applies to the installation dialogs only, but not to the device driver installation. When the `/quiet` parameter is specified, the device driver installation requests permission to reboot if required.
  - When `/quiet /norestart` is specified, the system doesn't reboot after the entire tools installation is complete. This behavior is independent of what the user specifies in the reboot dialog.
  - When `/quiet /forcerestart` is specified, the system reboots after the entire tools installation is complete. This behavior is independent of what the user specifies in the reboot dialog.
  - When the device driver installation requests permission to reboot, a tools installation with the `quiet` parameter specified can still be in progress. Use the Task Manager to confirm whether the installer is still running.

Warning:

> Installing or upgrading the Citrix VM Tools for Windows can cause the friendly name and identifier of some network adapters to change. Any software which is configured to use a particular adapter might have to be reconfigured following Citrix VM Tools for Windows installation or upgrade.

Create a Windows VM by using the CLI

To create a Windows VM from an ISO repository by using the xe CLI:

1. Create a VM from a template:

   ```
   xe vm-install new-name-label=vm_name template=template_name
   ```

   This command returns the UUID of the new VM.

2. Create an ISO Storage Repository:

   ```
   xe-mount-iso-sr path_to_iso_sr
   ```

3. List all of the available ISOs:

   ```
   xe cd-list
   ```

4. Insert the specified ISO into the virtual CD drive of the specified VM:

   ```
   xe vm-cd-add vm=vm_name cd-name=iso_name device=3
   ```

5. Start the VM and install the operating system:

   ```
   xe vm-start vm=vm_name
   ```

At this point, the VM console is visible in XenCenter.

For more information on using the CLI, see Command Line Interface.

Update Windows operating systems

This section discusses updating Windows VMs with updated operating systems.

Upgrades to VMs are typically required when moving to a newer version of Citrix Hypervisor. Note the following limitations when upgrading your VMs to a newer version of Citrix Hypervisor:

- Before migrating Windows VMs using live migration, you must upgrade the Citrix VM Tools for Windows on each VM.
- Suspend/Resume operation is not supported on Windows VMs until the Citrix VM Tools for Windows are upgraded.
- The use of certain antivirus and firewall applications can crash Windows VMs, unless the Citrix VM Tools for Windows are upgraded.

We recommend that you do not remove the Citrix VM Tools from your Windows VM before automatically updating the version of Windows on the VM.

Use Windows Update to upgrade the version of the Windows operating system on your Windows VMs.

> **Note:**
>
> Windows installation disks typically provide an upgrade option if you boot them on a server which has an earlier version of Windows already installed. However, if you use Windows Update to update your Citrix VM Tools, do not upgrade the Windows operating system from an installation disk. Instead, use Windows Update.

Update Citrix VM Tools for Windows

Citrix Hypervisor has a simpler mechanism to update I/O drivers (PV drivers) and the Management Agent automatically for Windows VMs. This mechanism enables customers to install updates as they become available, without having to wait for a hotfix.

Ensure that your Citrix VM Tools for Windows are regularly updated to the latest version.

We recommend using the following settings for updating the different components of the Citrix VM Tools for Windows:

1. Set the value of the following registry key to a REG_DWORD value of '3': `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`
2. Ensure your VM is configured to receive I/O drivers from Windows Update.
3. Configure the Management Agent to automatically update itself.

The **Virtualization state** section on a VM's **General** tab in XenCenter specifies whether the VM can receive updates from Windows Update. The mechanism to receive I/O driver updates from Windows Update is turned on by default. If you do not want to receive I/O driver updates from Windows Update, disable Windows Update on your VM, or specify a group policy.

> **Important:**
>
> Ensure that all requested VM restarts are completed as part of the update. Multiple restarts might be required. If all requested restarts are not completed, this might result in unexpected behavior.

The following sections contain information about automatically updating the I/O drivers and the Management Agent.

Update the I/O drivers

You can get I/O driver updates automatically from Microsoft Windows Update, provided:

- You are running Citrix Hypervisor 8.2 Premium Edition, or have access to Citrix Hypervisor through Citrix Virtual Apps and Desktops entitlement.
- You have created a Windows VM using XenCenter issued with Citrix Hypervisor 8.2
- Windows Update is enabled within the VM
- The VM has access to the internet, or it can connect to a WSUS proxy server

> **Note:**
>
> Windows Server Core does not support using Windows Update to install or update the I/O drivers. Instead use the Citrix VM Tools for Windows installer available from the Citrix Hypervisor downloads page
>
> Customers can also receive I/O driver updates automatically through the automatic Management Agent update mechanism. You can configure this setting during Citrix VM Tools for Windows installation. For more information, see Install Citrix VM Tools for Windows.

Automatic reboots

Ensure that all requested VM restarts are completed as part of the update. Multiple restarts might be required. If all requested restarts are not completed, you might see unexpected behavior.

You can set a registry key that specifies the maximum number of automatic reboots that are performed when you install the drivers through Device Manager or Windows Update. After you have installed the xenbus driver version 9.1.1.8 or later, the Citrix VM Tools for Windows use the guidance provided by this registry key.

To use this feature, we recommend that you set the following registry key as soon as possible: `HLKM\System\CurrentControlSet\services\xenbus_monitor\Parameters\Autoreboot`. The value of the registry key must be a positive integer. We recommend that you set the number of reboots in the registry key to 3.

When this registry key is set, the Citrix VM Tools for Windows perform as many reboots as are needed to complete the updates or the number of reboots specified by the registry key - whichever value is lower.

Before each reboot, Windows can display an alert for 60 seconds that warns of the upcoming reboot. You can dismiss the alert, but this action does not cancel the reboot. Because of this delay between the reboots, wait a few minutes after the initial reboot for the reboot cycle to complete.

> **Notes:**
>
> This setting is required for headless servers with static IP addresses.
>
> This automatic reboot feature only applies to updates to the Windows I/O drivers through Device Manager or Windows Update. If you are using the Management Agent installer to deploy your

drivers, the installer disregards this registry key and manages the VM reboots according to its own settings.

Find the I/O driver version

To find out the version of the I/O drivers installed on the VM:

1. Navigate to `C:\Windows\System32\drivers`.
2. Locate the driver from the list.
3. Right-click the driver and select **Properties** and then **Details**.

   The **File version** field displays the version of the driver installed on the VM.

Update the Management Agent

Citrix Hypervisor enables you to update the Management Agent automatically on both new and existing Windows VMs. By default, Citrix Hypervisor allows the automatic updating of the Management Agent. However, it does not allow the Management Agent to update the I/O drivers automatically. You can customize the Management Agent update settings during Citrix VM Tools for Windows installation. The automatic updating of the Management Agent occurs seamlessly, and does not reboot your VM. In scenarios where a VM reboot is required, a message appears on the Console tab of the VM notifying users about the required action.

You can get the Management Agent updates automatically, provided:

- You are running Citrix Hypervisor 8.2 Premium Edition, or have access to Citrix Hypervisor through Citrix Virtual Apps and Desktops entitlement.
- You have installed Citrix VM Tools for Windows issued with Citrix Hypervisor 7.0 or higher
- The Windows VM has access to the Internet

Find the Management Agent version

To find out the version of the Management Agent installed on the VM:

1. Navigate to `C:\Program Files\Citrix\XenTools`.
2. Right-click `XenGuestAgent` from the list and click **Properties** and then **Details**.

   The **File version** field displays the version of the Management Agent installed on the VM.

Manage Automatic Updates by using the CLI

Citrix Hypervisor enables you to use the command line to manage the automatic updating of the I/O drivers and the Management Agent. You can run `msiexec.exe` with the arguments listed in the following table to specify whether the I/O drivers and the Management Agent are automatically updated. For information about installing Citrix VM Tools for Windows by using `msiexec.exe`, see Silent installation.

Note:

For VMs managed using either PVS or MCS, automated updates are turned off automatically when the Citrix Virtual Desktops VDA is present and it reports that the machine is non-persistent.

Argument	Values	Description
ALLOWAUTOUPDATE	YES/NO	Allow/disallow auto updating of the Management Agent
ALLOWDRIVERINSTALL	YES/NO	Allow/disallow the Citrix VM Tools for Windows installer to install I/O drivers
ALLOWDRIVERUPDATE	YES/NO	Allow/disallow the Management Agent to update the I/O drivers automatically
IDENTIFYAUTOUPDATE	YES/NO	Allow/disallow the auto update mechanism to send anonymous usage information to Citrix

For example:

```
setup.exe  /passive /forcerestart ALLOWAUTOUPDATE=YES ALLOWDRIVERINSTALL=NO \
     ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Or

```
msiexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES ALLOWDRIVERINSTALL=NO \
    ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Redirect the Management Agent updates

Citrix Hypervisor enables customers to redirect Management Agent updates to an internal web server before they are installed. This redirection allows customers to review the updates before they are automatically installed on the VM.

To redirect the Management Agent updates:

The Management Agent uses an updates file to get information about the available updates. The name of this updates file depends on the version of the Management Agent that you use:

- For Management Agent 9.0.0.x and later use https://pvupdates.vmd.citrix.com/updates.v9.json.
- Windows 7 VMs only: For Management Agent 7.1.0.1396 and later use https://pvupdates.vmd.citrix.com/updates.json.
- For Management Agent 7.1.0.1354 and earlier use https://pvupdates.vmd.citrix.com/updates.tsv.

Complete the following steps to redirect the Management Agent updates:

1. Download the updates file.

2. Download the Management Agent MSI files referenced in the updates file.
3. Upload the MSI files to an internal web server that your VMs can access.
4. Update the updates file to point to the MSI files on the internal web server.
5. Upload the updates file to the web server.

Automatic updates can also be redirected on a per-VM or a per-pool basis. To redirect updates on a per-VM basis:

1. On the VM, open a command prompt as an administrator.
2. Run the command

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url /d \
    url of the update file on the web server
```

To redirect automatic updating of the Management Agent on a per-pool basis, run the following command:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url of the
update file on the web server
```

Disable the Management Agent updates

To disable automatic updating of the Management Agent on a per-VM basis:

1. On the VM, open a command prompt as an administrator.
2. Run the following command:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_DWORD /v DisableAutoUpdate
/d 1
```

To disable automatic updating of the Management Agent on a per-pool basis, run the following command:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=false
```

Modify the automatic I/O driver update settings

During Citrix VM Tools for Windows installation, you can specify whether you would like to allow the Management Agent to update the I/O drivers automatically. If you prefer to update this setting after completing the Citrix VM Tools for Windows installation process, perform the following steps:

1. On the VM, open a command prompt as an administrator.

2. Run the following command:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v \
    InstallDrivers /d YES/NO
```

To send anonymous usage information to Citrix:

During Citrix VM Tools for Windows installation, you can specify whether you would like to send anonymous usage information to Citrix. If you would like to update this setting after completing the Citrix VM Tools for Windows installation process, perform the following steps:

1. On the VM, open a command prompt as an administrator.
2. Run the following command:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \
    IDENTIFYAUTOUPDATE /d YES/NO
```

Prepare to clone a Windows VM by using Sysprep

The only supported way to clone a Windows VM is by using the Windows utility `sysprep` to prepare the VM.

The `sysprep` utility changes the local computer SID to make it unique to each computer. The `sysprep` binaries are in the `C:\Windows\System32\Sysprep` folder.

> **Note:**
>
> For older versions of Windows, the `sysprep` binaries are on the Windows product CDs in the `\support\tools\deploy.cab` file. These binaries must be copied to your Windows VM before using.

To clone Windows VMs:

1. Create, install, and configure the Windows VM as desired.
2. Apply all relevant Service Packs and updates.
3. Install the Citrix VM Tools for Windows.
4. Install any applications and perform any other configuration.
5. Run `sysprep`. This utility shuts down the VM when it completes.
6. Using XenCenter convert the VM into a template.
7. Clone the newly created template into new VMs as required.
8. When the cloned VM starts, it completes the following actions before being available for use:

- It gets a new SID and name
- It runs a mini-setup to prompt for configuration values as necessary
- Finally, it restarts

> **Note:**
>
> Do not restart the original, sys-prepped VM (the "source" VM) again after the `sysprep` stage. Immediately convert it to a template afterwards to prevent restarts. If the source VM is restarted, `sysprep` must be run on it again before it can be safely used to make more clones.

For more information about using `sysprep`, visit the following Microsoft website:

- The Windows Automated Installation Kit (AIK)

Windows VM release notes

There are many versions and variations of Windows with different levels of support for the features provided by Citrix Hypervisor. This section lists notes and errata for the known differences.

General Windows issues

- When installing Windows VMs, start off with no more than three virtual disks. After the VM and Citrix VM Tools for Windows have been installed, you can add extra virtual disks. Ensure that the boot device is always one of the initial disks so that the VM can successfully boot without the Citrix VM Tools for Windows.
- When the boot mode for a Windows VM is BIOS boot, Windows formats the primary disk with a Master Boot Record (MBR). MBR limits the maximum addressable storage space of a disk to 2 TiB. To use a disk that is larger than 2 TiB with a Windows VM, do one of the following things:
  - If UEFI boot is supported for the version of Windows, ensure that you use UEFI as the boot mode for the Windows VM.
  - Create the large disk as the secondary disk for the VM and select GUID Partition Table (GPT) format.
- Multiple vCPUs are exposed as CPU sockets to Windows guests, and are subject to the licensing limitations present in the VM. The number of CPUs present in the guest can be confirmed by checking Device Manager. The number of CPUs actually being used by Windows can be seen in the Task Manager.
- The disk enumeration order in a Windows guest might differ from the order in which they were initially added. This behavior is because of interaction between the I/O drivers and the Plug-and-Play subsystem in Windows. For example, the first disk might show up as `Disk 1`, the next disk hot plugged as `Disk 0`, a subsequent disk as `Disk 2`, and then upwards in the expected fashion.
- A bug in the VLC player DirectX back-end replaces yellow with blue during video playback when the Windows display properties are set to 24-bit color. VLC using OpenGL as a back-end works correctly, and any other DirectX-based or OpenGL-based video player works too. It is not a problem if the guest is set to use 16-bit color rather than 24.

- The PV Ethernet Adapter reports a speed of 100 Gbps in Windows VMs. This speed is an artificial hardcoded value and is not relevant in a virtual environment because the virtual NIC is connected to a virtual switch. The Windows VM uses the full speed that is available, but the network might not be capable of the full 100 Gbps.
- If you attempt to make an insecure RDP connection to a Windows VM, this action might fail with the following error message: "This could be due to CredSSP encryption oracle remediation." This error occurs when the Credential Security Support Provider protocol (CredSSP) update is applied to only one of the client and server in the RDP connection. For more information, see https://support.microsoft.com/en-gb/help/4295591/credssp-encryption-oracle-remediation-error-when-to-rdp-to-azure-vm.

Windows 8

We no longer support Windows 8 guests. If you install a Windows 8 VM, it is upgraded to Windows 8.1.

Linux VMs

When you want to create a Linux VM, create the VM using a template for the operating system you want to run on the VM. You can use a template that Citrix Hypervisor provides for your operating system, or one that you created previously. You can create the VM from either XenCenter or the CLI. This section focuses on using the CLI.

> **Note:**
>
> To create a VM of a newer minor update of a RHEL release than is supported for installation by Citrix Hypervisor, complete the following steps:
>
> - Install from the latest supported media
> - Use `yum update` to bring the VM up-to-date
>
> This process also applies to RHEL derivatives such as CentOS and Oracle Linux.

We recommend that you install the Citrix VM Tools for Linux immediately after installing the operating system. For more information, see Install Citrix VM Tools for Linux.

The overview for creating a Linux VM is as following:

1. Create the VM for your target operating system using XenCenter or the CLI.
2. Install the operating system using vendor installation media.
3. Install the Citrix VM Tools for Linux (recommended).
4. Configure the correct time and time zone on the VM and VNC as you would in a normal non-virtual environment.

Citrix Hypervisor supports the installation of many Linux distributions as VMs.

> **Warning:**
>
> The **Other install media** template is for advanced users who want to attempt to install VMs running unsupported operating systems. Citrix Hypervisor has been tested running only the supported distributions and specific versions covered by the standard supplied templates. Any VMs installed using the **Other install media** template are *not* supported.

For information regarding specific Linux distributions, see Installation notes for Linux distributions.

Supported Linux distributions

For a list of supported Linux distributions, see Guest operating system support.

Other Linux distributions are **not** supported. However, distributions that use the same installation mechanism as Red Hat Enterprise Linux (for example, Fedora Core) might be successfully installed using the same

template.

Create a Linux VM

This section shows the CLI procedure for creating a Linux VM by installing the OS from a physical CD/DVD or from a network-accessible ISO.

1. Create a VM from the appropriate template. The UUID of the VM is returned:

   ```
   xe vm-install template=template-name new-name-label=vm-name
   ```

2. Add a virtual CD-ROM to the new VM:

   - If you are installing from a CD or DVD, get the name of the physical CD drive on the Citrix Hypervisor server:

     ```
     xe cd-list
     ```

     The result of this command gives you something like SCSI 0:0:0:0 for the `name-label` field.

     Use this value parameter as the `cd-name` parameter:

     ```
     xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label" device=3
     ```

   - If you are installing from a network-accessible ISO, use the name of the ISO from the ISO library-label as the value for the `cd-name` parameter:

     ```
     xe vm-cd-add vm=vm_name cd-name="iso_name.iso" device=3
     ```

3. Insert the operating system installation CD into the CD drive on the Citrix Hypervisor server.

4. Open a console to the VM with XenCenter or an SSH terminal and follow the steps to perform the OS installation.

5. Start the VM. It boots straight into the operating system installer:

   ```
   xe vm-start uuid=UUID
   ```

6. Install the guest utilities and configure graphical display. For more information, see Install the Citrix VM Tools for Linux.

Create a Linux VM by using PXE boot

You can use PXE boot to install the operating system of your Linux VM. This approach can be useful when you have to create many Linux VMs.

To install by using PXE boot, set up the following prerequisites in the network where your Linux VMs are located:

- DHCP server that is configured to direct any PXE boot installation requests to the TFTP server
- TFTP server that hosts the installation files for the Linux operating system

When creating the Linux VM, run the following commands:

1. Create a VM from the appropriate template. The UUID of the VM is returned:

   ```
   xe vm-install template=template-name new-name-label=vm-name
   ```

2. Set the boot order to boot from the disk and then from the network:

   ```
   xe vm-param-set uuid=<UUID> HVM-boot-params:order=cn
   ```

3. Start the VM to begin the PXE boot installation:

   ```
   xe vm-start uuid=<UUID>
   ```

4. Install the guest utilities and configure graphical display. For more information, see Install the Citrix VM Tools for Linux.

For more information about using PXE boot to install Linux operating systems, see the operating system documentation:

- Debian: Installing Debian using network booting
- RedHat: Starting a Kickstart installation automatically using PXE
- CentOS: PXE Setup
- SLES: Setting up a PXE Boot Server

Install Citrix VM Tools for Linux

Although all supported Linux distributions are natively paravirtualized (and don't need special drivers for full performance), Citrix VM Tools for Linux provide a guest agent. This guest agent provides extra information about the VM to the host. Install the guest agent on each Linux VM to enable Dynamic Memory Control (DMC).

It is important to keep the Linux guest agent up-to-date as you upgrade your Citrix Hypervisor server. For more information, see Update Linux kernels and guest utilities.

Note:

> Before installing the guest agent on a SUSE Linux Enterprise Desktop or Server 15 guest, ensure that `insserv-compat-0.1-2.15.noarch.rpm` is installed on the guest.

To install the Citrix VM Tools for Linux:

1. Download the Citrix VM Tools for Linux file from the Citrix Hypervisor downloads page.
2. Copy the `LinuxGuestTools-xxx.tar.gz` file to your Linux VM or to a shared drive that the Linux VM can access.
3. Extract the contents of the tar file: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Execute the installation script as the root user:

   ```
   /<extract-directory>/install.sh
   ```

5. If the kernel has been upgraded, or the VM was upgraded from a previous version, reboot the VM now.

Installation notes for Linux distributions

This following section lists vendor-specific, configuration information to consider before creating the specified Linux VMs.

For more detailed release notes on all distributions, see Linux VM Release Notes.

Red Hat Enterprise Linux* 7 (32-/64-bit)

The new template for these guests specifies 2 GB RAM. This amount of RAM is a requirement for a successful install of v7.4 and later. For v7.0 - v7.3, the template specifies 2 GB RAM, but as with previous versions of Citrix Hypervisor, 1 GB RAM is sufficient.

> **Note:**
>
> This information applies to both Red Hat and Red Hat derivatives.

Apt repositories (Debian)

For infrequent or one-off installations, it is reasonable to use a Debian mirror directly. However, if you intend to do several VM installations, we recommend that you use a caching proxy or local mirror. Either of the following tools can be installed into a VM.

- `Apt-cacher`: An implementation of proxy server that keeps a local cache of packages
- `debmirror`: A tool that creates a partial or full mirror of a Debian repository

Prepare to clone a Linux VM

Typically, when cloning a VM or a computer, unless you generalize the cloned image, attributes unique to that machine are duplicated in your environments. Some of the unique attributes that are duplicated when cloning

are the IP address, SID, or MAC address.

As a result, Citrix Hypervisor automatically changes some virtual hardware parameters when you clone a Linux VM. When you copy the VM using XenCenter, XenCenter automatically changes the MAC address and IP address for you. If these interfaces are configured dynamically in your environment, you might not need to modify the cloned VM. However, if the interfaces are statically configured, you might need to modify their network configurations.

The VM may need to be customized to be made aware of these changes. For instructions for specific supported Linux distributions, see Linux VM Release Notes.

Machine name

A cloned VM is another computer, and like any new computer in a network, it must have a unique name within the network domain.

IP address

A cloned VM must have a unique IP address within the network domain it is part of. Generally, this requirement is not a problem when DHCP is used to assign addresses. When the VM boots, the DHCP server assigns it an IP address. If the cloned VM had a static IP address, the clone must be given an unused IP address before being booted.

MAC address

There are two situations when we recommend disabling MAC address rules before cloning:

1. In some Linux distributions, the MAC address for the virtual network interface of a cloned VM is recorded in the network configuration files. However, when you clone a VM, XenCenter assigns the new cloned VM a different MAC address. As a result, when the new VM is started for the first time, the network does recognize the new VM and does not come up automatically.

2. Some Linux distributions use `udev` rules to remember the MAC address of each network interface, and persist a name for that interface. This behavior is intended so that the same physical NIC always maps to the same `eth`*n* interface, which is useful with removable NICs (like laptops). However, this behavior is problematic in the context of VMs.

   For example, consider the behavior in the following case:

   ```
   1.  Configure two virtual NICs when installing a VM
   1.  Shut down the VM
   1.  Remove the first NIC
   ```

   When the VM reboots, XenCenter shows just one NIC, but calls it `eth0`. Meanwhile the VM is deliberately forcing this NIC to be `eth1`. The result is that networking does not work.

For VMs that use persistent names, disable these rules before cloning. If you do not want to turn off persistent names, you must reconfigure networking inside the VM (in the usual way). However, the information shown in XenCenter does not match the addresses actually in your network.

Update Linux kernels and guest utilities

The Linux guest utilities can be updated by rerunning the `install.sh` script from the Citrix VM Tools for Linux (see Install the Citrix VM Tools for Linux).

For `yum`-enabled distributions, CentOS and RHEL, `xe-guest-utilities` installs a `yum` configuration file to enable subsequent updates to be done using `yum` in the standard manner.

For Debian, `/etc/apt/sources.list` is populated to enable updates using apt by default.

When upgrading, we recommend that you always rerun `install.sh`. This script automatically determines if your VM needs any updates and installs if necessary.

Upgrade from PV to HVM guests

To upgrade *existing* unsupported PV Linux guests to supported versions that operate in **HVM** mode, perform an in-guest upgrade. At this point, the upgraded guest only runs in PV mode - which is not supported and has known issues. Run the following script to convert the newly upgraded guest to the supported HVM mode.

On the Citrix Hypervisor server, open a local shell, log on as root, and enter the following command:

```
/opt/xensource/bin/pv2hvm vm_name
```

Or

```
/opt/xensource/bin/pv2hvm vm_uuid
```

Restart the VM to complete the process.

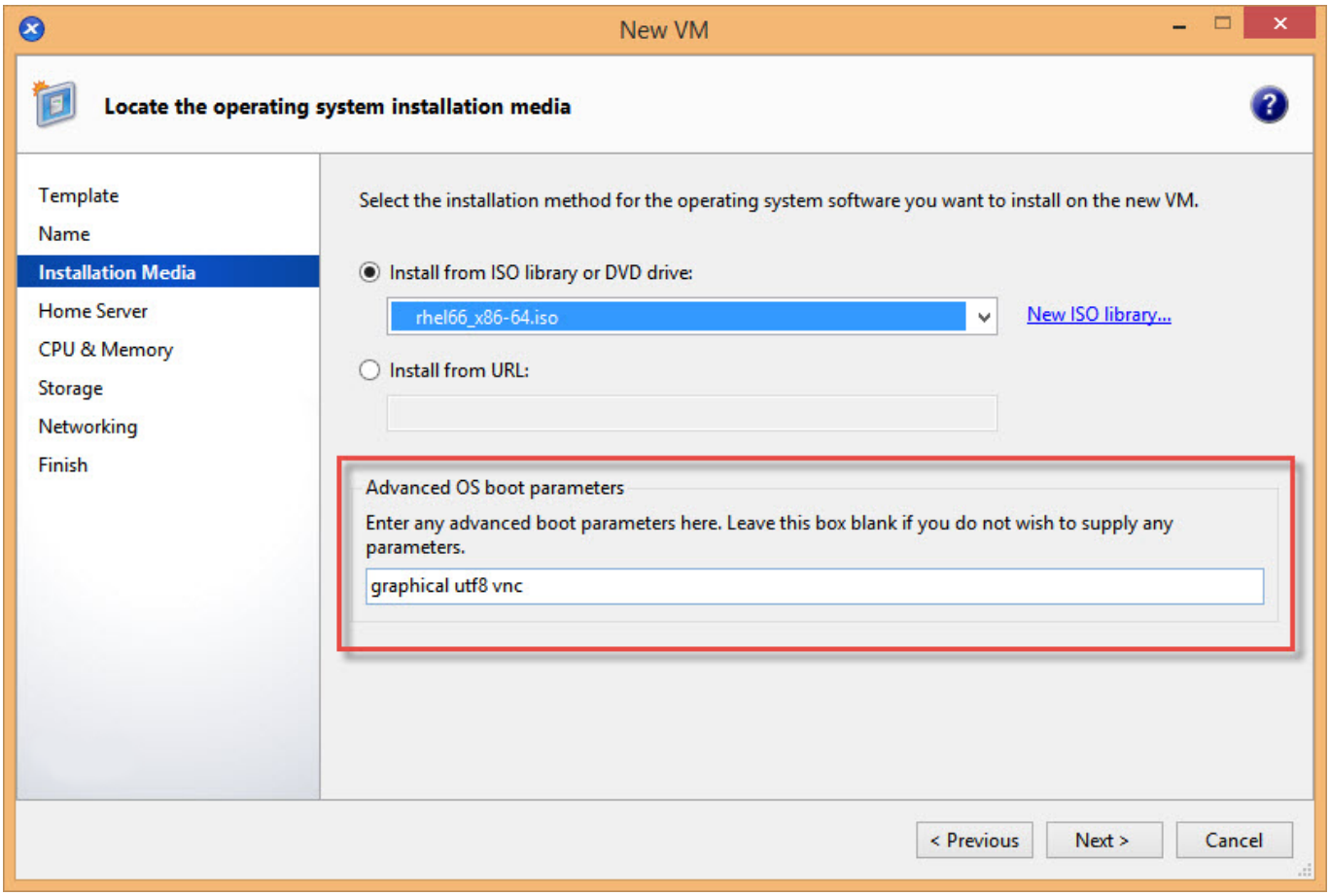
Linux VM release notes

Most modern Linux distributions support Xen paravirtualization directly, but have different installation mechanisms and some kernel limitations.

RHEL graphical install support

To use the graphical installer, in XenCenter step through the **New VM** wizard. In the **Installation Media** page, in the **Advanced OS boot parameters** section, add `vnc` to the list parameters:

```
graphical utf8 vnc
```



You are prompted to provide networking configuration for the new VM to enable VNC communication. Work through the remainder of the New VM wizard. When the wizard completes, in the **Infrastructure** view, select the VM, and click **Console** to view a console session of the VM. At this point, it uses the standard installer. The VM installation initially starts in text mode, and may request network configuration. Once provided, the **Switch to Graphical Console** button is displayed in the top right corner of the XenCenter window.

Red Hat Enterprise Linux 7

After migrating or suspending the VM, RHEL 7 guests might freeze during resume. For more information, see Red Hat issue 1141249.

CentOS 7

For the list of CentOS 7 release notes, see Red Hat Enterprise Linux 7.

Oracle Linux 7

For the list of Oracle Linux 7 release notes, see Red Hat Enterprise Linux 7.

Scientific Linux 7

For the list of Scientific Linux 7 release notes, see Red Hat Enterprise Linux 7.

Debian 10

If you install Debian 10 (Buster) by using PXE network boot, do not add `console=tty0` to the boot parameters. This parameter can cause issues with the installation process. Use only `console=hvc0` in the

boot parameters. For more information, see Debian issues 944106 and 944125.

SUSE Linux Enterprise 12

Prepare a SLES guest for cloning

> **Note:**
>
> Before you prepare a SLES guest for cloning, ensure that you clear the `udev` configuration for network devices as follows:
>
> ```
> cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
> ```

To prepare a SLES guest for cloning:

1. Open the file `/etc/sysconfig/network/config`
2. Edit the line that reads:

   ```
   FORCE_PERSISTENT_NAMES=yes
   ```

   To

   ```
   FORCE_PERSISTENT_NAMES=no
   ```

3. Save the changes and reboot the VM.

For more information, see Prepare to Clone a Linux VM.

Ubuntu 18.04

Ubuntu 18.04 offers the following types of kernel:

- The General Availability (GA) kernel, which is not updated at point releases
- The Hardware Enablement (HWE) kernel, which is updated at point releases

Some minor versions of Ubuntu 18.04 (for example 18.04.2 and 18.04.3) use a HWE kernel by default that can experience issues when running the graphical console. To work around these issues, you can choose to run these minor versions of Ubuntu 18.04 with the GA kernel or to change some of the graphics settings. For more information, see CTX265663 - Ubuntu 18.04.2 VMs can fail to boot on Citrix Hypervisor.

VM memory

When you create a VM, a fixed amount of memory is allocated to the VM. You can use Dynamic Memory Control (DMC) to improve the utilization of physical memory in your Citrix Hypervisor environment. DMC is a memory management feature that enables dynamic reallocation of memory between VMs.

XenCenter provides a graphical display of memory usage in its **Memory** tab. For more information, see the XenCenter documentation.

Dynamic Memory Control (DMC) provides the following benefits:

- You can add or delete memory without restarting the VMs, providing a seamless experience to the user.
- When servers are full, DMC allows you to start more VMs on these servers, reducing the amount of memory allocated to the running VMs proportionally.

What is Dynamic Memory Control (DMC)?

Citrix Hypervisor DMC works by automatically adjusting the memory of running VMs, keeping the amount of memory allocated to each VM between specified minimum and maximum memory values, guaranteeing performance, and permitting greater density of VMs per server.

Without DMC, when a server is full, starting additional VMs fail with "out of memory" errors. To reduce the existing VM memory allocation and make room for more VMs, edit each VM's memory allocation and then restart the VM. When using DMC, Citrix Hypervisor attempts to reclaim memory by automatically reducing the current memory allocation of running VMs within their defined memory ranges. Citrix Hypervisor attempts to reclaim memory even when the server is full.

Notes:

- Dynamic Memory Control is deprecated in Citrix Hypervisor 8.1 and will be removed in a future release.
- Dynamic Memory Control is not supported with VMs that have a virtual GPU.

The concept of dynamic range

For each VM, the administrator can set a dynamic memory range. The dynamic memory range is the range within which memory can be added/removed from the VM without requiring a restart. When a VM is running, the administrator can adjust the dynamic range. Citrix Hypervisor always guarantees to keep the amount of memory allocated to the VM within the dynamic range. Therefore adjusting it while the VM is running may cause Citrix Hypervisor to adjust the amount of memory allocated to the VM. The most extreme case is where the administrator sets the dynamic min/max to the same value, forcing Citrix Hypervisor to ensure that this amount of memory is allocated to the VM. If new VMs are required to start on "full" servers, running VMs have their memory ‘squeezed’ to start new ones. The required extra memory is obtained by squeezing the existing running VMs proportionally within their pre-defined dynamic ranges

DMC allows you to configure dynamic minimum and maximum memory levels – creating a Dynamic Memory Range (DMR) that the VM operates in.

- Dynamic Minimum Memory: A lower memory limit that you assign to the VM.
- Dynamic Higher Limit: An upper memory limit that you assign to the VM.

For example, if the Dynamic Minimum Memory was set at 512 MB and the Dynamic Maximum Memory was set at 1,024 MB, it gives the VM a Dynamic Memory Range (DMR) of 512–1024 MB, within which it operates. Citrix Hypervisor *guarantees* always to assign each VM memory within its specified DMR when using DMC.

The concept of static range

Many Operating Systems that Citrix Hypervisor supports do not fully 'understand' the notion of dynamically adding or deleting memory. As a result, Citrix Hypervisor must declare the maximum amount of memory that a VM is asked to consume at the time that it restarts. Declaring the maximum amount of memory allows the guest operating system to size its page tables and other memory management structures accordingly. This introduces the concept of a static memory range within Citrix Hypervisor. The static memory range cannot be adjusted when the VM is running. For a particular boot, the dynamic range is constrained such as to be always contained within this static range. The static minimum (the lower bound of the static range) protects the administrator and is set to the lowest amount of memory that the OS can run with Citrix Hypervisor.

> **Note:**
>
> We recommend that you do not change the static minimum level as the static minimum level is set at the supported level per operating system. See the memory constraints table for more details.
>
> Setting a static maximum level higher than a dynamic max allows you to allocate more memory to a VM in future without restarting the VM.

DMC behavior

Automatic VM squeezing

- If DMC is not enabled, when hosts are full, new VM starts fail with 'out of memory' errors.
- When DMC is enabled, even when hosts are full, Citrix Hypervisor attempts to reclaim memory by reducing the memory allocation of running VMs within their defined dynamic ranges. In this way, running VMs are squeezed proportionally at the same distance between the dynamic minimum and dynamic maximum for all VMs on the host

When DMC is enabled

- When the host's memory is plentiful - All running VMs receive their Dynamic Maximum Memory level
- When the host's memory is scarce - All running VMs receive their Dynamic Minimum Memory level.

When you are configuring DMC, remember that allocating only a small amount of memory to a VM can negatively impact it. For example, allocating too little memory:

- Using Dynamic Memory Control to reduce the amount of physical memory available to a VM can cause it to restart slowly. Likewise, if you allocate too little memory to a VM, it can start slowly.
- Setting the dynamic memory minimum for a VM too low can result in poor performance or stability problems when the VM is starting.

How does DMC work?

Using DMC, it is possible to operate a guest virtual machine in one of two modes:

1. **Target Mode:** The administrator specifies a memory target for the guest. Citrix Hypervisor adjusts the guest's memory allocation to meet the target. Specifying a target is useful in virtual server environments, and in situations where you know exactly how much memory you want a guest to use. Citrix Hypervisor adjusts the guest's memory allocation to meet the target you specify.
2. **Dynamic Range Mode:** The administrator specifies a dynamic memory range for the guest. Citrix Hypervisor selects a target from the range and adjusts the guest's memory allocation to meet the target. Specifying a dynamic range is useful in virtual desktop environments, and in any situation where you want Citrix Hypervisor to repartition host memory dynamically in response to changing numbers of guests, or changing host memory pressure. Citrix Hypervisor selects a target from within the range and adjusts the guest's memory allocation to meet the target.

> **Note:**
>
> It is possible to change between target mode and dynamic range mode at any time for any running guest. Specify a new target, or a new dynamic range, and Citrix Hypervisor takes care of the rest.

Memory constraints

Citrix Hypervisor allows administrators to use all memory control operations with any guest operating system. However, Citrix Hypervisor enforces the following memory property ordering constraint for all guests:

```
0 memory-static-min memory-dynamic-min memory-dynamic-max memory-static-max
```

Citrix Hypervisor allows administrators to change guest memory properties to any values that satisfy this constraint, subject to validation checks. However, in addition to the previous constraint, we support only certain guest memory configurations for each supported operating system. The range of supported configurations depends on the guest operating system in use. Citrix Hypervisor does not prevent administrators from configuring guests to exceed the supported limit. However, customers are advised to keep memory properties within the supported limits to avoid performance or stability problems. For detailed guidelines on the minimum and maximum memory limits for each supported operating system, see Guest operating system support.

> **Warning:**
>
> When configuring guest memory, we advise NOT to exceed the maximum amount of physical memory addressable by your operating system. Setting a memory maximum that is greater than the operating system supported limit can lead to stability problems within your guest.

> The dynamic minimum must be greater than or equal to a quarter of the static maximum for all supported operating systems. Reducing the lower limit below the dynamic minimum can also lead to stability problems. Administrators are encouraged to calibrate the sizes of their VMs carefully, and ensure that their working set of applications function reliably at dynamic-minimum.

xe CLI commands

Display the static memory properties of a VM

1. Find the uuid of the required VM:

```
xe vm-list
```

2. Note the uuid, and then run the command `param-name=memory-static`

```
xe vm-param-get uuid=uuid param-name=memory-static-{min,max}
```

For example, the following displays the static maximum memory properties for the VM with the uuid beginning ec77:

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-static-max;
    268435456
```

The example shows that the static maximum memory for this VM is 268,435,456 bytes (256 MB).

Display the dynamic memory properties of a VM

To display the dynamic memory properties, follow the procedure as above but use the command `param-name=memory-dynamic`:

1. Find the uuid of the required VM:

```
xe vm-list
```

2. Note the uuid, and then run the command `param-name=memory-dynamic`:

```
xe vm-param-get uuid=uuid param-name=memory-dynamic-{min,max}
```

For example, the following displays the dynamic maximum memory properties for the VM with uuid beginning ec77

```
xe vm-param-get uuid= \
    ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
    param-name=memory-dynamic-max;
    134217728
```

The example shows that the dynamic maximum memory for this VM is 134,217,728 bytes (128 MB).

Update memory properties

Warning:

Use the correct ordering when setting the static/dynamic minimum/maximum parameters. In addition, you must not invalidate the following constraint:

```
0 memory-static-min memory-dynamic-min memory-dynamic-max memory-static-max
```

Update the static memory range of a virtual machine:

```
xe vm-memory-static-range-set uuid=uuid min=valuemax=value
```

Update the dynamic memory range of a virtual machine:

```
xe vm-memory-dynamic-range-set \
      uuid=uuid min=value \
      max=value
```

Specifying a target is useful in virtual server environments, and in any situation where you know exactly how much memory you want a guest to use. Citrix Hypervisor adjusts the guest's memory allocation to meet the target you specify. For example:

```
xe vm-target-set target=value vm=vm-name
```

Update all memory limits (static and dynamic) of a virtual machine:

```
xe vm-memory-limits-set \
      uuid=uuid \
      static-min=value \
      dynamic-min=value \
      dynamic-max=value static-max=value
```

Notes:

- To allocate a specific amount memory to a VM that doesn't change, set the Dynamic Maximum and Dynamic Minimum to the same value.
- You cannot increase the dynamic memory of a VM beyond the static maximum.
- To alter the static maximum of a VM, you must shut down the VM.

Update individual memory properties

Warning:

Do not change the static minimum level as it is set at the supported level per operating system. For more information, see Memory constraints.

Update the dynamic memory properties of a VM.

1. Find the uuid of the required VM:

```
xe vm-list
```

2. Note the uuid, and then use the command `memory-dynamic-{min,max}=value`

```
xe vm-param-set uuid=uuidmemory-dynamic-{min,max}=value
```

The following example changes the dynamic maximum to 128 MB:

```
xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-dynamic-
max=128MiB
```

Import and export VMs

Citrix Hypervisor allows you to import VMs from and export them to various different formats. Using the XenCenter Import wizard, you can import VMs from disk images (VHD and VMDK), Open Virtualization Format (OVF and OVA) and Citrix Hypervisor XVA format. You can even import VMs that have been created on other virtualization platforms, such as those offered by VMware and Microsoft.

> **Note:**
>
> When importing VMs that have been created using other virtualization platforms, configure or *fix up* the guest operating system to ensure that it boots on Citrix Hypervisor. The Operating System Fixup feature in XenCenter aims to provide this basic level of interoperability. For more information, see Operating system fixup.

Using the XenCenter **Export** wizard, you can export VMs to Open Virtualization Format (OVF and OVA) and Citrix Hypervisor XVA format.

You can also use the xe CLI to import VMs from and export them to Citrix Hypervisor XVA format.

Supported formats

Format	Description
Open Virtualization Format (OVF and OVA)	OVF is an open standard for packaging and distributing a virtual appliance consisting of one or more VMs.
Disk image formats (VHD and VMDK)	Virtual Hard Disk (VHD) and Virtual Machine Disk (VMDK) format disk image files can be imported using the Import wizard. Importing a disk image may be appropriate when there is a virtual disk image available, with no OVF metadata associated.
Citrix Hypervisor XVA format	XVA is a format specific to Xen-based hypervisors for packaging an individual VM as a single file archive, including a descriptor and disk images. Its file name extension is `.xva`.

Which format to use?

Consider using OVF/OVA format to:

- Share Citrix Hypervisor vApps and VMs with other virtualization platforms that support OVF
- Save more than one VM
- Secure a vApp or VM from corruption and tampering
- Include a license agreement
- Simplify vApp distribution by storing an OVF package in an OVA file

Consider using XVA format to:

- Import and export VMs from a script with a CLI

Open virtualization format (OVF and OVA)

OVF is an open standard, specified by the Distributed Management Task Force, for packaging and distributing a virtual appliance consisting of one or more VMs. For further details about OVF and OVA formats, see the following information:

- Knowledge Base Article CTX121652: Overview of the Open Virtualization Format
- Open Virtualization Format Specification

> **Note:**
>
> To import or export OVF or OVA packages, you must be logged in as root or have the Pool Administrator Role Based Access Control (RBAC) role associated with your user account.

An **OVF Package** is the set of files that comprises the virtual appliance. It always includes a descriptor file and any other files that represent the following attributes of the package:

Attributes

Descriptor (`.ovf`): The descriptor always specifies the virtual hardware requirements of the package. It may also specify other information, including:

- Descriptions of virtual disks, the package itself, and guest operating systems
- A license agreement
- Instructions to start and stop VMs in the appliance
- Instructions to install the package

Signature (`.cert`): The signature is the digital signature used by a public key certificate in the X.509 format to authenticate the author of the package.

Manifest (`.mf`): The manifest allows you to verify the integrity of the package contents. It contains the SHA-1 digests of every file in the package.

Virtual disks: OVF does not specify a disk image format. An OVF package includes files comprising virtual disks in the format defined by the virtualization product that exported the virtual disks. Citrix Hypervisor produces OVF packages with disk images in Dynamic VHD format; VMware products and Virtual Box produce OVF packages with virtual disks in Stream-Optimized VMDK format.

OVF packages also support other non-metadata related capabilities, such as compression, archiving, EULA attachment, and annotations.

> **Note:**
>
> When importing an OVF package that has been compressed or contains compressed files, you may need to free up extra disk space on the Citrix Hypervisor server to import it properly.

An **Open Virtual Appliance (OVA) package** is a single archive file, in the Tape Archive (.tar) format, containing the files that comprise an OVF Package.

Select OVF or OVA format

OVF packages contain a series of uncompressed files, which makes it easier when you want to access individual disk images in the file. An OVA package contains one large file, and while you can compress this file, it does not give you the flexibility of a series of files.

Using the OVA format is useful for specific applications for which it is beneficial to have just one file, such as creating packages for Web downloads. Consider using OVA only as an option to make the package easier to handle. Using this format lengthens both the export and import processes.

Disk image formats (VHD and VMDK)

Using XenCenter, you can import disk images in the Virtual Hard Disk (VHD) and Virtual Machine Disk (VMDK) formats. Exporting standalone disk images is not supported.

> **Note:**
>
> To import disk images, ensure that you are logged in as root or have the Pool Administrator RBAC role associated with your user account.

You might choose to import a disk image when a virtual disk image is available without any associated OVF metadata. This option might occur in the following situations:

- It is possible to import a disk image, but the associated OVF metadata is not readable
- A virtual disk is not defined in an OVF package
- You are moving from a platform that does not allow you to create an OVF package (for example, older platforms or images)
- You want to import an older VMware appliance that does not have any OVF information
- You want to import a standalone VM that does not have any OVF information

When available, we recommend importing appliance packages that contain OVF metadata rather than an individual disk image. The OVF data provides information the Import wizard requires to recreate a VM from its disk image, This information includes the number of disk images associated with the VM, the processor, storage, network, memory requirements and so on. Without this information, it can be much more complex and error-prone to recreate the VM.

XVA format

XVA is a virtual appliance format specific to Citrix Hypervisor, which packages a single VM as a single set of files, including a descriptor and disk images. The file name extension is `.xva`.

The descriptor (file name extension `ova.xml`) specifies the virtual hardware of a single VM.

The disk image format is a directory of files. The directory name corresponds to a reference name in the descriptor and contains two files for each 1 MB block of the disk image. The base name of each file is the block number in decimal. The first file contains one block of the disk image in raw binary format and does not have an extension. The second file is a checksum of the first file. If the VM was exported from Citrix Hypervisor 8.0 or earlier, this file has the extension `.checksum`. If the VM was exported from Citrix Hypervisor 8.1 or later, this file has the extension `.xxhash`.

> **Important:**
>
> If a VM is exported from the Citrix Hypervisor server and then imported into another Citrix Hypervisor server with a different CPU type, it may not run properly. For example, a Windows VM exported from a host with an Intel® VT Enabled CPU might not run when imported into a host with an AMD-VTM CPU.

Operating system fixup

When importing a virtual appliance or disk image created and exported from a virtualization platform other than Citrix Hypervisor, you might have to configure the VM before it boots properly on the Citrix Hypervisor server.

XenCenter includes an advanced hypervisor interoperability feature – Operating System Fixup – which aims to ensure a basic level of interoperability for VMs that you import into Citrix Hypervisor. Use Operating System Fixup when importing VMs from OVF/OVA packages and disk images created on other virtualization platforms.

The Operating System Fixup process addresses the operating system device and driver issues inherent when moving from one hypervisor to another. The process attempts to repair boot device-related problems with the imported VM that might prevent the operating system within from booting in the Citrix Hypervisor environment. This feature is not designed to perform conversions from one platform to another.

> **Note:**
>
> This feature requires an ISO storage repository with 40 MB of free space and 256 MB of virtual memory.

Operating System Fixup is supplied as an automatically booting ISO image that is attached to the DVD drive of the imported VM. It performs the necessary repair operations when the VM is first started, and then shuts down the VM. The next time the new VM is started, the boot device is reset, and the VM starts normally.

To use Operating System Fixup on imported disk images or OVF/OVA packages, enable the feature on the Advanced Options page of the XenCenter Import wizard. Specify a location where the Fixup ISO is copied so that Citrix Hypervisor can use it.

What does operating system fixup do to the VM?

The Operating System Fixup option is designed to make the minimal changes possible to enable a virtual system to boot. Depending on the guest operating system and the hypervisor of the original host, further

actions might be required after using Operating System Fixup. These actions can include configuration changes and driver installation.

During the Fixup process, an ISO is copied to an ISO SR. The ISO is attached to a VM. The boot order is set to boot from the virtual DVD drive, and the VM boots into the ISO. The environment within the ISO then checks each disk of the VM to determine if it is a Linux or a Windows system.

If a Linux system is detected, the location of the GRUB configuration file is determined. Any pointers to SCSI disk boot devices are modified to point to IDE disks. For example, if GRUB contains an entry of `/dev/sda1` representing the first disk on the first SCSI controller, this entry is changed to `/dev/hda1` representing the first disk on the first IDE controller.

If a Windows system is detected, a generic critical boot device driver is extracted from the driver database of the installed OS and registered with the OS. This process is especially important for older Windows operating systems when the boot device is changed between a SCSI and IDE interface.

If certain virtualization tool sets are discovered in the VM, they are disabled to prevent performance problems and unnecessary event messages.

Import VMs

When you import a VM, you effectively create a VM, using many of the same steps required to provision a new VM. These steps include nominating a host, and configuring storage and networking.

You can import OVF/OVA, disk image, XVA, and XVA Version 1 files using the XenCenter Import wizard. You can also import XVA files via the xe CLI.

Import VMs from OVF/OVA

> **Note:**
>
> To import OVF or OVA packages, you must be logged in as root or have the Pool Administrator Role Based Access Control (RBAC) role associated with your user account.

The XenCenter Import wizard allows you to import VMs that have been saved as OVF/OVA files. The Import wizard takes you through the usual steps to create a VM in XenCenter: nominating a host, and then configuring storage and networking for the new VM. When importing OVF and OVA files, extra steps may be required, such as:

- When importing VMs that have been created using other virtualization platforms, run the Operating System Fixup feature to ensure a basic level of interoperability for the VM. For more information, see Operating system fixup.

> **Tip:**
>
> Ensure that the target host has enough RAM to support the virtual machines being imported. A lack of available RAM results in a failed import. For more information about resolving this issue, see CTX125120 - Appliance Import Wizard Fails Because of Lack of Memory.

Imported OVF packages appear as vApps when imported using XenCenter. When the import is complete, the new VMs appear in the XenCenter **Resources** pane, and the new vApp appears in the **Manage vApps** dialog box.

To import VMs from OVF/OVA by using XenCenter:

1. Open the Import wizard by doing one of the following:
    - In the **Resources** pane, right-click, and then select **Import** on the shortcut menu.
    - On the **File** menu, select **Import**.
2. On the first page of the wizard, locate the file you want to import, and then click **Next** to continue.
3. Review and accept EULAs, if applicable.

    If the package you are importing includes any EULAs, accept them and click **Next** to continue. When no EULAs are included in the package, the wizard skips this step and advance straight to the next page.
4. Specify the pool or host to which you want to import the VMs, and then (optionally) assign the VMs to a home Citrix Hypervisor server.

    To select a host or pool, choose from the **Import VM(s)** to list.

    To assign each VM a home Citrix Hypervisor server, select a server from the list in the **Home Server**. If you want not to assign a home server, select **Don't assign a home server**.

    Click **Next** to continue.
5. Configure storage for the imported VMs: Choose one or more storage repositories on which to place the imported virtual disks, and then click **Next** to continue.

    To place all the imported virtual disks on the same SR, select **Place all imported VMs on this target SR**. Select an SR from the list.

    To place the virtual disks of incoming VMs onto different SRs, select **Place imported VMs on the specified target SRs**. For each VM, select the target SR from the list in the SR column.
6. Configure networking for the imported VMs: map the virtual network interfaces in the VMs you are importing to target networks in the destination pool. The Network and MAC address shown in the list of incoming VMs are stored as part of the definition of the original (exported) VM in the export file. To map an incoming virtual network interface to a target network, select a network from the list in the Target Network column. Click **Next** to continue.
7. Specify security settings: If the selected OVF/OVA package is configured with security features, such as certificates or a manifest, specify the information necessary, and then click **Next** to continue.

    Different options appear on the Security page depending on which security features have been configured on the OVF appliance:

    - If the appliance is signed, a **Verify digital signature** check box appears, automatically selected. Click **View Certificate** to display the certificate used to sign the package. If the certificate

appears as untrusted, it is likely that either the Root Certificate or the Issuing Certificate Authority is not trusted on the local computer. Clear the **Verify digital signature** check box if you do not want to verify the signature.

- If the appliance includes a manifest, a **Verify manifest content** check box appears. Select this check box to have the wizard verify the list of files in the package.

When packages are digitally signed, the associated manifest is verified automatically, so the **Verify manifest content** check box does not appear on the Security page.

> **Note:**
>
> VMware Workstation 7.1.x OVF files fail to import when you choose to verify the manifest. This failure occurs because VMware Workstation 7.1.x produces an OVF file with a manifest that has invalid SHA-1 hashes. If you do not choose to verify the manifest, the import is successful.

8. Enable Operating System Fixup: If the VMs in the package you are importing were built on a virtualization platform other than Citrix Hypervisor, select the **Use Operating System Fixup** check box. Select an ISO SR where the Fixup ISO can be copied so that Citrix Hypervisor can access it. For more information about this feature, see Operating system fixup.

   Click **Next** to continue.

9. (XenCenter 8.2.2 and earlier) Configure Transfer VM networking.

   Select a network from the list of network interfaces available in the destination pool or host. Choose to configure the network settings automatically or manually.

   - To use automated Dynamic Host Configuration Protocol to assign networking settings including the IP address, subnet mask and gateway, select **Automatically obtain network settings using DHCP**.
   - To configure networking settings manually, select **Use these network settings**, and then enter the required values. Enter an IP address. Optionally, set the subnet mask and gateway settings.

   Click **Next** to continue.

10. Review the import settings, and then click **Finish** to begin the import process and close the wizard.

> **Note:**
>
> Importing a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The import progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. When the newly imported VM is available, it appears in the **Resources** pane, and the new vApp appears in the **Manage vApps** dialog box.

> **Note:**

After using XenCenter to import an OVF package that contains Windows operating systems, you must set the `platform` parameter.

1. Set the `platform` parameter to `device_id=0002`. For example:

   ```
   xe vm-param-set uuid=VM uuid platform:device_id=0002
   ```

2. Set the `platform` parameter to `viridian=true`. For example:

   ```
   xe vm-param-set uuid=VM uuid platform:viridian=true
   ```

Import disk images

The XenCenter Import wizard allows you to import a disk image into a pool or specific host as a VM. The Import wizard takes you through the usual steps to create a VM in XenCenter: nominating a host, and then configuring storage and networking for the new VM.

Requirements

- You must be logged in as root or have the Pool Administrator Role Based Access Control (RBAC) role associated with your user account.
- Ensure that DHCP runs on the management network Citrix Hypervisor is using.
- The Import wizard requires local storage on the server on which you are running it.

To import VMs from a Disk Image by using XenCenter:

1. Open the Import wizard by doing one of the following:
   - In the **Resources** pane, right-click, and then select **Import** on the shortcut menu.
   - On the **File** menu, select **Import**.
2. On the first page of the wizard, locate the file you want to import, and then click **Next** to continue.
3. Specify the VM name and allocate CPU and memory resources.

   Enter a name for the new VM to be created from the imported disk image, and then allocate the number of CPUs and amount of memory. Click **Next** to continue.
4. Specify the pool or host to which you want to import the VMs, and then (optionally) assign the VMs to a home Citrix Hypervisor server.

   To select a host or pool, choose from the **Import VM(s)** to list.

   To assign each VM a home Citrix Hypervisor server, select a server from the list in the **Home Server**. If you want not to assign a home server, select **Don't assign a home server**.

Click **Next** to continue.

5. Configure storage for the imported VMs: Select one or more storage repositories on which to place the imported virtual disks, and then click **Next** to continue.

   To place all the imported virtual disks on the same SR, select **Place all imported VMs on this target SR**. Select an SR from the list.

   To place the virtual disks of incoming VMs onto different SRs, select **Place imported VMs on the specified target SRs**. For each VM, select the target SR from the list in the SR column.

6. Configure networking for the imported VMs: map the virtual network interfaces in the VMs you are importing to target networks in the destination pool. The Network and MAC address shown in the list of incoming VMs are stored as part of the definition of the original (exported) VM in the export file. To map an incoming virtual network interface to a target network, select a network from the list in the Target Network column. Click **Next** to continue.

7. Enable Operating System Fixup: If the disk images you are importing were built on a virtualization platform other than Citrix Hypervisor, select the Use Operating System Fixup check box. Select an ISO SR where the Fixup ISO can be copied so that Citrix Hypervisor can access it. For more information about this feature, see Operating system fixup.

   Click **Next** to continue.

8. (XenCenter 8.2.2 and earlier) Configure Transfer VM networking.

   Select a network from the list of network interfaces available in the destination pool or host. Choose to configure the network settings automatically or manually.

   - To use automated Dynamic Host Configuration Protocol to assign networking settings including the IP address, subnet mask and gateway, select **Automatically obtain network settings using DHCP**.
   - To configure networking settings manually, select Use these network settings, and then enter the required values. Enter an IP address. Optionally, set the subnet mask and gateway settings.

   Click **Next** to continue.

9. Review the import settings, and then click **Finish** to begin the import process and close the wizard.

> **Note:**
>
> Importing a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The import progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. When the newly imported VM is available, it appears in the **Resources** pane.

> **Note:**

After using XenCenter to import a disk image that contains Windows operating systems, you must set the `platform` parameter. The value of this parameter varies according to the version of Windows contained in the disk image:

- For Windows Server 2016 and later, set the `platform` parameter to `device_id=0002`. For example:

```
xe vm-param-set uuid=VM uuid platform:device_id=0002
```

- For all other versions of Windows, set the `platform` parameter to `viridian=true`. For example:

```
xe vm-param-set uuid=VM uuid platform:viridian=true
```

Import VMs from XVA

You can import VMs, templates, and snapshots that have previously been exported and stored locally in XVA format (`.xva`). To do so, you follow the usual steps to create a VM: nominating a host, and then configuring storage and networking for the new VM.

Warning:

It may not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM exported from a server with an Intel VT Enabled CPU might not run when imported to a server with an AMD-VTM CPU.

To import VMs from XVA by using XenCenter:

1. Open the Import wizard by doing one of the following:
   - In the **Resources** pane, right-click, and then select **Import** on the shortcut menu.
   - On the **File** menu, select **Import**.
2. On the first page of the wizard, locate the file you want to import (`.xva` or `ova.xml`), and then click **Next** to continue.

   If you enter a URL location (`http`, `https`, `file`, or `ftp`) in the **Filename** box. Click **Next**, a Download Package dialog box opens and you must specify a folder on your XenCenter host where the file is copied.
3. Select a pool or host for the imported VM to start on, and then choose **Next** to continue.
4. Select the storage repositories on which to place the imported virtual disk, and then click **Next** to continue.
5. Configure networking for the imported VM: map the virtual network interface in the VM you are importing to target a network in the destination pool. The Network and MAC address shown in the list of incoming VMs are stored as part of the definition of the original (exported) VM in the export file. To map

an incoming virtual network interface to a target network, select a network from the list in the Target Network column. Click **Next** to continue.

6. Review the import settings, and then click **Finish** to begin the import process and close the wizard.

> **Note:**
>
> Importing a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The import progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. When the newly imported VM is available, it appears in the **Resources** pane.

To import a VM from XVA by using the xe CLI:

To import the VM to the default SR on the target Citrix Hypervisor server, enter the following:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file
```

To import the VM to a different SR on the target Citrix Hypervisor server, add the optional `sr-uuid` parameter:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
```

If you want to preserve the MAC address of the original VM, add the optional `preserve` parameter and set to `true`:

```
xe vm-import -h hostname -u root -pw password \
    filename=pathname_of_export_file preserve=true
```

> **Note:**
>
> Importing a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

After the VM has been imported, the command prompt returns the UUID of the newly imported VM.

Export VMs

You can export OVF/OVA and XVA files using the XenCenter Export wizard; you can also export XVA files via the xe CLI.

Export VMs as OVF/OVA

Using the XenCenter Export wizard, you can export one or more VMs as an OVF/OVA package. When you export VMs as an OVF/OVA package, the configuration data is exported along with the virtual hard disks of each VM.

> **Note:**
>
> To export OVF or OVA packages, you must be logged in as root or have the Pool Administrator Role Based Access Control (RBAC) role associated with your user account.

To export VMs as OVF/OVA by using XenCenter:

1. Shut down or suspend the VMs that you want to export.
2. Open the Export wizard: in the **Resources** pane, right-click the pool or host containing the VMs you want to export, and then select **Export**.
3. On the first page of the wizard:
   - Enter the name of the export file
   - Specify the folder where you want the files to be saved
   - Select **OVF/OVA Package (*.ovf, *.ova)** from the **Format** list
   - Click **Next** to continue
4. From the list of available VMs, select the VMs that you want to include in the OVF/OVA package, and then click **Next** to continue.
5. If necessary, you can add to a previously prepared End User Licensing Agreement (EULA) document (.rtf, .txt) to the package.

   To add a EULA, click **Add** and browse to the file you want to add. Once you have added the file, you can view the document by selecting it from the **EULA files** list and then clicking **View**.

   EULAs can provide the legal terms and conditions for using the appliance and the applications delivered in the appliance.

   The ability to include one or more EULAs lets you legally protect the software on the appliance. For example, if your appliance includes a proprietary operating system on its VMs, you might want to include the EULA text from that operating system. The text is displayed and the person who imports the appliance must accept it.

   > **Note:**
   >
   > Attempting to add EULA files that are not in supported formats, including XML or binary files, can cause the import EULA functionality to fail.

   Select **Next** to continue.
6. On the **Advanced options** page, specify a manifest, signature and output file options, or just click **Next** to continue.

1. To create a manifest for the package, select the **Create a manifest** check box.

   The manifest provides an inventory or list of the other files in a package. The manifest is used to ensure that the files originally included when the package was created are the same files present when the package arrives. When the files are imported, a checksum is used to verify that the files have not changed since the package was created.

2. To add a digital signature to the package

   1. Select **Sign the OVF package**.

      The digital signature (`.cert`) contains the signature of the manifest file and the certificate used to create that signature. When a signed package is imported, the user can verify the identity of the package creator by using the public key of the certificate to validate the digital signature.

   2. Browse to locate a certificate.

      Use an X.509 certificate that you have already created from a Trusted Authority and exported as a `.pfx` file. For certificates with SHA-256 digest export using the "Microsoft Enhanced RSA and AES Cryptographic Provider" as CSP.

   3. In **Private key password** enter the export (PFX) password, or, if an export password was not provided, the private key associated with the certificate.

3. To output the selected VMs as a single (tar) file in OVA format, select the **Create OVA package (single OVA export file)** check box. For more on the different file formats, see Open virtualization format.

4. To compress virtual hard disk images (.VHD files) included in the package, select the Compress OVF files check box.

   When you create an OVF package, the virtual hard disk images are, by default, allocated the same amount of space as the exported VM. For example, a VM that is allocated 26 GB of space has a hard disk image that consumes 26 GB of space. The hard disk image uses this space regardless of whether or not the VM actually requires it.

   > **Note:**
   >
   > Compressing the VHD files makes the export process take longer to complete. Importing a package containing compressed VHD files also takes longer, as the Import wizard must extract all of the VHD images as it imports them.

If both **Create OVA package (single OVA export file)** and **Compress OVF files** are checked, the result is a compressed OVA file with the extension `.ova.gz`.

7. (XenCenter 8.2.2 and earlier) Configure Transfer VM networking.

   Select a network from the list of network interfaces available in the destination pool or host. Choose to configure the network settings automatically or manually.

- To use automated Dynamic Host Configuration Protocol to assign networking settings including the IP address, subnet mask and gateway, select **Automatically obtain network settings using DHCP**.
- To configure networking settings manually, select **Use these network settings**, and then enter the required values. Enter an IP address. Optionally, set the subnet mask and gateway settings.

Click **Next** to continue.

8. Review the export settings.

   To have the wizard verify the exported package, select the **Verify export on completion** check box. Click **Finish** to begin the export process and close the wizard.

> **Note:**
>
> Exporting a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The export progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. To cancel an export in progress, click the **Logs** tab, find the export in the list of events, and click the **Cancel** button.

Export VMs as XVA

You can export an existing VM as an XVA file using the XenCenter Export wizard or the xe CLI. We recommend exporting a VM to a machine other than the Citrix Hypervisor server, on which you can maintain a library of export files. For example, you can export the VM to the machine running XenCenter.

> **Warning:**
>
> It may not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM exported from a server with an Intel VT Enabled CPU might not run when imported to a server with an AMD-VTM CPU.

To export VMs as XVA files by using XenCenter:

1. Shut down or suspend the VM that you want to export.
2. Open the Export wizard: from the **Resources** pane, right-click the VM which you want to export, and then select **Export**.
3. On the first page of the wizard:
   - Enter the name of the export file
   - Specify the folder where you want the files to be saved
   - Select **XVA File (*.xva)** from the **Format** list
   - Click **Next** to continue

4. From the list of available VMs, select the VM that you want to export, and then click **Next** to continue.
5. Review the export settings.

   To have the wizard verify the exported package, select the **Verify export on completion** check box. Click Finish to begin the export process and close the wizard.

   > **Note:**
   >
   > Exporting a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The export progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. To cancel an export in progress, click the **Logs** tab, find the export in the list of events, and click the **Cancel** button.

To export VMs as XVA files by using the xe CLI:

1. Shut down the VM that you want to export.
2. Export the VM by running the following:

```
xe vm-export -h hostname -u root -pw password vm=vm_name \
    filename=pathname_of_file
```

   > **Note:**
   >
   > Be sure to include the `.xva` extension when specifying the export file name. If the exported VM doesn't have this extension, XenCenter might fail to recognize the file as a valid XVA file when you attempt to import it.

Delete VMs

You can delete VMs by using the xe CLI or XenCenter.

Deleting a virtual machine removes its configuration and its filesystem from the server. When you delete a VM, you can choose to delete or preserve any virtual disks attached to the VM, in addition to any snapshots of the VM.

Delete a VM by using the xe CLI

To delete a VM:

1. Find the VM UUID:

   ```
   xe vm-list
   ```

2. Shutdown the VM:

   ```
   xe vm-shutdown uuid=<uuid>
   ```

3. (Optional) You can choose to delete the attached virtual disks:

   1. Find the virtual disk UUIDs:

      ```
      xe vm-disk-list vm=<uuid>
      ```

   2. Delete the virtual disk:

      ```
      xe vdi-destroy uuid=<uuid>
      ```

   Important:

   Any data stored in the VM's virtual disk drives is lost.

4. (Optional) You can choose to delete the snapshots associated with the VM:

   1. Find the UUIDs of the snapshots:

      ```
      xe snapshot-list vm=<uuid>
      ```

2. For each snapshot to delete, find the UUIDs of the virtual disks for that snapshot:

```
xe snapshot-disk-list snapshot-uuid=<uuid>
```

3. Delete each snapshot disk:

```
xe vdi-destroy uuid=<uuid>
```

4. Delete the snapshot:

```
xe snapshot-destroy uuid=<uuid>
```

5. Delete the VM:

```
xe vm-destroy uuid=<uuid>
```

Delete a VM by using XenCenter

To delete a VM:

1. Shut down the VM.
2. Select the stopped VM in the **Resources** panel, right-click, and select **Delete** on the shortcut menu. Alternatively, on the **VM** menu, select **Delete**.
3. To delete an attached virtual disk, select its check box.

> **Important:**
>
> Any data stored in the VM's virtual disk drives is lost.

4. To delete a snapshot of the VM, select its check box.
5. Click **Delete**.

   When the delete operation is completed, the VM is removed from the **Resources** pane.

> **Note:**
>
> VM snapshots whose parent VM has been deleted (*orphan snapshots*) can still be accessed from the **Resources** pane. These snapshots can be exported, deleted, or used to create VMs and templates. To view snapshots in the **Resources** pane, select **Objects** in the Navigation pane and then expand the **Snapshots** group in the Resources pane.

Bromium Secure Platform

Citrix Hypervisor supports Bromium Secure Platform on Windows VMs. This feature protects your enterprise from breaches and enables users to perform any operations without compromising security.

> **Note:**
>
> The minimum supported Bromium version is 4.0.4.

Using this feature, you can:

- Protect your enterprise against known and unknown threats.
- Detect and monitor threat activity as it happens.
- Respond to a visualization of the attack and view the remedial measures taken.

Compatibility requirements and caveats

Citrix Hypervisor supports Bromium on:

- **CPU**: Intel Core i3, i5, i7 v3 (Haswell) or later with Intel Virtualization Technology (Intel VT) and Extended Page Tables (EPT) enabled in the system BIOS.

  AMD CPUs are not supported.

- **VMs**: Windows 8.1 (64-bit) and Windows 10 (64-bit).
- **VM resources**: At least 2 vCPUs, 4 GB RAM and 32 GB disk space.

For VMs that are running Bromium, Citrix Hypervisor does not support and prevents the use of the following features:

- Any form of VM motion (for example: live migration, storage live migration).
- Use of Dynamic Memory Control (DMC).

> **Note:**
>
> It is possible to use PCI pass-through and vGPU for a VM that has enabled nested virtualization. However, Citrix does not support such configurations.
>
> **Important:**
>
> Bromium Secure Platform uses nested virtualization support. Citrix supports this feature for use with Bromium Secure Platform only. Nested virtualization is not supported for other use cases. To use this feature, you must run Citrix Hypervisor Premium Edition or have access to Citrix Hypervisor through a Citrix Virtual Apps and Desktops entitlement.

Configuration

To prepare your Citrix Hypervisor system for use with Bromium Secure Platform, perform the following steps:

1. On each host, force the use of software VMCS shadowing by running the following command at the command prompt:

   ```
   /opt/xensource/libexec/xen-cmdline --set-xen force_software_vmcs_shadow
   ```

2. Restart the host.

3. On each VM, enable nested-virtualized support using the following commands:

   ```
   xe vm-list name-label='vm_name' --minimal

   xe vm-param-set uuid=$VM platform:nested-virt=1
   ```

   Note:

   For Citrix Virtual Desktops, use the gold image for nested virtualization.

4. Install Bromium Secure Platform in the VM by following its installation instructions.

vApps

A vApp is a logical group of one or more related Virtual Machines (VMs) which can be started up as a single entity. When a vApp is started, the VMs contained within the vApp start in a user-predefined order. This feature enables VMs which depend upon one another to be automatically sequenced. An administrator no longer has to manually sequence the startup of dependent VMs when a whole service requires restarting (for instance for a software update). The VMs within the vApp do not have to reside on one host and can be distributed within a pool using the normal rules.

The vApp feature is useful in the Disaster Recovery situation. You can group all VMs that are on the same Storage Repository or all VMs that relate to the same Service Level Agreement (SLA).

> **Note:**
>
> vApps can be created and changed using both XenCenter and the xe CLI. For information on working with vApps using the CLI, see Command Line Interface.

Manage vApps in XenCenter

The **Manage vApps** dialog box enables you to create, delete, change, start, and shut down vApps, and import and export vApps within the selected pool. If you select a vApp in the list, the VMs it contains are listed in the details pane on the right.

You can use **Manage vApps** to do the following actions:

- To change the name or description of a vApp
- To add or remove VMs from the vApp
- To change the startup sequence of the VMs in the vApp

To change vApps:

1. Select the pool and, on the **Pool** menu, select **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.

2. Select the vApp and choose **Properties** to open its Properties dialog box.

3. Select the **General** tab to change the vApp name or description.

4. Select the **Virtual Machines** tab to add or remove VMs from the vApp.

5. Select the **VM Startup Sequence** tab to change the start order and delay interval values for individual VMs in the vApp.

6. Click **OK** to save your changes and close **Properties**.

Create vApps

To group VMs together in a vApp follow the procedure:

1. Choose the pool and, on the **Pool** menu, select **Manage vApps**.
2. Type a name for the vApp, and optionally a description. Click **Next**.

   You can choose any name you like, but a name that describes the vApp is best. Although it is advisable to avoid creating multiple vApps that have the same name, it is not a requirement. XenCenter does not force vApp names to be unique. It is not necessary to use quotation marks for names that include spaces.
3. Choose which VMs to include in the new vApp. Click **Next**.

   You can use the search field to list only VMs that have names that include the specified text string.
4. Specify the startup sequence for the VMs in the vApp. Click **Next**.

Value	Description
Start Order	Specifies the order in which individual VMs are started up within the vApp, allowing certain VMs to be restarted before others. VMs that have a start order value of 0 (zero) are started first. VMs that have a start order value of 1 are started next. Then VMs that have a start order value of 2 are started, and so on.
Attempt to start next VM after	Specifies how long to wait after starting the VM before attempting to start the next group of VMs in the startup sequence. That next group is the set of VMs that have a lower start order.

1. On the final page of **Manage vApps**, you can review the vApp configuration. Click **Previous** to go back and change any settings or **Finish** to create the vApp and close **Manage vApps**.

> **Note:**
>
> A vApp can span across multiple servers in a single pool, but cannot span across several pools.

Delete vApps

To delete a vApp, follow the procedure:

1. Choose the pool and, on the **Pool** menu, select **Manage vApps**.
2. Select the vApp you want to delete from the list. Click **Delete**.

> **Note:**
>
> The VMs in the vApp are **not** deleted.

Start and shut down vApps by using XenCenter

To start or shut down a vApp, use **Manage vApps**, accessed from the **Pool** menu. When you start a vApp, all the VMs within it are started up automatically in sequence. The start order and delay interval values specified for each individual VM control the startup sequence. These values can be set when you first create the vApp. Change these values at any time from the vApp Properties dialog box or individual VM Properties dialog box.

To start a vApp:

1. Open **Manage vApps**: Choose the pool where the VMs in the vApp are located and, on the **Pool** menu, select **Manage vApps**. Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.
2. Choose the vApp and click **Start** to start all the VMs it contains.

To shut down a vApp:

1. Open **Manage vApps**: Choose the pool where the VMs in the vApp are located and, on the **Pool** menu, select **Manage vApps**. Alternatively, right-click in the **Resources** pane and select **Manage vApps** on the shortcut menu.
2. Choose the vApp and click **Shut Down** to shut down all the VMs in the vApp.

   A soft shutdown is attempted on all VMs. If a soft shutdown is not possible, then a forced shutdown is performed.

> **Note:**
>
> A soft shutdown performs a graceful shutdown of the VM, and all running processes are halted individually.
>
> A forced shutdown performs a hard shutdown and is the equivalent of unplugging a physical server. It might not always shut down all running processes. If you shut down a VM in this way, you risk losing data. Only use a forced shutdown when a soft shutdown is not possible.

Import and export vApps

vApps can be imported and exported as OVF/OVA packages. For more information, see Import and Export VMs.

To export a vApp:

1. Open **Manage vApps**: on the **Pool** menu, select **Manage vApps**.
2. Choose the vApp you want to export in the list. Click **Export**.
3. Follow the procedure described in Export VMs as OVF/OVA.

Exporting a vApp can take some time.

To import a vApp:

1. Open **Manage vApps**: on the **Pool** menu, select **Manage vApps**.

2. Click **Import** to open the **Import** dialog box.

3. Follow the procedure described in Import VMs as OVF/OVA.

After the import is complete, the new vApp appears in the list of vApps in **Manage vApps**.

Demo Linux virtual appliance

We provide a fully functional installation of a Demo Linux Virtual Appliance, based on a CentOS 7.5 distribution.

The appliance is available for download, in a single `xva` file from the Citrix Hypervisor Download page.

The `xva` file can be quickly imported into XenCenter to create a fully working Linux Virtual Machine. No additional configuration steps are required.

The Demo Linux Virtual Appliance enables you to deploy a VM quickly and simply. Use this appliance to test Citrix Hypervisor product features such as live migration and high availability.

The Demo Linux Virtual Appliance comes with the following items already set up:

- Citrix VM Tools for Linux
- Pre-configured networking connectivity
- A web server for test purposes

> **Warning:**
>
> Do not use the Demo Linux Virtual Appliance for running production workloads.

Import the Demo Linux virtual appliance

1. Download the Demo Linux Virtual Appliance from the Citrix Hypervisor Download page.

   Customers require access to **My Account** to access this page. If you do not have an account, you can register on the Citrix home page.

2. In the **Resources** pane, select a host or a Pool, then right-click and select **Import**. The Import Wizard is displayed.

3. Click **Browse** and navigate to the location of the downloaded Demo Linux Virtual Appliance `xva` file on your computer.

4. Click **Next**.

5. Select the target Citrix Hypervisor server or pool, then click **Next**.

6. Select a storage repository on which to create the virtual appliance's disk, then click **Next**.

7. Click **Finish** to import the virtual appliance.

> **Note:**
>
> When you first start the VM, you are prompted to enter a root password. The IP address of the VM is then displayed. Ensure that you record the IP address, as it is useful for test purposes.

Useful tests

This section lists some useful tests to carry out to ensure that your Demo Linux Virtual Appliance is correctly configured.

1. Test that you have external networking connectivity.

   Log in to the VM from the XenCenter console. Run this comment to send ping packets to Google and back:

   ```
   ping -c 10 google.com
   ```

   Other installed networking tools include `ifconfig`, `netstat`, and `tracepath`.

2. Using the IP address displayed on VM boot, test that you can ping the VM from an external computer.

3. Test that the web server is configured.

   In a web browser, enter the VM IP address. The "Demonstration Linux Virtual Machine" page opens. This page displays simple information about the VM mounted disks, their size, location, and usage.

You can also use the webpage to mount a disk.

Mount a disk using the Demonstration Linux Virtual Machine webpage

1. In XenCenter, add a virtual disk to your VM. Select the VM in the **Resources** pane, open the **Storage** tab, and then click **Add**.

2. Enter the name of the new virtual disk and, optionally, a description.

3. Enter the size of the new virtual disk.

   Ensure that the storage repository where the virtual disk is stored has sufficient space for the new virtual disk.

4. Select the SR where the new virtual disk is stored.

5. Click **Create** to add the new virtual disk and close the dialog box.

6. Click the **Console** tab, and user your normal tools to partition and format the disk as required.

7. Refresh the Demonstration Linux Virtual Machine webpage, the new disk is displayed.

8. Click **Mount**. This action mounts the disk, and filesystem information is displayed.

For more information on adding virtual disks, see the XenCenter documentation.

Advanced notes for virtual machines

This section provides some advanced notes for Virtual Machines.

VM boot behavior

There are two options for the behavior of a Virtual Machine's VDI when the VM is booted:

> **Note:**
>
> The VM must be shut down before you can change its boot behavior setting.

Persist (Citrix Virtual Desktops - Private Desktop Mode)

This behavior is the default on VM boot. The VDI is left in the state it was at the last shutdown.

Select this option if you plan to allow users to make permanent changes to their desktops. To select persist, shut down the VM, and then enter the following command:

```
xe vdi-param-set uuid=vdi_uuid on-boot=persist
```

Reset (Citrix Virtual Desktops - Shared Desktop Mode)

On VM boot, the VDI is reverted to the state it was in at the previous boot. Any changes made while the VM is running are lost when the VM is next booted.

Select this option if you plan to deliver standardized desktops that users cannot permanently change. To select reset, shut down the VM, and then enter the following command:

```
xe vdi-param-set uuid=vdi_uuid on-boot=reset
```

> **Warning:**
>
> After you change `on-boot=reset`, any data saved to the VDI is discarded after the next shutdown/start or reboot.

Make the ISO library available to Citrix Hypervisor servers

To make an ISO library available to Citrix Hypervisor servers, create an external NFS or SMB/CIFS share directory. The NFS or SMB/CIFS server must allow root access to the share. For NFS shares, allow access by setting the `no_root_squash` flag when you create the share entry in `/etc/exports` on the NFS server.

Then either use XenCenter to attach the ISO library, or connect to the host console and run the command:

```
xe-mount-iso-sr host:/volume
```

For advanced use, you can pass extra arguments to the mount command.

To make a Windows SMB/CIFS share available to the host, either use XenCenter, or connect to the host console and run the following command:

```
xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
```

Replace back slashes in the `unc_path` argument with forward-slashes. For example:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
```

After mounting the share, any available ISOs are available from the **Install from ISO Library or DVD drive** list in XenCenter. These ISOs are also available as CD images from the CLI commands.

Attach the ISO to an appropriate Windows template.

Connect to a Windows VM by using Remote Desktop

You can use one of the following ways of viewing a Windows VM console, both of which support full use of the keyboard and mouse.

- Using XenCenter. This method provides a standard graphical console and uses the VNC technology built in to Citrix Hypervisor to provide remote access to your virtual machine console.
- Connecting using Windows Remote Desktop. This method uses the Remote Desktop Protocol technology

In XenCenter on the **Console** tab, there is a **Switch to Remote Desktop** button. This button disables the standard graphical console within XenCenter, and switches to using Remote Desktop.

If you do not have Remote Desktop enabled in the VM, this button is disabled. To enable it, install the Citrix VM Tools for Windows. Follow the procedure below to enable it in each VM that you want to connect using Remote Desktop.

To enable Remote Desktop on a Windows VM:

1. Open **System** by clicking the **Start** button, right-click on **Computer**, and then select **Properties**.
2. Click **Remote settings**. If you're prompted for an administrator password, type the password you created during the VM setup.
3. In the **Remote Desktop** area, click the check box labeled **Allow connections from computers running any version of Remote Desktop**.

4. To select any non-administrator users that can connect to this Windows VM, click the **Select Remote Users** button and provide the user names. Users with Administrator privileges on the Windows domain can connect by default.

You can now connect to this VM using Remote Desktop. For more information, see the Microsoft Knowledge Base article, Connect to another computer using Remote Desktop Connection.

> **Note:**
>
> You cannot connect to a VM that is asleep or hibernating. Set the settings for sleep and hibernation on the remote computer to **Never**.

Time handling in Windows VMs

For Windows guests, initially the control domain clock drives the time. The time updates during VM lifecycle operations such as suspend and reboot.We recommend running a reliable NTP service in the control domain and all Windows VMs.

If you manually set a VM to be two hours ahead of the control domain, then it persists. You might set the VM ahead by using a time-zone offset within the VM. If you later change the control domain time (either manually or by NTP), the VM shifts accordingly but maintains the two hours offset. Changing the control domain time-zone does not affect VM time-zones or offset. Citrix Hypervisor uses the hardware clock setting of the VM to synchronize the VM. Citrix Hypervisor does not use the system clock setting of the VM.

When performing suspend and resume operations or using live migration, ensure that you have up-to-date Citrix VM Tools for Windows installed. Citrix VM Tools for Windows notify the Windows kernel that a time synchronization is required after resuming (potentially on a different physical host).

> **Note:**
>
> If you are running Windows VMs in Citrix Virtual Desktops environment, you must ensure that the host clock has the same source as the Active Directory (AD) domain. Failure to synchronize the clocks can cause the VMs to display an incorrect time and cause the Windows PV drivers to crash.

Time handling in Linux VMs

In addition to the behavior defined by Citrix Hypervisor, operating system settings and behaviors can affect the time handling behavior of your Linux VMs. Some Linux operating systems might periodically synchronize their system clock and hardware clock, or the operating system might use its own NTP service by default. For more information, see the documentation for the operating system of your Linux VM.

> **Note:**
>
> When installing a new Linux VM, ensure that you change the time-zone from the default UTC to your local value. For specific distribution instructions, see Linux Release Notes.

Hardware clocks in Linux VMs are **not** synchronized to the clock running on the control domain and can be altered. When the VM first starts, the control domain time is used to set the initial time of the hardware clock and system clock.

If you change the time on the hardware clock, this change is persisted when the VM reboots.

System clock behavior depends on the operating system of the VM. For more information, see the documentation for your VM operating system.

You cannot change this Citrix Hypervisor time handling behavior.

Install VMs from Reseller Option Kit (BIOS-locked) media

There are two types of VM: BIOS-generic and BIOS-customized. To enable installation of Reseller Option Kit (BIOS-locked) OEM versions of Windows onto a VM, copy the BIOS strings of the VM from the host with which the media was supplied. Alternatively, advanced users can set user-defined values to the BIOS strings.

BIOS-generic

The VM has generic Citrix Hypervisor BIOS strings.

> **Note:**
>
> If a VM doesn't have BIOS strings set when it starts, the standard Citrix Hypervisor BIOS strings are inserted into it and the VM becomes BIOS-generic.

BIOS-customized

For HVM VMs you can customize the BIOS in two ways: Copy-Host BIOS strings and User-Defined BIOS strings.

> **Note:**
>
> After you first start a VM, you cannot change its BIOS strings. Ensure that the BIOS strings are correct before starting the VM for the first time.

Copy-Host BIOS strings

The VM has a copy of the BIOS strings of a particular server in the pool. To install the BIOS-locked media that came with your host, follow the procedures given below.

Using XenCenter:

1. Click the **Copy host BIOS strings to VM** check box in the New VM Wizard.

Using the CLI:

1. Run the `vm-install copy-bios-strings-from` command. Specify the `host-uuid` as the host from which the strings are copied (that is, the host that the media was supplied with):

```
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
```

This command returns the UUID of the newly created VM.

For example:

```
xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786ef4 \
    template="win7sp1" sr-name-label=Local\ storage  \
    new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
```

2. If the relevant BIOS strings from the host have been successfully copied into the VM, the command `vm-is-bios-customized` confirms this success:

```
xe vm-is-bios-customized uuid=VM uuid
```

For example:

```
xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
    This VM is BIOS-customized.
```

> **Note:**
>
> When you start the VM, it is started on the physical host from which you copied the BIOS strings.

> **Warning:**
>
> It is your responsibility to comply with any EULAs governing the use of any BIOS-locked operating systems that you install.

User-defined BIOS strings

The user has option to set custom values in selected BIOS strings using CLI/API. To install the media in HVM VM with customized BIOS, follow the procedure given below.

Using the CLI:

1. Run the `vm-install` command (without `copy-bios-strings-from`):

```
xe vm-install template=template name sr-name-label=name of sr \
      new-name-label=name for new VM
```

This command returns the UUID of the newly created VM.

For example:

```
xe vm-install template="win7sp1" sr-name-label=Local\ storage  \
      new-name-label=newcentos
    7cd98710-bf56-2045-48b7-e4ae219799db
```

2. To set user-defined BIOS strings, run the following command before starting the VM for the first time:

```
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
```

For example:

```
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
```

Notes:

- Once the user-defined BIOS strings are set in a single CLI/API call, they cannot be modified.
- You can decide on the number of parameters you want to provide to set the user-defined BIOS strings.

Warning:

It is your responsibility to:

- Comply with any EULAs and standards for the values being set in VM's BIOS.

- Ensure that the values you provide for the parameters are working parameters. Providing incorrect parameters can lead to boot/media installation failure.

Assign a GPU to a Windows VM (for use with Citrix Virtual Desktops)

Citrix Hypervisor enables you to assign a physical GPU in the Citrix Hypervisor server to a Windows VM running on the same host. This GPU Pass-Through feature benefits graphics power users, such as CAD designers, who require high performance graphics capabilities. It is supported only for use with Citrix Virtual Desktops.

While Citrix Hypervisor supports only one GPU for each VM, it automatically detects and groups identical physical GPUs across hosts in the same pool. Once assigned to a group of GPUs, a VM may be started on any host in the pool that has an available GPU in the group. When attached to a GPU, a VM has certain features that are no longer available, including live migration, VM snapshots with memory, and suspend/resume.

Assigning a GPU to a VM in a pool does not interfere with the operation of other VMs in the pool. However, VMs with GPUs attached are considered non-agile. If VMs with GPUs attached are members of a pool with high availability enabled, both features overlook these VMs. The VMs cannot be migrated automatically.

GPU Pass-Through is available to Windows VMs only. It can be enabled using XenCenter or the xe CLI.

Requirements

GPU Pass-Through is supported for specific machines and GPUs. In all cases, the IOMMU chipset feature (known as VT-d for Intel models) must be available and enabled on the Citrix Hypervisor server. Before enabling the GPU Pass-Through feature, visit the Hardware Compatibility List.

Before assigning a GPU to a VM

Before you assign a GPU to a VM, put the appropriate physical GPUs in your Citrix Hypervisor server and then restart the machine. Upon restart, Citrix Hypervisor automatically detects any physical GPUs. To view all physical GPUs across hosts in the pool, use the `xe pgpu-list` command.

Ensure that the IOMMU chipset feature is enabled on the host. To do so, enter the following:

```
xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=iommu
```

If the value printed is `false`, IOMMU is not enabled, and GPU Pass-Through is not available using the specified Citrix Hypervisor server.

To assign a GPU to a Windows VM by using XenCenter:

1. Shut down the VM that you want to assign a GPU.
2. Open the VM properties: right-click the VM and select **Properties**.
3. Assign a GPU to the VM: Select GPU from the list of VM properties, and then select a GPU type. Click **OK**.

4. Start the VM.

To assign a GPU to a Windows VM by using the xe CLI:

1. Shut down the VM that you want to assign a GPU group by using the `xe vm-shutdown` command.
2. Find the UUID of the GPU group by entering the following:

   ```
   xe gpu-group-list
   ```

   This command prints all GPU groups in the pool. Note the UUID of the appropriate GPU group.
3. Attach the VM to a GPU group by entering the following:

   ```
   xe vpgu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
   ```

   To ensure that the GPU group has been attached, run the `xe vgpu-list` command.
4. Start the VM by using the `xe vm-start` command.
5. Once the VM starts, install the graphics card drivers on the VM.

   Installing the drivers is essential, as the VM has direct access to the hardware on the host. Drivers are provided by your hardware vendor.

> **Note:**
>
> If you try to start a VM with GPU Pass-Through on the host without an available GPU in the appropriate GPU group, Citrix Hypervisor prints an error.

To detach a Windows VM from a GPU by using XenCenter:

1. Shut down the VM.
2. Open the VM properties: right-click the VM and select **Properties**.
3. Detach the GPU from the VM: Select **GPU** from the list of VM properties, and then select **None** as the GPU type. Click **OK**.
4. Start the VM.

To detach a Windows VM from a GPU by using the xe CLI:

1. Shut down the VM by using the `xe vm-shutdown` command.
2. Find the UUID of the vGPU attached to the VM by entering the following:

   ```
   xe vgpu-list vm-uuid=uuid_of_vm
   ```

3. Detach the GPU from the VM by entering the following:

```
xe vgpu-destroy uuid=uuid_of_vgpu
```

4. Start the VM by using the `xe vm-start` command.

Create ISO images

Citrix Hypervisor can use ISO images as installation media and data sources for Windows or Linux VMs. This section describes how to make ISO images from CD/DVD media.

To create an ISO on a Linux system:

1. Put the CD- or DVD-ROM disk into the drive. Ensure that the disk is not mounted. To check, run the command:

   ```
   mount
   ```

   If the disk is mounted, unmount the disk. See your operating system documentation for assistance if necessary.

2. As root, run the command

   ```
   dd if=/dev/cdrom of=/path/cdimg_filename.iso
   ```

   This command takes some time. When the operation is completed successfully, you see something like:

   ```
   1187972+0 records in
   1187972+0 records out
   ```

   Your ISO file is ready.

To create an ISO on a Windows system:

Windows computers do not have an equivalent operating system command to create an ISO. Most CD-burning tools have a means of saving a CD as an ISO file.

Enable VNC for Linux VMs

VMs might not be set up to support Virtual Network Computing (VNC), which Citrix Hypervisor uses to control VMs remotely, by default. Before you can connect with XenCenter, ensure that the VNC server and an X display manager are installed on the VM and properly configured. This section describes how to configure VNC on each of the supported Linux operating system distributions to allow proper interactions with XenCenter.

For CentOS-based VMs, use the instructions for the Red Hat-based VMs below, as they use the same base code to provide graphical VNC access. CentOS *X* is based on Red Hat Enterprise Linux *X*.

Enable a graphical console on Debian VMs

> **Note:**
>
> Before enabling a graphical console on your Debian VM, ensure that you have installed the Citrix VM Tools for Linux. For more information, see Install the Citrix VM Tools for Linux.

The graphical console for Debian virtual machines is provided by a VNC server running inside the VM. In the recommended configuration, a standard display manager controls the console so that a login dialog box is provided.

1. Install your Debian guest with the desktop system packages, or install GDM (the display manager) using apt (following standard procedures).
2. Install the Xvnc server using `apt-get` (or similar):

   ```
   apt-get install vnc4server
   ```

   > **Note:**
   >
   > The Debian Graphical Desktop Environment, which uses the Gnome Display Manager version 3 daemon, can take significant CPU time. Uninstall the Gnome Display Manager `gdm3` package and install the `gdm` package as follows:

   ```
   apt-get install gdm
   apt-get purge gdm3
   ```

3. Set up a VNC password (not having one is a serious security risk) by using the `vncpasswd` command. Pass in a file name to write the password information to. For example:

   ```
   vncpasswd /etc/vncpass
   ```

4. Modify your `gdm.conf` file (`/etc/gdm/gdm.conf`) to configure a VNC server to manage display `0` by extending the `[servers]` and `[daemon]` sections as follows:

```
    [servers]
    0=VNC
    [daemon]
    VTAllocation=false
    [server-VNC]
    name=VNC
    command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/vncpass
BlacklistTimeout=0
    flexible=true
```

5. Restart GDM, and then wait for XenCenter to detect the graphical console:

```
/etc/init.d/gdm restart
```

Note:

You can check that the VNC server is running using a command like `ps ax | grep vnc`.

Enable a graphical console on Red Hat, CentOS, or Oracle Linux VMs

Note:

Before setting up your Red Hat VMs for VNC, be sure that you have installed the Citrix VM Tools for Linux. For more information, see Install the Citrix VM Tools for Linux.

To configure VNC on Red Hat VMs, modify the GDM configuration. The GDM configuration is held in a file whose location varies depending on the version of Red Hat Linux you are using. Before modifying it, first determine the location of this configuration file. This file is modified in several subsequent procedures in this section.

Determine the location of your VNC configuration file

If you are using Red Hat Linux, the GDM configuration file is `/etc/gdm/custom.conf`. This file is a split configuration file that contains only user-specified values that override the default configuration. This type of file is used by default in newer versions of GDM. It is included in these versions of Red Hat Linux.

Configure GDM to use VNC

1. As root on the text CLI in the VM, run the command `rpm -q vnc-server gdm`. The package names `vnc-server` and `gdm` appear, with their version numbers specified.

The package names that are displayed show the packages that are already installed. If you see a message that says that a package is not installed, you might have not selected the graphical desktop options during installation. Install these packages before you can continue. For details regarding installing more software on your VM, see the appropriate Red Hat Linux x86 Installation Guide.

2. Open the GDM configuration file with your preferred text editor and add the following lines to the file:

```
[server-VNC]
name=VNC Server
command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -depth 16 \
-BlacklistTimeout 0
flexible=true
```

   With configuration files on Red Hat Linux, add these lines into the empty `[servers]` section.

3. Modify the configuration so that the `Xvnc` server is used instead of the standard X server:

   - `0=Standard`

     Modify it to read:

     `0=VNC`

   - If you are using Red Hat Linux, add the above line just below the `[servers]` section and before the `[server-VNC]` section.

4. Save and close the file.

Restart GDM for your change in configuration to take effect, by running the command `/usr/sbin/gdm-restart`.

> **Note:**
>
> Red Hat Linux uses runlevel 5 for graphical startup. If your installation starts up in runlevel 3, change this configuration for the display manager to be started and get access to a graphical console. For more information, see Check Run levels.

Firewall settings

The firewall configuration by default does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, allow traffic over the port that the VNC connection uses. By default, a VNC server listens for connections from a VNC viewer on TCP port `5900 + n`, where `n` is the display number (usually zero). So a VNC server setup for Display-0 listens on TCP port `5900`, Display-1 is `TCP-5901`, and so on. Consult your firewall documentation to ensure that these ports are open.

If you want to use IP connection tracking or limit the initiation of connections to be from one side only, further configure your firewall.

To configure Red Hat-base VMS firewall to open the VNC port:

1. For Red Hat Linux, use `system-config-securitylevel-tui`.
2. Select **Customize** and add `5900` to the other ports list.

Alternatively, you can disable the firewall until the next reboot by running the command `service iptables stop`, or permanently by running `chkconfig iptables off`. This configuration can expose extra services to the outside world and reduce the overall security of your VM.

VNC screen resolution

After connecting to a VM with the graphical console, the screen resolution sometimes doesn't match. For example, the VM display is too large to fit comfortably in the Graphical Console pane. Control this behavior by setting the VNC server `geometry` parameter as follows:

1. Open the GDM configuration file with your preferred text editor. For more information, see Determine the Location of your VNC Configuration File.
2. Find the `[server-VNC]` section you added above.
3. Edit the command line to read, for example:

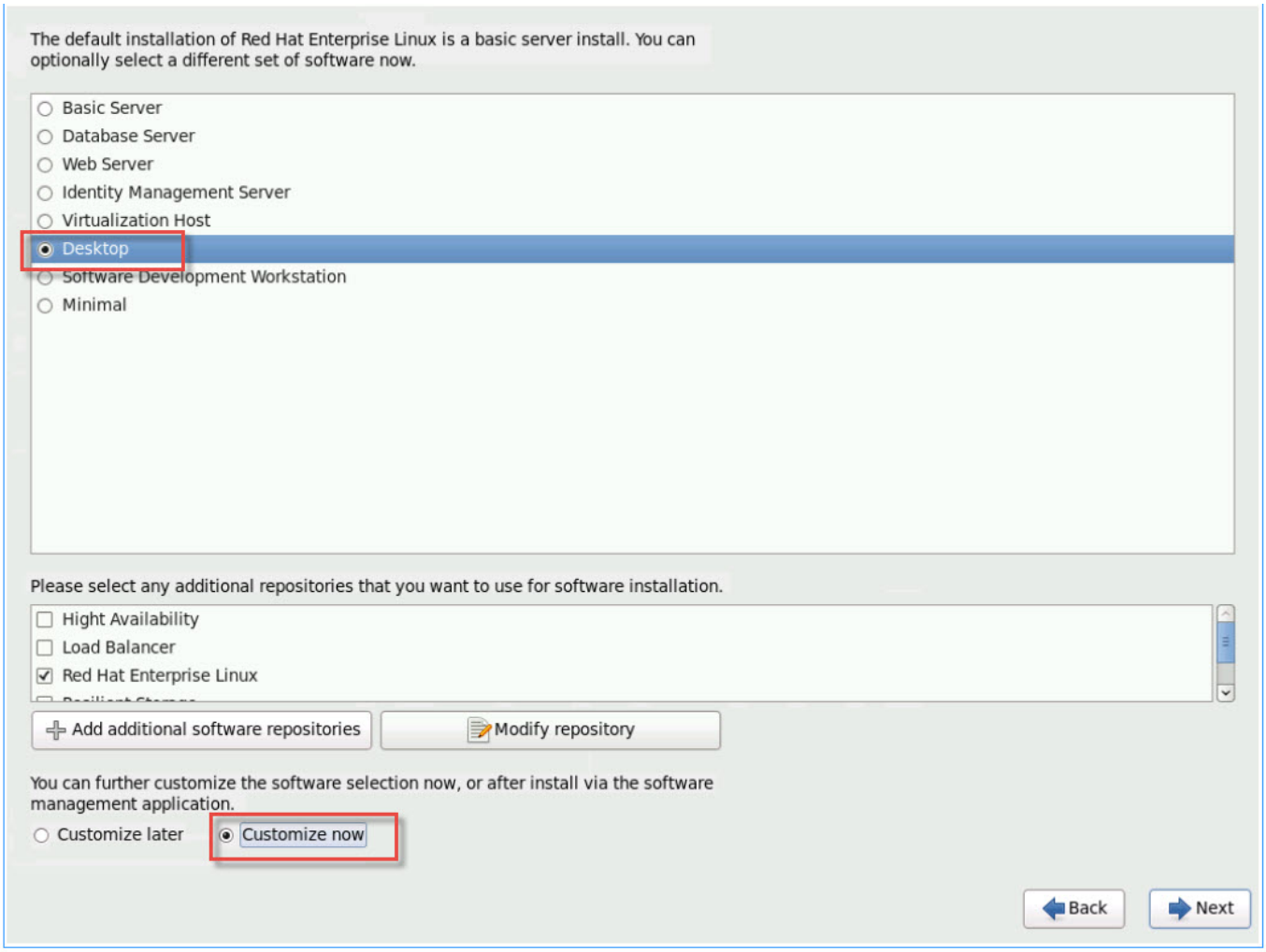
   ```
   command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
   ```

   The value of the `geometry` parameter can be any valid screen width and height.
4. Save and close the file.

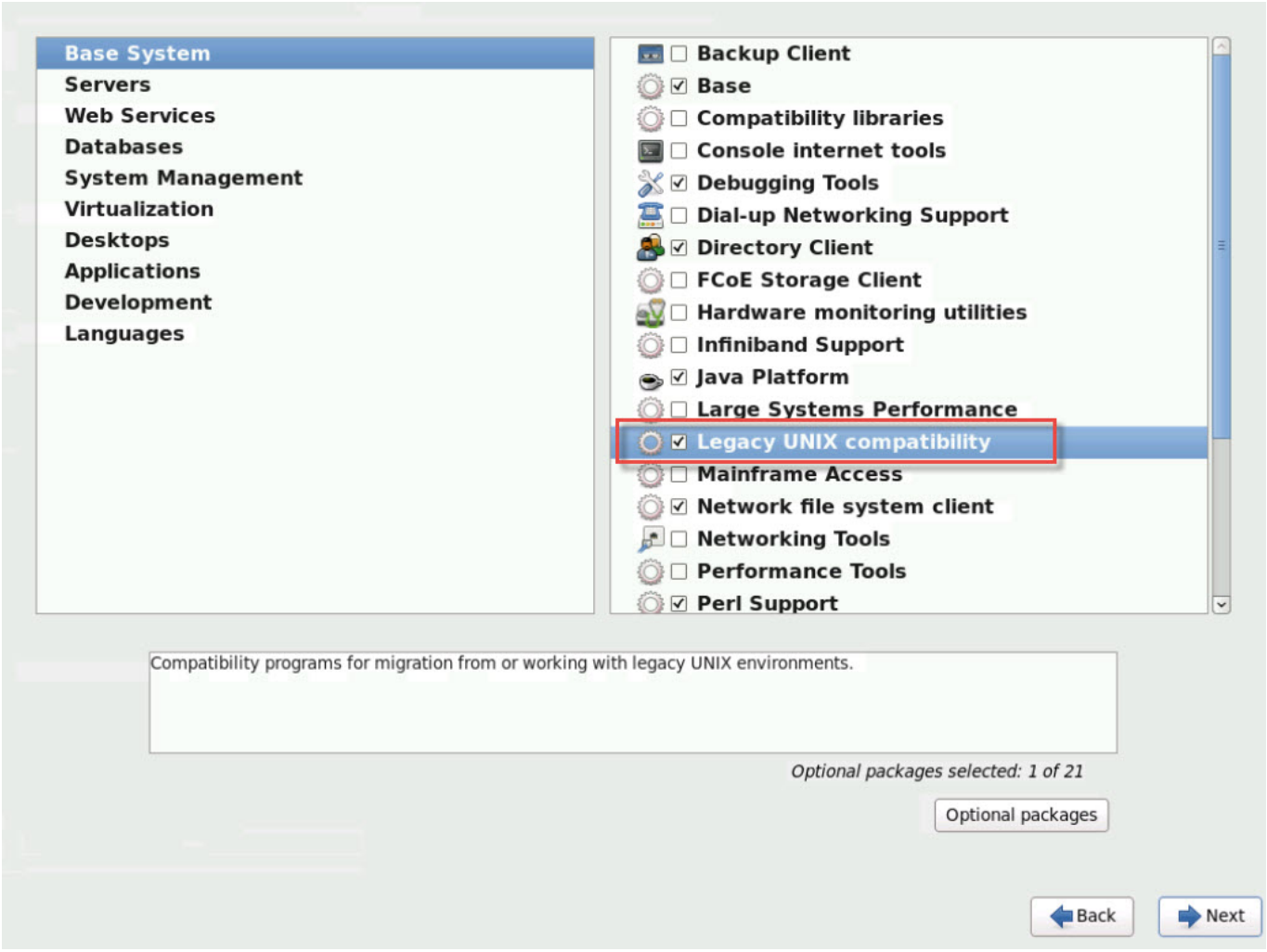
Enable VNC for RHEL, CentOS, or OEL VMs

If you are using Red Hat Linux, the GDM configuration file is `/etc/gdm/custom.conf`. This file is a split configuration file that contains only user-specified values that override the default configuration. By default, this type of file is used in newer versions of GDM and is included in these versions of Red Hat Linux.

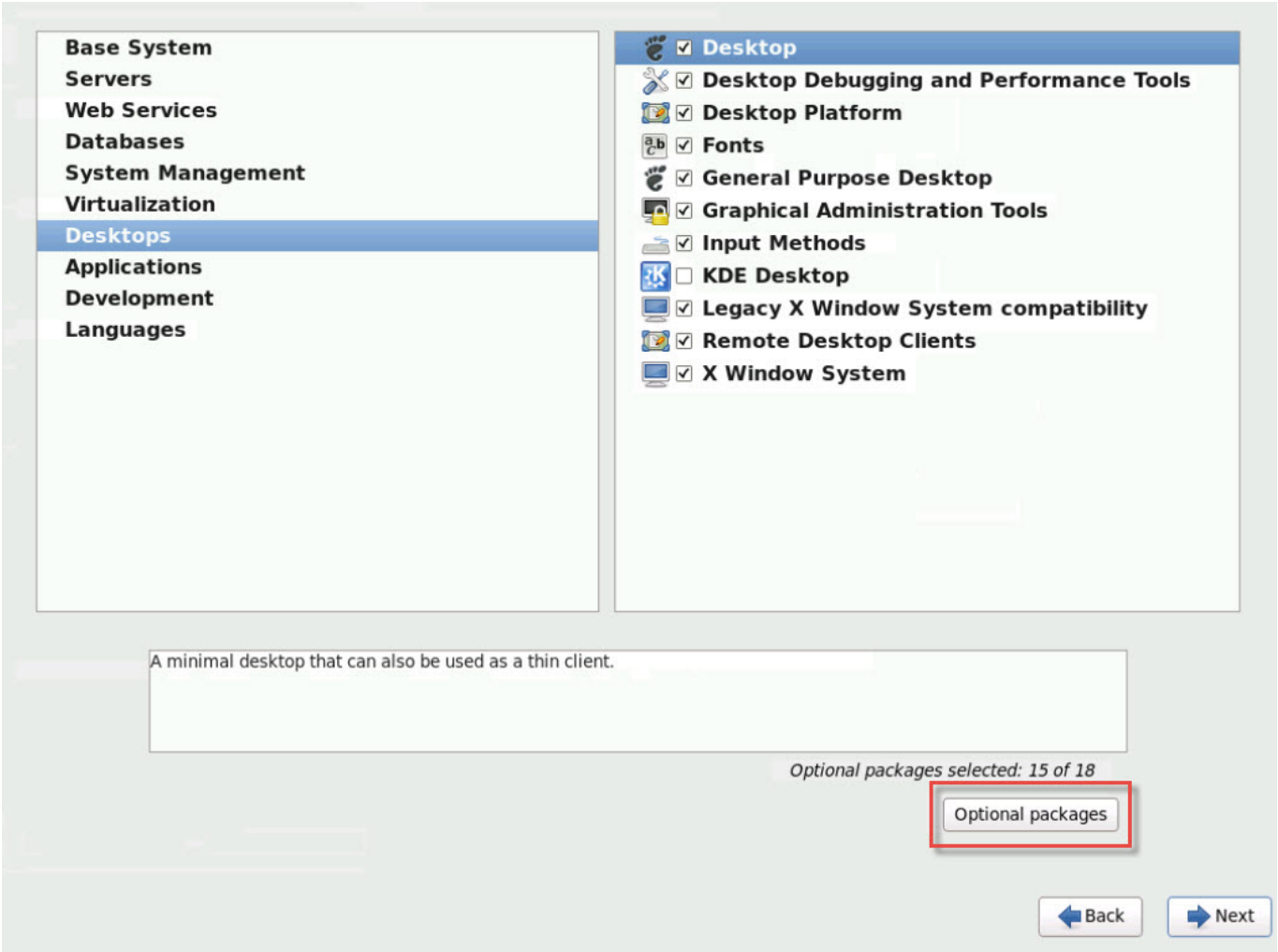
During the operating system installation, select **Desktop** mode. On the RHEL installation screen, select **Desktop** > **Customize now** and then click **Next**:



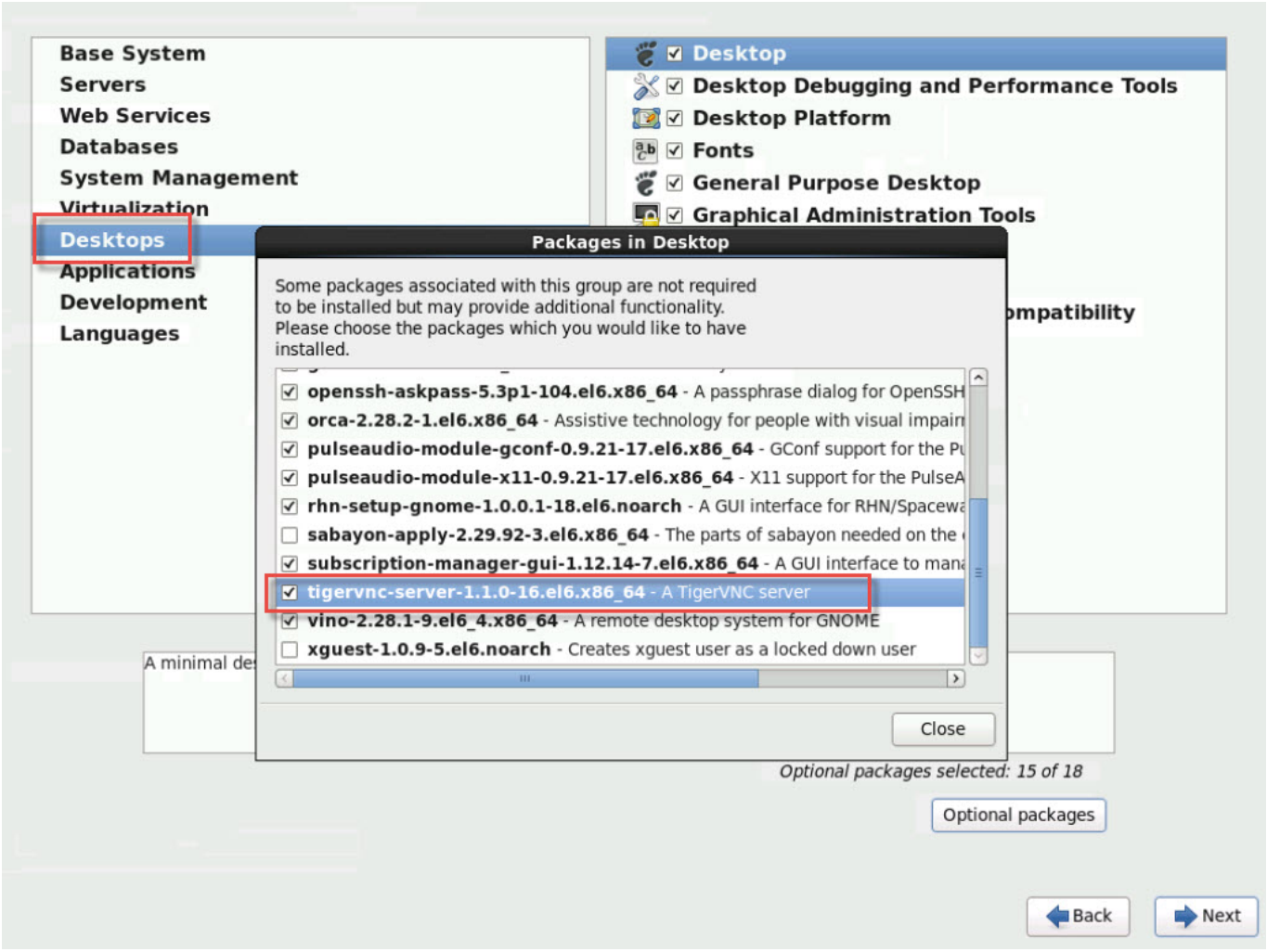
This action displays the Base System screen, ensure that **Legacy UNIX compatibility** is selected:



Select **Desktops** > **Optional packages**, then click **Next**:



This action displays the **Packages in Desktop** window, select **tigervnc-server-<version_number>** and then click **Next**:



Work through the following steps to continue the setup of your RHEL VMs:

1. Open the GDM configuration file with your preferred text editor and add the following lines to the appropriate sections:

```
[security]
DisallowTCP=false

[xdmcp]
Enable=true
```

2. Create the file, `/etc/xinetd.d/vnc-server-stream`:

```
service vnc-server
{
              id = vnc-server
         disable = no
            type = UNLISTED
            port = 5900
     socket_type = stream
            wait = no
            user = nobody
           group = tty
```

```
            server = /usr/bin/Xvnc
        server_args = -inetd -once -query localhost -SecurityTypes None \
        -geometry 800x600 -depth 16
    }
```

3. Enter the following command to start the `xinetd` service:

```
# service xinetd start
```

4. Open the file `/etc/sysconfig/iptables`. Add the following line above the line reading, `-A INPUT -j REJECT --reject-with icmp-host-prohibited`:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

5. Enter the following command to restart `iptables`:

```
# service iptables restart
```

6. Enter the following command to restart `gdm`:

```
    # telinit 3
    # telinit 5
```

Note:

Red Hat Linux uses runlevel 5 for graphical startup. If your installation starts up in runlevel 3, change this configuration for the display manager be started and to get access to a graphical console. For more information, see Check run levels.

Set up SLES-based VMs for VNC

Note:

Before setting up your SUSE Linux Enterprise Server VMs for VNC, be sure that you have installed the Citrix VM Tools for Linux. See Install the Citrix VM Tools for Linux for details.

SLES has support for enabling “Remote Administration” as a configuration option in `YaST`. You can select to enable Remote Administration at install time, available on the **Network Services** screen of the SLES installer. This feature allows you to connect an external VNC viewer to your guest to allow you to view the graphical console. The method for using the SLES remote administration feature is slightly different than the method

provided by XenCenter. However, it is possible to modify the configuration files in your SUSE Linux VM such that it is integrated with the graphical console feature.

Check for a VNC server

Before making configuration changes, verify that you have a VNC server installed. SUSE ships the `tightvnc` server by default. This server is a suitable VNC server, but you can also use the standard RealVNC distribution.

You can check that you have the `tightvnc` software installed by running the command:

```
rpm -q tightvnc
```

Enable remote administration

If Remote Administration was not enabled during installation of the SLES software, you can enable it as follows:

1. Open a text console on the VM and run the `YaST` utility:

   ```
   yast
   ```

2. Use the arrow keys to select **Network Services** in the left menu. **Tab** to the right menu and use the arrow keys to select **Remote Administration**. Press **Enter**.

3. In the **Remote Administration** screen, **Tab** to the **Remote Administration Settings** section. Use the arrow keys to select **Allow Remote Administration** and press **Enter** to place an X in the check box.

4. **Tab** to the **Firewall Settings** section. Use the arrow keys to select **Open Port in Firewall** and press **Enter** to place an X in the check box.

5. **Tab** to the **Finish** button and press **Enter**.

6. A message box is displayed, telling you to restart the display manager for your settings to take effect. Press **Enter** to acknowledge the message.

7. The original top-level menu of `YaST` appears. **Tab** to the **Quit** button and press **Enter**.

Modify the `xinetd` configuration

After enabling Remote Administration, modify a configuration file if you want to allow XenCenter to connect. Alternatively, use a third party VNC client.

1. Open the file `/etc/xinetd.d/vnc` in your preferred text editor.

2. The file contains sections like the following:

   ```
   ```

```
    service vnc1
    {
    socket_type = stream
    protocol    = tcp
    wait        = no
    user        = nobody
    server      = /usr/X11R6/bin/Xvnc
    server_args = :42 -inetd -once -query localhost -geometry 1024x768 -depth
16
    type        = UNLISTED
    port        = 5901
    }
```

3. Edit the `port` line to read

```
port = 5900
```

4. Save and close the file.

5. Restart the display manager and `xinetd` service with the following commands:

```
/etc/init.d/xinetd restart
rcxdm restart
```

SUSE Linux uses runlevel 5 for graphical startup. If your remote desktop does not appear, verify that your VM is configured to start up in runlevel 5. For more information, see Check Run levels.

Firewall settings

By default the firewall configuration does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, allow traffic over the port that the VNC connection uses. By default, a VNC server listens for connections from a VNC viewer on TCP port `5900 + n`, where `n` is the display number (usually zero). So a VNC server setup for Display-0 listens on TCP port `5900`, Display-1 is `TCP-5901`, and so forth. Consult your firewall documentation to ensure that these ports are open.

If you want to use IP connection tracking or limit the initiation of connections to be from one side only, further configure your firewall.

To Open the VNC Port on SLES 11.x VMs Firewall:

1. Open a text console on the VM and run the `YaST` utility:

```
yast
```

2. Use the arrow keys to select **Security and Users** in the left menu. **Tab** to the right menu and use the arrow keys to select **Firewall**. Press **Enter**.
3. In the **Firewall** screen, use the arrow keys to select **Custom Rules** in the left menu and then press **Enter**.
4. **Tab** to the **Add** button in the **Custom Allowed Rules** section and then press **Enter**.
5. In the **Source Network** field, enter *0/0*. **Tab** to the **Destination Port** field and enter *5900*.
6. **Tab** to the **Add** button and then press **Enter**.
7. **Tab** to the **Next** button and press **Enter**.
8. In the **Summary** screen **Tab** to the **Finish** button and press **Enter**.
9. On the top-level `YaST` screen **Tab** to the **Quit** button and press **Enter**.
10. Restart the display manager and `xinetd` service with the following commands:

```
/etc/init.d/xinetd restart
rcxdm restart
```

Alternatively, you can disable the firewall until the next reboot by running the **rcSuSEfirewall2 stop** command, or permanently by using `YaST`. This configuration can expose extra services to the outside world and reduce the overall security of your VM.

VNC screen resolution

After connecting to a Virtual Machine with the Graphical Console, the screen resolution sometimes does not match. For example, the VM display is too large to fit comfortably in the Graphical Console pane. Control this behavior by setting the VNC server `geometry` parameter as follows:

1. Open the `/etc/xinetd.d/vnc` file with your preferred text editor and find the `service_vnc1` section (corresponding to `displayID` 1).
2. Edit the `geometry` argument in the `server-args` line to the desired display resolution. For example,

```
server_args  = :42 -inetd -once -query localhost -geometry 800x600 -depth 16
```

   The value of the `geometry` parameter can be any valid screen width and height.

3. Save and close the file.
4. Restart the VNC server:

```
/etc/init.d/xinetd restart
rcxdm restart
```

Check run levels

Red Hat and SUSE Linux VMs use runlevel 5 for graphical startup. This section describes how to verify that your VM starts up in runlevel 5 and how to change this setting.

1. Check `/etc/inittab` to see what the default runlevel is set to. Look for the line that reads:

   ```
   id:n:initdefault:
   ```

   If *n* is not 5, edit the file to make it so.

2. You can run the command `telinit q ; telinit 5` after this change to avoid having to reboot to switch run levels.

Troubleshoot VM problems

Citrix provides two forms of support:

- Free, self-help support on the Citrix website
- Paid-for Support Services, which you can purchase from the Support Site.

With Citrix Technical Support, you can open a Support Case online or contact the support center by phone if you experience technical difficulties.

The Citrix Support site hosts several resources that might be helpful to you if you experience unusual behavior, crashes, or other problems. Resources include: Support Forums, Knowledge Base articles, and product documentation.

If you see unusual VM behavior, this section aims to help you solve the problem. This section describes where application logs are located and other information that can help your Citrix Hypervisor Solution Provider track and resolve the issue.

> **Important:**
>
> Follow the troubleshooting information in this section only under the guidance of your Citrix Hypervisor Solution Provider or the Support Team.
>
> Vendor Updates: Keep your VMs up-to-date with operating system vendor-supplied updates. The vendor might have provided fixes for VM crashed and other failures.

VM crashes

If you are experiencing VM crashes, it is possible that a kernel crash dump can help identify the problem. Reproduce the crash, if possible, and follow this procedure. Consult your guest OS vendor for further investigation on this issue.

Control Linux VM crashdump behavior

For Linux VMs, the crashdump behavior can be controlled through the `actions-after-crash` parameter. The following are the possible values:

Value	Description
`preserve`	Leave the VM in a paused state. (For analysis)
`restart`	No core dump, reboot VM. (This is the default)
`destroy`	No core dump, leave VM halted.

To enable saving of Linux VM crash dumps:

1. On the Citrix Hypervisor server, determine the UUID of the desired VM by running the following command:

```
xe vm-list name-label=name params=uuid --minimal
```

2. Change the `actions-after-crash` value using `xe vm-param-set`; for example, run the following command on dom0:

```
xe vm-param-set uuid=vm_uuid actions-after-crash=preserve
```

3. Crash the VM.
   - For PV guests, run the following command on the VM:

```
echo c | sudo tee /proc/sysrq-trigger
```

4. Execute the dump core command on dom0. For example, run:

```
xl dump-core domid filename
```

Control Windows VM crashdump behavior

For Windows VMs, the `actions-after-crash` parameter cannot control the core dump behavior. By default Windows crash dumps are put into `%SystemRoot%\Minidump` in the Windows VM itself.

You can configure the VMs dump level by following the menu path **My Computer > Properties > Advanced > Startup and Recovery**.

Troubleshoot boot problems on Linux VMs

There is a utility script named `xe-edit-bootloader` in the Citrix Hypervisor server control domain. This script can be used to edit the bootloader configuration of a shutdown Linux VM and fix problems that prevent the VM from booting.

To use this script:

1. Run the following command:

```
xe vm-list
```

   This command ensures that the VM in question is shut down (the value of *power-state* is *halted*).

2. You can use the UUID as follows:

```
xe-edit-bootloader -u linux_vm_uuid -p partition_number
```

```
```

Or, you can use the name-label as follows:

```
xe-edit-bootloader -n linux_vm_name_label -p partition_number
```

The partition number represents the slice of the disk which has the filesystem. For the default Debian template, the partition number is *1* since it is the first partition.

3. You are dropped into an editor with the `grub.conf` file for the specified VM loaded. Change the file to fix it, and save the file, exit the editor, and start the VM.

Troubleshoot UEFI and Secure Boot problems on Windows VMs

How do I change the screen resolution of the XenCenter console on a UEFI-enabled VM?

To change the screen resolution of the XenCenter console on a UEFI-enabled VM:

1. Open the **Windows Settings**
2. Click the **Update & Security** button
3. Under the recovery tab, press the **Restart now** button.
4. Navigate to **Troubleshoot** > **Advanced Options** > **UEFI firmware settings**.
5. Press **Restart**. During restart, the UEFI settings menu loads.
6. Navigate to **Device Manager** > **OVMF Platform Configuration**. This displays the current screen resolution.
7. Press **Enter** to see the screen resolution options.
8. Use the arrow keys to select the desired screen resolution and press **Enter**.
9. Press **F10** to save the changes and confirm your choice.
10. Reboot the VM to see the XenCenter console in an updated screen resolution.

Why can't I create a UEFI Secure Boot VM?

Check that your VM operating system supports UEFI Secure Boot mode. In Citrix Hypervisor 8.2, only the following operating systems support Secure Boot: Windows 10 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit), Windows Server 2022 (64-bit).

Check that your Citrix Hypervisor server is booted in UEFI mode. You can only create UEFI Secure Boot VMs on a Citrix Hypervisor server that has the Secure Boot certificates present. Secure Boot certificates are only present on servers booted in UEFI mode or servers in the same pool as a server booted in UEFI mode. For more information, see Network Boot.

Check that the UEFI-booted Citrix Hypervisor server is included in the Hardware Compatibility List. Older servers might not include the Secure Boot certificates when booted in UEFI mode.

How do I know if the Citrix Hypervisor server that I create a Secure Boot VM on has the Secure Boot certificates?

If your Citrix Hypervisor server is booted in UEFI mode, the Secure Boot certificates are available on the server. Citrix Hypervisor servers share their certificates with other servers in the same resource pool. If you

have a UEFI booted server in your resource pool, all servers in that pool have the Secure Boot certificates available.

Run the following command on a Citrix Hypervisor server:

```
xe pool-param-get param-name=uefi-certificates uuid=<pool-uuid> | wc -c
```

If it returns a value that is greater than zero, the Secure Boot certificates are present.

To check that the certificates are valid, run the following command on your Citrix Hypervisor server:

```
xe pool-param-get uuid=$(xe pool-list --minimal)  param-name=uefi-
certificates|base64 -d|tar tv
-rw-r--r-- root/root      1600 2019-11-11 17:09 KEK.auth
-rw-r--r-- root/root      3212 2019-11-11 17:09 db.auth
```

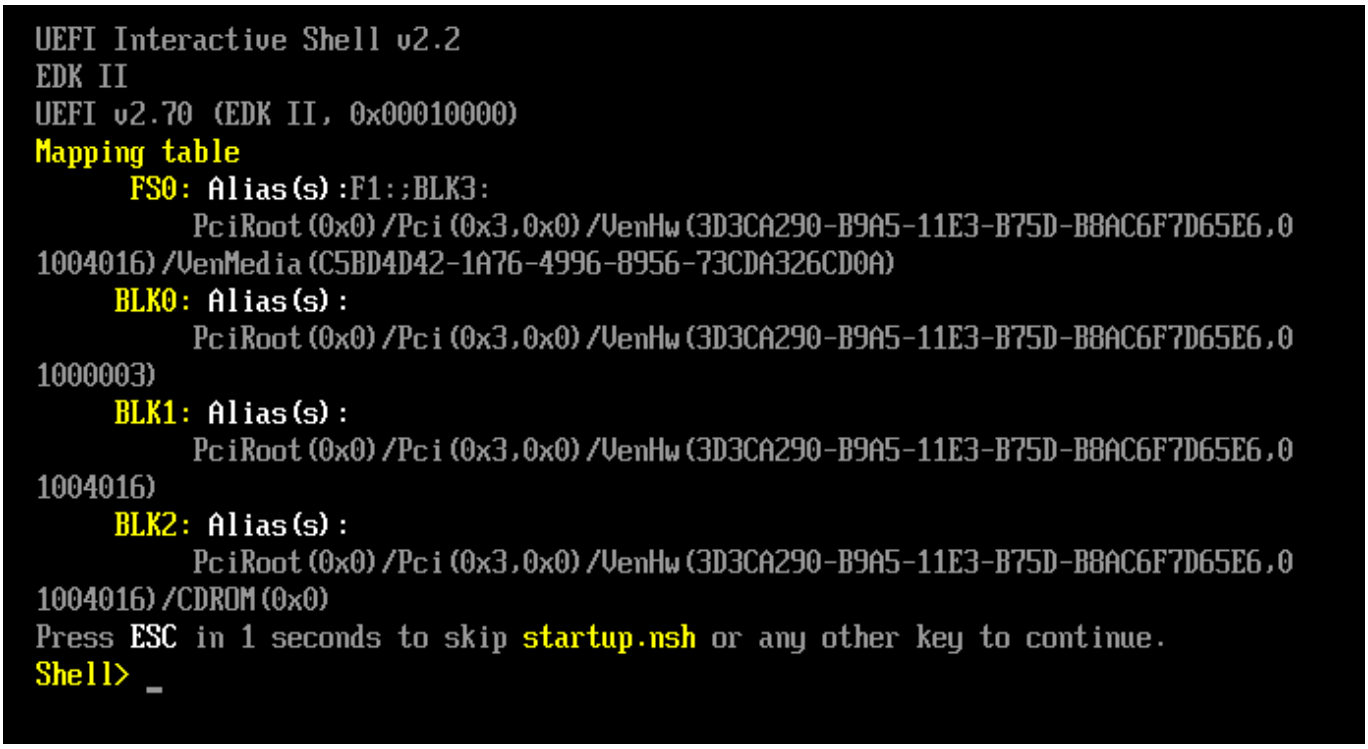
If the Secure Boot certificates are absent, run the following command on your Citrix Hypervisor server:

```
ls /sys/firmware/efi/efivars | grep KEK
```

If this command returns empty, Secure Boot VMs cannot be created on that server because the the required certificates are missing from the UEFI firmware.

Why is my UEFI Secure Boot VM failing to start?

If you see the following messages on the console of your UEFI Secure Boot VM and an alert in XenCenter, the Secure Boot process has failed and your VM does not start.



This is usually caused by the installation of unsigned drivers into the VM. Investigate what drivers have been updated or installed since the last successful Secure Boot.

You can disable Secure Boot and start the VM in setup mode to remove the unsigned drivers.

> **Important:**
>
> Before doing this, back up your VM by taking a snapshot.

To change a UEFI Secure Boot VM into a UEFI boot VM, run the following command on the Citrix Hypervisor server that hosts the VM:

```
varstore-sb-state <VM_UUID> setup
```

After you have fixed your VM, run the following command to re-enable Secure Boot:

```
varstore-sb-state <VM_UUID> user
```

Is Secure Boot causing an issue on my Windows VM?

To diagnose whether an issue on your Windows VM is caused by Secure Boot being enabled for the VM, disable Secure Boot and try to reproduce the issue.

To disable Secure Boot, run the following command on the Citrix Hypervisor server that hosts the VM:

```
varstore-sb-state <VM_UUID> setup
```

After you have debugged the issue, you can run the following command to re-enable Secure Boot:

```
varstore-sb-state <VM_UUID> user
```

How do I run Windows debug on a Secure Boot VM?

You cannot run Windows debug on a Secure Boot VM. To run Windows debug on your VM, you can do one of the following things:

- Switch your VM to UEFI boot mode by running the following command:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=false
  ```

  Reboot the VM.

  After you have debugged the issue, you can run the following command to re-enable Secure Boot:

  ```
  xe vm-param-set uuid=<UUID> platform:secureboot=auto
  ```

  Reboot the VM.

- Disable Secure Boot by running the following command on the Citrix Hypervisor server that hosts the VM:

  ```
  varstore-sb-state <VM_UUID> setup
  ```

  After you have debugged the issue, you can run the following command to re-enable Secure Boot:

  ```
  varstore-sb-state <VM_UUID> user
  ```

Why are only two NICs showing up for my UEFI VM?

Even if you set up more than two NICs when you created your UEFI-enabled VM, when the VM first starts you only see two NICs. This information displays correctly after the Citrix VM Tools for Windows have been installed in the VM.

Why are my emulated devices showing as different types than expected?

A UEFI Secure Boot VMs use NVME and E1000 for emulated devices. However, when the VM first starts the emulated devices show as different types. This information displays correctly after the Citrix VM Tools for Windows have been installed in the VM.

Why can't I convert my templates from BIOS mode to UEFI or UEFI Secure Boot mode?

You can only create a UEFI-enabled VM template from a template supplied with Citrix Hypervisor.

Do not use the `xe template-param-set` command for templates that have something installed on them or templates that you created from a snapshot. The boot mode of these snapshots cannot be changed and, if you attempt to change the boot mode, the VM fails to boot.

How do I check UEFI and UEFI Secure Boot variables?

On the Citrix Hypervisor server where the UEFI or UEFI Secure Boot VM is hosted, run the following commands:

```
varstore-ls
```

This command lists the GUIDs and names of the available variables. Use the GUID and name in the following command:

```
varstore-get <VM_ID> <GUID> <name> | hexdump -C
```

Why can't I use a 'test' driver with a Secure Boot VM?

If a customer is also working with a third party to debug and fix issues in their UEFI Secure Boot VM, the third party provide might provide unsigned drivers for test or verification purpose. These drivers will not work in a UEFI Secure Boot VM.

Tell the customer to request a signed driver from the third party. Or the customer can switch their UEFI Secure Boot VM into setup mode to run with the unsigned driver.

Troubleshooting

Support

Citrix provides two forms of support: free, self-help support on the Citrix Support website and paid-for Support Services, which you can purchase from the Support site. With Citrix Technical Support, you can open a Support Case online or contact the support center by phone if you experience technical difficulties.

The Citrix Knowledge Center hosts several resources that might be helpful to you in the event of odd behavior, crashes, or other problems. Resources include: Forums, Knowledge Base articles, White Papers, product documentation, hotfixes, and other updates.

If you experience technical difficulties with the Citrix Hypervisor server, this section is meant to help you solve the problem if possible. If it isn't possible, use the information in this section to gather the application logs and other data that can help your Solution Provider track and resolve the issue.

For information about troubleshooting Citrix Hypervisor installation issues, see Troubleshoot the installation. For information about troubleshooting virtual machine issues, see Troubleshoot VM problems.

> **Important:**
>
> We recommend that you follow the troubleshooting information in this section solely under the guidance of your Solution Provider or the Support team.

In some support cases, serial console access is required for debug purposes. Therefore, when setting up your Citrix Hypervisor configuration, it is recommended that serial console access is configured. For hosts that do not have physical serial port (such as a Blade server) or where suitable physical infrastructure is not available, investigate whether an embedded management device, such as Dell DRAC can be configured.

For information on setting up serial console access, see CTX121442.

Health Check

Use the Health Check feature to generate and upload the server status report to Citrix Insight Services (CIS) and to receive CIS analysis reports in XenCenter.

When you connect any eligible pool to XenCenter, you are prompted to enable Health Check for the pool. During the enrollment process, you can take the following actions:

- Specify the schedule to use for uploading the server status report automatically to CIS
- Enter Citrix Hypervisor credentials that are used to establish a connection with the pool
- Authenticate your uploads with CIS

After the pool is successfully enrolled to Health Check, you receive notifications in XenCenter regarding the health of the pool. This feature enables you to monitor proactively the health of the Citrix Hypervisor systems based on the report that CIS generates.

Requirements

To use the Health Check feature:

- All hosts in the pool must be running Citrix Hypervisor 8.2
- Connect to the Citrix Hypervisor pool using XenCenter shipped with Citrix Hypervisor 8.2
- XenCenter must have access to the internet
- The Health Check Service must be installed and running on the XenCenter machine.
- If using Active Directory (AD), you must have a Pool Operator or a higher role

For detailed information about Health Check and for step-by-step instructions on enrolling a pool to Health Check, see Health Check.

Citrix Hypervisor server logs

XenCenter can be used to gather Citrix Hypervisor server information.

Click **Server Status Report** in the **Tools** menu to open the **Server Status Report** task. You can select from a list of different types of information (various logs, crash dumps, and so on). The information is compiled and downloaded to the machine that XenCenter is running on. For more information, see the XenCenter documentation.

By default, the files gathered for a server status report can be limited in size. If you need log files that are larger than the default, you can run the command `xenserver-status-report -u` in the Citrix Hypervisor server console.

Additionally, the Citrix Hypervisor server has several CLI commands that collate the output of logs and various other bits of system information using the utility `xen-bugtool`. Use the xe command `host-bugreport-upload` to collect the appropriate log files and system information and upload them to the Support FTP site. For a full description of this command and its optional parameters, see `host-bugreport-upload` . If you are requested to send a crashdump to the Support team, use the xe command `host-crashdump-upload`. For a full description of this command and its optional parameters, see `host-crashdump-upload`.

> **Important:**
>
> Citrix Hypervisor server logs may contain sensitive information.

Sending host log messages to a central server

Rather than have logs written to the control domain filesystem, you can configure your Citrix Hypervisor server to write them to a remote server. The remote server must have the `syslogd` daemon running on it to receive the logs and aggregate them correctly. The `syslogd` daemon is a standard part of all flavors of Linux and Unix, and third-party versions are available for Windows and other operating systems.

Set the syslog_destination parameter to the hostname or IP address of the remote server where you want the logs to be written:

```
xe host-param-set uuid=BRAND_SERVER_host_uuid logging:syslog_destination=hostname
```

Run the command:

```
xe host-syslog-reconfigure uuid= BRAND_SERVER_host_uuid
```

To enforce the change. (You can also execute this command remotely by specifying the `host` parameter.)

XenCenter logs

XenCenter also has client-side log. This file includes a complete description of all operations and errors that occur when using XenCenter. It also contains informational logging of events that provide you with an audit trail of various actions that have occurred. The XenCenter log file is stored in your profile folder. If XenCenter is installed on Windows 2008, the path is

`%userprofile%\AppData\Citrix\XenCenter\logs\XenCenter.log`

If XenCenter is installed on Windows 8.1, the path is

`%userprofile%\AppData\Citrix\Roaming\XenCenter\logs\XenCenter.log`

To locate the XenCenter log files - for example, when you want to open or email the log file - click **View Application Log Files** in the XenCenter **Help** menu.

Troubleshooting connections between XenCenter and the Citrix Hypervisor server

If you have trouble connecting to the Citrix Hypervisor server with XenCenter, check the following:

- Is your XenCenter an older version than the Citrix Hypervisor server you are attempting to connect to?

  The XenCenter application is backward-compatible and can communicate properly with older Citrix Hypervisor servers, but an older XenCenter cannot communicate properly with newer Citrix Hypervisor servers.

  To correct this issue, install the XenCenter version that is the same, or newer, than the Citrix Hypervisor server version.

- Is your license current?

  You can see the expiration date for your license access code in the Citrix Hypervisor server **General** tab under the **License Details** section in XenCenter.

  For more information on licensing a host, see Licensing.

- The Citrix Hypervisor server talks to XenCenter using HTTPS over the following ports:

  - Port 443 (a two-way connection for commands and responses using the management API)
  - Port 5900 for graphical VNC connections with paravirtualized Linux VMs.

If you have a firewall enabled between the Citrix Hypervisor server and the machine running the client software, ensure that it allows traffic from these ports.

Other troubleshooting information

The following articles provide troubleshooting information about specific areas of the product:

- Install troubleshooting
- VM troubleshooting
- Networking troubleshooting

Command-line interface

The *xe* CLI enables you to script and automate system administration tasks. Use the CLI to integrate Citrix Hypervisor into an existing IT infrastructure.

Installing the xe CLI

The xe command line interface is installed by default on all Citrix Hypervisor servers and is included with XenCenter. A stand-alone remote CLI is also available for Linux.

On Windows

On Windows, the `xe.exe` command is installed along with XenCenter.

To use the `xe.exe` command, open a Windows Command Prompt and change directories to the directory where the `xe.exe` file is located (typically `C:\Program Files\Citrix\XenCenter`). If you add the `xe.exe` installation location to your system path, you can use the command without having to change into the directory.

On Linux

On RPM-based distributions (such as Red Hat), you can install the stand-alone xe command from the RPM named `client_install/xapi-xe-BUILD.x86_64.rpm` on the main Citrix Hypervisor installation ISO.

To install from the RPM, use the following command:

```
rpm -ivh xapi-xe-BUILD.x86_64.rpm
```

You can use parameters at the command line to define the Citrix Hypervisor server, user name, and password to use when running xe commands. However, you also have the option to set this information as an environment variable. For example:

```
export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password=<password>"
```

Note:

The remote xe CLI on Linux might hang when attempting to run commands over a secure connection and these commands involve file transfer. If so, you can use the `--no-ssl` parameter to run the command over an insecure connection to the Citrix Hypervisor server.

Getting help with xe commands

Basic help is available for CLI commands on-host by typing:

```
xe help command
```

A list of the most commonly used xe commands is displayed if you type:

```
xe help
```

Or a list of all xe commands is displayed if you type:

```
xe help --all
```

Basic xe syntax

The basic syntax of all Citrix Hypervisor xe CLI commands is:

```
xe command-name argument=value argument=value
```

Each specific command contains its own set of arguments that are of the form `argument=value`. Some commands have required arguments, and most have some set of optional arguments. Typically a command assumes default values for some of the optional arguments when invoked without them.

If the xe command runs remotely, extra arguments are used to connect and authenticate. These arguments also take the form `argument=argument_value`.

The `server` argument is used to specify the host name or IP address. The `username` and `password` arguments are used to specify credentials.

A `password-file` argument can be specified instead of the password directly. In this case, the xe command attempts to read the password from the specified file and uses that password to connect. (Any trailing CRs and LFs at the end of the file are stripped off.) This method is more secure than specifying the password directly at the command line.

The optional `port` argument can be used to specify the agent port on the remote Citrix Hypervisor server (defaults to 443).

Example: On the local Citrix Hypervisor server:

```
xe vm-list
```

Example: On a remote Citrix Hypervisor server:

```
xe vm-list username=username password=password server=hostname
```

Shorthand syntax is also available for remote connection arguments:

- `-u` user name
- `-pw` password
- `-pwf` password file
- `-p` port
- `-s` server

Example: On a remote Citrix Hypervisor server:

```
xe vm-list -u myuser -pw mypassword -s hostname
```

Arguments are also taken from the environment variable XE_EXTRA_ARGS, in the form of comma-separated key/value pairs. For example, to enter commands that are run on a remote Citrix Hypervisor server, first run the following command:

```
export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=pass"
```

After running this command, you no longer have to specify the remote Citrix Hypervisor server parameters in each xe command that you run.

Using the XE_EXTRA_ARGS environment variable also enables tab completion of xe commands when issued against a remote Citrix Hypervisor server, which is disabled by default.

Special characters and syntax

To specify argument/value pairs on the `xe` command line, write: `argument=value`

Unless the value includes spaces, do not use quotes. There should be no whitespace in between the argument name, the equals sign (=), and the value. Any argument not conforming to this format is ignored.

For values containing spaces, write: `argument="value with spaces"`

When you use the CLI on your Citrix Hypervisor server, commands have a tab completion feature similar to the feature in the standard Linux bash shell. For example, if you type `xe vm-l` and then press the **TAB** key, the rest of the command is displayed. If more than one command begins with `vm-l`, pressing **TAB** a second time lists the possibilities. This feature is useful when specifying object UUIDs in commands.

> **Note:**
>
> Tab completion does not normally work when executing commands on a remote Citrix Hypervisor server. However, if you set the XE_EXTRA_ARGS variable on the machine where you enter the commands, tab completion is enabled. For more information, see Basic xe syntax.

Command types

The CLI commands can be split in two halves. Low-level commands are concerned with listing and parameter manipulation of API objects. Higher level commands are used to interact with VMs or hosts in a more abstract level.

The low-level commands are:

- *class*-list
- *class*-param-get
- *class*-param-set
- *class*-param-list
- *class*-param-add
- *class*-param-remove
- *class*-param-clear

Where *class* is one of:

- `bond`
- `console`
- `host`
- `host-crashdump`
- `host-cpu`
- `network`
- `patch`
- `pbd`
- `pif`
- `pool`
- `sm`
- `sr`
- `task`
- `template`
- `vbd`
- `vdi`
- `vif`

- `vlan`
- `vm`

Not every value of *class* has the full set of *class*-param-*action* commands. Some values of *class* have a smaller set of commands.

Parameter types

The objects that are addressed with the xe commands have sets of parameters that identify them and define their states.

Most parameters take a single value. For example, the `name-label` parameter of a VM contains a single string value. In the output from parameter list commands, such as `xe vm-param-list`, a value in parentheses indicates whether parameters are read-write (RW) or read-only (RO). The output of `xe vm-param-list` on a specified VM might have the following lines:

```
user-version ( RW): 1
 is-control-domain ( RO): false
```

The first parameter, `user-version`, is writable and has the value 1. The second, `is-control-domain`, is read-only and has a value of false.

The two other types of parameters are multi-valued. A *set* parameter contains a list of values. A *map* parameter is a set of key/value pairs. As an example, look at the following piece of sample output of the `xe vm-param-list` on a specified VM:

```
platform (MRW): acpi: true; apic: true; pae: true; nx: false
allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
hard_shutdown; hard_reboot; suspend
```

The `platform` parameter has a list of items that represent key/value pairs. The key names are followed by a colon character (:). Each key/value pair is separated from the next by a semicolon character (;). The M preceding the RW indicates that this parameter is a map parameter and is readable and writable. The `allowed-operations` parameter has a list that makes up a set of items. The S preceding the RO indicates that this is a set parameter and is readable but not writable.

To filter on a map parameter or set a map parameter, use a colon (:) to separate the map parameter name and the key/value pair. For example, to set the value of the `foo` key of the `other-config` parameter of a VM to `baa`, the command would be

```
xe vm-param-set uuid=VM uuid other-config:foo=baa
```

Note:

> In previous releases, the hyphen character (-) was used to specify map parameters. This syntax still works but is deprecated.

Low-level parameter commands

There are several commands for operating on parameters of objects: *class*-param-get, *class*-param-set, *class*-param-add, *class*-param-remove, *class*-param-clear, and *class*-param-list. Each of these commands takes a `uuid` parameter to specify the particular object. Since these commands are considered low-level commands, they must use the UUID and not the VM name label.

- `xe class-param-list uuid=uuid`

  Lists all of the parameters and their associated values. Unlike the *class*-list command, this command lists the values of "expensive" fields.

- `xe class-param-get uuid=uuid param-name=parameter param-key=key`

  Returns the value of a particular parameter. For a map parameter, specifying the param-key gets the value associated with that key in the map. If param-key is not specified or if the parameter is a set, the command returns a string representation of the set or map.

- `xe class-param-set uuid=uuid param=value`

  Sets the value of one or more parameters.

- `xe class-param-add uuid=uuid param-name=parameter key=value param-key=key`

  Adds to either a map or a set parameter. For a map parameter, add key/value pairs by using the key=value syntax. If the parameter is a set, add keys with the param-key=key syntax.

- `xe class-param-remove uuid=uuid param-name=parameter param-key=key`

  Removes either a key/value pair from a map, or a key from a set.

- `xe class-param-clear uuid=uuid param-name=parameter`

  Completely clears a set or a map.

Low-level list commands

The *class*-list command lists the objects of type *class*. By default, this type of command lists all objects, printing a subset of the parameters. This behavior can be modified in the following ways:

- It can filter the objects so that it only outputs a subset
- The parameters that are printed can be modified.

To change the parameters that are printed, specify the argument *params* as a comma-separated list of the required parameters. For example:

```
xe vm-list params=name-label,other-config
```

Alternatively, to list all of the parameters, use the syntax:

```
xe vm-list params=all
```

The list command doesn't show some parameters that are expensive to calculate. These parameters are shown as, for example:

```
allowed-VBD-devices (SRO): <expensive field>
```

To obtain these fields, use either the command *class*-param-list or *class*-param-get

To filter the list, the CLI matches parameter values with those values specified on the command-line, only printing objects that match all of the specified constraints. For example:

```
xe vm-list HVM-boot-policy="BIOS order" power-state=halted
```

This command lists only those VMs for which *both* the field `power-state` has the value *halted* and the field `HVM-boot-policy` has the value *BIOS order*.

You can also filter the list by the value of keys in maps or by the existence of values in a set. The syntax for filtering based on keys in maps is `map-name:key=value`. The syntax for filtering based on values existing in a set is `set-name:contains=value`.

When scripting, a useful technique is passing `--minimal` on the command line, causing `xe` to print only the first field in a comma-separated list. For example, the command `xe vm-list --minimal` on a host with three VMs installed gives the three UUIDs of the VMs:

```
    a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-af10baea96b7, \
    42c044de-df69-4b30-89d9-2c199564581d
```

Secrets

Citrix Hypervisor provides a secrets mechanism to avoid passwords being stored in plaintext in command-line history or on API objects. XenCenter uses this feature automatically and it can also be used from the xe CLI for any command that requires a password.

> Note
>
> Password secrets cannot be used to authenticate with a Citrix Hypervisor host from a remote instance of the xe CLI.

To create a secret object, run the following command on your Citrix Hypervisor host.

```
xe secret-create value=my-password
```

A secret is created and stored on the Citrix Hypervisor host. The command outputs the UUID of the secret object. For example, `99945d96-5890-de2a-3899-8c04ef2521db`. Append `_secret` to the name of the password argument to pass this UUID to any command that requires a password.

Example: On the Citrix Hypervisor host where you created the secret, you can run the following command:

```
    xe sr-create device-config:location=sr_address device-config:type=cifs device-
config:username=cifs_username  \
    device-config:cifspassword_secret=secret_uuid name-label="CIFS ISO SR"
type="iso" content-type="iso" shared="true"
```

Command history

Some xe commands, for example `xe vm-migrate` or `xe pool-enable-external-auth`, take secrets like passwords as parameters. These can end up in the shell history and during execution of the command are visible in the process table. It is therefore important to execute these commands only in trustworthy environments.

For the bash shell, you can use the `HISTCONTROL` variable to control which commands are stored in the shell history.

xe command reference

This section groups the commands by the objects that the command addresses. These objects are listed alphabetically.

Appliance commands

Commands for creating and modifying VM appliances (also known as vApps). For more information, see vApps.

Appliance parameters

Appliance commands have the following parameters:

Parameter Name	Description	Type
`uuid`	The appliance uuid	Required
`name-description`	The appliance description	Optional
`paused`		Optional
`force`	Force shutdown	Optional

`appliance-assert-can-be-recovered`

```
xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid=vdi-
uuid
```

Tests whether storage is available to recover this VM appliance/vApp.

appliance-create

```
xe appliance-create name-label=name-label [name-description=name-description]
```

Creates an appliance/vApp. For example:

```
xe appliance-create name-label=my_appliance
```

Add VMs to the appliance:

```
xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
```

appliance-destroy

```
xe appliance-destroy uuid=appliance-uuid
```

Destroys an appliance/vApp. For example:

```
xe appliance-destroy uuid=appliance-uuid
```

appliance-recover

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid
[paused=true|false]
```

Recover a VM appliance/vApp from the database contained in the supplied VDI.

appliance-shutdown

```
xe appliance-shutdown uuid=appliance-uuid [force=true|false]
```

Shuts down all VMs in an appliance/vApp. For example:

```
xe appliance-shutdown uuid=appliance-uuid
```

`appliance-start`

```
xe appliance-start uuid=appliance-uuid [paused=true|false]
```

Starts an appliance/vApp. For example:

```
xe appliance-start uuid=appliance-uuid
```

Audit commands

Audit commands download all of the available records of the RBAC audit file in the pool. If the optional parameter `since` is present, it downloads only the records from that specific point in time.

`audit-log-get` parameters

`audit-log-get` has the following parameters

Parameter Name	Description	Type
`filename`	Write the audit log of the pool to *file name*	Required
`since`	Specific date/time point	Optional

`audit-log-get`

```
xe audit-log-get [since=timestamp] filename=filename
```

For example, to obtain audit records of the pool since a precise millisecond timestamp, run the following command:

Run the following command:

```
xe audit-log-get since=2009-09-24T17:56:20.530Z filename=/tmp/auditlog-pool-
actions.out
```

Bonding commands

Commands for working with network bonds, for resilience with physical interface failover. For more information, see Networking.

The bond object is a reference object which glues together *master* and *member* PIFs. The master PIF is the bonding interface which must be used as the overall PIF to refer to the bond. The member PIFs are a set of two or more physical interfaces that have been combined into the high-level bonded interface.

Bond parameters

Bonds have the following parameters:

Parameter Name	Description	Type
`uuid`	Unique identifier/object reference for the bond	Read only
`master`	UUID for the master bond PIF	Read only
`members`	Set of UUIDs for the underlying bonded PIFs	Read only

`bond-create`

```
xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,pif_uuid_2,...
```

Create a bonded network interface on the network specified from a list of existing PIF objects. The command fails in any of the following cases:

- If PIFs are in another bond already
- If any member has a VLAN tag set
- If the referenced PIFs are not on the same Citrix Hypervisor server
- If fewer than 2 PIFs are supplied

`bond-destroy`

```
xe bond-destroy uuid=bond_uuid
```

Deletes a bonded interface specified by its UUID from a host.

`bond-set-mode`

```
xe bond-set-mode uuid=bond_uuid mode=bond_mode
```

Change the bond mode.

CD commands

Commands for working with physical CD/DVD drives on Citrix Hypervisor servers.

CD parameters

CDs have the following parameters:

Parameter Name	Description	Type
`uuid`	Unique identifier/object reference for the CD	Read only
`name-label`	Name for the CD	Read/write
`name-description`	Description text for the CD	Read/write
`allowed-operations`	A list of the operations that can be performed on this CD	Read only set parameter
`current-operations`	A list of the operations that are currently in progress on this CD	Read only set parameter
`sr-uuid`	The unique identifier/object reference for the SR this CD is part of	Read only
`sr-name-label`	The name for the SR this CD is part of	Read only
`vbd-uuids`	A list of the unique identifiers for the VBDs on VMs that connect to this CD	Read only set parameter
`crashdump-uuids`	Not used on CDs. Because crashdumps cannot be written to CDs	Read only set parameter
`virtual-size`	Size of the CD as it appears to VMs (in bytes)	Read only
`physical-utilisation`	Amount of physical space that the CD image takes up on the SR (in bytes)	Read only
`type`	Set to User for CDs	Read only
`sharable`	Whether or not the CD drive is sharable. Default is `false`.	Read only
`read-only`	Whether the CD is read-only, if `false`, the device is writable. Always true for CDs.	Read only
`storage-lock`	Value is `true` if this disk is locked at the storage level.	Read only
`parent`	Reference to the parent disk, if this CD is part of a chain.	Read only
`missing`	Value is `true` if SR scan operation reported this CD as not present on disk	Read only
`other-config`	A list of key/value pairs that specify extra configuration parameters for the CD	Read/write map parameter
`location`	The path on which the device is mounted	Read only
`managed`	Value is `true` if the device is managed	Read only

Parameter Name	Description	Type
xenstore-data	Data to be inserted into the xenstore tree	Read only map parameter
sm-config	Names and descriptions of storage manager device config keys	Read only map parameter
is-a-snapshot	Value is true if this template is a CD snapshot	Read only
snapshot_of	The UUID of the CD that this template is a snapshot of	Read only
snapshots	The UUIDs of any snapshots that have been taken of this CD	Read only
snapshot_time	The timestamp of the snapshot operation	Read only

cd-list

```
xe cd-list [params=param1,param2,...] [parameter=parameter_value]
```

List the CDs and ISOs (CD image files) on the Citrix Hypervisor server or pool, filtering on the optional argument params.

If the optional argument params is used, the value of params is a string containing a list of parameters of this object that you want to display. Alternatively, you can use the keyword all to show all parameters. When params is not used, the returned list shows a default subset of all available parameters.

Optional arguments can be any number of the CD parameters listed at the beginning of this section.

Cluster commands

Commands for working with clustered pools.

Clustered pools are resource pools that have the clustering feature enabled. Use these pools with GFS2 SRs. For more information, see Clustered pools

The cluster and cluster-host objects can be listed with the standard object listing commands (xe cluster-list and xe cluster-host-list), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands. Commands for working with clustered pools.

Cluster parameters

Clusters have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the cluster	Read only

Parameter Name	Description	Type
cluster-hosts	A list of unique identifiers/object references for the hosts in the cluster	Read only set parameter
cluster-token	The secret key used by xapi-clusterd when it talks to itself on other hosts	Read only
cluster-stack	The technology stack providing the clustering capabilities. Possible values are corosync.	Read only
allowed-operations	Lists the operations allowed in this state. This list is advisory only and the cluster state may have changed by the time a client reads this field.	Read only set parameter
current-operations	Lists the operations currently in process. This list is advisory only and the cluster state may have changed by the time a client reads this field.	Read only set parameter
token-timeout	The corosync token timeout in seconds	Read only
token-timeout-coefficient	The corosync token timeout coefficient in seconds	Read only
pool-auto-join	True if automatically joining new pool members to the cluster. This is set to true.	Read only
cluster-config	A list of key/value pairs that specify extra configuration parameters for the cluster.	Read only map parameter
other-config	A list of key/value pairs that specify extra configuration parameters for the cluster.	Read/write map parameter

cluster-host-create

```
xe cluster-host-create cluster-uuid=cluster_uuid host-uuid=host_uuid pif-
uuid=pif_uuid
```

Add a host to an existing cluster.

cluster-host-destroy

```
xe cluster-host-destroy uuid=host_uuid
```

Destroy a cluster host, effectively leaving the cluster.

cluster-host-disable

```
xe cluster-host-disable uuid=cluster_uuid
```

Disable cluster membership for an enabled cluster host.

cluster-host-enable

```
xe cluster-host-enable uuid=cluster_uuid
```

Enable cluster membership for a disabled cluster host.

cluster-host-force-destroy

```
xe cluster-host-force-destroy uuid=cluster_host
```

Destroy a cluster host object forcefully, effectively leaving the cluster.

cluster-pool-create

```
xe cluster-pool-create network-uuid=network_uuid [cluster-stack=cluster_stack]
[token-timeout=token_timeout] [token-timeout-
coefficient=token_timeout_coefficient]
```

Create pool-wide cluster.

cluster-pool-destroy

```
xe cluster-pool-destroy cluster-uuid=cluster_uuid
```

Destroy pool-wide cluster. The pool continues to exist, but it is no longer clustered and can no longer use GFS2 SRs.

cluster-pool-force-destroy

```
xe cluster-pool-force-destroy cluster-uuid=cluster_uuid
```

Force destroy pool-wide cluster.

`cluster-pool-resync`

```
xe cluster-pool-resync cluster-uuid=cluster_uuid
```

Resync a cluster across a pool.

Console commands

Commands for working with consoles.

The console objects can be listed with the standard object listing command (`xe console-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands.

Console parameters

Consoles have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the console	Read only
`vm-uuid`	The unique identifier/object reference of the VM this console is open on	Read only
`vm-name-label`	The name of the VM this console is open on	Read only
`protocol`	Protocol this console uses. Possible values are `vt100`: VT100 terminal, `rfb`: Remote Framebuffer Protocol (as used in VNC), or `rdp`: Remote Desktop Protocol	Read only
`location`	URI for the console service	Read only
`other-config`	A list of key/value pairs that specify extra configuration parameters for the console.	Read/write map parameter

`console`

```
xe console
```

Attach to a particular console.

Diagnostic commands

Commands for gathering diagnostic information from Citrix Hypervisor.

diagnostic-compact

```
xe diagnostic-compact
```

Perform a major GC collection and heap compaction.

DEPRECATED: diagnostic-db-log

```
xe diagnostic-db-log
```

Start logging the database operations. Warning: once started, this cannot be stopped.

diagnostic-db-stats

```
xe diagnostic-db-stats
```

Print database statistics.

diagnostic-gc-stats

```
xe diagnostic-gc-stats
```

Print GC statistics.

diagnostic-license-status

```
xe diagnostic-license-status
```

Help diagnose pool-wide licensing problems.

diagnostic-net-stats

```
xe diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2...]
```

Print network statistics.

diagnostic-timing-stats

```
xe diagnostic-timing-stats
```

Print timing statistics.

diagnostic-vdi-status

```
xe diagnostic-vdi-status uuid=vdi_uuid
```

Query the locking and sharing status of a VDI.

diagnostic-vm-status

```
xe diagnostic-vm-status uuid=vm_uuid
```

Query the hosts on which the VM can boot, check the sharing/locking status of all VBDs.

Disaster recovery commands

Commands for recovering VMs after a disaster

drtask-create

```
xe drtask-create type=type sr-whitelist=sr-white-list device-config=device-config
```

Creates a disaster recovery task. For example, to connect to an iSCSI SR in preparation for Disaster Recovery:

```
xe drtask-create type=lvmoiscsi device-config:target=target-ip-address \
    device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
    sr-whitelist=sr-uuid-list
```

> **Note:**
>
> The command `sr-whitelist` lists SR UUIDs that are allowed. The `drtask-create` command only introduces and connects to an SR which has one of the allowed UUIDs

drtask-destroy

```
xe drtask-destroy uuid=dr-task-uuid
```

Destroys a disaster recovery task and forgets the introduced SR.

vm-assert-can-be-recovered

```
xe vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

Tests whether storage is available to recover this VM.

appliance-assert-can-be-recovered

```
xe appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid=vdi-
uuid
```

Checks whether the storage (containing the appliance's/vAPP disk) is visible.

appliance-recover

```
xe appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid
[force=true|false]
```

Recover an appliance/vAPP from the database contained in the supplied VDI.

vm-recover

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true|false]
```

Recovers a VM from the database contained in the supplied VDI.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
```

Enables XAPI database replication to the specified (shared) SR.

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
```

Disables XAPI database replication to the specified SR.

Example usage

The example below shows the DR CLI commands in context:

On the primary site, enable database replication:

```
xe sr-database-replication uuid=sr=uuid
```

After a disaster, on the secondary site, connect to the SR. The `device-config` command has the same fields as `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
```

Look for database VDIs on the SR:

```
xe vdi-list sr-uuid=sr-uuid type=Metadata
```

Query a database VDI for VMs present:

```
xe vm-list database:vdi-uuid=vdi-uuid
```

Recover a VM:

```
xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

Destroy the DR task. Any SRs introduced by the DR task and not required by VMs are destroyed:

```
xe drtask-destroy uuid=drtask-uuid
```

Event commands

Commands for working with events.

Event classes

Event classes are listed in the following table:

Class name	Description

Class name	Description
`pool`	A pool of physical hosts
`vm`	A Virtual Machine
`host`	A physical host
`network`	A virtual network
`vif`	A virtual network interface
`pif`	A physical network interface (separate VLANs are represented as several PIFs)
`sr`	A storage repository
`vdi`	A virtual disk image
`vbd`	A virtual block device
`pbd`	The physical block devices through which hosts access SRs

`event-wait`

```
xe event-wait class=class_name [param-name=param_value] [param-name=/=param_value]
```

Blocks other commands from executing until an object exists that satisfies the conditions given on the command line. The argument `x=y` means "wait for field x to take value y" and `x=/=y` means "wait for field x to take any value other than y."

Example: wait for a specific VM to be running.

```
xe event-wait class=vm name-label=myvm power-state=running
```

Blocks other commands until a VM called `myvm` is in the `power-state` "running."

Example: wait for a specific VM to reboot:

```
xe event-wait class=vm uuid=$VM start-time=/=$(xe vm-list uuid=$VM params=start-
time --minimal)
```

Blocks other commands until a VM with UUID *$VM* reboots. The command uses the value of `start-time` to decide when the VM reboots.

The class name can be any of the event classes listed at the beginning of this section. The parameters can be any of the parameters listed in the CLI command *class*-param-list.

GPU commands

Commands for working with physical GPUs, GPU groups, and virtual GPUs.

The GPU objects can be listed with the standard object listing commands: `xe pgpu-list`, `xe gpu-group-list`, and `xe vgpu-list`. The parameters can be manipulated with the standard parameter commands. For more information, see Low-level parameter commands.

Physical GPU parameters

Physical GPUS (pGPUs) have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the pGPU	Read only
`vendor-name`	The vendor name of the pGPU	Read only
`device-name`	The name assigned by the vendor to this pGPU model	Read only
`gpu-group-uuid`	The unique identifier/object reference for the GPU group that this pGPU has been automatically assigned to by Citrix Hypervisor. Identical pGPUs across hosts in a pool are grouped	Read only
`gpu-group-name-label`	The name of the GPU group to which the pGPU is assigned	Read only
`host-uuid`	The unique identifier/object reference for the Citrix Hypervisor server to which the pGPU is connected	Read only
`host-name-label`	The name of the Citrix Hypervisor server to which the pGPU is connected	Read only
`pci-id`	PCI identifier	Read only
`dependencies`	Lists the dependent PCI devices passed-through to the same VM	Read/write map parameter
`other-config`	A list of key/value pairs that specify extra configuration parameters for the pGPU	Read/write map parameter
`supported-VGPU-types`	List of virtual GPU types supported by the underlying hardware	Read only
`enabled-VGPU-types`	List of virtual GPU types which have been enabled for this pGPU	Read/Write
`resident-VGPUs`	List of vGPUs running on this pGPU	Read only

`pgpu-disable-dom0-access`

```
xe pgpu-disable-dom0-access uuid=uuid
```

Disable PGPU access to dom0.

pgpu-enable-dom0-access

```
xe pgpu-enable-dom0-access uuid=uuid
```

Enable PGPU access to dom0.

GPU group parameters

GPU groups have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the GPU group	Read only
name-label	The name of the GPU group	Read/write
name-description	The descriptive text of the GPU group	Read/write
VGPU-uuids	Lists the unique identifier/object references for the virtual GPUs in the GPU group	Read only set parameter
PGPU-uuids	Lists the unique identifier/object references for the pGPUs in the GPU group	Read only set parameter
other-config	A list of key/value pairs that specify extra configuration parameters for the GPU group	Read/write map parameter
supported-VGPU-types	Union of all virtual GPU types supported by the underlying hardware	Read only
enabled-VGPU-types	Union of all virtual GPU types which have been enabled on the underlying pGPUs	Read only
allocation-algorithm	Depth-first/Breadth-first setting for allocation virtual GPUs on pGPUs within the group	Read/write enum parameter

GPU group operations

Commands for working with GPU Groups

gpu-group-create

```
```

```
xe gpu-group-create name-label=name_for_group [name-description=description]
```

Creates a new (empty) GPU Group into which pGPUs can be moved.

gpu-group-destroy

```
xe gpu-group-destroy uuid=uuid_of_group
```

Destroys the GPU Group; only permitted for empty groups.

gpu-group-get-remaining-capacity

```
xe gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-
uuid=uuid_of_vgpu_type
```

Returns how many more virtual GPUs of the specified type can be instantiated in this GPU Group.

gpu-group-param-set

```
xe gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
first|depth-first
```

Changes the algorithm that the GPU group uses to allocate virtual GPUs to pGPUs.

gpu-group-param-get-uuid

```
xe gpu-group-param-get-uuid uuid=uuid_of_group param-name=supported-vGPU-
types|enabled-vGPU-types
```

Returns the supported or enabled types for this GPU Group.

Virtual GPU parameters

Virtual GPUs have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the virtual GPU	Read only

Parameter Name	Description	Type
vm-uuid	The unique identifier/object reference for the VM to which the virtual GPU is assigned	Read only
vm-name-label	The name of the VM to which the virtual GPU is assigned	Read only
gpu-group-uuid	The unique identifier/object reference for the GPU group in which the virtual GPU is contained	Read only
gpu-group-name-label	The name of the GPU group in which the virtual GPU is contained	Read only
currently-attached	True if a VM with GPU Pass-Through is running, false otherwise	Read only
other-config	A list of key/value pairs that specify extra configuration parameters for the virtual GPU	Read/write map parameter
type-uuid	The unique identifier/object reference for the virtual GPU type of this virtual GPU	Read/write map parameter
type-model-name	Model name associated with the virtual GPU type	Read only

Virtual GPU type parameters

> **Note:**
>
> GPU Passthrough and virtual GPUs are not compatible with live migration, storage live migration, or VM Suspend unless supported software and graphics cards from GPU vendors are present. VMs without this support cannot be migrated to avoid downtime. For information about NVIDIA vGPU compatibility with live migration, storage live migration, and VM Suspend, see Graphics.

Virtual GPU Types have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the virtual GPU type	Read only
vendor-name	Name of virtual GPU vendor	Read only
model-name	Model name associated with the virtual GPU type	Read only
freeze-frame	Frame buffer size of the virtual GPU type, in bytes	Read only
max-heads	Maximum number of displays supported by the virtual GPU type	Read only
supported-on-PGPUs	List of pGPUs that support this virtual GPU type	Read only
enabled-on-PGPUs	List of pGPUs that have this virtual GPU type enabled	Read only
VGPU-uuids	List of virtual GPUs of this type	Read only

Virtual GPU operations

`vgpu-create`

```
xe vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [vgpu-type-
uuid=uuid_of_vgpu-type]
```

Creates a virtual GPU. This command attaches the VM to the specified GPU group and optionally specifies the virtual GPU type. If no virtual GPU type is specified, the 'pass-through' type is assumed.

`vgpu-destroy`

```
xe vgpu-destroy uuid=uuid_of_vgpu
```

Destroy the specified virtual GPU.

Disabling VNC for VMs with virtual GPU

```
xe vm-param-add uuid=uuid_of_vmparam-name=platform vgpu_vnc_enabled=true|false
```

Using `false` disables the VNC console for a VM as it passes `disablevnc=1` through to the display emulator. By default, VNC is enabled.

Host commands

Commands for interacting with Citrix Hypervisor server.

Citrix Hypervisor servers are the physical servers running Citrix Hypervisor software. They have VMs running on them under the control of a special privileged Virtual Machine, known as the control domain or domain 0.

The Citrix Hypervisor server objects can be listed with the standard object listing commands: `xe host-list`, `xe host-cpu-list`, and `xe host-crashdump-list`). The parameters can be manipulated with the standard parameter commands. For more information, see Low-level parameter commands.

Host selectors

Several of the commands listed here have a common mechanism for selecting one or more Citrix Hypervisor servers on which to perform the operation. The simplest is by supplying the argument `host=uuid_or_name_label`. You can also specify Citrix Hypervisor by filtering the full list of hosts on the values of fields. For example, specifying `enabled=true` selects all Citrix Hypervisor servers whose `enabled` field is equal to `true`. Where multiple Citrix Hypervisor servers match and the operation can be performed on multiple Citrix Hypervisor servers, you must specify `--multiple` to perform the operation. The full list of parameters that can be matched is described at the beginning of this section. You can obtain this list of

commands by running the command `xe host-list params=all`. If no parameters to select Citrix Hypervisor servers are given, the operation is performed on all Citrix Hypervisor servers.

Host parameters

Citrix Hypervisor servers have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the Citrix Hypervisor server	Read only
`name-label`	The name of the Citrix Hypervisor server	Read/write
`name-description`	The description string of the Citrix Hypervisor server	Read only
`enabled`	Value is `false` if disabled. This prevents any new VMs from starting on the hosts and prepares the hosts to be shut down or rebooted. Value is `true` if the host is enabled	Read only
`API-version-major`	Major version number	Read only
`API-version-minor`	Minor version number	Read only
`API-version-vendor`	Identification of API vendor	Read only
`API-version-vendor-implementation`	Details of vendor implementation	Read only map parameter
`logging`	Logging configuration	Read/write map parameter
`suspend-image-sr-uuid`	The unique identifier/object reference for the SR where suspended images are put	Read/write
`crash-dump-sr-uuid`	The unique identifier/object reference for the SR where crash dumps are put	Read/write
`software-version`	List of versioning parameters and their values	Read only map parameter
`capabilities`	List of Xen versions that the Citrix Hypervisor server can run	Read only set parameter

Parameter Name	Description	Type
other-config	A list of key/value pairs that specify extra configuration parameters for the Citrix Hypervisor server	Read/write map parameter
chipset-info	A list of key/value pairs that specify information about the chipset	Read only map parameter
hostname	Citrix Hypervisor server host name	Read only
address	Citrix Hypervisor server IP address	Read only
license-server	A list of key/value pairs that specify information about the license server. The default port for communications with Citrix products is 27000. For information on changing port numbers due to conflicts, see Change port numbers	Read only map parameter
supported-bootloaders	List of bootloaders that the Citrix Hypervisor server supports, for example, pygrub, eliloader	Read only set parameter
memory-total	Total amount of physical RAM on the Citrix Hypervisor server, in bytes	Read only
memory-free	Total amount of physical RAM remaining that can be allocated to VMs, in bytes	Read only
host-metrics-live	True if the host is operational	Read only
logging	The syslog_destination key can be set to the host name of a remote listening syslog service.	Read/write map parameter
allowed-operations	Lists the operations allowed in this state. This list is advisory only and the server state may have changed by the time a client reads this field.	Read only set parameter
current-operations	Lists the operations currently in process. This list is advisory only and the server state may have changed by the time a client reads this field.	Read only set parameter
patches	Set of host patches	Read only set parameter
blobs	Binary data store	Read only
memory-free-computed	A conservative estimate of the maximum amount of memory free on a host	Read only
ha-statefiles	The UUIDs of all HA state files	Read only

Parameter Name	Description	Type
ha-network-peers	The UUIDs of all hosts that can host the VMs on this host if there is a failure	Read only
external-auth-type	Type of external authentication, for example, Active Directory.	Read only
external-auth-service-name	The name of the external authentication service	Read only
external-auth-configuration	Configuration information for the external authentication service.	Read only map parameter

Citrix Hypervisor servers contain some other objects that also have parameter lists.

CPUs on Citrix Hypervisor servers have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the CPU	Read only
number	The number of the physical CPU core within the Citrix Hypervisor server	Read only
vendor	The vendor string for the CPU name	Read only
speed	The CPU clock speed, in Hz	Read only
modelname	The vendor string for the CPU model, for example, "Intel(R) Xeon(TM) CPU 3.00 GHz"	Read only
stepping	The CPU revision number	Read only
flags	The flags of the physical CPU (a decoded version of the features field)	Read only
Utilisation	The current CPU utilization	Read only
host-uuid	The UUID if the host the CPU is in	Read only
model	The model number of the physical CPU	Read only

Parameter Name	Description	Type
`family`	The physical CPU family number	Read only

Crash dumps on Citrix Hypervisor servers have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the crashdump	Read only
`host`	Citrix Hypervisor server the crashdump corresponds to	Read only
`timestamp`	Timestamp of the date and time that the crashdump occurred, in the form `yyyymmdd-hhmmss-ABC`, where *ABC* is the timezone indicator, for example, GMT	Read only
`size`	Size of the crashdump, in bytes	Read only

`host-all-editions`

```
xe host-all-editions
```

Get a list of all available editions

`host-apply-edition`

```
xe host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition="free"
"per-socket" "xendesktop"]
```

Assigns the Citrix Hypervisor license to a host server. When you assign a license, Citrix Hypervisor contacts the License Server and requests the specified type of license. If a license is available, it is then checked out from the license server.

For Citrix Hypervisor for Citrix Virtual Desktops editions, use `"xendesktop"`.

For initial licensing configuration, see also `license-server-address` and `license-server-port`.

`host-backup`

```
xe host-backup file-name=backup_filename host=host_name
```

Download a backup of the control domain of the specified Citrix Hypervisor server to the machine that the command is invoked from. Save it there as a file with the name `file-name`.

> **Important:**
>
> While the `xe host-backup` command works if executed on the local host (that is, without a specific host name specified), do not use it this way. Doing so would fill up the control domain partition with the backup file. Only use the command from a remote off-host machine where you have space to hold the backup file.

host-bugreport-upload

```
xe host-bugreport-upload [host-selector=host_selector_value...]
[url=destination_url http-proxy=http_proxy_name]
```

Generate a fresh bug report (using `xen-bugtool`, with all optional files included) and upload to the Support FTP site or some other location.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

Optional parameters are `http-proxy`: use specified HTTP proxy, and `url`: upload to this destination URL. If optional parameters are not used, no proxy server is identified and the destination is the default Support FTP site.

host-call-plugin

```
xe host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args=args]
```

Calls the function within the plug-in on the given host with optional arguments.

host-compute-free-memory

```
xe host-compute-free-memory
```

Computes the amount of free memory on the host.

host-compute-memory-overhead

```
xe host-compute-memory-overhead
```

Computes the virtualization memory overhead of a host.

host-cpu-info

```
xe host-cpu-info [uuid=uuid]
```

Lists information about the host's physical CPUs.

host-crashdump-destroy

```
xe host-crashdump-destroy uuid=crashdump_uuid
```

Delete a host crashdump specified by its UUID from the Citrix Hypervisor server.

host-crashdump-upload

```
xe host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [http-
proxy=http_proxy_name]
```

Upload a crashdump to the Support FTP site or other location. If optional parameters are not used, no proxy server is identified and the destination is the default Support FTP site. Optional parameters are `http-proxy`: use specified HTTP proxy, and `url`: upload to this destination URL.

host-declare-dead

```
xe host-declare-dead uuid=host_uuid
```

Declare that the the host is dead without contacting it explicitly.

> **Warning:**
>
> This call is dangerous and can cause data loss if the host is not actually dead.

host-disable

```
xe host-disable [host-selector=host_selector_value...]
```

Disables the specified Citrix Hypervisor servers, which prevents any new VMs from starting on them. This action prepares the Citrix Hypervisor servers to be shut down or rebooted.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors). Optional arguments can be any number of the host parameters listed at the beginning of this section.

host-disable-display

```
xe host-disable-display uuid=host_uuid
```

Disable display for the host.

host-disable-local-storage-caching

```
xe host-disable-local-storage-caching
```

Disable local storage caching on the specified host.

host-dmesg

```
xe host-dmesg [host-selector=host_selector_value...]
```

Get a Xen `dmesg` (the output of the kernel ring buffer) from specified Citrix Hypervisor servers.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

host-emergency-ha-disable

```
xe host-emergency-ha-disable  [--force]
```

Disable HA on the local host. Only to be used to recover a pool with a broken HA setup.

host-emergency-management-reconfigure

```
xe host-emergency-management-reconfigure
interface=uuid_of_management_interface_pif
```

Reconfigure the management interface of this Citrix Hypervisor server. Use this command only if the Citrix Hypervisor server is in emergency mode. Emergency mode means that the host is a member in a resource pool whose master has disappeared from the network and cannot be contacted after a number of retries.

host-emergency-reset-server-certificate

```
xe host-emergency-reset-server-certificate
```

Installs a self-signed certificate on the Citrix Hypervisor server where the command is run.

host-enable

```
xe host-enable [host-selector=host_selector_value...]
```

Enables the specified Citrix Hypervisor servers, which allows new VMs to be started on them.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

host-enable-display

```
xe host-enable-display uuid=host_uuid
```

Enable display for the host.

host-enable-local-storage-caching

```
xe host-enable-local-storage-caching  sr-uuid=sr_uuid
```

Enable local storage caching on the specified host.

host-evacuate

```
xe host-evacuate [host-selector=host_selector_value...]
```

Live migrates all running VMs to other suitable hosts on a pool. First, disable the host by using the `host-disable` command.

If the evacuated host is the pool master, then another host must be selected to be the pool master. To change the pool master with HA disabled, use the `pool-designate-new-master` command. For more information, see pool-designate-new-master.

With HA enabled, your only option is to shut down the server, which causes HA to elect a new master at random. For more information, see host-shutdown.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the

beginning of this section.

host-forget

```
xe host-forget uuid=host_uuid
```

The XAPI agent forgets about the specified Citrix Hypervisor server without contacting it explicitly.

Use the `--force` parameter to avoid being prompted to confirm that you really want to perform this operation.

> **Warning:**
>
> Do not use this command if HA is enabled on the pool. Disable HA first, then enable it again after you've forgotten the host.

This command is useful if the Citrix Hypervisor server to "forget" is dead. However, if the Citrix Hypervisor server is live and part of the pool, use `xe pool-eject` instead.

host-get-cpu-features

```
xe host-get-cpu-features {features=pool_master_cpu_features} [uuid=host_uuid]
```

Prints a hexadecimal representation of the host's physical-CPU features.

host-get-server-certificate

```
xe host-get-server-certificate
```

Get the installed server TLS certificate.

host-get-sm-diagnostics

```
xe host-get-sm-diagnostics uuid=uuid
```

Display per-host SM diagnostic information.

host-get-system-status

```
xe host-get-system-status filename=name_for_status_file
[entries=comma_separated_list] [output=tar.bz2|zip] [host-
selector=host_selector_value...]
```

Download system status information into the specified file. The optional parameter `entries` is a comma-separated list of system status entries, taken from the capabilities XML fragment returned by the `host-get-system-status-capabilities` command. For more information, see host-get-system-status-capabilities. If not specified, all system status information is saved in the file. The parameter `output` may be *tar.bz2* (the default) or *zip*. If this parameter is not specified, the file is saved in `tar.bz2` form.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above).

host-get-system-status-capabilities

```
xe host-get-system-status-capabilities [host-selector=host_selector_value...]
```

Get system status capabilities for the specified hosts. The capabilities are returned as an XML fragment that similar to the following example:

```
<?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>
```

Each capability entity can have the following attributes.

- `key` A unique identifier for the capability.
- `content-type` Can be either text/plain or application/data. Indicates whether a UI can render the entries for human consumption.
- `default-checked` Can be either yes or no. Indicates whether a UI should select this entry by default.
- `min-size`, `max-size` Indicates an approximate range for the size, in bytes, of this entry. -1 indicates that the size is unimportant.
- `min-time`, `max-time` Indicate an approximate range for the time, in seconds, taken to collect this entry. -1 indicates that the time is unimportant.
- `pii` Personally identifiable information. Indicates whether the entry has information that can identify the system owner or details of their network topology. The attribute can have one of the following values:
    - `no`: no PII is in these entries
    - `yes`: PII likely or certainly is in these entries

- `maybe`: you might want to audit these entries for PII
- `if_customized` if the files are unmodified, then they contain no PII. However, because we encourage editing of these files, PII might have been introduced by such customization. This value is used in particular for the networking scripts in the control domain.

Passwords are never to be included in any bug report, regardless of any PII declaration.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above).

`host-get-thread-diagnostics`

```
xe host-get-thread-diagnostics uuid=uuid
```

Display per-host thread diagnostic information.

`host-get-vms-which-prevent-evacuation`

```
xe host-get-vms-which-prevent-evacuation uuid=uuid
```

Return a list of VMs which prevent the evacuation of a specific host and display reasons for each one.

`host-is-in-emergency-mode`

```
xe host-is-in-emergency-mode
```

Returns `true` if the host the CLI is talking to is in emergency mode, `false` otherwise. This CLI command works directly on pool member servers even with no master server present.

`host-license-add`

```
xe host-license-add [license-file=path/license_filename] [host-uuid=host_uuid]
```

For Citrix Hypervisor (free edition), use to parse a local license file and add it to the specified Citrix Hypervisor server.

`host-license-remove`

```
xe host-license-remove [host-uuid=host_uuid]
```

Remove any licensing applied to a host.

host-license-view

```
xe host-license-view [host-uuid=host_uuid]
```

Displays the contents of the Citrix Hypervisor server license.

host-logs-download

```
xe host-logs-download [file-name=logfile_name] [host-
selector=host_selector_value...]
```

Download a copy of the logs of the specified Citrix Hypervisor servers. The copy is saved by default in a time-stamped file named `hostname-yyyy-mm-dd T hh:mm:ssZ.tar.gz`. You can specify a different file name using the optional parameter *file-name*.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

> **Important:**
>
> While the `xe host-logs-download` command works if executed on the local host (that is, without a specific host name specified), do *not* use it this way. Doing so clutters the control domain partition with the copy of the logs. The command should *only* be used from a remote off-host machine where you have space to hold the copy of the logs.

host-management-disable

```
xe host-management-disable
```

Disables the host agent listening on an external management network interface and disconnects all connected API clients (such as the XenCenter). This command operates directly on the Citrix Hypervisor server the CLI is connected to. The command is not forwarded to the pool master when applied to a member Citrix Hypervisor server.

> **Warning:**
>
> Be careful when using this CLI command off-host. After this command is run, you cannot connect to the control domain remotely over the network to re-enable the host agent.

host-management-reconfigure

```
xe host-management-reconfigure [interface=device] [pif-uuid=uuid]
```

Reconfigures the Citrix Hypervisor server to use the specified network interface as its management interface, which is the interface that is used to connect to the XenCenter. The command rewrites the MANAGEMENT_INTERFACE key in `/etc/xensource-inventory`.

If the device name of an interface (which must have an IP address) is specified, the Citrix Hypervisor server immediately rebinds. This command works both in normal and emergency mode.

If the UUID of a PIF object is specified, the Citrix Hypervisor server determines which IP address to rebind to itself. It must not be in emergency mode when this command is executed.

> **Warning:**
>
> Be careful when using this CLI command off-host and ensure that you have network connectivity on the new interface. Use `xe pif-reconfigure` to set one up first. Otherwise, subsequent CLI commands are unable to reach the Citrix Hypervisor server.

host-power-on

```
xe host-power-on [host=host_uuid]
```

Turns on power on Citrix Hypervisor servers with the *Host Power On* function enabled. Before using this command, enable `host-set-power-on` on the host.

host-reboot

```
xe host-reboot [host-selector=host_selector_value...]
```

Reboot the specified Citrix Hypervisor servers. The specified hosts must be disabled first using the `xe host-disable` command, otherwise a `HOST_IN_USE` error message is displayed.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

If the specified Citrix Hypervisor servers are members of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the Citrix Hypervisor servers returns. The other members and the master continue to function.

If you shut down the master, the pool is out of action until one of the following actions occurs:

- You make one of the members into the master
- The original master is rebooted and back on line.

When the master is back online, the members reconnect and synchronize with the master.

host-restore

```
xe host-restore [file-name=backup_filename] [host-selector=host_selector_value...]
```

Restore a backup named `file-name` of the Citrix Hypervisor server control software. The use of the word "restore" here does not mean a full restore in the usual sense, it merely means that the compressed backup file has been uncompressed and unpacked onto the secondary partition. After you've done a `xe host-restore`, you have to boot the Install CD and use its Restore from Backup option.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

host-send-debug-keys

```
xe host-send-debug-keys  host-uuid=host_uuid keys=keys
```

Send specified hypervisor debug keys to specified host.

host-server-certificate-install

```
xe host-server-certificate-install certificate=path_to_certificate_file private-
key=path_to_private_key [certificate-chain=path_to_chain_file] [host=host_name |
uuid=host_uuid]
```

Install a TLS certificate on a Citrix Hypervisor server.

host-set-hostname-live

```
xe host-set-hostname-live host-uuid=uuid_of_host host-name=new_hostname
```

Change the host name of the Citrix Hypervisor server specified by `host-uuid`. This command persistently sets both the host name in the control domain database and the actual Linux host name of the Citrix Hypervisor server. The value of `host-name` is *not* the same as the value of the `name_label` field.

host-set-power-on-mode

```
xe host-set-power-on-mode host=host_uuid power-on-mode={"" | "wake-on-lan" |
"DRAC" | "custom"} \
    [ power-on-config:power_on_ip=ip-address power-on-config:power_on_user=user
power-on-config:power_on_password_secret=secret-uuid ]
```

```
```

Use to enable the *Host Power On* function on Citrix Hypervisor hosts that are compatible with remote power solutions. When using the `host-set-power-on` command, you must specify the type of power management solution on the host (that is, the power-on-mode). Then specify configuration options using the power-on-config argument and its associated key-value pairs.

To use the secrets feature to store your password, specify the key `"power_on_password_secret"`. For more information, see Secrets.

host-shutdown

```
xe host-shutdown [host-selector=host_selector_value...]
```

Shut down the specified Citrix Hypervisor servers. The specified Citrix Hypervisor servers must be disabled first using the `xe host-disable` command, otherwise a `HOST_IN_USE` error message is displayed.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

If the specified Citrix Hypervisor servers are members of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the Citrix Hypervisor servers returns. The other members and the master continue to function.

If you shut down the master, the pool is out of action until one of the following actions occurs:

- You make one of the members into the master
- The original master is rebooted and back on line.

  When the master is back online, the members reconnect and synchronize with the master.

If HA is enabled for the pool, one of the members is made into a master automatically. If HA is disabled, you must manually designate the desired server as master with the `pool-designate-new-master` command. For more information, see pool-designate-new-master.

host-sm-dp-destroy

```
xe host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
```

Attempt to destroy and clean up a storage datapath on a host. If `allow-leak=true` is provided then it deletes all records of the datapath even if it is not shut down cleanly.

host-sync-data

```
xe host-sync-data
```

Synchronize the data stored on the pool master with the named host. This does not include the database data).

host-syslog-reconfigure

```
xe host-syslog-reconfigure [host-selector=host_selector_value...]
```

Reconfigure the `syslog` daemon on the specified Citrix Hypervisor servers. This command applies the configuration information defined in the host `logging` parameter.

The hosts on which this operation should be performed are selected using the standard selection mechanism (see host selectors above). Optional arguments can be any number of the host parameters listed at the beginning of this section.

host-data-source-list

```
xe host-data-source-list [host-selectors=host selector value...]
```

List the data sources that can be recorded for a host.

Select the hosts on which to perform this operation by using the standard selection mechanism (see host selectors). Optional arguments can be any number of the host parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all hosts.

Data sources have two parameters – `standard` and `enabled`. This command outputs the values of the parameters:

- If a data source has `enabled` set to `true`, the metrics are currently being recorded to the performance database.
- If a data source has `standard` set to `true`, the metrics are recorded to the performance database *by default*. The value of `enabled` is also set to `true` for this data source.
- If a data source has `standard` set to `false`, the metrics are *not* recorded to the performance database by default. The value of `enabled` is also set to `false` for this data source.

To start recording data source metrics to the performance database, run the `host-data-source-record` command. This command sets `enabled` to `true`. To stop, run the `host-data-source-forget`. This command sets `enabled` to `false`.

host-data-source-record

```
xe host-data-source-record data-source=name_description_of_data_source [host-
selectors=host_selector_value...]
```

Record the specified data source for a host.

This operation writes the information from the data source to the persistent performance metrics database of the specified hosts. For performance reasons, this database is distinct from the normal agent database.

Select the hosts on which to perform this operation by using the standard selection mechanism (see host selectors). Optional arguments can be any number of the host parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all hosts.

`host-data-source-forget`

```
xe host-data-source-forget data-source=name_description_of_data_source [host-
selectors=host_selector_value...]
```

Stop recording the specified data source for a host and forget all of the recorded data.

Select the hosts on which to perform this operation by using the standard selection mechanism (see host selectors). Optional arguments can be any number of the host parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all hosts.

`host-data-source-query`

```
xe host-data-source-query data-source=name_description_of_data_source [host-
selectors=host_selector_value...]
```

Display the specified data source for a host.

Select the hosts on which to perform this operation by using the standard selection mechanism (see host selectors). Optional arguments can be any number of the host parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all hosts.

DEPRECATED: Log commands

Commands for working with logs.

DEPRECATED: `log-get`

```
xe log-get
```

Return the log currently stored in the string logger.

DEPRECATED: `log-get-keys`

```
xe log-get-keys
```

List the keys known by the logger.

DEPRECATED: `log-reopen`

```
xe log-reopen
```

Reopen all loggers (use this for rotating files).

DEPRECATED: `log-set-output`

```
xe log-set-output output=output [key=key] [level=level]
```

Set all loggers to the specified output (`nil`, `stderr`, `string`, `file:`*file name*, `syslog:`*something*).

Message commands

Commands for working with messages. Messages are created to notify users of significant events, and are displayed in XenCenter as alerts.

The message objects can be listed with the standard object listing command (`xe message-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

Message parameters

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the message	Read only
`name`	The unique name of the message	Read only
`priority`	The message priority. Higher numbers indicate greater priority	Read only
`class`	The message class, for example VM.	Read only
`obj-uuid`	The uuid of the affected object.	Read only
`timestamp`	The time that the message was generated.	Read only
`body`	The message content.	Read only

`message-create`

```
xe message-create name=message_name body=message_text [[host-uuid=uuid_of_host] |
[sr-uuid=uuid_of_sr] | [vm-uuid=uuid_of_vm] | [pool-uuid=uuid_of_pool]]
```

Creates a message.

`message-destroy`

```
xe message-destroy [uuid=message_uuid]
```

Destroys an existing message. You can build a script to destroy all messages. For example:

```
# Dismiss all alerts   \
    IFS=","; for m in $(xe message-list params=uuid --minimal); do  \
    xe message-destroy uuid=$m  \
    done
```

Network commands

Commands for working with networks.

The network objects can be listed with the standard object listing command (`xe network-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

Network parameters

Networks have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the network	Read only
`name-label`	The name of the network	Read/write
`name-description`	The description text of the network	Read/write
`VIF-uuids`	A list of unique identifiers of the VIFs (virtual network interfaces) that are attached from VMs to this network	Read only set parameter
`PIF-uuids`	A list of unique identifiers of the PIFs (physical network interfaces) that are attached from Citrix Hypervisor servers to this network	Read only set parameter
`bridge`	Name of the bridge corresponding to this network on the local Citrix Hypervisor server	Read only
`default-locking-mode`	A network object used with VIF objects for ARP filtering. Set to `unlocked` to remove all the filtering rules associated with the VIF. Set to `disabled` so the VIF drops all traffic.	Read/write
`purpose`	Set of purposes for which the Citrix Hypervisor server uses this network. Set to `nbd` to use the network to make NBD connections.	Read/write

Parameter Name	Description	Type
other-config:staticroutes	Comma-separated list of *subnet*/*netmask*/*gateway* formatted entries specifying the gateway address through which to route subnets. For example, setting other-config:static-routes to 172.16.0.0/15/192.168.0.3,172.18.0.0/16/192.168.0.4 causes traffic on 172.16.0.0/15 to be routed over 192.168.0.3 and traffic on 172.18.0.0/16 to be routed over 192.168.0.4.	Read/write
other-config:ethtoolautoneg	Set to no to disable autonegotiation of the physical interface or bridge. Default is yes.	Read/write
other-config:ethtool-rx	Set to on to enable receive checksum, off to disable	Read/write
other-config:ethtool-tx	Set to on to enable transmit checksum, off to disable	Read/write
other-config:ethtool-sg	Set to on to enable scatter gather, off to disable	Read/write
other-config:ethtool-tso	Set to on to enable TCP segmentation offload, off to disable	Read/write
other-config:ethtool-ufo	Set to on to enable UDP fragment offload, off to disable	Read/write
other-config:ethtool-gso	Set to on to enable generic segmentation offload, off to disable	Read/write
blobs	Binary data store	Read only

network-create

```
xe network-create name-label=name_for_network [name-description=descriptive_text]
```

Creates a network.

network-destroy

```
xe network-destroy uuid=network_uuid
```

Destroys an existing network.

SR-IOV commands

Commands for working with SR-IOV.

The `network-sriov` objects can be listed with the standard object listing command (`xe network-sriov-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

SR-IOV parameters

SR-IOV has the following parameters:

Parameter Name	Description	Type
`physical-PIF`	The PIF to enable SR-IOV.	Read only
`logical-PIF`	An SR-IOV logical PIF. Users can use this parameter to create an SR-IOV VLAN network.	Read only
`requires-reboot`	If set to True, used to reboot host to bring SR-IOV enabling into effect.	Read only
`remaining-capacity`	Number of available VFs remaining.	Read only

`network-sriov-create`

```
xe network-sriov-create network-uuid=network_uuid pif-uuid=physical_pif_uuid
```

Creates an SR-IOV network object for a given physical PIF and enables SR-IOV on the physical PIF.

`network-sriov-destroy`

```
xe network-sriov-destroy uuid=network_sriov_uuid
```

Removes a network SR-IOV object and disables SR-IOV on its physical PIF.

Assign an SR-IOV VF

```
xe vif-create device=device_index mac=vf_mac_address network-uuid=sriov_network
vm-uuid=vm_uuid
```

Assigns a VF from an SR-IOV network to a VM.

SDN Controller commands

Commands for working with the SDN controller.

`sdn-controller-forget`

```
xe sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
port=tcp_port]
```

Introduce an SDN controller.

`sdn-controller-introduce`

```
xe sdn-controller-forget uuid=uuid
```

Remove an SDN controller.

Tunnel commands

Commands for working with tunnels.

`tunnel-create`

```
xe tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
```

Create a new tunnel on a host.

`tunnel-destroy`

```
xe tunnel-destroy uuid=uuid
```

Destroy a tunnel.

Patch commands

Commands for working with patches.

`patch-apply`

```
xe patch-apply uuid=patch_uuid host-uuid=host_uuid
```

Apply the previously uploaded patch to the specified host.

`patch-clean`

```
xe patch-clean uuid=uuid
```

Delete a previously uploaded patch file.

patch-destroy

```
xe patch-destroy uuid=uuid
```

Remove an unapplied patch record and files from the server.

patch-pool-apply

```
xe patch-pool-apply uuid=uuid
```

Apply the previously uploaded patch to all hosts in the pool.

patch-pool-clean

```
xe patch-pool-clean uuid=uuid
```

Delete a previously uploaded patch file on all hosts in the pool.

patch-precheck

```
xe patch-precheck uuid=uuid host-uuid=host_uuid
```

Run the prechecks contained within the patch previously uploaded to the specified host.

patch-upload

```
xe patch-upload file-name=file_name
```

Upload a patch file to the server.

PBD commands

Commands for working with PBDs (Physical Block Devices). PBDs are the software objects through which the Citrix Hypervisor server accesses storage repositories (SRs).

The PBD objects can be listed with the standard object listing command (`xe pbd-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

PBD parameters

PBDs have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the PBD.	Read only
sr-uuid	The storage repository that the PBD points to	Read only
device-config	Extra configuration information that is provided to the SR-backend-driver of a host	Read only map parameter
currently-attached	True if the SR is attached on this host, False otherwise	Read only
host-uuid	UUID of the physical machine on which the PBD is available	Read only
host	The host field is deprecated. Use host_uuid instead.	Read only
other-config	Extra configuration information.	Read/write map parameter

pbd-create

```
xe pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-
config:key=corresponding_value]
```

Create a PBD on your Citrix Hypervisor server. The read-only `device-config` parameter can only be set on creation.

To add a mapping from 'path' to '/tmp', the command line should contain the argument `device-config:path=/tmp`

For a full list of supported device-config key/value pairs on each SR type, see Storage.

pbd-destroy

```
xe pbd-destroy uuid=uuid_of_pbd
```

Destroy the specified PBD.

pbd-plug

```
xe pbd-plug uuid=uuid_of_pbd
```

Attempts to plug in the PBD to the Citrix Hypervisor server. If this command succeeds, the referenced SR (and the VDIs contained within) should then become visible to the Citrix Hypervisor server.

pbd-unplug

```
xe pbd-unplug uuid=uuid_of_pbd
```

Attempt to unplug the PBD from the Citrix Hypervisor server.

PIF commands

Commands for working with PIFs (objects representing the physical network interfaces).

The PIF objects can be listed with the standard object listing command (`xe pif-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

PIF parameters

PIFs have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the PIF	Read only
`device machine-readable`	Name of the interface (for example, eth0)	Read only
`MAC`	The MAC address of the PIF	Read only
`other-config`	Extra PIF configuration `name:value` pairs.	Read/write map parameter
`physical`	If true, the PIF points to an actual physical network interface	Read only
`currently-attached`	Is the PIF currently attached on this host? `true` or `false`	Read only
`MTU`	Maximum Transmission Unit of the PIF in bytes.	Read only
`VLAN`	VLAN tag for all traffic passing through this interface. -1 indicates that no VLAN tag is assigned	Read only
`bond-master-of`	The UUID of the bond this PIF is the master of (if any)	Read only
`bond-slave-of`	The UUID of the bond this PIF is part of (if any)	Read only
`management`	Is this PIF designated to be a management interface for the control domain	Read only
`network-uuid`	The unique identifier/object reference of the virtual network to which this PIF is connected	Read only
`network-name-label`	The name of the virtual network to which this PIF is connected	Read only

Parameter Name	Description	Type
host-uuid	The unique identifier/object reference of the Citrix Hypervisor server to which this PIF is connected	Read only
host-name-label	The name of the Citrix Hypervisor server to which this PIF is connected	Read only
IP-configuration-mode	Type of network address configuration used; DHCP or static	Read only
IP	IP address of the PIF. Defined here when IP-configuration-mode is static; undefined when DHCP	Read only
netmask	Netmask of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP	Read only
gateway	Gateway address of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP	Read only
DNS	DNS address of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP	Read only
io_read_kbs	Average read rate in kB/s for the device	Read only
io_write_kbs	Average write rate in kB/s for the device	Read only
carrier	Link state for this device	Read only
vendor-id	The ID assigned to NIC's vendor	Read only
vendor-name	The NIC vendor's name	Read only
device-id	The ID assigned by the vendor to this NIC model	Read only
device-name	The name assigned by the vendor to this NIC model	Read only
speed	Data transfer rate of the NIC	Read only
duplex	Duplexing mode of the NIC; full or half	Read only
pci-bus-path	PCI bus path address	Read only
other-config:ethtoolspeed	Sets the speed of connection in Mbps	Read/write
other-config:ethtoolautoneg	Set to no to disable autonegotiation of the physical interface or bridge. Default is yes.	Read/write
other-config:ethtoolduplex	Sets duplexing capability of the PIF, either full or half.	Read/write
other-config:ethtool-rx	Set to on to enable receive checksum, off to disable	Read/write
other-config:ethtool-tx	Set to on to enable transmit checksum, off to disable	Read/write

Parameter Name	Description	Type
other-config:ethtool-sg	Set to on to enable scatter gather, off to disable	Read/write
other-config:ethtool-tso	Set to on to enable TCP segmentation offload, off to disable	Read/write
other-config:ethtool-ufo	Set to on to enable UDP fragment offload, off to disable	Read/write
other-config:ethtool-gso	Set to on to enable generic segmentation offload, off to disable	Read/write
other-config:domain	Comma-separated list used to set the DNS search path	Read/write
other-config:bondmiimon	Interval between link liveness checks, in milliseconds	Read/write
other-config:bonddowndelay	Number of milliseconds to wait after link is lost before really considering the link to have gone. This parameter allows for transient link loss	Read/write
other-config:bondupdelay	Number of milliseconds to wait after the link comes up before really considering it up. Allows for links flapping up. Default is 31s to allow for time for switches to begin forwarding traffic.	Read/write
disallow-unplug	True if this PIF is a dedicated storage NIC, false otherwise	Read/write

Note:

Changes made to the other-config fields of a PIF will only take effect after a reboot. Alternately, use the xe pif-unplug and xe pif-plug commands to cause the PIF configuration to be rewritten.

pif-forget

```
xe pif-forget uuid=uuid_of_pif
```

Destroy the specified PIF object on a particular host.

pif-introduce

```
xe pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=interface_name
```

Create a PIF object representing a physical interface on the specified Citrix Hypervisor server.

pif-plug

```
xe pif-plug uuid=uuid_of_pif
```

Attempt to bring up the specified physical interface.

pif-reconfigure-ip

```
xe pif-reconfigure-ip uuid=uuid_of_pif [mode=dhcp|mode=static]
gateway=network_gateway_address IP=static_ip_for_this_pif
netmask=netmask_for_this_pif [DNS=dns_address]
```

Modify the IP address of the PIF. For static IP configuration, set the `mode` parameter to `static`, with the `gateway`, `IP`, and `netmask` parameters set to the appropriate values. To use DHCP, set the `mode` parameter to `DHCP` and leave the static parameters undefined.

> **Note:**
>
> Using static IP addresses on physical network interfaces connected to a port on a switch using Spanning Tree Protocol with STP Fast Link turned off (or unsupported) results in a period during which there is no traffic.

pif-reconfigure-ipv6

```
xe pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode
[gateway=network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=dns_address]
```

Reconfigure the IPv6 address settings on a PIF.

pif-scan

```
xe pif-scan host-uuid=host_uuid
```

Scan for new physical interfaces on your Citrix Hypervisor server.

pif-set-primary-address-type

```
xe pif-set-primary-address-type  uuid=uuid primary_address_type=address_type
```

Change the primary address type used by this PIF.

pif-unplug

```
xe pif-unplug uuid=uuid_of_pif
```

Attempt to bring down the specified physical interface.

Pool commands

Commands for working with pools. A *pool* is an aggregate of one or more Citrix Hypervisor servers. A pool uses one or more shared storage repositories so that the VMs running on one host in the pool can be migrated in near-real time to another host in the pool. This migration happens while the VM is still running, without it needing to be shut down and brought back up. Each Citrix Hypervisor server is really a pool consisting of a single member by default. When your Citrix Hypervisor server is joined to a pool, it is designated as a member, and the pool it has joined becomes the master for the pool.

The singleton pool object can be listed with the standard object listing command (`xe pool-list`). Its parameters can be manipulated with the standard parameter commands. For more information, see Low-level parameter commands

Pool parameters

Pools have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the pool	Read only
`name-label`	The name of the pool	Read/write
`name-description`	The description string of the pool	Read/write
`master`	The unique identifier/object reference of Citrix Hypervisor server designated as the pool's master	Read only
`default-SR`	The unique identifier/object reference of the default SR for the pool	Read/write
`crash-dump-SR`	The unique identifier/object reference of the SR where any crash dumps for pool members are saved	Read/write
`metadata-vdis`	All known metadata VDIs for the pool	Read only
`suspend-image-SR`	The unique identifier/object reference of the SR where suspended VMs on pool members are saved	Read/write
`other-config`	A list of key/value pairs that specify extra configuration parameters for the pool	Read/write map parameter
`supported-sr-types`	SR types that this pool can use	Read only
`ha-enabled`	True if HA is enabled for the pool, false otherwise	Read only

Parameter Name	Description	Type
ha-configuration	Reserved for future use.	Read only
ha-statefiles	Lists the UUIDs of the VDIs being used by HA to determine storage health	Read only
ha-host-failures-to-tolerate	The number of host failures to tolerate before sending a system alert	Read/write
ha-plan-exists-for	The number of hosts failures that can actually be handled, according to the calculations of the HA algorithm	Read only
ha-allow-overcommit	True if the pool is allowed to be overcommitted, False otherwise	Read/write
ha-overcommitted	True if the pool is overcommitted	Read only
blobs	Binary data store	Read only
live-patching-disabled	Set to False to enable live patching. Set to True to disable live patching.	Read/write
igmp-snooping-enabled	Set to True to enable IGMP snooping. Set to False to disable IGMP snooping.	Read/write

pool-apply-edition

```
xe pool-apply-edition edition=edition [uuid=uuid] [license-server-address=address]
[license-server-port=port]
```

Apply an edition across the pool.

pool-certificate-install

```
xe pool-certificate-install filename=file_name
```

Install an TLS certificate, pool-wide.

pool-certificate-list

```
xe pool-certificate-list
```

List all installed TLS certificates in a pool.

pool-certificate-sync

```
xe pool-certificate-sync
```

Sync TLS certificates and certificate revocation lists from pool master to the other pool members.

pool-certificate-uninstall

```
xe pool-certificate-uninstall name=name
```

Uninstall a TLS certificate.

pool-crl-install

```
xe pool-crl-install filename=file_name
```

Install a TLS certificate revocation list, pool-wide.

pool-crl-list

```
xe pool-crl-list
```

List all installed TLS certificate revocation lists.

pool-crl-uninstall

```
xe pool-crl-uninstall name=name
```

Uninstall an TLS certificate revocation list.

pool-deconfigure-wlb

```
xe pool-deconfigure-wlb
```

Permanently remove the configuration for workload balancing.

pool-designate-new-master

```
xe pool-designate-new-master host-uuid=uuid_of_new_master
```

Instruct the specified member Citrix Hypervisor server to become the master of an existing pool. This command performs an orderly handover of the role of master host to another host in the resource pool. This command only works when the current master is online. It is not a replacement for the emergency mode commands listed below.

pool-disable-external-auth

```
xe pool-disable-external-auth [uuid=uuid] [config=config]
```

Disables external authentication in all the hosts in a pool.

pool-disable-local-storage-caching

```
xe pool-disable-local-storage-caching uuid=uuid
```

Disable local storage caching across the pool.

pool-disable-redo-log

```
xe pool-disable-redo-log
```

Disable the redo log if in use, unless HA is enabled.

pool-dump-database

```
xe pool-dump-database file-name=filename_to_dump_database_into_(on_client)
```

Download a copy of the entire pool database and dump it into a file on the client.

pool-enable-external-auth

```
xe pool-enable-external-auth  auth-type=auth_type service-name=service_name
[uuid=uuid] [config:=config]
```

Enables external authentication in all the hosts in a pool. Note that some values of `auth-type` will require particular `config:` values.

pool-enable-local-storage-caching

```
xe pool-enable-local-storage-caching uuid=uuid
```

Enable local storage caching across the pool.

pool-enable-redo-log

```
xe pool-ensable-redo-log sr-uuid=sr_uuid
```

Enable the redo log on the given SR if in use, unless HA is enabled.

pool-eject

```
xe pool-eject host-uuid=uuid_of_host_to_eject
```

Instruct the specified Citrix Hypervisor server to leave an existing pool.

pool-emergency-reset-master

```
xe pool-emergency-reset-master master-address=address_of_pool_master
```

Instruct a pool member server to reset its master server address to the new value and attempt to connect to it. Do not run this command on master servers.

pool-emergency-transition-to-master

```
xe pool-emergency-transition-to-master
```

Instruct a member Citrix Hypervisor server to become the pool master. The Citrix Hypervisor server accepts this command only after the host has transitioned to emergency mode. Emergency mode means it is a member of a pool whose master has disappeared from the network and cannot be contacted after some number of retries.

If the host password has been modified since the host joined the pool, this command can cause the password of the host to reset. For more information, see (User commands).

pool-ha-enable

```
xe pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
```

Enable high availability on the resource pool, using the specified SR UUID as the central storage heartbeat repository.

pool-ha-disable

```
xe pool-ha-disable
```

Disables the high availability feature on the resource pool.

pool-ha-compute-hypothetical-max-host-failures-to-tolerate

Compute the maximum number of host failures to tolerate under the current pool configuration.

pool-ha-compute-max-host-failures-to-tolerate

```
xe pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=vm_uuid]
[restart-priority=restart_priority]
```

Compute the maximum number of host failures to tolerate with the supplied, proposed protected VMs.

pool-initialize-wlb

```
xe pool-initialize-wlb wlb_url=url wlb_username=wlb_username
wlb_password=wlb_password xenserver_username=username xenserver_password=password
```

Initialize workload balancing for the current pool with the target Workload Balancing server.

pool-join

```
xe pool-join master-address=address master-username=username master-
password=password
```

Instruct your Citrix Hypervisor server to join an existing pool.

pool-management-reconfigure

```
xe pool-management-reconfigure [network-uuid=network-uuid]
```

Reconfigures the management interface of all the hosts in the pool to use the specified network interface, which is the interface that is used to connect to the XenCenter. The command rewrites the MANAGEMENT_INTERFACE key in `/etc/xensource-inventory` for all the hosts in the pool.

If the device name of an interface (which must have an IP address) is specified, the Citrix Hypervisor master host immediately rebinds. This command works both in normal and emergency mode.

From the network UUID specified, UUID of the PIF object is identified and mapped to the Citrix Hypervisor server, which determines which IP address to rebind to itself. It must not be in emergency mode when this

command is executed.

> **Warning:**
>
> Be careful when using this CLI command off-host and ensure that you have network connectivity on the new interface. Use `xe pif-reconfigure` to set one up first. Otherwise, subsequent CLI commands are unable to reach the Citrix Hypervisor server.

`pool-recover-slaves`

```
xe pool-recover-slaves
```

Instruct the pool master to try to reset the master address of all members currently running in emergency mode. This command is typically used after `pool-emergency-transition-to-master` has been used to set one of the members as the new master.

`pool-restore-database`

```
xe pool-restore-database file-name=filename_to_restore_from_on_client [dry-
run=true|false]
```

Upload a database backup (created with `pool-dump-database`) to a pool. On receiving the upload, the master restarts itself with the new database.

There is also a *dry run* option, which allows you to check that the pool database can be restored without actually perform the operation. By default, `dry-run` is set to false.

`pool-retrieve-wlb-configuration`

```
xe pool-retrieve-wlb-configuration
```

Retrieves the pool optimization criteria from the Workload Balancing server.

`pool-retrieve-wlb-diagnostics`

```
xe pool-retrieve-wlb-diagnostics [filename=file_name]
```

Retrieves diagnostics from the Workload Balancing server.

`pool-retrieve-wlb-recommendations`

```

```

```
xe pool-retrieve-wlb-recommendations
```

Retrieves VM migrate recommendations for the pool from the Workload Balancing server.

pool-retrieve-wlb-report

```
xe pool-retrieve-wlb-report report=report [filename=file_name]
```

Retrieves reports from the Workload Balancing server.

pool-rotate-secret

```
xe pool-rotate-secret
```

Rotate the pool secret.

The pool secret is a secret shared among the servers in a pool that enables the server to prove its membership to a pool. Users with the Pool Admin role can view this secret when connecting to the server over SSH. Rotate the pool secret if one of these users leaves your organization or loses their Pool Admin role.

pool-send-test-post

```
xe pool-send-test-post dest-host=destination_host dest-port=destination_port
body=post_body
```

Send the given body to the given host and port, using HTTPS, and print the response. This is used for debugging the TLS layer.

pool-send-wlb-configuration

```
xe pool-send-wlb-configuration [config:=config]
```

Sets the pool optimization criteria for the Workload Balancing server.

pool-sync-database

```
xe pool-sync-database
```

Force the pool database to be synchronized across all hosts in the resource pool. This command is not necessary in normal operation since the database is regularly automatically replicated. However, the command can be useful for ensuring changes are rapidly replicated after performing a significant set of CLI operations.

Set pool `igmp-snooping`

```
xe pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|false]
```

Enables or disables IGMP snooping on a Citrix Hypervisor pool.

PVS Accelerator commands

Commands for working with the PVS Accelerator.

`pvs-cache-storage-create`

```
xe pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid size=size
```

Configure a PVS cache on a given SR for a given host.

`pvs-cache-storage-destroy`

```
xe pvs-cache-storage-destroy uuid=uuid
```

Remove a PVS cache.

`pvs-proxy-create`

```
xe pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
```

Configure a VM/VIF to use a PVS proxy.

`pvs-proxy-destroy`

```
xe pvs-proxy-destroy uuid=uuid
```

Remove (or switch off) a PVS proxy for this VIF/VM.

`pvs-server-forget`

```
xe pvs-server-forget uuid=uuid
```

Forget a PVS server.

`pvs-server-introduce`

```
xe pvs-server-introduce addresses=adresses first-port=first_port last-
port=last_port pvs-site-uuid=pvs_site_uuid
```

Introduce new PVS server.

`pvs-site-forget`

```
xe pvs-site-forget uuid=uuid
```

Forget a PVS site.

`pvs-site-introduce`

```
xe pvs-site-introduce name-label=name_label [name-description=name_description]
[pvs-uuid=pvs_uuid]
```

Introduce new PVS site.

Storage Manager commands

Commands for controlling Storage Manager plug-ins.

The storage manager objects can be listed with the standard object listing command (`xe sm-list`). The parameters can be manipulated with the standard parameter commands. For more information, see Low-level parameter commands

SM parameters

SMs have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the SM plug-in	Read only
`name-label`	The name of the SM plug-in	Read only
`name-description`	The description string of the SM plug-in	Read only
`type`	The SR type that this plug-in connects to	Read only

Parameter Name	Description	Type
vendor	Name of the vendor who created this plug-in	Read only
copyright	Copyright statement for this SM plug-in	Read only
required-api-version	Minimum SM API version required on the Citrix Hypervisor server	Read only
configuration	Names and descriptions of device configuration keys	Read only
capabilities	Capabilities of the SM plug-in	Read only
driver-filename	The file name of the SR driver.	Read only

Snapshot commands

Commands for working with snapshots.

snapshot-clone

```
xe snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-
description=description]
```

Create a new template by cloning an existing snapshot, using storage-level fast disk clone operation where available.

snapshot-copy

```
xe snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-
description=name_description] [sr-uuid=sr_uuid]
```

Create a new template by copying an existing VM, but without using storage-level fast disk clone operation (even if this is available). The disk images of the copied VM are guaranteed to be 'full images' - i.e. not part of a CoW chain.

snapshot-destroy

```
xe snapshot-destroy  [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

Destroy a snapshot. This leaves the storage associated with the snapshot intact. To delete storage too, use snapshot-uninstall.

snapshot-disk-list

```

```

```
xe snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-
params=vbd_params] [vdi-params=vdi_params]
```

List the disks on the selected VM(s).

`snapshot-export-to-template`

```
xe snapshot-export-to-template filename=file_name snapshot-uuid=snapshot_uuid
[preserve-power-state=true|false]
```

Export a snapshot to *file name*.

`snapshot-reset-powerstate`

```
xe snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

Force the VM power state to halted in the management toolstack database only. This command is used to recover a snapshot that is marked as 'suspended'. This is a potentially dangerous operation: you must ensure that you do not need the memory image anymore. You will not be able to resume your snapshot anymore.

`snapshot-revert`

```
xe snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

Revert an existing VM to a previous checkpointed or snapshot state.

`snapshot-uninstall`

```
xe snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

Uninstall a snapshot. This operation will destroy those VDIs that are marked RW and connected to this snapshot only. To simply destroy the VM record, use snapshot-destroy.

SR commands

Commands for controlling SRs (storage repositories).

The SR objects can be listed with the standard object listing command (`xe sr-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

SR parameters

SRs have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the SR	Read only
`name-label`	The name of the SR	Read/write
`name-description`	The description string of the SR	Read/write
`allowed-operations`	List of the operations allowed on the SR in this state	Read only set parameter
`current-operations`	List of the operations that are currently in progress on this SR	Read only set parameter
`VDIs`	Unique identifier/object reference for the virtual disks in this SR	Read only set parameter
`PBDs`	Unique identifier/object reference for the PBDs attached to this SR	Read only set parameter
`physical-utilisation`	Physical space currently utilized on this SR, in bytes. For thin provisioned disk formats, physical utilization may be less than virtual allocation	Read only
`physical-size`	Total physical size of the SR, in bytes	Read only
`type`	Type of the SR, used to specify the SR back-end driver to use	Read only
`introduced-by`	The `drtask` (if any) which introduced the SR	Read only
`content-type`	The type of the SR's content. Used to distinguish ISO libraries from other SRs. For storage repositories that store a library of ISOs, the content-type must be set to iso. In other cases, we recommend that you set this parameter either to empty, or the string user.	Read only
`shared`	True if this SR can be shared between multiple Citrix Hypervisor servers; False otherwise	Read/write
`other-config`	List of key/value pairs that specify extra configuration parameters for the SR	Read/write map parameter
`host`	The storage repository host name	Read only

Parameter Name	Description	Type
virtual-allocation	Sum of virtual-size values of all VDIs in this storage repository (in bytes)	Read only
sm-config	SM dependent data	Read only map parameter
blobs	Binary data store	Read only

sr-create

```
xe sr-create name-label=name physical-size=size type=type content-
type=content_type device-config:config_name=value [host-uuid=host_uuid]
[shared=true|false]
```

Creates an SR on the disk, introduces it into the database, and creates a PBD attaching the SR to the Citrix Hypervisor server. If `shared` is set to `true`, a PBD is created for each Citrix Hypervisor server in the pool. If `shared` is not specified or set to `false`, a PBD is created only for the Citrix Hypervisor server specified with `host-uuid`.

The exact `device-config` parameters differ depending on the device `type`. For details of these parameters across the different storage back-ends, see Storage.

sr-data-source-forget

```
xe sr-data-source-forget data-source=data_source
```

Stop recording the specified data source for a SR, and forget all of the recorded data.

sr-data-source-list

```
xe sr-data-source-list
```

List the data sources that can be recorded for a SR.

sr-data-source-query

```
xe sr-data-source-query data-source=data_source
```

Query the last value read from a SR data source.

sr-data-source-record

```
xe sr-data-source-record  data-source=data_source
```

Record the specified data source for a SR.

sr-destroy

```
xe sr-destroy uuid=sr_uuid
```

Destroys the specified SR on the Citrix Hypervisor server.

sr-enable-database-replication

```
xe sr-enable-database-replication uuid=sr_uuid
```

Enables XAPI database replication to the specified (shared) SR.

sr-disable-database-replication

```
xe sr-disable-database-replication uuid=sr_uuid
```

Disables XAPI database replication to the specified SR.

sr-forget

```
xe sr-forget uuid=sr_uuid
```

The XAPI agent forgets about a specified SR on the Citrix Hypervisor server. When the XAPI agent forgets an SR, the SR is detached and you cannot access VDIs on it, but it remains intact on the source media (the data is not lost).

sr-introduce

```
xe sr-introduce name-label=name physical-size=physical_size type=type content-
type=content_type uuid=sr_uuid
```

Just places an SR record into the database. Use `device-config` to specify additional parameters in the form `device-config:parameter_key=parameter_value`, for example:

```
xe sr-introduce device-config:device=/dev/sdb1
```

> **Note:**
>
> This command is never used in normal operation. This advanced operation might be useful when an SR must be reconfigured as shared after it was created or to help recover from various failure scenarios.

sr-probe

```
xe sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=value]
```

Performs a scan of the backend, using the provided `device-config` keys. If the `device-config` is complete for the SR back-end, this command returns a list of the SRs present on the device, if any. If the `device-config` parameters are only partial, a back-end-specific scan is performed, returning results that guide you in improving the remaining `device-config` parameters. The scan results are returned as XML specific to the back end, printed on the CLI.

The exact `device-config` parameters differ depending on the device `type`. For details of these parameters across the different storage back-ends, see Storage.

sr-probe-ext

```
xe sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config] [sm-
config:-sm_config]
```

Perform a storage probe. The device-config parameters can be specified by for example device-config:devs=/dev/sdb1. Unlike sr-probe, this command returns results in the same human-readable format for every SR type.

sr-scan

```
xe sr-scan uuid=sr_uuid
```

Force an SR scan, syncing the XAPI database with VDIs present in the underlying storage substrate.

sr-update

```
xe sr-update uuid=uuid
```

Refresh the fields of the SR object in the database.

lvhd-enable-thin-provisioning

```
xe lvhd-enable-thin-provisioning  sr-uuid=sr_uuid initial-
allocation=initial_allocation allocation-quantum=allocation_quantum
```

Enable thin-provisioning on an LVHD SR.

Subject commands

Commands for working with subjects.

session-subject-identifier-list

```
xe session-subject-identifier-list
```

Return a list of all the user subject ids of all externally-authenticated existing sessions.

session-subject-identifier-logout

```
xe session-subject-identifier-logout subject-identifier=subject_identifier
```

Log out all externally-authenticated sessions associated to a user subject id.

session-subject-identifier-logout-all

```
xe session-subject-identifier-logout-all
```

Log out all externally-authenticated sessions.

subject-add

```
xe subject-add subject-name=subject_name
```

Add a subject to the list of subjects that can access the pool.

subject-remove

```
xe subject-remove subject-uuid=subject_uuid
```

Remove a subject from the list of subjects that can access the pool.

`subject-role-add`

```
xe subject-role-add uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

Add a role to a subject.

`subject-role-remove`

```
xe subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

Remove a role from a subject.

`secret-create`

```
xe secret-create value=value
```

Create a secret.

`secret-destroy`

```
xe secret-destroy uuid=uuid
```

Destroy a secret.

Task commands

Commands for working with long-running asynchronous tasks. These commands are tasks such as starting, stopping, and suspending a virtual machine. The tasks are typically made up of a set of other atomic subtasks that together accomplish the requested operation.

The task objects can be listed with the standard object listing command (`xe task-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

Task parameters

Tasks have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the Task	Read only

Parameter Name	Description	Type
name-label	The name of the Task	Read only
name-description	The description string of the Task	Read only
resident-on	The unique identifier/object reference of the host on which the task is running	Read only
status	Status of the Task	Read only
progress	If the Task is still pending, this field contains the estimated percentage complete, from 0 to 1. If the Task has completed, successfully or unsuccessfully, the value is 1.	Read only
type	If the Task has successfully completed, this parameter contains the type of the encoded result. The type is the name of the class whose reference is in the result field. Otherwise, this parameter's value is undefined	Read only
result	If the Task has completed successfully, this field contains the result value, either Void or an object reference; otherwise, this parameter's value is undefined	Read only
error_info	If the Task has failed, this parameter contains the set of associated error strings. Otherwise, this parameter's value is undefined	Read only
allowed_operations	List of the operations allowed in this state	Read only
created	Time the task has been created	Read only
finished	Time task finished (that is, succeeded or failed). If task-status is pending, then the value of this field has no meaning	Read only
subtask_of	Contains the UUID of the tasks this task is a subtask of	Read only
subtasks	Contains the UUIDs of all the subtasks of this task	Read only

task-cancel

```
xe task-cancel [uuid=task_uuid]
```

Direct the specified Task to cancel and return.

Template commands

Commands for working with VM templates.

Templates are essentially VMs with the `is-a-template` parameter set to `true`. A template is a "gold image" that contains all the various configuration settings to instantiate a specific VM. Citrix Hypervisor ships with a base set of templates, which are generic "raw" VMs that can boot an OS vendor installation CD (for example: RHEL, CentOS, SLES, Windows). You can create VMs, configure them in standard forms for your particular needs, and save a copy of them as templates for future use in VM deployment.

The template objects can be listed with the standard object listing command (`xe template-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

> **Note:**
>
> Templates cannot be directly converted into VMs by setting the `is-a-template` parameter to `false`. Setting `is-a-template` parameter to `false` is not supported and results in a VM that cannot be started.

VM template parameters

Templates have the following parameters:

- `uuid` (read only) the unique identifier/object reference for the template
- `name-label` (read/write) the name of the template
- `name-description` (read/write) the description string of the template
- `user-version` (read/write) string for creators of VMs and templates to put version information
- `is-a-template` (read/write) true if this VM is a template. Template VMs can never be started, they are used only for cloning other VMs. After this value has been set to true, it cannot be reset to false. Template VMs cannot be converted into VMs using this parameter.
- `is-control-domain` (read only) true if this is a control domain (domain 0 or a driver domain)
- `power-state` (read only) current power state. The value is always halted for a template
- `memory-dynamic-max` (read only) dynamic maximum memory in bytes. Currently unused, but if changed the following constraint must be obeyed: `memory_static_max` >= `memory_dynamic_max` >= `memory_dynamic_min` >= `memory_static_min`.
- `memory-dynamic-min` (read/write) dynamic minimum memory in bytes. Currently unused, but if changed the same constraints for `memory-dynamic-max` must be obeyed.
- `memory-static-max` (read/write) statically set (absolute) maximum memory in bytes. This field is the main value used to determine the amount of memory assigned to a VM.

- `memory-static-min` (read/write) statically set (absolute) minimum memory in bytes. This field represents the absolute minimum memory, and `memory-static-min` must be less than `memory-static-max`. This value is unused in normal operation, but the previous constraint must be obeyed.
- `suspend-VDI-uuid` (read only) the VDI that a suspend image is stored on (has no meaning for a template)
- `VCPUs-params` (read/write map parameter) configuration parameters for the selected vCPU policy.

  You can tune a vCPU's pinning with:

  ```
  xe template-param-set uuid=<template_uuid> vCPUs-params:mask=1,2,3
  ```

  A VM created from this template run on physical CPUs 1, 2, and 3 only.

  You can also tune the vCPU priority (xen scheduling) with the cap and weight parameters. For example:

  ```
  xe template-param-set uuid=<template_uuid> VCPUs-params:weight=512 xe
  template-param-set uuid=<template_uuid> VCPUs-params:cap=100
  ```

  A VM based on this template with a weight of 512 get twice as much CPU as a domain with a weight of 256 on a contended host. Legal weights range from 1 to 65535 and the default is 256.

  The cap optionally fixes the maximum amount of CPU a VM based on this template can consume, even if the Citrix Hypervisor server has idle CPU cycles. The cap is expressed in percentage of one physical CPU: 100 is 1 physical CPU, 50 is half a CPU, 400 is 4 CPUs, and so on The default, 0, means that there is no upper cap.
- `VCPUs-max` (read/write) maximum number of vCPUs
- `VCPUs-at-startup` (read/write) boot number of vCPUs
- `actions-after-crash` (read/write) action to take when a VM based on this template crashes
- `console-uuids` (read only set parameter) virtual console devices
- `platform` (read/write map parameter) platform specific configuration

  To disable the emulation of a parallel port for HVM guests (for example, Windows guests):

  ```
  xe vm-param-set uuid=<vm_uuid> platform:parallel=none
  ```

  To disable the emulation of a serial port for HVM guests:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
  ```

To disable the emulation of a USB controller and a USB tablet device for HVM guests:

```
xe vm-param-set uuid=<vm_uuid> platform:usb=false
xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
```

- `allowed-operations` (read only set parameter) list of the operations allowed in this state
- `current-operations` (read only set parameter) list of the operations that are currently in progress on this template
- `allowed-VBD-devices` (read only set parameter) list of VBD identifiers available for use, represented by integers of the range 0–15. This list is informational only, and other devices may be used (but may not work).
- `allowed-VIF-devices` (read only set parameter) list of VIF identifiers available for use, represented by integers of the range 0–15. This list is informational only, and other devices may be used (but may not work).
- `HVM-boot-policy` (read/write) the boot policy for HVM guests. Either BIOS Order or an empty string.
- `HVM-boot-params` (read/write map parameter) the order key controls the HVM guest boot order, represented as a string where each character is a boot method: d for the CD/DVD, c for the root disk, and n for network PXE boot. The default is dc.
- `PV-kernel` (read/write) path to the kernel
- `PV-ramdisk` (read/write) path to the `initrd`
- `PV-args` (read/write) string of kernel command line arguments
- `PV-legacy-args` (read/write) string of arguments to make legacy VMs based on this template boot
- `PV-bootloader` (read/write) name of or path to bootloader
- `PV-bootloader-args` (read/write) string of miscellaneous arguments for the bootloader
- `last-boot-CPU-flags` (read only) describes the CPU flags on which a VM based on this template was last booted; not populated for a template
- `resident-on` (read only) the Citrix Hypervisor server on which a VM based on this template is resident. Appears as `not in database` for a template
- `affinity` (read/write) the Citrix Hypervisor server which a VM based on this template has preference for running on. Used by the `xe vm-start` command to decide where to run the VM
- `other-config` (read/write map parameter) list of key/value pairs that specify extra configuration parameters for the template
- `start-time` (read only) timestamp of the date and time that the metrics for a VM based on this template were read, in the form `yyyymmddThh:mm:ss z`, where z is the single-letter military timezone

indicator, for example, Z for UTC(GMT). Set to `1 Jan 1970 Z` (beginning of Unix/POSIX epoch) for a template

- `install-time` (read only) timestamp of the date and time that the metrics for a VM based on this template were read, in the form `yyyymmddThh:mm:ss z`, where z is the single-letter military timezone indicator, for example, Z for UTC (GMT). Set to `1 Jan 1970 Z` (beginning of Unix/POSIX epoch) for a template
- `memory-actual` (read only) the actual memory being used by a VM based on this template; 0 for a template
- `VCPUs-number` (read only) the number of virtual CPUs assigned to a VM based on this template; 0 for a template
- `VCPUs-Utilization` (read only map parameter) list of virtual CPUs and their weight read only map parameter `os-version` the version of the operating system for a VM based on this template. Appears as `not in database` for a template
- `PV-drivers-version` (read only map parameter) the versions of the paravirtualized drivers for a VM based on this template. Appears as `not in database` for a template
- `PV-drivers-detected` (read only) flag for latest version of the paravirtualized drivers for a VM based on this template. Appears as `not in database` for a template
- `memory` (read only map parameter) memory metrics reported by the agent on a VM based on this template. Appears as `not in database` for a template
- `disks` (read only map parameter) disk metrics reported by the agent on a VM based on this template. Appears as `not in database` for a template
- `networks` (read only map parameter) network metrics reported by the agent on a VM based on this template. Appears as `not in database` for a template
- `other` (read only map parameter) other metrics reported by the agent on a VM based on this template. Appears as `not in database` for a template
- `guest-metrics-last-updated` (read only) timestamp when the in-guest agent performed the last write to these fields. In the form `yyyymmddThh:mm:ss z`, where z is the single-letter military timezone indicator, for example, Z for UTC (GMT)
- `actions-after-shutdown` (read/write) action to take after the VM has shutdown
- `actions-after-reboot` (read/write) action to take after the VM has rebooted
- `possible-hosts` (read only) list of hosts that can potentially host the VM
- `HVM-shadow-multiplier` (read/write) multiplier applied to the amount of shadow that is made available to the guest
- `dom-id` (read only) domain ID (if available, -1 otherwise)

- `recommendations` (read only) XML specification of recommended values and ranges for properties of this VM
- `xenstore-data` (read/write map parameter) data to be inserted into the `xenstore` tree (`/local/domain/*domid*/vmdata`) after the VM is created.
- `is-a-snapshot` (read only) True if this template is a VM snapshot
- `snapshot_of` (read only) the UUID of the VM that this template is a snapshot of
- `snapshots` (read only) the UUIDs of any snapshots that have been taken of this template
- `snapshot_time` (read only) the timestamp of the most recent VM snapshot taken
- `memory-target` (read only) the target amount of memory set for this template
- `blocked-operations` (read/write map parameter) lists the operations that cannot be performed on this template
- `last-boot-record` (read only) record of the last boot parameters for this template, in XML format
- `ha-always-run` (read/write) True if an instance of this template is always restarted on another host if there is a failure of the host it is resident on. This parameter is now deprecated. Use the `ha-restartpriority` parameter instead.
- `ha-restart-priority` (read only) restart or best-effort read/write blobs binary data store
- `live` (read only) relevant only to a running VM.

`template-export`

```
xe template-export template-uuid=uuid_of_existing_template
filename=filename_for_new_template
```

Exports a copy of a specified template to a file with the specified new file name.

`template-uninstall`

```
xe template-uninstall template-uuid=template_uuid [--force]
```

Uninstall a custom template. This operation will destroy those VDIs that are marked as 'owned' by this template.

Update commands

The following section contains Citrix Hypervisor server update commands.

The update objects can be listed with the standard object listing command (`xe update-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level

parameter commands

Update parameters

Citrix Hypervisor server updates have the following parameters:

Parameter Name	Description	Type
`uuid`	The unique identifier/object reference for the update	Read only
`host`	The list of hosts that this update is applied to	Read only
`host-uuid`	The unique identifier for the Citrix Hypervisor server to query	Read only
`name-label`	The name of the update	Read only
`name-description`	The description string of the update	Read only
`applied`	Whether or not the update has been applied; true or false	Read only
`installation-size`	The size of the update in bytes	Read only
`after-apply-guidance`	Whether the XAPI toolstack or the host requires a restart	Read only
`version`	The version of the update	Read only

`update-upload`

```
xe update-upload file-name=update_filename
```

Upload a specified update file to the Citrix Hypervisor server. This command prepares an update to be applied. On success, the UUID of the uploaded update is printed. If the update has previously been uploaded, `UPDATE_ALREADY_EXISTS` error is returned instead and the patch is not uploaded again.

`update-precheck`

```
xe update-precheck uuid=update_uuid host-uuid=host_uuid
```

Run the prechecks contained within the specified update on the specified Citrix Hypervisor server.

`update-destroy`

```
xe update-destroy uuid=update_file_uuid
```

Deletes an update file that has not been applied from the pool. Can be used to delete an update file that cannot be applied to the hosts.

`update-apply`

```
xe update-apply host-uuid=host_uuid uuid=update_file_uuid
```

Apply the specified update file.

update-pool-apply

```
xe update-pool-apply uuid=update_uuid
```

Apply the specified update to all Citrix Hypervisor servers in the pool.

update-introduce

```
xe update-introduce vdi-uuid=vdi_uuid
```

Introduce update VDI.

update-pool-clean

```
xe update-pool-clean uuid=uuid
```

Removes the update's files from all hosts in the pool.

User commands

user-password-change

```
xe user-password-change old=old_password new=new_password
```

Changes the password of the logged-in user. The old password field is not checked because you require supervisor privilege to use this command.

VBD commands

Commands for working with VBDs (Virtual Block Devices).

A VBD is a software object that connects a VM to the VDI, which represents the contents of the virtual disk. The VBD has the attributes which tie the VDI to the VM (is it bootable, its read/write metrics, and so on). The VDI has the information on the physical attributes of the virtual disk (which type of SR, whether the disk is sharable, whether the media is read/write or read only, and so on).

The VBD objects can be listed with the standard object listing command (`xe vbd-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter

commands

VBD parameters

VBDs have the following parameters:

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the VBD	Read only
vm-uuid	The unique identifier/object reference for the VM this VBD is attached to	Read only
vm-name-label	The name of the VM this VBD is attached to	Read only
vdi-uuid	The unique identifier/object reference for the VDI this VBD is mapped to	Read only
vdi-name-label	The name of the VDI this VBD is mapped to	Read only
empty	If true, this VBD represents an empty drive	Read only
device	The device seen by the guest, for example hda	Read only
userdevice	Device number specified by the device parameter during vbd-create, for example, 0 for hda, 1 for hdb, and so on	Read/write
bootable	True if this VBD is bootable	Read/write
mode	The mode the VBD should be mounted with	Read/write
type	How the VBD appears to the VM, for example disk or CD	Read/write
currently-attached	True if the VBD is attached on this host, false otherwise	Read only
storage-lock	True if a storage-level lock was acquired	Read only
status-code	Error/success code associated with the last attach operation	Read only
status-detail	Error/success information associated with the last attach operation status	Read only
qos_algorithm_type	The QoS algorithm to use	Read/write
qos_algorithm_params	Parameters for the chosen QoS algorithm	Read/write map parameter
qos_supported_algorithms	Supported QoS algorithms for this VBD	Read only set parameter
io_read_kbs	Average read rate in kB per second for this VBD	Read only
io_write_kbs	Average write rate in kB per second for this VBD	Read only

Parameter Name	Description	Type
allowed-operations	List of the operations allowed in this state. This list is advisory only and the server state may have changed by the time this field is read by a client.	Read only set parameter
current-operations	Links each of the running tasks using this object (by reference) to a current_operation enum which describes the nature of the task.	Read only set parameter
unpluggable	True if this VBD supports hot unplug	Read/write
attachable	True if the device can be attached	Read only
other-config	Extra configuration	Read/write map parameter

vbd-create

```
xe vbd-create vm-uuid=uuid_of_the_vm device=device_value vdi-
uuid=uuid_of_vdi_to_connect_to [bootable=true] [type=Disk|CD] [mode=RW|RO]
```

Create a VBD on a VM.

The allowable values for the `device` field are integers 0–15, and the number must be unique for each VM. The current allowable values can be seen in the `allowed-VBD-devices` parameter on the specified VM. This is seen as `userdevice` in the `vbd` parameters.

If the `type` is `Disk`, `vdi-uuid` is required. Mode can be `RO` or `RW` for a Disk.

If the `type` is `CD`, `vdi-uuid` is optional. If no VDI is specified, an empty VBD is created for the CD. Mode must be `RO` for a CD.

vbd-destroy

```
xe vbd-destroy uuid=uuid_of_vbd
```

Destroy the specified VBD.

If the VBD has its `other-config:owner` parameter set to `true`, the associated VDI is also destroyed.

vbd-eject

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

Remove the media from the drive represented by a VBD. This command only works if the media is of a removable type (a physical CD or an ISO). Otherwise, an error message `VBD_NOT_REMOVABLE_MEDIA` is returned.

`vbd-insert`

```
xe vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
```

Insert new media into the drive represented by a VBD. This command only works if the media is of a removable type (a physical CD or an ISO). Otherwise, an error message `VBD_NOT_REMOVABLE_MEDIA` is returned.

`vbd-plug`

```
xe vbd-plug uuid=uuid_of_vbd
```

Attempt to attach the VBD while the VM is in the running state.

`vbd-unplug`

```
xe vbd-unplug uuid=uuid_of_vbd
```

Attempts to detach the VBD from the VM while it is in the running state.

VDI commands

Commands for working with VDIs (Virtual Disk Images).

A VDI is a software object that represents the contents of the virtual disk seen by a VM. This is different to the VBD, which is an object that ties a VM to the VDI. The VDI has the information on the physical attributes of the virtual disk (which type of SR, whether the disk is sharable, whether the media is read/write or read only, and so on). The VBD has the attributes that tie the VDI to the VM (is it bootable, its read/write metrics, and so on).

The VDI objects can be listed with the standard object listing command (`xe vdi-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

VDI parameters

VDIs have the following parameters:

Parameter Name	Description	Type

Parameter Name	Description	Type
uuid	The unique identifier/object reference for the VDI	Read only
name-label	The name of the VDI	Read/write
name-description	The description string of the VDI	Read/write
allowed-operations	A list of the operations allowed in this state	Read only set parameter
current-operations	A list of the operations that are currently in progress on this VDI	Read only set parameter
sr-uuid	SR in which the VDI resides	Read only
vbd-uuids	A list of VBDs that refer to this VDI	Read only set parameter
crashdump-uuids	List of crash dumps that refer to this VDI	Read only set parameter
virtual-size	Size of disk as presented to the VM, in bytes. Depending on the storage back-end type, the size may not be respected exactly	Read only
physical-utilisation	Amount of physical space that the VDI is taking up on the SR, in bytes	Read only
type	Type of VDI, for example, System or User	Read only
sharable	True if this VDI may be shared	Read only
read-only	True if this VDI can only be mounted read-only	Read only
storage-lock	True if this VDI is locked at the storage level	Read only
parent	References the parent VDI when this VDI is part of a chain	Read only
missing	True if SR scan operation reported this VDI as not present	Read only
other-config	Extra configuration information for this VDI	Read/write map parameter
sr-name-label	Name of the containing storage repository	Read only
location	Location information	Read only
managed	True if the VDI is managed	Read only

Parameter Name	Description	Type
xenstore-data	Data to be inserted into the xenstore tree (/local/domain/0/backend/vbd/*domid*/*device-id*/smdata) after the VDI is attached. The SM back-ends usually set this field on vdi_attach.	Read only map parameter
sm-config	SM dependent data	Read only map parameter
is-a-snapshot	True if this VDI is a VM storage snapshot	Read only
snapshot_of	The UUID of the storage this VDI is a snapshot of	Read only
snapshots	The UUIDs of all snapshots of this VDI	Read only
snapshot_time	The timestamp of the snapshot operation that created this VDI	Read only
metadata-of-pool	The uuid of the pool which created this metadata VDI	Read only
metadata-latest	Flag indicating whether the VDI contains the latest known metadata for this pool	Read only
cbt-enabled	Flag indicating whether changed block tracking is enabled for the VDI	Read/write

vdi-clone

```
xe vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
```

Create a new, writable copy of the specified VDI that can be used directly. It is a variant of vdi-copy that is can expose high-speed image clone facilities where they exist.

Use the optional driver-params map parameter to pass extra vendor-specific configuration information to the back-end storage driver that the VDI is based on. For more information, see the storage vendor driver documentation.

vdi-copy

```
xe vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
```

Copy a VDI to a specified SR.

vdi-create

```
xe vdi-create sr-uuid=uuid_of_sr_to_create_vdi_on name-label=name_for_the_vdi
type=system|user|suspend|crashdump virtual-size=size_of_virtual_disk sm-config-
```

```
\*=storage_specific_configuration_data
```

Create a VDI.

The `virtual-size` parameter can be specified in bytes or using the IEC standard suffixes KiB, MiB, GiB, and TiB.

> **Note:**
>
> SR types that support thin provisioning of disks (such as Local VHD and NFS) do not enforce virtual allocation of disks. Take great care when over-allocating virtual disk space on an SR. If an over-allocated SR becomes full, disk space must be made available either on the SR target substrate or by deleting unused VDIs in the SR.
>
> Some SR types might round up the `virtual-size` value to make it divisible by a configured block size.

`vdi-data-destroy`

```
xe vdi-data-destroy uuid=uuid_of_vdi
```

Destroy the data associated with the specified VDI, but keep the changed block tracking metadata.

> **Note:**
>
> If you use changed block tracking to take incremental backups of the VDI, ensure that you use the `vdi-data-destroy` command to delete snapshots but keep the metadata. Do not use `vdi-destroy` on snapshots of VDIs that have changed block tracking enabled.

`vdi-destroy`

```
xe vdi-destroy uuid=uuid_of_vdi
```

Destroy the specified VDI.

> **Note:**
>
> If you use changed block tracking to take incremental backups of the VDI, ensure that you use the `vdi-data-destroy` command to delete snapshots but keep the metadata. Do not use `vdi-destroy` on snapshots of VDIs that have changed block tracking enabled.
>
> For Local VHD and NFS SR types, disk space is not immediately released on `vdi-destroy`, but periodically during a storage repository scan operation. If you must force deleted disk space to be

made available, call `sr-scan` manually.

`vdi-disable-cbt`

```
xe vdi-disable-cbt uuid=uuid_of_vdi
```

Disable changed block tracking for the VDI.

`vdi-enable-cbt`

```
xe vdi-enable-cbt uuid=uuid_of_vdi
```

Enable changed block tracking for the VDI.

> **Note:**
>
> You can enable changed block tracking only on licensed instances of Citrix Hypervisor Premium Edition.

`vdi-export`

```
xe vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=format]
[base=uuid_of_base_vdi] [--progress]
```

Export a VDI to the specified file name. You can export a VDI in one of the following formats:

- `raw`
- `vhd`

The VHD format can be *sparse*. If there are unallocated blocks within the VDI, these blocks might be omitted from the VHD file, therefore making the VHD file smaller. You can export to VHD format from all supported VHD-based storage types (EXT3/EXT4, NFS).

If you specify the `base` parameter, this command exports only those blocks that have changed between the exported VDI and the base VDI.

`vdi-forget`

```
xe vdi-forget uuid=uuid_of_vdi
```

Unconditionally removes a VDI record from the database without touching the storage back-end. In normal operation, you should be using `vdi-destroy` instead.

vdi-import

```
xe vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format=format] [-
-progress]
```

Import a VDI. You can import a VDI from one of the following formats:

- raw
- vhd

vdi-introduce

```
xe vdi-introduce uuid=uuid_of_vdi sr-uuid=uuid_of_sr name-label=name_of_new_vdi
type=system|user|suspend|crashdump
location=device_location_(varies_by_storage_type) [name-
description=description_of_vdi] [sharable=yes|no] [read-only=yes|no] [other-
config=map_to_store_misc_user_specific_data] [xenstore-
data=map_to_of_additional_xenstore_keys] [sm-
config=storage_specific_configuration_data]
```

Create a VDI object representing an existing storage device, without actually modifying or creating any storage. This command is primarily used internally to introduce hot-plugged storage devices automatically.

vdi-list-changed-blocks

```
xe vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=second-vdi-
uuid
```

Compare two VDIs and return the list of blocks that have changed between the two as a base64-encoded string. This command works only for VDIs that have changed block tracking enabled.

For more information, see Changed block tracking.

vdi-pool-migrate

```
xe vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
```

Migrate a VDI to a specified SR, while the VDI is attached to a running guest. (Storage live migration)

For more information, see Migrate VMs.

vdi-resize

```

```

```
xe vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
```

Change the size of the VDI specified by UUID.

vdi-snapshot

```
xe vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
```

Produces a read-write version of a VDI that can be used as a reference for backup or template creation purposes or both. Use the snapshot to perform a backup rather than installing and running backup software inside the VM. The VM continues running while external backup software streams the contents of the snapshot to the backup media. Similarly, a snapshot can be used as a "gold image" on which to base a template. A template can be made using any VDIs.

Use the optional `driver-params` map parameter to pass extra vendor-specific configuration information to the back-end storage driver that the VDI is based on. For more information, see the storage vendor driver documentation.

A clone of a snapshot should always produce a writable VDI.

vdi-unlock

```
xe vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
```

Attempts to unlock the specified VDIs. If `force=true` is passed to the command, it forces the unlocking operation.

vdi-update

```
xe vdi-update uuid=uuid
```

Refresh the fields of the VDI object in the database.

VIF commands

Commands for working with VIFs (Virtual network interfaces).

The VIF objects can be listed with the standard object listing command (`xe vif-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

VIF parameters

VIFs have the following parameters:

- `uuid` (read only) the unique identifier/object reference for the VIF
- `vm-uuid` (read only) the unique identifier/object reference for the VM that this VIF resides on
- `vm-name-label` (read only) the name of the VM that this VIF resides on
- `allowed-operations` (read only set parameter) a list of the operations allowed in this state
- `current-operations` (read only set parameter) a list of the operations that are currently in progress on this VIF
- `device` (read only) integer label of this VIF, indicating the order in which VIF back-ends were created
- `MAC` (read only) MAC address of VIF, as exposed to the VM
- `MTU` (read only) Maximum Transmission Unit of the VIF in bytes.

  This parameter is read-only, but you can override the MTU setting with the `mtu` key using the `other-config` map parameter. For example, to reset the MTU on a virtual NIC to use jumbo frames:

  ```
  xe vif-param-set \
      uuid=<vif_uuid> \
      other-config:mtu=9000
  ```

- `currently-attached` (read only) true if the device is attached
- `qos_algorithm_type` (read/write) QoS algorithm to use
- `qos_algorithm_params` (read/write map parameter) parameters for the chosen QoS algorithm
- `qos_supported_algorithms` (read only set parameter) supported QoS algorithms for this VIF
- `MAC-autogenerated` (read only) True if the MAC address of the VIF was automatically generated
- `other-config` (read/write map parameter) extra configuration `key:value` pairs
- `other-config:ethtoolrx` (read/write) set to on to enable receive checksum, off to disable
- `other-config:ethtooltx` (read/write) set to on to enable transmit checksum, off to disable
- `other-config:ethtoolsg` (read/write) set to on to enable scatter gather, off to disable
- `other-config:ethtooltso` (read/write) set to on to enable TCP segmentation offload, off to disable
- `other-config:ethtoolufo` (read/write) set to on to enable UDP fragment offload, off to disable
- `other-config:ethtoolgso` (read/write) set to on to enable generic segmentation offload, off to disable
- `other-config:promiscuous` (read/write) true to a VIF to be promiscuous on the bridge, so that it sees all traffic over the bridge. Useful for running an Intrusion Detection System (IDS) or similar in a VM.

- `network-uuid` (read only) the unique identifier/object reference of the virtual network to which this VIF is connected
- `network-name-label` (read only) the descriptive name of the virtual network to which this VIF is connected
- `io_read_kbs` (read only) average read rate in kB/s for this VIF
- `io_write_kbs` (read only) average write rate in kB/s for this VIF
- `locking_mode` (read/write) Affects the VIFs ability to filter traffic to/from a list of MAC and IP addresses. Requires extra parameters.
- `locking_mode:default` (read/write) Varies according to the default locking mode for the VIF network.

  If the default-locking-mode is set to `disabled`, Citrix Hypervisor applies a filtering rule so that the VIF cannot send or receive traffic. If the default-lockingmode is set to `unlocked`, Citrix Hypervisor removes all the filtering rules associated with the VIF. For more information, see Network Commands.
- `locking_mode:locked` (read/write) Only traffic sent to or sent from the specified MAC and IP addresses is allowed on the VIF. If no IP addresses are specified, no traffic is allowed.
- `locking_mode:unlocked` (read/write) No filters are applied to any traffic going to or from the VIF.
- `locking_mode:disabled` (read/write) Citrix Hypervisor applies a filtering rule is applied so that the VIF drops all traffic.

`vif-create`

```
xe vif-create vm-uuid=uuid_of_the_vm device=see below network-
uuid=uuid_of_network_to_connect_to [mac=mac_address]
```

Create a VIF on a VM.

Appropriate values for the `device` field are listed in the parameter `allowed-VIF-devices` on the specified VM. Before any VIFs exist there, the values allowed are integers from 0-15.

The `mac` parameter is the standard MAC address in the form `aa:bb:cc:dd:ee:ff`. If you leave it unspecified, an appropriate random MAC address is created. You can also explicitly set a random MAC address by specifying `mac=random`.

`vif-destroy`

```
xe vif-destroy uuid=uuid_of_vif
```

Destroy a VIF.

`vif-move`

```
xe vif-move uuid=uuid network-uuid=network_uuid
```

Move the VIF to another network.

vif-plug

```
xe vif-plug uuid=uuid_of_vif
```

Attempt to attach the VIF while the VM is in the running state.

vif-unplug

```
xe vif-unplug uuid=uuid_of_vif
```

Attempts to detach the VIF from the VM while it is running.

vif-configure-ipv4

Configure IPv4 settings for this virtual interface. Set IPv4 settings as below:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
gateway=gateway_address
```

For example:

```
VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", " 192.168.1.1")
```

Clean IPv4 settings as below:

```
xe vif-configure-ipv4 uuid=uuid_of_vif mode=none
```

vif-configure-ipv6

Configure IPv6 settings for this virtual interface. Set IPv6 settings as below:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
gateway=gateway_address
```

For example:

```
VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
"fd06:7768:b9e5:8b00::1")
```

Clean IPv6 settings as below:

```
xe vif-configure-ipv6 uuid=uuid_of_vif mode=none
```

VLAN commands

Commands for working with VLANs (virtual networks). To list and edit virtual interfaces, refer to the PIF commands, which have a VLAN parameter to signal that they have an associated virtual network. For more information, see PIF commands. For example, to list VLANs, use `xe pif-list`.

`vlan-create`

```
xe vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=uuid_of_network
```

Create a VLAN on your Citrix Hypervisor server.

`pool-vlan-create`

```
xe pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-
uuid=uuid_of_network
```

Create a VLAN on all hosts on a pool, by determining which interface (for example, `eth0`) the specified network is on (on each host) and creating and plugging a new PIF object one each host accordingly.

`vlan-destroy`

```
xe vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
```

Destroy a VLAN. Requires the UUID of the PIF that represents the VLAN.

VM commands

Commands for controlling VMs and their attributes.

VM selectors

Several of the commands listed here have a common mechanism for selecting one or more VMs on which to perform the operation. The simplest way is by supplying the argument `vm=name_or_uuid`. An easy way to get

the uuid of an actual VM is to, for example, execute `xe vm-list power-state=running`. (Get the full list of fields that can be matched by using the command `xe vm-list params=all`.) For example, specifying `power-state=halted` selects VMs whose `power-state` parameter is equal to `halted`. Where multiple VMs are matching, specify the option `--multiple` to perform the operation. The full list of parameters that can be matched is described at the beginning of this section.

The VM objects can be listed with the standard object listing command (`xe vm-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

VM parameters

VMs have the following parameters:

> **Note:**
>
> All writable VM parameter values can be changed while the VM is running, but new parameters are *not* applied dynamically and cannot be applied until the VM is rebooted.

- `appliance` (read/write) the appliance/vApp to which the VM belongs
- `uuid` (read only) the unique identifier/object reference for the VM
- `name-label` (read/write) the name of the VM
- `name-description` (read/write) the description string of the VM
- `order start order` (read/write) for vApp startup/shutdown and for startup after HA failover
- `version` (read only) the number of times this VM has been recovered. If you want to overwrite a new VM with an older version, call `vm-recover`
- `user-version` (read/write) string for creators of VMs and templates to put version information
- `is-a-template` (read/write) False unless this VM is a template. Template VMs can never be started, they are used only for cloning other VMs After this value has been set to true it cannot be reset to false. Template VMs cannot be converted into VMs using this parameter.
- `is-control-domain` (read only) True if this is a control domain (domain 0 or a driver domain)
- `power-state` (read only) current power state
- `start-delay` (read/write) the delay to wait before a call to start up the VM returns
- `shutdown-delay` (read/write) the delay to wait before a call to shut down the VM returns
- `memory-dynamic-max` (read/write) dynamic maximum in bytes
- `memory-dynamic-min` (read/write) dynamic minimum in bytes
- `memory-static-max` (read/write) statically set (absolute) maximum in bytes. If you want to change this value, the VM must be shut down.

- `memory-static-min` (read/write) statically set (absolute) minimum in bytes. If you want to change this value, the VM must be shut down.
- `suspend-VDI-uuid` (read only) the VDI that a suspend image is stored on
- `VCPUs-params` (read/write map parameter) configuration parameters for the selected vCPU policy.

  You can tune a vCPU's pinning with

  ```
  xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
  ```

  The selected VM then runs on physical CPUs 1, 2, and 3 only. You can also tune the vCPU priority (xen scheduling) with the cap and weight parameters. For example:

  ```
  xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-param-set uuid=
  <vm_uuid> VCPUs-params:cap=100
  ```

  A VM with a weight of 512 get twice as much CPU as a domain with a weight of 256 on a contended Citrix Hypervisor server. Legal weights range from 1 to 65535 and the default is 256. The cap optionally fixes the maximum amount of CPU a VM will be able to consume, even if the Citrix Hypervisor server has idle CPU cycles. The cap is expressed in percentage of one physical CPU: 100 is 1 physical CPU, 50 is half a CPU, 400 is 4 CPUs, and so on The default, 0, means that there is no upper cap.
- `VCPUs-max` (read/write) maximum number of virtual CPUs.
- `VCPUs-at-startup` (read/write) boot number of virtual CPUs
- `actions-after-crash` (read/write) action to take if the VM crashes. For PV guests, valid parameters are:
  - `preserve` (for analysis only)
  - `coredump_and_restart` (record a coredump and reboot VM)
  - `coredump_and_destroy` (record a coredump and leave VM halted)
  - `restart` (no coredump and restart VM)
  - `destroy` (no coredump and leave VM halted)
- `console-uuids` (read only set parameter) virtual console devices
- `platform` (read/write map parameter) platform-specific configuration

  To disable VDA to switch Windows 10 into Tablet mode:

  ```
  xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
  ```

  To enable VDA to switch Windows 10 into Tablet mode:

```
xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
```

To check current state:

```
xe vm-param-get uuid=<vm_uuid> param-name=platform param-
key=acpi_laptop_slate
```

- `allowed-operations` (read only set parameter) list of the operations allowed in this state
- `current-operations` (read only set parameter) a list of the operations that are currently in progress on the VM
- `allowed-VBD-devices` (read only set parameter) list of VBD identifiers available for use, represented by integers of the range 0–15. This list is informational only, and other devices may be used (but might not work).
- `allowed-VIF-devices` (read only set parameter) list of VIF identifiers available for use, represented by integers of the range 0–15. This list is informational only, and other devices may be used (but might not work).
- `HVM-boot-policy` (read/write) the boot policy for HVM guests. Either BIOS Order or an empty string.
- `HVM-boot-params` (read/write map parameter) the order key controls the HVM guest boot order, represented as a string where each character is a boot method: d for the CD/DVD, c for the root disk, and n for network PXE boot. The default is dc.
- `HVM-shadow-multiplier` (read/write) Floating point value which controls the amount of shadow memory overhead to grant the VM. Defaults to 1.0 (the minimum value), and only advanced users should change this value.
- `PV-kernel` (read/write) path to the kernel
- `PV-ramdisk` (read/write) path to the `initrd`
- `PV-args` (read/write) string of kernel command line arguments
- `PV-legacy-args` (read/write) string of arguments to make legacy VMs boot
- `PV-bootloader` (read/write) name of or path to bootloader
- `PV-bootloader-args` (read/write) string of miscellaneous arguments for the bootloader
- `last-boot-CPU-flags` (read only) describes the CPU flags on which the VM was last booted
- `resident-on` (read only) the Citrix Hypervisor server on which a VM is resident
- `affinity` (read/write) The Citrix Hypervisor server which the VM has preference for running on. Used by the `xe vm-start` command to decide where to run the VM

- `other-config` (read/write map parameter) A list of key/value pairs that specify extra configuration parameters for the VM. For example, a VM is started automatically after host boot when the `other-config` parameter includes the key/value pair `auto_poweron: true`
- `start-time` (read only) timestamp of the date and time that the metrics for the VM were read. This timestamp is in the form `yyyymmddThh:mm:ss z`, where z is the single letter military timezone indicator, for example, Z for UTC (GMT)
- `install-time` (read only) timestamp of the date and time that the metrics for the VM were read. This timestamp is in the form `yyyymmddThh:mm:ss z`, where z is the single letter military timezone indicator, for example, Z for UTC (GMT)
- `memory-actual` (read only) the actual memory being used by a VM
- `VCPUs-number` (read only) the number of virtual CPUs assigned to the VM for a Linux VM. This number can differ from `VCPUS-max` and can be changed without rebooting the VM using the `vm-vcpu-hotplug` command. For more information, see `vm-vcpu-hotplug`. Windows VMs always run with the number of vCPUs set to `VCPUsmax` and must be rebooted to change this value. Performance drops sharply when you set `VCPUs-number` to a value greater than the number of physical CPUs on the Citrix Hypervisor server.
- `VCPUs-Utilization` (read only map parameter) a list of virtual CPUs and their weight
- `os-version` (read only map parameter) the version of the operating system for the VM
- `PV-drivers-version` (read only map parameter) the versions of the paravirtualized drivers for the VM
- `PV-drivers-detected` (read only) flag for latest version of the paravirtualized drivers for the VM
- `memory` (read only map parameter) memory metrics reported by the agent on the VM
- `disks` (read only map parameter) disk metrics reported by the agent on the VM
- `networks` (read only map parameter) network metrics reported by the agent on the VM
- `other` (read only map parameter) other metrics reported by the agent on the VM
- `guest-metrics-lastupdated` (read only) timestamp when the in-guest agent performed the last write to these fields. The timestamp is in the form `yyyymmddThh:mm:ss z`, where z is the single letter military timezone indicator, for example, Z for UTC (GMT)
- `actions-after-shutdown` (read/write) action to take after the VM has shutdown
- `actions-after-reboot` (read/write) action to take after the VM has rebooted
- `possible-hosts` potential hosts of this VM read only
- `dom-id` (read only) domain ID (if available, -1 otherwise)
- `recommendations` (read only) XML specification of recommended values and ranges for properties of this VM

- `xenstore-data` (read/write map parameter) data to be inserted into the `xenstore` tree (`/local/domain/*domid*/vm-data`) after the VM is created
- `is-a-snapshot` (read only) True if this VM is a snapshot
- `snapshot_of` (read only) the UUID of the VM that this snapshot is of
- `snapshots` (read only) the UUIDs of all snapshots of this VM
- `snapshot_time` (read only) the timestamp of the snapshot operation that created this VM snapshot
- `memory-target` (read only) the target amount of memory set for this VM
- `blocked-operations` (read/write map parameter) lists the operations that cannot be performed on this VM
- `last-boot-record` (read only) record of the last boot parameters for this template, in XML format
- `ha-always-run` (read/write) True if this VM is always restarted on another host if there is a failure of the host it is resident on. This parameter is now deprecated. Use the `ha-restart-priority` parameter instead.
- `ha-restart-priority` (read/write) restart or best-effort
- `blobs` (read only) binary data store
- `live` (read only) True if the VM is running. False if HA suspects that the VM is not be running.

vm-assert-can-be-recovered

```
xe vm-assert-can-be-recovered uuid [database] vdi-uuid
```

Tests whether storage is available to recover this VM.

vm-call-plugin

```
xe vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=value]
```

Calls the function within the plug-in on the given VM with optional arguments (args:key=value). To pass a "value" string with special characters in it (for example new line), an alternative syntax args:key:file=local_file can be used in place, where the content of local_file will be retrieved and assigned to "key" as a whole.

vm-cd-add

```
xe vm-cd-add cd-name=name_of_new_cd device=integer_value_of_an_available_vbd [vm-
selector=vm_selector_value...]
```

Add a new virtual CD to the selected VM. The `device` parameter should be selected from the value of the `allowed-VBD-devices` parameter of the VM.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-cd-eject

```
xe vm-cd-eject [vm-selector=vm_selector_value...]
```

Eject a CD from the virtual CD drive. This command only works if exactly one CD is attached to the VM. When there are two or more CDs, use the command `xe vbd-eject` and specify the UUID of the VBD.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-cd-insert

```
xe vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

Insert a CD into the virtual CD drive. This command only works if there is exactly one empty CD device attached to the VM. When there are two or more empty CD devices, use the `xe vbd-insert` command and specify the UUIDs of the VBD and of the VDI to insert.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-cd-list

```
xe vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

Lists CDs attached to the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

You can also select which VBD and VDI parameters to list.

vm-cd-remove

```

```

```
xe vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

Remove a virtual CD from the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-checkpoint

```
xe vm-checkpoint new-name-label=name_label [new-name-description=description]
```

Checkpoint an existing VM, using storage-level fast disk snapshot operation where available.

vm-clone

```
xe vm-clone new-name-label=name_for_clone [new-name-
description=description_for_clone] [vm-selector=vm_selector_value...]
```

Clone an existing VM, using storage-level fast disk clone operation where available. Specify the name and the optional description for the resulting cloned VM using the `new-name-label` and `new-name-description` arguments.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-compute-maximum-memory

```
xe vm-compute-maximum-memory total=amount_of_available_physical_ram_in_bytes
[approximate=add overhead memory for additional vCPUS? true|false]
[vm_selector=vm_selector_value...]
```

Calculate the maximum amount of static memory which can be allocated to an existing VM, using the total amount of physical RAM as an upper bound. The optional parameter `approximate` reserves sufficient extra memory in the calculation to account for adding extra vCPUs into the VM later.

For example:

```
xe vm-compute-maximum-memory vm=testvm total=`xe host-list params=memory-free --
minimal`
```

This command uses the value of the `memory-free` parameter returned by the `xe host-list` command to set the maximum memory of the VM named `testvm`.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-compute-memory-overhead

```
xe vm-compute-memory-overhead
```

Computes the virtualization memory overhead of a VM.

vm-copy

```
xe vm-copy new-name-label=name_for_copy [new-name-
description=description_for_copy] [sr-uuid=uuid_of_sr] [vm-
selector=vm_selector_value...]
```

Copy an existing VM, but without using storage-level fast disk clone operation (even if this option is available). The disk images of the copied VM are guaranteed to be *full images*, that is, not part of a copy-on-write (CoW) chain.

Specify the name and the optional description for the resulting copied VM using the `new-name-label` and `new-name-description` arguments.

Specify the destination SR for the resulting copied VM using the `sr-uuid`. If this parameter is not specified, the destination is the same SR that the original VM is in.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-copy-bios-strings

```
xe vm-copy-bios-strings host-uuid=host_uuid
```

Copy the BIOS strings of the given host to the VM.

> **Note:**
>
> After you first start a VM, you cannot change its BIOS strings. Ensure that the BIOS strings are correct before starting the VM for the first time.

vm-crashdump-list

```
xe vm-crashdump-list [vm-selector=vm selector value...]
```

List crashdumps associated with the specified VMs.

When you use the optional argument `params`, the value of params is a string containing a list of parameters of this object that you want to display. Alternatively, you can use the keyword `all` to show all parameters. If `params` is not used, the returned list shows a default subset of all available parameters.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-data-source-list

```
xe vm-data-source-list [vm-selector=vm selector value...]
```

List the data sources that can be recorded for a VM.

Select the VMs on which to perform this operation by using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all VMs.

Data sources have two parameters – `standard` and `enabled` – which you can seen in the output of this command. If a data source has `enabled` set to `true`, the metrics are currently being recorded to the performance database. If a data source has `standard` set to `true`, the metrics are recorded to the performance database by default (and `enabled` is also set to `true` for this data source). If a data source has `standard` set to `false`, the metrics are *not* recorded to the performance database by default (and `enabled` is also set to `false` for this data source).

To start recording data source metrics to the performance database, run the `vm-data-source-record` command. This command sets `enabled` to `true`. To stop, run the `vm-data-source-forget`. This command sets `enabled` to `false`.

vm-data-source-record

```
xe vm-data-source-record data-source=name_description_of_data-source [vm-
selector=vm selector value...]
```

Record the specified data source for a VM.

This operation writes the information from the data source to the persistent performance metrics database of the specified VMs. For performance reasons, this database is distinct from the normal agent database.

Select the VMs on which to perform this operation by using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all VMs.

vm-data-source-forget

```
xe vm-data-source-forget data-source=name_description_of_data-source [vm-
selector=vm selector value...]
```

Stop recording the specified data source for a VM and forget all of the recorded data.

Select the VMs on which to perform this operation by using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all VMs.

vm-data-source-query

```
xe vm-data-source-query data-source=name_description_of_data-source [vm-
selector=vm_selector_value...]
```

Display the specified data source for a VM.

Select the VMs on which to perform this operation by using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section. If no parameters to select hosts are given, the operation is performed on all VMs.

vm-destroy

```
xe vm-destroy uuid=uuid_of_vm
```

Destroy the specified VM. This leaves the storage associated with the VM intact. To delete storage as well, use `xe vm-uninstall`.

vm-disk-add

```
xe vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-
selector=vm_selector_value...]
```

Add a disk to the specified VMs. Select the `device` parameter from the value of the `allowed-VBD-devices` parameter of the VMs.

The `disk-size` parameter can be specified in bytes or using the IEC standard suffixes KiB, MiB, GiB, and TiB.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-disk-list

```
xe vm-disk-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

Lists disks attached to the specified VMs. The `vbd-params` and `vdi-params` parameters control the fields of the respective objects to output. Give the parameters as a comma-separated list, or the special key `all` for the complete list.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-disk-remove

```
xe vm-disk-remove device=integer_label_of_disk [vm-selector=vm_selector_value...]
```

Remove a disk from the specified VMs and destroy it.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-export

```
xe vm-export filename=export_filename [metadata=true|false] [vm-
selector=vm_selector_value...]
```

Export the specified VMs (including disk images) to a file on the local machine. Specify the file name to export the VM into using the `filename` parameter. By convention, the file name should have a `.xva` extension.

If the `metadata` parameter is `true`, the disks are not exported. Only the VM metadata is written to the output file. Use this parameter when the underlying storage is transferred through other mechanisms, and permits the VM information to be recreated. For more information, see `vm-import`.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

vm-import

```
```

```
xe vm-import filename=export_filename [metadata=true|false] [preserve=true|false]
[sr-uuid=destination_sr_uuid]
```

Import a VM from a previously exported file. If `preserve` is set to `true`, the MAC address of the original VM is preserved. The `sr-uuid` determines the destination SR to import the VM into. If this parameter is not specified, the default SR is used.

If the `metadata` is `true`, you can import a previously exported set of metadata without their associated disk blocks. Metadata-only import fails if any VDIs cannot be found (named by SR and `VDI.location`) unless the `--force` option is specified, in which case the import proceeds regardless. If disks can be mirrored or moved out-of-band, metadata import/export is a fast way of moving VMs between disjoint pools. For example, as part of a disaster recovery plan.

> **Note:**
>
> Multiple VM imports are performed faster in serial that in parallel.

`vm-install`

```
xe vm-install new-name-label=name [template-uuid=uuid_of_desired_template]
[template=template_uuid_or_name] [sr-uuid=sr_uuid | sr-name-label=name_of_sr]
[copy-bios-strings-from=host_uuid]
```

Install or clone a VM from a template. Specify the template name using either the `template-uuid` or `template` argument. Specify an SR using either the `sr-uuid` or `sr-name-label` argument. Specify to install BIOS-locked media using the `copy-bios-strings-from` argument.

> **Note:**
>
> When installing from a template that has existing disks, by default, new disks are created in the same SR as these existing disks. Where the SR supports it, these disks are fast copies. If a different SR is specified on the command line, the new disks are created there. In this case, a fast copy is not possible and the disks are full copies.
>
> When installing from a template that doesn't have existing disks, any new disks are created in the SR specified, or the pool default SR when an SR is not specified.

`vm-is-bios-customized`

```
xe vm-is-bios-customized
```

Indicates whether the BIOS strings of the VM have been customized.

vm-memory-balloon

```
xe vm-memory-balloon target=target
```

Set the memory target for a running VM. The given value must be within the range defined by the VM's memory_dynamic_min and memory_dynamic_max values.

vm-memory-dynamic-range-set

```
xe vm-memory-dynamic-range-set min=min max=max
```

Configure the dynamic memory range of a VM. The dynamic memory range defines soft lower and upper limits for a VM's memory. It's possible to change these fields when a VM is running or halted. The dynamic range must fit within the static range.

vm-memory-limits-set

```
xe vm-memory-limits-set static-min=static_min static-max=static_max dynamic-
min=dynamic_min dynamic-max=dynamic_max
```

Configure the memory limits of a VM.

vm-memory-set

```
xe vm-memory-set memory=memory
```

Configure the memory allocation of a VM.

vm-memory-shadow-multiplier-set

```
xe vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...]
[multiplier=float_memory_multiplier]
```

Set the shadow memory multiplier for the specified VM.

This is an advanced option which modifies the amount of *shadow memory* assigned to a hardware-assisted VM.

In some specialized application workloads, such as Citrix Virtual Apps, extra shadow memory is required to achieve full performance.

This memory is considered to be an overhead. It is separated from the normal memory calculations for accounting memory to a VM. When this command is invoked, the amount of free host memory decreases according to the multiplier and the `HVM_shadow_multiplier` field is updated with the value that Xen has assigned to the VM. If there is not enough Citrix Hypervisor server memory free, an error is returned.

The VMs on which this operation should be performed are selected using the standard selection mechanism. For more information, see VM selectors.

vm-memory-static-range-set

```
xe vm-memory-static-range-set min=min max=max
```

Configure the static memory range of a VM. The static memory range defines hard lower and upper limits for a VM's memory. It's possible to change these fields only when a VM is halted. The static range must encompass the dynamic range.

vm-memory-target-set

```
xe vm-memory-target-set target=target
```

Set the memory target for a halted or running VM. The given value must be within the range defined by the VM's memory_static_min and memory_static_max values.

vm-memory-target-wait

```
xe vm-memory-target-wait
```

Wait for a running VM to reach its current memory target.

vm-migrate

```
xe 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]
```

This command migrates the specified VMs between physical hosts. The `host` parameter can be either the name or the UUID of the Citrix Hypervisor server. For example, to migrate the VM to another host in the pool, where the VM disks are on storage shared by both hosts:

```
xe vm-migrate uuid=vm_uuid host-uuid=host_uuid
```

To move VMs between hosts in the same pool, which do not share storage (storage live 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
```

You can choose the SR where each VDI gets stored:

```
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
```

Additionally, you can choose which network to attach the VM after migration:

```
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
```

For cross-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
```

For more information on storage live migration, live migration, and live VDI migration, see Migrate VMs.

By default, the VM is suspended, migrated, and resumed on the other host. The `live` parameter selects live migration. Live migration keeps the VM running while performing the migration, thus minimizing VM downtime to less than a second. In some circumstances, such as extremely memory-heavy workloads in the VM, live migration falls back into default mode and suspends the VM for a short time before completing the memory transfer.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

`vm-pause`


```
xe vm-pause
```

Pause a running VM. Note this operation does not free the associated memory (see `vm-suspend`).

`vm-query-services`

```
xe vm-query-services
```

Query the system services offered by the given VMs.

`vm-reboot`

```
xe vm-reboot [vm-selector=vm_selector_value...] [force=true]
```

Reboot the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

Use the `force` argument to cause an ungraceful reboot. Where the shutdown is akin to pulling the plug on a physical server.

`vm-recover`

```
xe vm-recover vm-uuid [database] [vdi-uuid] [force]
```

Recovers a VM from the database contained in the supplied VDI.

`vm-reset-powerstate`

```
xe vm-reset-powerstate [vm-selector=vm_selector_value...] {force=true}
```

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

This is an *advanced* command only to be used when a member host in a pool goes down. You can use this command to force the pool master to reset the power-state of the VMs to be `halted`. Essentially, this command forces the lock on the VM and its disks so it can be started next on another pool host. This call *requires* the force flag to be specified, and fails if it is not on the command-line.

vm-resume

```
xe vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=host_uuid]
```

Resume the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

If the VM is on a shared SR in a pool of hosts, use the `on` argument to specify which pool member to start it on. By default the system determines an appropriate host, which might be any of the members of the pool.

vm-retrieve-wlb-recommendations

```
xe vm-retrieve-wlb-recommendations
```

Retrieve the workload balancing recommendations for the selected VM.

vm-shutdown

```
xe vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
```

Shut down the specified VM.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

Use the `force` argument to cause an ungraceful shutdown, similar to pulling the plug on a physical server.

vm-snapshot

```
xe vm-snapshot new-name-label=name_label [new-name-description+name_description]
```

Snapshot an existing VM, using storage-level fast disk snapshot operation where available.

vm-start

```
xe vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=host_uuid]
[--multiple]
```

Start the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

If the VMs are on a shared SR in a pool of hosts, use the `on` argument to specify which pool member to start the VMs on. By default the system determines an appropriate host, which might be any of the members of the pool.

`vm-suspend`

```
xe vm-suspend [vm-selector=vm_selector_value...]
```

Suspend the specified VM.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

`vm-uninstall`

```
xe vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
```

Uninstall a VM, destroying its disks (those VDIs that are marked RW and connected to this VM only) in addition to its metadata record. To destroy just the VM metadata, use `xe vm-destroy`.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

`vm-unpause`

```
xe vm-unpause
```

Unpause a paused VM.

`vm-vcpu-hotplug`

```
xe vm-vcpu-hotplug new-vcpus=new_vcpu_count [vm-selector=vm_selector_value...]
```

Dynamically adjust the number of vCPUs available to a running Linux VM. The number of vCPUs is bounded by the parameter `VCPUs-max`. Windows VMs always run with the number of vCPUs set to `VCPUs-max` and

must be rebooted to change this value.

The Linux VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

> **Note:**
>
> When running Linux VMs without Citrix VM Tools installed, run the following command on the VM as `root` to ensure the newly hot plugged vCPUs are used: `# for i in /sys/devices/system/cpu/cpu[1-9]*/online; do if [ "$(cat $i)" = 0 ]; then echo 1 > $i; fi; done`

`vm-vif-list`

```
xe vm-vif-list [vm-selector=vm_selector_value...]
```

Lists the VIFs from the specified VMs.

The VM or VMs on which this operation is performed are selected using the standard selection mechanism. For more information, see VM selectors. The selectors operate on the VM records when filtering, and *not* on the VIF values. Optional arguments can be any number of the VM parameters listed at the beginning of this section.

Scheduled snapshots

Commands for controlling VM scheduled snapshots and their attributes.

The `vmss` objects can be listed with the standard object listing command (`xe vmss-list`), and the parameters manipulated with the standard parameter commands. For more information, see Low-level parameter commands

`vmss-create`

```
xe vmss-create enabled=True/False name-label=name type=type frequency=frequency
retained-snapshots=value name-description=description schedule:schedule
```

Creates a snapshot schedule in the pool.

For example:

```
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 schedules have the following parameters:

Parameter Name	Description	Type
`name-label`	Name of the snapshot schedule.	Read/write
`name-description`	Description of the snapshot schedule.	Read/write
`type`	Disk snapshot or memory snapshot.	Read/write
`frequency`	Hourly; Daily; Weekly	Read/write
`retained-snapshots`	Snapshots to be retained. Range: 1-10.	Read/write
`schedule`	`schedule:days` (Monday to Sunday), `schedule:hours` (0 to 23), `schedule:minutes` (0, 15, 30, 45)	Read/write

`vmss-destroy`

```
xe vmss-destroy uuid=uuid
```

Destroys a snapshot schedule in the pool.

USB passthrough

USB passthrough enable/disable

```
xe pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
```

Enable/disable USB Pass-through.

`pusb-scan`

```
xe pusb-scan host-uuid=host_uuid
```

Scan PUSB and update.

`vusb-create`

```
xe vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
```

Creates a virtual USB in the pool. Start the VM to pass through the USB to the VM.

vusb-unplug

```
xe vusb-unplug uuid=vusb_uuid
```

Unplugs USB from VM.

vusb-destroy

```
xe vusb-destroy uuid=vusb_uuid
```

Removes the virtual USB list from VM.

Data Governance

This article provides information regarding the collection, storage, and retention of logs by Citrix Hypervisor.

Citrix Hypervisor is a server virtualization platform that enables the customer to create and manage a deployment of virtual machines. XenCenter is the management UI for Citrix Hypervisor. Citrix Hypervisor and XenCenter can collect and store customer data as part of providing the following capabilities:

- **Health Check** - The Health Check service runs on your XenCenter machine and generates server status reports for Citrix Hypervisor servers and pools that are enrolled in the service. The information is collected and automatically uploaded to Citrix Insight Services on a schedule defined by the customer. For more information, see Health Check.
- **Server status reports** - A server status report can also be generated on-demand and uploaded to Citrix Insight Services or provided to Citrix Support. The server status report contains information that can aid in diagnosing issues in the customer's environment.
- **Automatic updates for the Management Agent** - The Management Agent runs within VMs hosted on a Citrix Hypervisor server or pool. If the server or pool is licensed, the Management Agent can check for and apply updates to itself and to the I/O drivers in the VM. As part of checking for updates, the automatic update feature makes a web request to Citrix that can identify the VM where the Management Agent runs.
- **XenCenter check for updates** - This feature determines whether any hotfixes, cumulative updates, or new releases are available for the Citrix Hypervisor servers and pools XenCenter manages. As part of checking for updates, this feature makes a web request to Citrix that includes telemetry. This telemetry is not user-specific and is used to estimate the total number of XenCenter instances worldwide.
- **XenCenter email alerts** XenCenter can be configured to send email notifications when alert thresholds are exceeded. To send these email alerts, XenCenter collects and stores the target email address.

Data residency

Citrix Hypervisor diagnostic logs are on the server where you installed Citrix Hypervisor.

Server status reports that are uploaded to Citrix Insight Services are stored in Amazon S3 environments located in the United States.

The web logs captured from the requests made by the Management Agent automatic updates feature and the XenCenter check for updates feature are located in a Microsoft Azure Cloud environment located in the United States. These logs are then copied to a log management server in the United Kingdom.

The email address that XenCenter uses to send email alerts is stored on the machine where you installed XenCenter.

Data collection

Citrix Hypervisor and XenCenter collect information from the following data sources:

- XenCenter
- Citrix Hypervisor servers and pools
- Hosted VMs

Data transmission

XenCenter and the Health Check service transmit server status reports securely to Citrix Insight Services.

The web requests made by the Management Agent automatic updates feature and the XenCenter check for updates feature are made over HTTPS. Web log files are transmitted securely to the log management server.

Data control

Citrix Hypervisor servers and pools must be enrolled in Health Check by using your MyCitrix account to opt in to the data being collected and stored. These servers and pools can be unenrolled from Health Check at any time.

You can select which data items are included in the Health Check data and server status reports. You can also delete any Health Check data or server status reports that are uploaded to your MyCitrix account on Citrix Insight Services.

You can select whether your VM uses the Management Agent automatic update feature. If you choose to use the Management Agent automatic update feature, you can also choose whether the web request includes the VM identifying information.

The XenCenter check for updates feature is enabled by default. You can choose to disable this feature.

You can delete email alerts configured in XenCenter to remove the stored email information.

Data retention

Citrix Insight Services does not implement an automatic data retention for server status reports collected by the Health Check service or uploaded by the customer. The customer determines the data retention policy. You can choose to delete any Health Check data or server status reports that are uploaded to your MyCitrix account on Citrix Insight Services.

For more information about Citrix Insight Services data handling, see the Data Collection and Privacy statement in the Citrix Insight Services website.

Web logs containing information from web requests made by the Management Agent automatic updates feature and the XenCenter check for updates feature can be retained indefinitely.

XenCenter retains the email information used to provide email alerts for the lifetime of the email notification. When you delete the configured email alert, the data is removed.

Data collection agreement

The information that Health Check uploads to Citrix Insight Services is used for troubleshooting and diagnostics support purposes, as well as to improve the quality, reliability, and performance of our products subject to the Citrix Insight Services Policy and the Citrix Privacy Policy.

At all times, any information received by Citrix is treated in accordance with the Citrix Privacy Policy.

Appendix: data collected

- Server status report
- Management Agent automatic updates web log
- Check for updates web log
- XenCenter email alerts

Server status report

A server status report can contain the following log files:

Log type	Contains PII?
xapi-debug	maybe
xen-info	maybe
conntest	no
xha-liveset	maybe
high-availability	maybe
firstboot	yes
xenserver-databases	yes
multipath	maybe
disk-info	maybe
xenserver-logs	maybe
xenserver-install	maybe
process-list	yes
blobs	no
xapi	yes
host-crashdump-logs	maybe
xapi-subprocess	no
pam	no
control-slice	maybe
tapdisk-logs	no
kernel-info	maybe
xenserver-config	maybe

Log type	Contains PII?
xenserver-domains	no
device-model	yes
hardware-info	maybe
xenopsd	maybe
loopback-devices	maybe
system-services	no
system-logs	maybe
network-status	yes
v6d	maybe
CVSM	no
message-switch	maybe
VM-snapshot-schedule	no
xcp-rrdd-plugins	maybe
yum	if customized
fcoe	yes
xapi-clusterd	maybe
network-config	if customized
boot-loader	no

Management Agent automatic updates web log

The Management Agent automatic updates web requests can contain the following data points:

- IP address of the VM where the Management Agent is installed
- A VM UUID

XenCenter check for updates web log

The Check for updates feature web requests contain the following data points:

- IP address of the XenCenter host machine
- XenCenter version
- A UUID

XenCenter email alerts

To provide email alerts XenCenter stores the following data points:

- Email address
- SMTP server

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

Citrix Product Documentation | http://docs.citrix.com

December 9, 2021