



Citrix XenServer 7.6

Contents

Citrix XenServer 7.6 Current Release	3
What's new	3
Fixed issues	8
Known issues	9
System requirements	11
Configuration limits	16
Guest operating system support	20
Quick start	27
Technical overview	49
Licensing	57
Install	65
Installation and deployment scenarios	74
Upgrade from an existing version	79
Update your hosts	88
Troubleshoot the installation	100
Boot from SAN environments	101
Network boot installations	104
Host partition layout	110
Install on small devices	112
Hosts and resource pools	113
Clustered pools	126
Manage users	129
Role-based access control	137

RBAC roles and permissions	138
Use RBAC with the CLI	149
Configure networking	154
Manage networking	170
Troubleshoot networking	193
Configure storage	197
Storage repository formats	202
Manage storage repositories	218
Storage multipathing	230
IntelliCache	232
Storage read caching	236
PVS-Accelerator	239
Graphics overview	247
Prepare host for graphics	250
Create vGPU enabled VMs	261
Memory usage	266
Monitor and manage your deployment	268
Manage virtual machines	291
Windows VMs	296
Linux VMs	312
Configure VM memory	331
Migrate VMs	337
Import and export VMs	341
Bromium Secure Platform	358

Container management	360
vApps	368
Demo Linux virtual appliance	371
Advanced notes for virtual machines	373
Enable VNC for Linux VMs	385
Troubleshoot VM problems	397
Configure high availability	399
Disaster recovery and backup	407
Enable Disaster Recovery	410
vApps	414
Back up and restore hosts and VMs	416
VM snapshots	420
Cope with machine failures	428
Troubleshooting	432
Integration overview	435
Measured Boot Supplemental Pack	437
Workload Balancing	441
Get started with Workload Balancing	443
Administer the Workload Balancing virtual appliance	453
Configure Certificates for Workload Balancing	523
Conversion Manager	531
vSwitch and Controller	556
Manage vSwitch	561
Virtual network visibility and control	567

Administer and maintain the vSwitch Controller	584
Command-line interface	589
Troubleshoot vSwitch Controller issues	592
Command-line interface	597
SDKs and APIs	727

Citrix XenServer 7.6 Current Release

March 15, 2019

Citrix XenServer 7.6 is the latest Current Release version of Citrix XenServer (transitioning to Citrix Hypervisor in 2019). This documentation reflects features and configurations in this latest release. To learn about the new features in XenServer 7.6, see [What's New](#).

For documentation on the XenCenter 7.6 management console, see [XenCenter 7.6](#)

For documentation on previous Current Releases, see:

- [XenServer 7.5](#)
- [Legacy documentation](#)

The Citrix XenServer product lifecycle strategy for Current Releases and Long Term Service Releases is described in [Lifecycle Milestones for XenServer](#).

Note:

From XenServer 7.6 we no longer offer the XenServer documentation as individual PDF guides. The XenServer product documentation is now provided as an HTML documentation set. Use the table of contents on the left to navigate to the information that you need. On mobile, the table of contents can be accessed by clicking the menu icon.

For more information, see [New structure for the product documentation](#).

What's new

April 1, 2019

About this release

XenServer 7.6 is a Current Release (CR). The Current Release model allows customers to consume new features at the earliest possible juncture. A Current Release contrasts with the Long Term Service Release (XenServer 7.1 LTSR), which guarantees stability in terms of the feature set within XenServer.

XenServer 7.6 is available in the following editions:

- Enterprise Edition
- Standard Edition
- Free Edition

For information about the features available in each edition, see the [XenServer Feature Matrix](#).

XenServer 7.6 is available to download from the [XenServer Product Download page](#).

New features and improvements in XenServer 7.6

XenServer introduces enhanced features and functionality for application, desktop, and server virtualization use cases. All XenServer 7.6 features are available to all licensed Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) customers.

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

XenServer 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](#).

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

XenServer makes thin provisioning available to customers using block-based storage accessed through 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 [Storage](#).

It is not possible to upgrade or update from the experimental version of the feature provided in XenServer 7.5 to the fully supported feature in XenServer 7.6. If you previously used this feature as an experimental feature, complete the following steps when updating to XenServer 7.6:

1. Export any data that you want to keep from these SRs.
2. Detach and destroy any GFS2 SRs from your pool before upgrading.
3. Disable clustering on your pool.
4. Complete the update to XenServer 7.6
5. After the update completes, run the following command on all hosts in your pool:

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

6. Run the following command on the pool master:

```
1 systemctl restart xapi-clusterd
```

7. When creating a GFS2 SR for your updated pool, ensure that you select **Format** and not **Reattach**. You cannot reattach a GFS2 SR that was created with XenServer 7.5 to a XenServer 7.6 pool.

Changes to guest operating system support

XenServer now supports the following new Linux guests:

- Red Hat Enterprise Linux 7.5
- CentOS 7.5
- Oracle Linux 7.5
- Scientific Linux 7.5
- Ubuntu 18.04

For more information, see [Guest operating system support](#).

Automatic application of hotfixes during upgrade or update

XenServer simplifies the hotfix application mechanism when upgrading your XenServer 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 XenServer. 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 XenServer 7.6 to upgrade from any supported version of XenServer to XenServer 7.0 and later.

Note:

Rolling Pool Upgrade is an Enterprise Edition feature. Upgrading your XenServer hosts using the Rolling Pool Upgrade wizard is available for XenServer Enterprise Edition customers, or those who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement.

Using the Install Update wizard in XenCenter to update your version of XenServer is available to all users of XenServer. For more information about XenServer 7.6 licensing, see [Licensing](#).

New structure for the product documentation

The XenServer product documentation is now provided as an HTML documentation set.

- 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.

Support for new processors

The following processors are now supported in XenServer 7.6:

- Intel Processor families E-21xxG/21xx (Coffee Lake S)

For more information, see the [Hardware Compatibility List](#).

Installation options

XenServer 7.6 is available to download from the XenServer Product Download page in the following packages:

- XenServer 7.6 Update ISO. Use this file to update an existing installation of XenServer 7.5 or 7.4 CR.
- XenServer 7.6 Base Installation ISO. Use this file to create a fresh installation of XenServer 7.6 or to upgrade from XenServer 7.0 or 7.1 Cumulative Update 2.

Note:

- If you use XenCenter to update your hosts, update your XenCenter installation to the latest

version supplied on the XenServer 7.6 download page before beginning.

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

The following table shows the available options if moving from an existing supported version of XenServer to XenServer 7.6.

Installed Version	Update using XenServer 7.6 Update ISO	Upgrade using XenServer 7.6 Base Installation ISO
XenServer 7.5	Yes	No
XenServer 7.4	Yes	No
XenServer 7.1 Cumulative Update 2	No	Yes
XenServer 7.0	No	Yes

Upgrade from XenServer 7.1 with CU 1 applied. Ensure that you update your XenServer 7.1 to the latest Cumulative Update before upgrading to XenServer 7.6.

Before beginning installation, review the [System requirements](#) and [Installation and deployment scenarios](#).

Changing from the Long Term Service Release to the Current Release

If you're running a XenServer LTSR, but want to take advantage of new features, you can decide to change to the XenServer CR stream. Using the XenServer versions from the CR stream requires you to adopt new CRs regularly to remain in support.

Move to this Current Release by upgrading from XenServer 7.1 Cumulative Update 2 LTSR.

Changing from the Current Release to the Long Term Service Release

If you're running a XenServer CR, but instead want to move to a version of XenServer with a guaranteed and stable feature set, you can change to a XenServer LTSR. The latest XenServer LTSR is available to download from the XenServer Product Download page.

Move to the latest LTSR by creating a fresh installation of XenServer 7.1 Cumulative Update 2 LTSR.

For more information about LTSRs and CRs, see [Citrix Virtual Apps, Citrix Virtual Desktops, and XenServer Servicing Options](#).

Licensing

Customers must upgrade their Citrix License Server to version 11.14 or higher to use all XenServer 7.6 licensed features.

For more information about XenServer 7.6 licensing, see [Licensing](#).

Hardware compatibility

For the most recent additions and advice for all hardware compatibility questions, see the XenServer [Hardware Compatibility List](#).

Interoperability with Citrix products

XenServer 7.6 is interoperable with Citrix XenApp and XenDesktop 7.15 (LTSR), and Citrix Virtual Apps and Desktops 7 1808.

XenServer 7.6 is interoperable with Citrix Provisioning 7.15 and 1808.

Citrix product names are transitioning as we unify our product portfolio. For more information, see <https://www.citrix.com/about/citrix-product-guide/>.

Localization support

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

Product documentation

To access XenServer 7.6 product documentation, see [XenServer 7.6 Product Documentation](#). For FAQ about XenServer, see [Technical overview](#).

Documentation can be updated or changed after the initial release. We suggest that you regularly visit the [Citrix Product Documentation](#) to learn about updates.

Fixed issues

August 21, 2018

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

- For XenServer pools that use certain storage targets, a race condition in the iSCSI module can cause hosts in the pool to fail. (CA-287658)

- A Windows 10 VM with the I/O drivers installed can fail with bugcheck code 139. This is caused by a Windows issue which causes an inconsistent state during nonpaged memory allocation. (CA-290852)
- On reboot, VMs can fail to start with the error code SR_BACKEND_FAILURE_453. (CA-292268)
- Live migration of VMs newly created on XenServer 7.5 is incompatible with adding or removing a network device from a Windows VM configured with has-vendor-device to be true (to enable Windows Update for PV drivers). VMs live migrated from a previous version of XenServer are not affected by this issue. (CA-286948)
- After rebooting, a XenServer host can fail to connect to iSCSI targets on Compellent arrays. (CA-288738)
- When shutting down, the XenServer host can hang at 'reached target shutdown'. This happens if XAPI is unable to cleanly unplug PBDs to iSCSI SRs before shutdown. (CA-288738)
- When updating the PVS Accelerator Supplemental Pack, the update can fail with the following error in XenCenter: UPDATE_APPLY_ERROR. (CA-292633)
- XenCenter can fail after automatically reconnecting to a pool that it had previously lost connection to. (CA-289150)
- When a user with the Pool Operator role tries to create a new SR of the type Hardware HBA or Software FCoE by using XenCenter, the scan for LUNs can fail. (CA-290064)
- Importing a VHD type of VDI file larger than 1TiB was unsupported and led to an VDI_IO_ERROR. (CA-292288)
- When you attempt to migrate a VM between resource pools, the migration can fail with the following error: `Storage_interface.Internal_error("Jsonrpc.Parse_error(_)")`. This migration failure can cause some versions of XenCenter to fail. (CA-291048)
- An out-of-memory condition in the PV-IOMMU module of the Xen hypervisor can cause the XenServer host to fail. (CA-290664)

Known issues

February 5, 2019

This article contains advisories and minor issues in XenServer 7.6 release and any workarounds that you can apply.

General

- 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)

- Do not assign more than 32 GB of memory to Dom0, as intermittent VM freezes can occur, often during boot of VMs. (CA-236674)

Internationalization

- Non-ASCII characters, for example, characters with accents, cannot be used in the host console. (CA-40845)
 - XenServer root passwords must not contain non-ASCII characters. (CA-47461)
 - In a Windows VM with XenServer Tools 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)

Installation

- If you have previously upgraded your XenServer installation from XenServer 6.5 or earlier, with virtual machines using the server's "Local Storage" storage repository, or when a vendor utility partition is present on your disk, you are using a legacy disk layout. The legacy disk layout means that the control domain has less space available to it than the current layout (4 GB vs 18 GB).

When applying the XenServer 7.6 update to the XenServer 7.4 or 7.5 installation, you receive the error message "the server does not have enough space." The error message appears because installation of the XenServer 7.6 update requires sufficient free space to avoid filling the disk, which is not possible with the legacy layout.

When you receive this error, you cannot update to XenServer 7.6. You must perform a fresh installation instead. (CA-268846)

- For customers on AMD hardware, you cannot live migrate a VM from a host running a previous version of XenServer to a host running XenServer 7.6. For example, while upgrading or updating hosts in a pool to XenServer 7.6.

This issue is caused by a change in the AMD microcode level between the two versions of XenServer. For more information, see [CTX237585 - Unable to live migrate VMs on AMD hardware](#).

To work around this issue, shut down any VMs that you want to migrate from the older version of XenServer and restart the VMs after the host has been upgraded or updated to XenServer 7.6. (CA-293595)

Storage

- Operations on all 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. (CP-28758)

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)
- When XenCenter is installed on Windows Server 2008 SP2, it can fail to connect to a XenServer host with the message “Could not create SSL/TLS secure channel”. To resolve this issue, ensure that one of the following Windows Updates is installed on the Windows Server 2008 SP2 system: KB4056564 or KB4019276. For more information, see <http://support.microsoft.com/kb/4019276>. (CA-298456)

Guests

- On XenServer hosts that use the `bnxt_en` driver, Oracle 6.x VMs can crash when connecting to a network. Ensure that your `bnxt_en` driver is up-to-date by installing the following driver disk: [Driver Disk for Broadcom bnxt_en-1.8.29 - For XenServer 7.x CR](#). (CA-288010)
- When installing the XenServer PV Tools, the XenServer PV Tools can request to restart with `/quiet /norestart` or `/quiet /forcerestart` specified after the VM has already been restarted once as part of the installation. (CA-290693)
- Suspending or migrating a Linux VM with outstanding xenstore transactions can hang due to an issue in the VM’s Linux kernel. If your VM experiences this hang, force the VM to shut down and restart it. (CP-30551)

vSwitch Controller

- When changing the IP address assignment mode from DHCP to static, you must restart the vSwitch Controller Virtual Appliance. (CA-293927)

System requirements

October 4, 2018

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

Warning:

Citrix Systems, Inc. does not support installation third-party software directly in the control domain of the XenServer. The exception is for software supplied as a supplemental pack and explicitly endorsed by Citrix Systems, Inc.

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 XenServer CLI is also installed.

A standalone remote XenServer CLI can be installed on any general purpose Linux system.

XenServer host system requirements

Although XenServer is usually deployed on server-class hardware, XenServer 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 XenServer hardware specifications.

The XenServer host must be a 64-bit x86 server-class machine devoted to hosting VMs. XenServer 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.

XenServer can use:

- Up to 5 TB of RAM
- Up to 16 physical NICs
- Up to 288 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 XenServer host 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 XenServer host. 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 (PATA, SATA, SCSI) 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 P2V and 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.

XenServer 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 XenServer 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 or HP iLO. For more information about setting up serial console

access, see [CTX228930 - How to Configure Serial Console Access on XenServer and later](#).

XenCenter system requirements

XenCenter has the following system requirements:

- **Operating System:**
 - Windows 10
 - Windows 8.1
 - Windows 7 SP1
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2 SP1
 - Windows Server 2008 SP2 (see Note)
 - Windows Server 2016
- **.NET Framework:** Version 4.6
- **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 XenServer.

Note:

When XenCenter is installed on Windows Server 2008 SP2, ensure that one of the following Windows Updates is installed on the Windows Server 2008 SP2 system: KB4056564 or KB4019276. For more information, see <http://support.microsoft.com/kb/4019276>.

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 XenServer 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 XenServer, 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 XenServer 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 XenServer 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.

XenServer hosts 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 you want your environment to have hosts with varying CPUs in the same resource pool, you can force join a pool together using the CLI. For information about forcing the joining operation, see [Hosts and resource pools](#).

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

October 4, 2018

Citrix recommends using the following configuration limits as a guideline when selecting and configuring your virtual and physical environment for XenServer. Citrix fully supports for XenServer the following tested and recommended configuration limits.

- Virtual machine limits
- XenServer host 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 TB (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)	2 TB minus 4 GB
Virtual Disk Size (LVM)	2 TB minus 4 GB
Networking	
Virtual NICs per VM	7 (see note 4)

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 GB of RAM through use of the physical address extension (PAE) mode. The limit for 32-bit PV Virtual Machines is 64 GB. 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 XenServer Tools to achieve this limit.

XenServer host limits

Item	Limit
Compute	
Logical processors per host	288 (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	5 TB (see note 4)
Storage	
Concurrent active virtual disks per host	4096
Networking	
Physical NICs per host	16
Physical NICs per network bond	4
Virtual NICs per host	512
VLANs per host	800
Network Bonds per host	4
Graphics Capability	
GPUs per host	12 (See note 5)

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/host supported depends on VM workload, system load, net-

work configuration, and certain environmental factors. Citrix reserves the right to determine what specific environmental factors affect the maximum limit at which a system can function. For systems running over 500 VMs, Citrix recommends allocating 8 GB RAM to the Control Domain (Dom0).

For information about configuring Dom0 memory, see [CTX134951 - How to Configure dom0 Memory in XenServer 6.2 and Later](#).

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. If a host has one or more 32-bit paravirtualized guests (Linux VMs), running a maximum of 128 GB RAM is supported on the host.
5. This figure might change. For the current supported limits, see the [Hardware Compatibility List](#).

Resource pool limits

Item	Limit
Compute	
VMs per resource pool	4096
Hosts per resource pool	64 (See note 1)
Networking	
VLANs per resource pool	800
Active hosts per cross-server private network	64
Cross-server private networks per resource pool	16
Virtual NICs per cross-server private network	16
Cross-server private network virtual NICs per resource pool	256
Hosts per vSwitch controller	64
Virtual NICs per vSwitch controller	1024
VMs per vSwitch controller	1024

Item	Limit
Disaster recovery	
Integrated site recovery storage repositories per resource pool	8
Storage	
Paths to a LUN	8
Multipathed LUNs per host	256 (See note 2)
Multipathed LUNs per host (used by storage repositories)	256 (See note 2)
VDIs per SR (NFS, SMB, EXT, GFS2)	20000
VDIs per SR (LVM)	1000
Storage XenMotion	
(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, Citrix recommends 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

November 5, 2018

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	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Windows 7 SP1, Windows 8.1, Windows 10 (32-bit)	HVM	1 GB	4 GB	24 GB (40 GB or more recommended)
Windows 7 SP1 (64-bit)	HVM	2 GB	192 GB	24 GB (40 GB or more recommended)
Windows 8.1 (64-bit)	HVM	2 GB	512 GB	24 GB (40 GB or more recommended)
Windows 10 (64-bit)	HVM	2 GB	1.5 TB	24 GB (40 GB or more recommended)
Windows Server 2008 SP2 (32-bit)	HVM	512 MB	64 GB	24 GB (40 GB or more recommended)
Windows Server 2008 SP2 (64-bit)	HVM	512 MB	1 TB	24 GB (40 GB or more recommended)
Windows Server 2008 R2 SP1	HVM	512 MB	1.5 TB	24 GB (40 GB or more recommended)
Windows Server 2012, Windows Server 2012 R2 (64-bit), Windows Server 2016, Windows Server Core 2016 (64-bit)	HVM	1 GB	1.5 TB	24 GB (40 GB or more recommended)
CentOS 5.x (32-bit)	PV	512 MB	16 GB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
CentOS 5.0–5.7 (64-bit)	PV	512 MB	16 GB	8 GB
CentOS 5.8–5.11 (64-bit)	PV	512 MB	128 GB	8 GB
CentOS 6.0, 6.1 (32-bit)	PV	1 GB	8 GB	8 GB
CentOS 6.0, 6.1 (64-bit)	PV	512 MB	32 GB	8 GB
CentOS 6.2–6.9 (32-bit)	PV	512 MB	16 GB	8 GB
CentOS 6.2–6.9 (64-bit)	PV	1 GB	128 GB	8 GB
CentOS 7.x (64-bit)	HVM	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 5.x (32-bit)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 5.0–5.7 (64-bit)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 5.8–5.11 (64-bit)	PV	512 MB	128 GB	8 GB
Red Hat Enterprise Linux 6.0, 6.1 (32-bit)	PV	512 MB	8 GB	8 GB
Red Hat Enterprise Linux 6.0, 6.1 (64-bit)	PV	1 GB	32 GB	8 GB
Red Hat Enterprise Linux 6.2–6.9 (32-bit)	PV	512 MB	16 GB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Red Hat Enterprise Linux 6.2–6.9 (64-bit)	PV	1 GB	128 GB	8 GB
Red Hat Enterprise Linux 7.x (64-bit)	HVM	2 GB	1.5 TB	10 GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (32-bit)	PV	1 GB	16 GB	8 GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (64-bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64-bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12 SP3 (64-bit)	HVM	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 11 SP3 (64-bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64-bit)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12 SP3 (64-bit)	HVM	1 GB	1.5 TB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Oracle Linux 5.0–5.7, 5.10, 5.11 (32-bit)	PV	512 MB	64 GB	8 GB
Oracle Linux 5.8, 5.9 (32-bit)	PV	512 MB	16 GB	8 GB
Oracle Linux 5.x (64-bit)	PV	512 MB	128 GB	8 GB
Oracle Linux 6.x (32-bit)	PV	512 MB	8 GB	8 GB
Oracle Linux 6.0, 6.1 (64-bit)	PV	1 GB	32 GB	8 GB
Oracle Linux 6.2–6.9 (64-bit)	PV	1 GB	128 GB	8 GB
Oracle Linux 7.x (64-bit)	HVM	2 GB	1.5 TB	10 GB
Scientific Linux 6.6–6.9 (32-bit)	PV	512 MB	16 GB	8 GB
Scientific Linux 6.6–6.9 (64-bit)	PV	1 GB	128 GB	8 GB
Scientific Linux 7.x (64-bit)	HVM	2 GB	1.5 TB	10 GB
Debian Squeeze 6 (32-bit/64-bit)	PV	128 MB	32 GB	8 GB
Debian Wheezy 7 (32-bit)	PV	512 MB	32 GB	8 GB
Debian Wheezy 7 (64-bit)	PV	512 MB	128 GB	8 GB
Debian Jessie 8 (32-bit)	HVM	128 MB	64 GB	8 GB
Debian Jessie 8 (64-bit)	HVM	128 MB	1.5 TB	8 GB
Debian Stretch 9 (32-bit/64-bit)	HVM	256 MB	1.5 TB	10 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Ubuntu 12.04 (32-bit)	PV	128 MB	32 GB	8 GB
Ubuntu 12.04 (64-bit)	PV	128 MB	128 GB	8 GB
Ubuntu 14.04 (32-bit)	HVM	512 MB	64 GB	8 GB
Ubuntu 14.04 (64-bit)	HVM	512 MB	192 GB	8 GB
Ubuntu 16.04 (32-bit)	HVM	512 MB	64 GB	10 GB
Ubuntu 16.04 (64-bit)	HVM	512 MB	1.5 TB	10 GB
Ubuntu 18.04 (64-bit)	HVM	512 MB	1.5 TB	10 GB
CoreOS Stable (64-bit) [Latest tested version is 1632.3.0]	HVM	1 GB	512 GB	8 GB
NeoKylin Linux Advanced Server 6.5 (64-bit)	PV	1 GB	128 GB	8 GB
NeoKylin Linux Advanced Server 7.2 (64-bit)	PV	1 GB	1.5 TB	10 GB
NeoKylin Linux Security OS V5.0 (64-bit)	PV	1 GB	128 GB	8 GB
Asianux Server 4.2 (64-bit)	PV	1 GB	128 GB	8 GB
Asianux Server 4.4 (64-bit)	PV	1 GB	128 GB	8 GB
Asianux Server 4.5 (64-bit)	PV	1 GB	128 GB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
GreatTurbo Enterprise Server 12.2 (64-bit)	PV	1 GB	128 GB	8 GB
Linux v6.0 (64-bit)	HVM	1 GB	900 GB	10 GB
Linux v8.0 (64-bit)	HVM	1 GB	900 GB	10 GB
Yinhe Kylin 4.0 (64-bit)	HVM	1 GB	900 GB	10 GB

Important:

- RHEL, OL, and CentOS 5.x guest operating systems with the original kernel fail to start on XenServer 7.6. Before attempting to upgrade XenServer hosts to 7.6, update the kernel to version 5.4 (2.6.18-164.el5xen) or later.
- 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 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.

Notes:

- 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

XenServer 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

Quick start

October 17, 2018

This article steps through how to install and configure XenServer and its graphical, Windows-based user interface, XenCenter. After installation, it takes you through creating Windows virtual machines (VMs) and then making customized VM templates you can use to create multiple, similar VMs quickly. Finally, this article shows how to create a pool of hosts, which provides the foundation to migrate running VMs between hosts using XenMotion.

Focusing on the most basic scenarios, this article aims to get you set up quickly.

This article is primarily intended for new users of XenServer and XenCenter. It is intended for those users who want to administer XenServer by using XenCenter. For information on how to administer XenServer using the Linux-based `xe` commands through the XenServer Command Line Interface (CLI), see [Command-line interface](#).

Terminology and abbreviations

- *Host*: a physical computer that runs XenServer
- *Virtual Machine (VM)*: a computer composed entirely of software that can run its own operating system and applications as if it were a physical computer. A VM behaves exactly like a physical computer and contains its own virtual (software-based) CPU, RAM, hard disk, and NIC.
- *Pool*: a single managed entity that binds together multiple XenServer hosts and their VMs
- *Storage Repository (SR)*: a storage container in which virtual disks are stored

Major components

XenServer

XenServer is a complete server virtualization platform, with all the capabilities required to create and manage a virtual infrastructure. XenServer is optimized for both Windows and Linux virtual servers.

XenServer runs directly on server hardware without requiring an underlying operating system, which results in an efficient and scalable system. XenServer abstracts elements from the physical machine (such as hard drives, resources, and ports) and allocating them to the virtual machines (VMs) running on it.

XenServer lets you create VMs, take VM disk snapshots, and manage VM workloads.

XenCenter

XenCenter is a graphical, Windows-based user interface. XenCenter enables you to manage XenServer hosts, pools, and shared storage. Use XenCenter to deploy, manage, and monitor VMs from your Windows desktop machine.

The *XenCenter Online Help* is also a great resource for getting started with XenCenter. Press F1 at any time to access context-sensitive information.

Install XenServer and XenCenter

In this section, you set up a minimum XenServer installation.

What you'll learn

You'll learn how to:

- Install XenServer on a single physical host
- Install XenCenter on a Windows computer
- Connecting XenCenter and XenServer to form the infrastructure for creating and running virtual machines (VMs).

Requirements

To get started, you need the following items:

- A physical computer to be the XenServer host
- A Windows computer to run the XenCenter application
- Installation files for XenServer and XenCenter

The XenServer host computer is dedicated entirely to the task of running XenServer and hosting VMs, and is not used for other applications. The computer that runs XenCenter can be any general-purpose Windows computer that satisfies the hardware requirements. You can use this computer to run other applications too. For more information, see [System Requirements](#).

Install the XenServer host

All hosts have at least one IP address associated with them. To configure a static IP address for the host (instead of using DHCP), have the static IP address on hand before beginning this procedure.

Tip:

Press **F12** to advance quickly to the next installer screen. For general help, press **F1**.

To install the XenServer host:

1. Burn the installation files for XenServer to a CD.

Note:

For information about using HTTP, FTP, or NFS as your installation source, see [Install XenServer](#).

2. Back up data you want to preserve. Installing XenServer overwrites data on any hard drives that you select to use for the installation.
3. Insert the installation CD into the DVD drive of the host computer.
4. Restart the host computer.
5. Boot from the DVD drive (if necessary, see your hardware vendor documentation for information on changing the boot order).
6. Following the initial boot messages and the **Welcome to XenServer** screen, select your keyboard layout for the installation.
7. When the **Welcome to XenServer Setup** screen is displayed, select **Ok**.
8. Read and accept the XenServer EULA.

Note:

If you see a **System Hardware** warning and suspect that hardware virtualization assist support is available on your system, see your hardware manufacturer for BIOS upgrades.

9. Select **Ok** to do a clean installation.
10. If you have multiple hard disks, choose a Primary Disk for the installation. Select **Ok**.
Choose which disks you want to use for virtual machine storage. Choose **Ok**.
11. Select **Local media** as your installation source.
12. Select **Skip Verification**, and then choose **Ok**.

Note:

If you encounter problems during installation, verify the installation source.

13. Create and confirm a root password, which the XenCenter application uses to connect to the XenServer host.
14. Set up the management interface to use to connect to XenCenter.
If your computer has multiple NICs, select the NIC which you want to use for management traffic (typically the first NIC).
15. Configure the Management NIC IP address with a static IP address or use DHCP.
16. Specify the hostname and the DNS configuration manually or automatically through DHCP.
If you manually configure the DNS, enter the IP addresses of your primary (required), secondary (optional), and tertiary (optional) DNS servers in the fields provided.
17. Select your time zone.
18. Specify how you want the server to determine local time: using NTP or manual time entry. Choose **Ok**.
If using NTP, you can specify whether DHCP sets the time server. Alternatively, you can enter at least one NTP server name or IP address in the following fields.
19. Select **Install XenServer**.
20. If you selected to set the date and time manually, you are prompted to do so.
21. If you are installing from CD, the next screen asks if you want to install any supplemental packs from a CD. Choose **No** to continue.
22. From the **Installation Complete** screen, eject the installation CD from the drive, and then select ***Ok** to reboot the server.

After the server reboots, XenServer displays **xsconsole**, a system configuration console.

Note:

Make note of the IP address displayed. You use this IP address when you connect XenCenter to the host.



Install XenCenter

XenCenter is typically installed on your local system.

To install XenCenter:

1. Mount the XenCenter installation ISO on the computer that you want to run XenCenter.
2. Open the `client_install` folder.
3. Double-click `XenCenterSetup.exe` to begin the installation.
4. Follow the Setup wizard, which allows you to modify the default destination folder and then to install XenCenter.

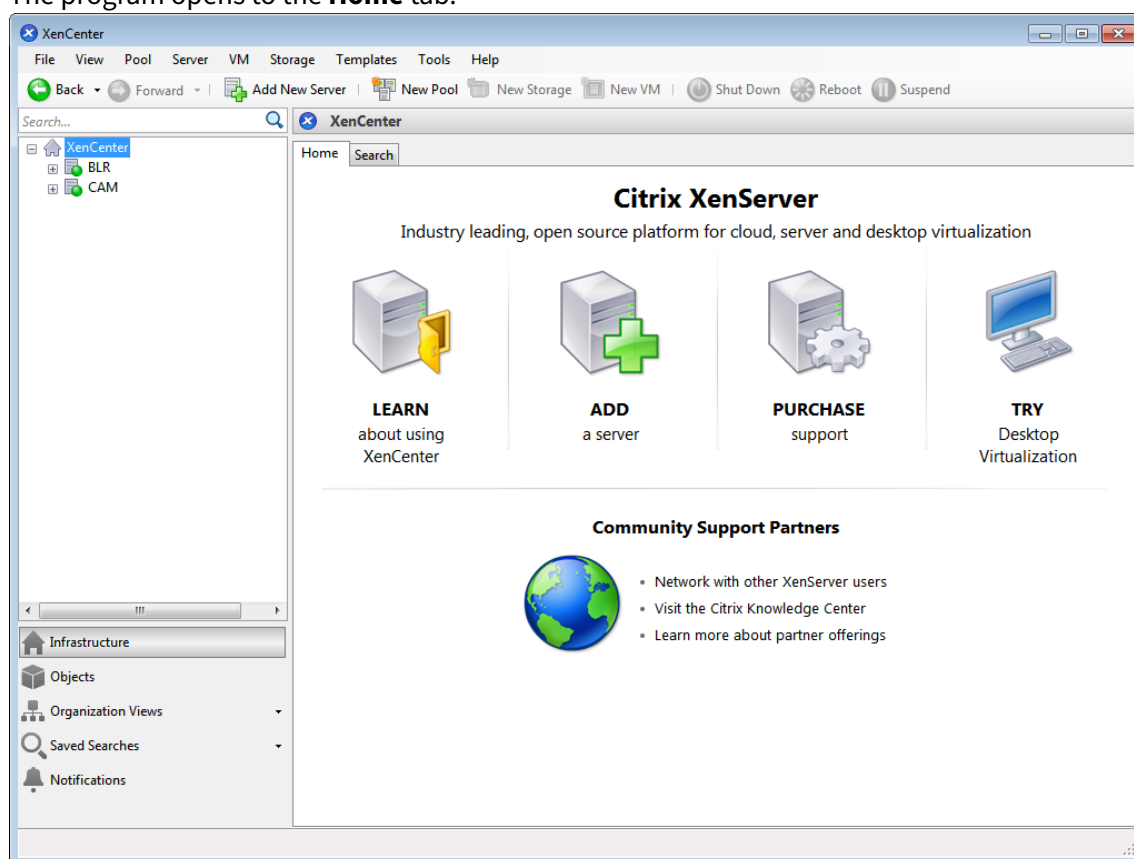
Connect XenCenter to the XenServer host

This procedure enables you to add a host to XenCenter.

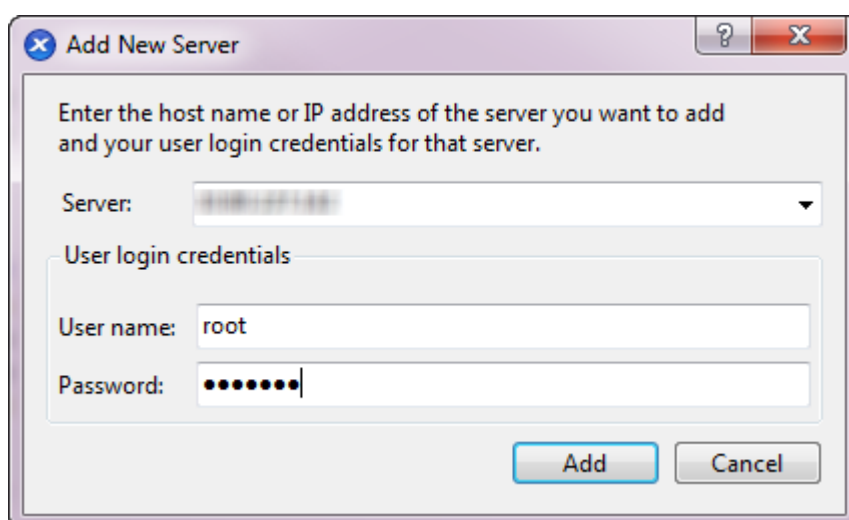
To connect XenCenter to the XenServer host:

1. Launch XenCenter.

The program opens to the **Home** tab.



2. Click the **ADD a server** icon to open the **Add New Server** dialog box.



3. In the **Server** field, enter the IP address of the host. Enter the root username and password that you set during XenServer installation. Choose **Add**.

Note:

The first time you add a host, the **Save and Restore Connection State** dialog box appears. This dialog box enables you to set your preferences for storing your host connection information and automatically restoring server connections.

License XenServer

You can use XenServer without a license (Free Edition). However, this edition provides a restricted set of features.

If you have a XenServer license, apply it now.

For more information, see [Licensing](#).

Create a pool of XenServer hosts

A resource pool is composed of multiple XenServer host installations, bound together as a single managed entity.

Resource pools enable you to view multiple hosts and their connected shared storage as a single unified resource. You can flexibly deploy of VMs across the resource pool based on resource needs and business priorities. A pool can contain up to 64 hosts running the same version of XenServer software, at the same patch level, and with broadly compatible hardware.

One host in the pool is designated as the *pool master*. The pool master provides a single point of contact for the whole pool, routing communication to other members of the pool as necessary. Every

member of a resource pool contains all the information necessary to take over the role of master if necessary. The pool master is the first host listed for the pool in the XenCenter Resources pane. You can find the pool master's IP address by selecting the pool master and clicking the **Search** tab.

In a pool with shared storage, you can start VMs on *any* pool member that has sufficient memory and dynamically move the VMs between hosts. The VMs are moved while running and with minimal downtime. If an individual XenServer host suffers a hardware failure, you can restart the failed VMs on another host in the same pool.

If the high availability feature is enabled, protected VMs are *automatically* moved if a host fails. On an HA-enabled pool, a new pool master is automatically nominated if the master is shut down.

Note:

For a description of heterogeneous pool technology, see [Hosts and resource pools](#).

What you'll learn

You'll learn how to:

- Create a pool of hosts
- Set up a network for the pool
- Bond NICs
- Set up shared storage for the pool

While XenServer accommodates many shared storage solutions, this section focuses on two common types: NFS and iSCSI.

Requirements

To create a pool with shared storage, you need the following items:

- A second XenServer host, with similar processor type.
Connect this host to your XenCenter application.
- A storage repository for IP-based storage

To get you started quickly, this section focuses on creating *homogeneous* pools. Within a homogeneous pool, all hosts must have compatible processors and be running the same version of XenServer, under the same type of XenServer product license. For a full list of homogeneous pool requirements, see [System requirements](#).

Create a pool

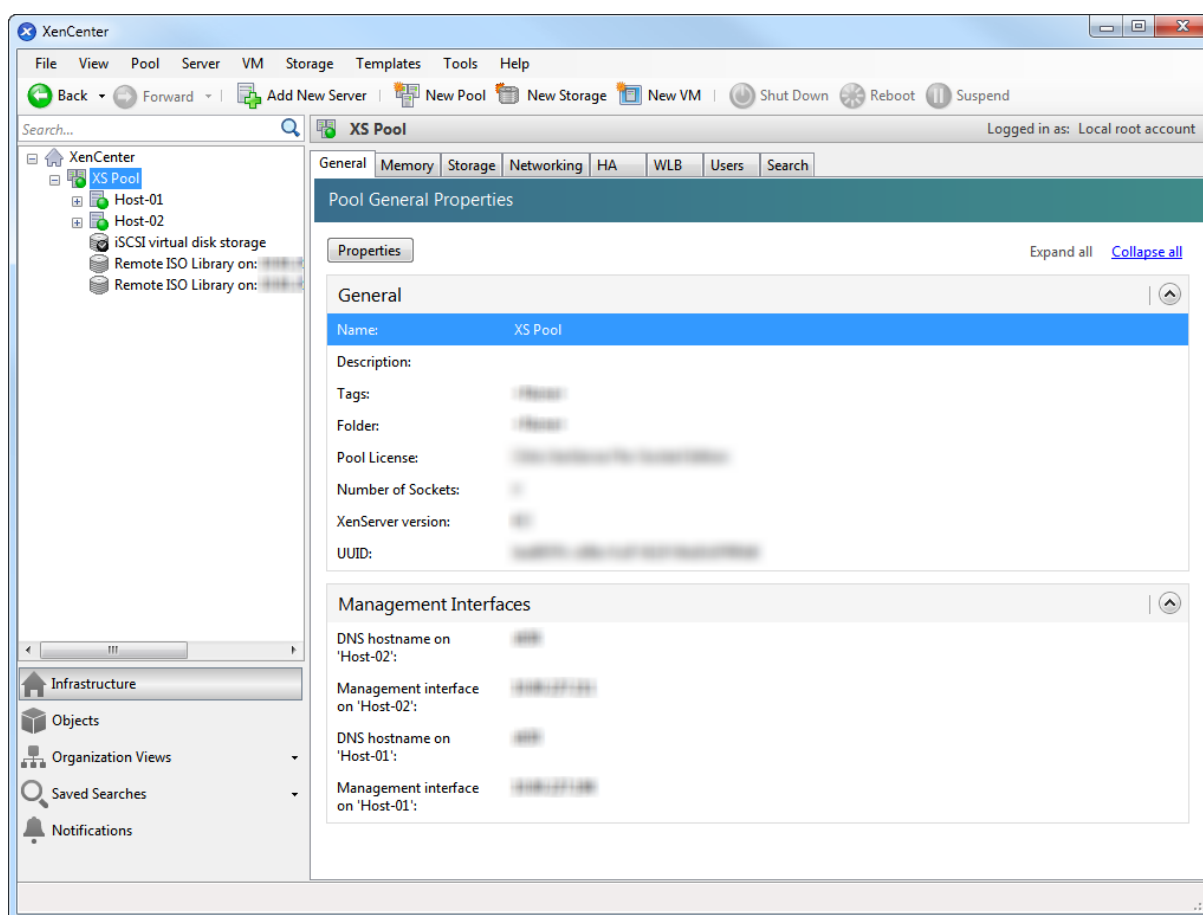
To create a pool:

1. On the toolbar, click the **New Pool** button.



2. Enter a name and optional description for the new pool.
3. Nominate the pool master by selecting a host from the **Master** list.
4. Select the second host to place in the new pool from the **Additional members** list.
5. Click **Create Pool**.

The new pool appears in the **Resources** pane.



Set up networks for the pool

When you install XenServer, you create a network connection, typically on the first NIC in the pool where you specified an IP address (during XenServer installation).

However, you may need to connect your pool to VLANs and other physical networks. To do so, you must add these networks to the pool. You can configure XenServer to connect each NIC to one physical network and numerous VLANs.

Before creating networks, ensure that the cabling matches on each host in the pool. Plug the NICs on each host into the same physical networks as the corresponding NICs on the other pool members.

Note:

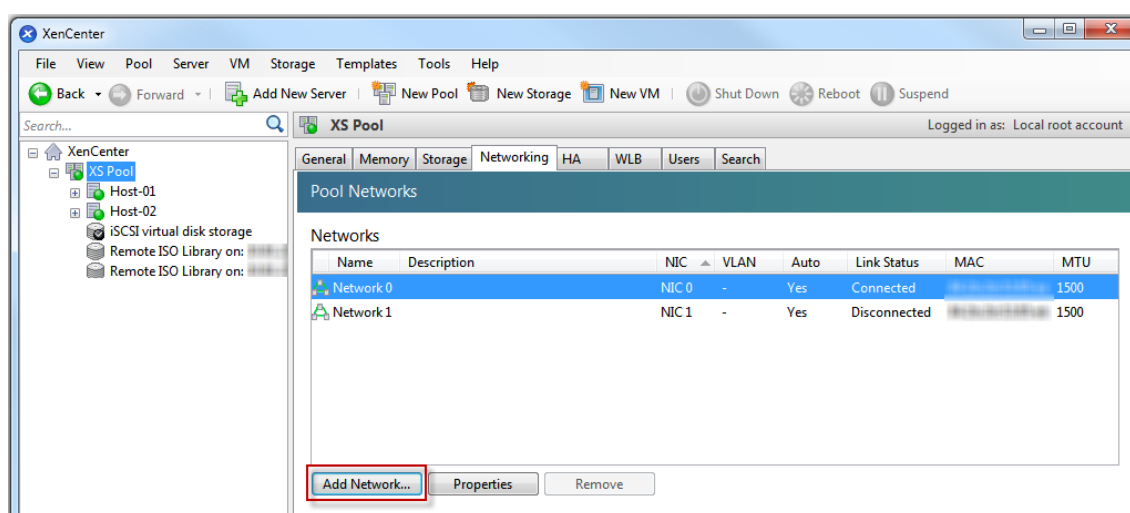
If the NICs were not plugged in to the NICs on the host when you installed XenServer:

- Plug the NICs in
- In XenCenter, select **<your host> > NICs** tab
- Click **Rescan** for them to appear

For additional information about configuring XenServer networking, see the *XenCenter Help* and [Networking](#).

To add a network to XenServer:

1. In the **Resources** pane in XenCenter, select the pool.
2. Click the **Networking** tab.
3. Click **Add Network**.



4. On the **Select Type** page, select **External Network**, and click **Next**.
5. On the **Name** page, enter a meaningful name for the network and description.
6. On the **Network settings** page, specify the following:
 - **NIC:** Select the NIC that you want XenServer to use to send and receive data from the network.
 - **VLAN:** If the network is a VLAN, enter the VLAN ID (or “tag”).
 - **MTU:** If the network uses jumbo frames, enter a value for the Maximum Transmission Unit (MTU) between 1500 to 9216. Otherwise, leave the MTU box at its default value of 1500.

If you configure many virtual machines to use this network, you can select the **Automatically add this network to new virtual machines** check box. This option adds the network by default.

7. Click **Finish**.

Bonding NICs

NIC bonding can make your server more resilient by using two or more physical NICs as if they were a single, high-performing channel. This section only provides a very brief overview of bonding, also known as *NIC teaming*. Before configuring bonds for use in a production environment, Citrix Systems, Inc. recommends reading more in-depth information about bonding. For more information, see [Networking](#).

XenServer supports the following bond modes: Active/active, active/passive (active/backup), and LACP. Active/active provides load balancing and redundancy for VM-based traffic. For other types of traffic (storage and management), active/active cannot load balance traffic. As a result, LACP or multipathing are better choice for storage traffic. For information about multipathing, see [Storage](#). For more information about bonding, see [Networking](#).

LACP options are not visible or available unless you configure the vSwitch as the network stack. Likewise, your switches must support the IEEE 802.3ad standard. The switch must contain a separate LAG group configured for each LACP bond on the host. For more details about creating LAG groups, see [Networking](#).

To bond NICs:

1. Ensure that the NICs you want to bind together (the bond slaves) are not in use: shut down any VMs with virtual network interfaces using the bond slaves before creating the bond. After you have created the bond, you will need to reconnect the virtual network interfaces to an appropriate network.
2. Select the server in the **Resources** pane then open the **NICs** tab and click **Create Bond**.
3. Select the NICs you want to bond together. To select a NIC, select its check box in the list. Up to four NICs may be selected in this list. Clear the check box to deselect a NIC. To maintain a flexible and secure network, you can bond either two, three, or four NICs when vSwitch is the network stack. However, you can only bond two NICs when Linux bridge is the network stack.
4. Under **Bond** mode, choose the type of bond:
 - Select **Active-active** to configure an active-active bond. Traffic is balanced between the bonded NICs. If one NIC within the bond fails, the host server's network traffic automatically routes over the second NIC.
 - Select **Active-passive** to configure an active-passive bond. Traffic passes over only one of the bonded NICs. In this mode, the second NIC only becomes active if the active NIC fails, for example, if it loses network connectivity.

- Select **LACP with load balancing based on source MAC address** to configure a LACP bond. The outgoing NIC is selected based on MAC address of the VM from which the traffic originated. Use this option to balance traffic in an environment where you have several VMs on the same host. This option is not suitable if there are fewer virtual interfaces (VIFs) than NICs: as load balancing is not optimal because the traffic cannot be split across NICs.
- Select **LACP with load balancing based on IP and port of source and destination** to configure a LACP bond. The source IP address, source port number, destination IP address, and destination port number are used to allocate the traffic across the NICs. Use this option to balance traffic from VMs in an environment where the number of NICs exceeds the number of VIFs.

Note:

LACP bonding is only available for the vSwitch, whereas active-active and active-passive bonding modes are available for both the vSwitch and Linux bridge. For information about networking stacks, see [Networking](#).

5. To use jumbo frames, set the Maximum Transmission Unit (MTU) to a value between 1500 to 9216.
6. To have the new bonded network automatically added to any new VMs created using the New VM wizard, select the check box.
7. Click **Create** to create the NIC bond and close the dialog box.

XenCenter automatically moves management and secondary interfaces from bond slaves to the bond master when the new bond is created. A server with its management interface on a bond is not permitted to join a pool. Before the server can join a pool, you must reconfigure the management interface and move it back on to a physical NIC.

Setting up shared storage for the pool

To connect the hosts in a pool to a remote storage array, create a XenServer SR. The SR is the storage container where a VM's virtual disks are stored. SRs are persistent, on-disk objects that exist independently of XenServer. SRs can exist on different types of physical storage devices, both internal and external. These types include local disk devices and shared network storage.

You can configure a XenServer SR for various different types of storage, including:

- NFS
- Software iSCSI
- Hardware HBA
- SMB

- Fibre Channel
- Software FCoE

This section steps through setting up two types of shared SRs for a pool of hosts: NFS and iSCSI. Before you create an SR, configure your NFS or iSCSI storage array. Setup differs depending on the type of storage solution that you use. For more information, see your vendor documentation. Generally, before you begin, complete the following setup for your storage solution:

- **iSCSI SR:** You must have created a volume and a LUN on the storage array.
- **NFS SR:** You must have created the volume on the storage device.
- **Hardware HBA:** You must have done the configuration required to expose the LUN before running the New Storage Repository wizard
- **Software FCoE SR:** You must have manually completed the configuration required to expose a LUN to the host. This setup includes configuring the FCoE fabric and allocating LUNs to your SAN's public world wide name (PWWN).

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 configure a different a NIC for storage traffic, assign an IP address to a NIC by creating a *management interface*.

When you create a management interface, you must assign it an IP address that meets the following criteria:

- The IP address is on the same subnet as the storage controller, if applicable
- The IP address is on a different subnet than the IP address you specified when you installed XenServer
- The IP address is not on the same subnet as any other management interfaces.

To assign an IP address to a NIC:

1. Ensure that the NIC is on a separate subnet or that routing is configured to suit your network topology. This configuration forces the desired traffic over the selected NIC.
2. In the **Resource** pane of XenCenter, select the pool (or standalone server). Click the **Networking** tab, and then click the **Configure** button.
3. In the **Configure IP Address** dialog, in the left pane, click **Add IP address**.
4. Give the new interface a meaningful name (for example, *yourstoragearray_network*). Select the **Network** associated with the NIC that you use for storage traffic.
5. Click **Use these network settings**. Enter a static IP address that you want to configure on the NIC, the subnet mask, and gateway. Click **OK**. The IP address must be on the same subnet as the storage controller the NIC is connected to.

Note:

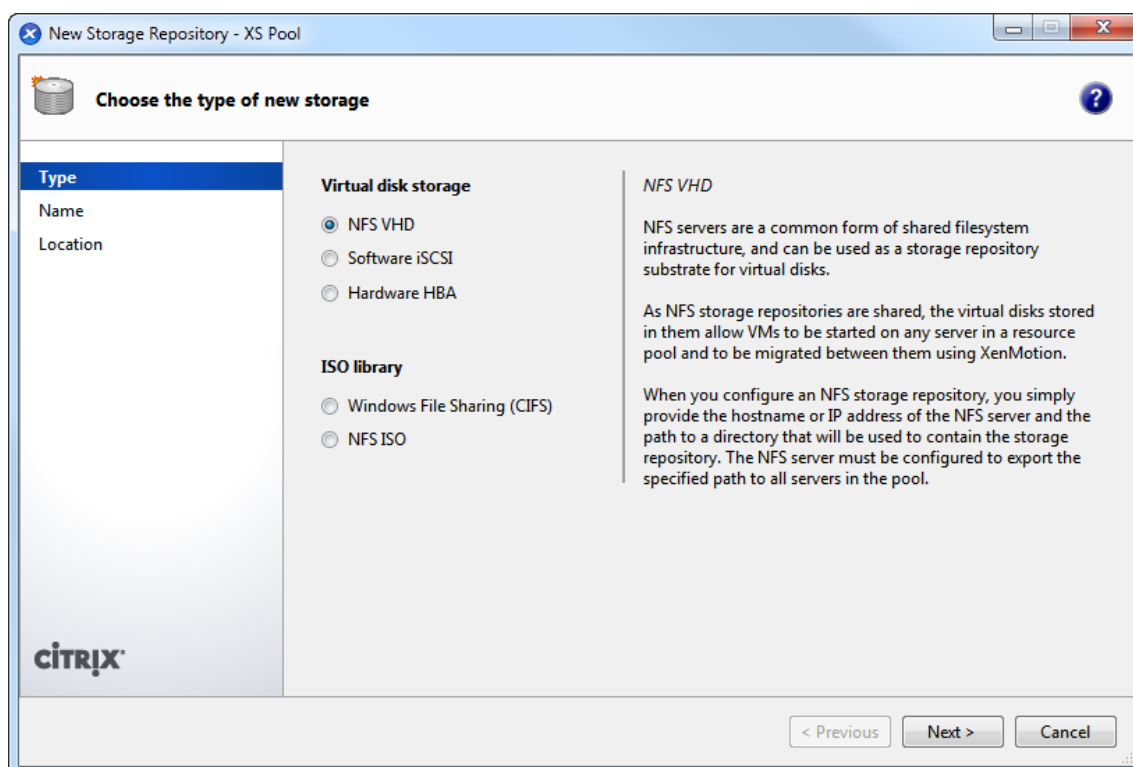
Whenever you assign a NIC an IP address, it must be on a different subnet than any other NICs with IP addresses in the pool. This includes the primary management interface.

To create a new shared NFS or iSCSI storage repository:

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 or iSCSI as the storage type. Click Next to continue.
3. If you choose NFS:
 - a) 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 XenServer hosts in the pool.

- b) Click **Finish**.

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

4. If you choose iSCSI:

- a) 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 XenServer host in the pool to have access to one or more LUNs.

- b) If you have configured the iSCSI target to use CHAP authentication, enter the user name and password.
- c) Click the **Scan Target Host** 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.

- d) Click **Target LUN**, and then select 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.

- e) Click **Finish**.

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

The new shared SR now becomes the default SR for the pool.

Create virtual machines

Through XenCenter, you can create virtual machines in various ways, according to your needs. Whether you are deploying individual VMs with distinct configurations or groups of multiple, similar VMs, XenCenter gets you up and running in just a few steps.

XenServer also provides an easy way to convert batches of virtual machines from VMware. For more information, see [Conversion Manager](#).

This section focuses on a few methods by which to create Windows VMs. To get started quickly, the procedures use the simplest setup of XenServer: a single XenServer host with local storage (after you connect XenCenter to the XenServer host, storage is automatically configured on the local disk of the host).

This section also demonstrates how to use XenMotion to live migrate VMs between hosts in the pool.

After explaining how to create and customize your new VM, this section demonstrates how to convert that existing VM into a VM template. A VM template preserves your customization so you can always use it to create VMs to the same (or to similar) specifications. It also reduces the time taken to create multiple VMs.

You can also create a VM template from a snapshot of an existing VM. A snapshot is a record of a running VM at a point in time. It saves the storage, configuration, and networking information of the original VM, which makes it useful for backup purposes. Snapshots provide a fast way to make VM templates. This section demonstrates how to take a snapshot of an existing VM and then how to convert that snapshot into a VM template. Finally, this section describes how to create VMs from a VM template.

What you'll learn

You'll learn how to:

- Create a Windows 8.1 VM
- Install XenServer Tools
- Migrate a running VM between hosts in the pool
- Create a VM template
- Create a VM from a VM template

Requirements

To create a pool with shared storage, you need the following items:

- The XenServer pool you set up
- XenCenter
- Installation files for Windows 8.1

Create a Windows 8.1 (32-bit) VM

Note:

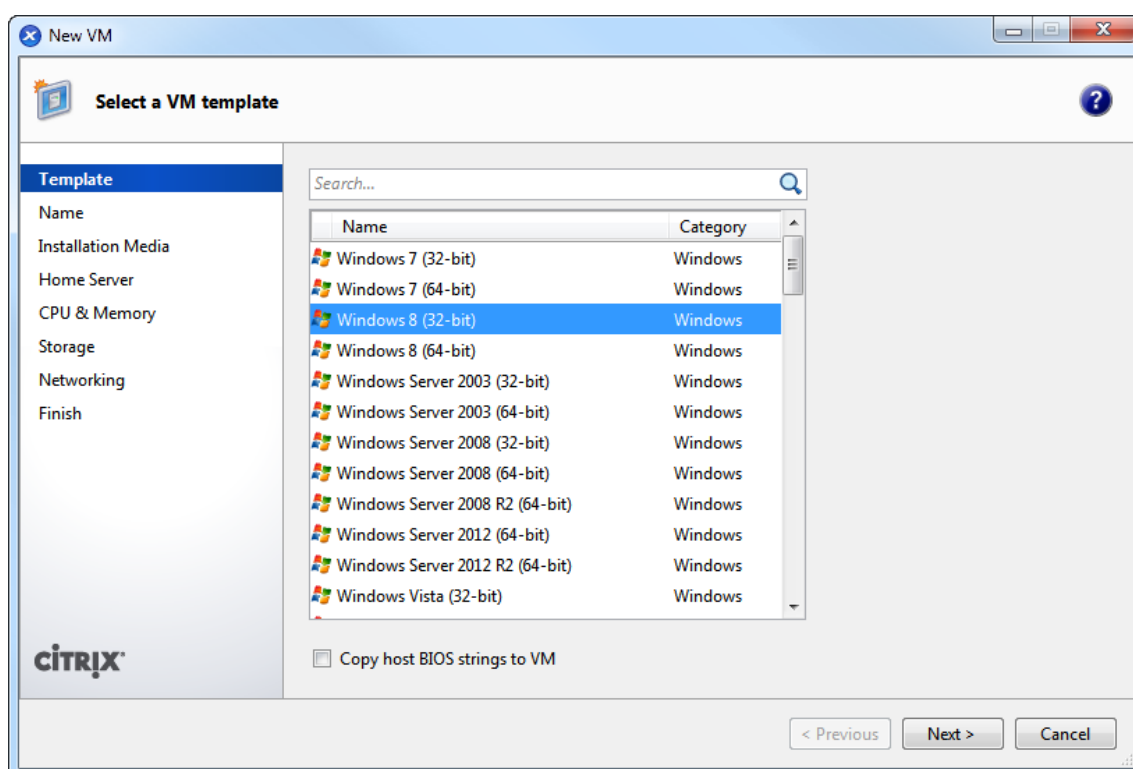
The following procedure provides an example of creating Windows 8.1 (32-bit) VM. The default values may vary depending on the operating system that you choose.

To create a Windows VM:

1. On the 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 for creating a VM with a specific guest operating system (OS), and with optimum storage. This list reflects the templates that XenServer currently supports.

Note:

If the OS you're installing on your new VM is compatible only with the original hardware, check the **Copy host BIOS strings to VM** box. For example, use this option for an OS installation CD that was packaged with a specific computer.

3. Enter a name for and optional description of 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. Choose the default installation source option (DVD drive), insert the disk into the DVD drive of the XenServer host, and choose **Next** to proceed.

XenServer also allows you to pull OS installation media from a range of sources, including a pre-existing ISO library.

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. The VM runs on the installed host. Choose **Next** to proceed.

6. Allocate processor and memory resources.

For a Windows 8.1 VM, the default is 1 virtual CPU, 1 socket with 1 core per socket and 2 GB of RAM. You may choose to modify the defaults if necessary. Click **Next** to continue.

Note:

Each OS has different configuration requirements which are reflected in the templates.

7. Assign a graphics processing unit (GPU).

The **New VM** wizard prompts you to assign a dedicated GPU or a virtual GPU to the VM. This option enables the VM to use the processing power of the GPU. It provides better support for high-end 3D professional graphics applications such as CAD, GIS, and Medical Imaging applications.

Note:

GPU Virtualization is available for XenServer Enterprise Edition customers, or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement.

8. Configure storage for the new VM.

Click **Next** to select the default allocation (24 GB) and configuration, or you might want to:

- a) Change the name, description, or size of your virtual disk by clicking **Properties**.
- b) Add a new virtual disk by selecting **Add**.

Note:

When you create a pool of XenServer hosts, you can configure shared storage at this point when creating a VM.

9. Configure networking on the new VM.

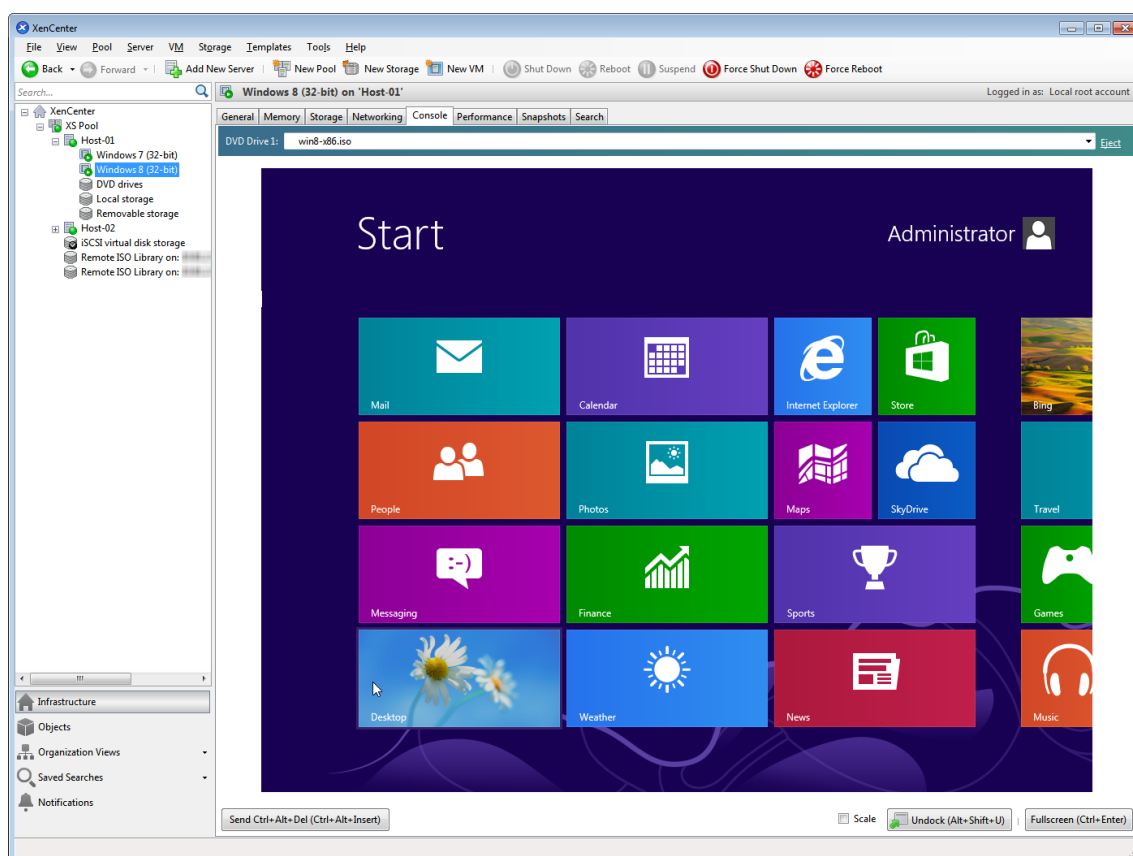
Click **Next** to select the default NIC and configurations, including an automatically created unique MAC address for each NIC, or you can:

- a) Change the physical network, MAC address, or Quality of Service (QoS) priority of the virtual disk by clicking **Properties**.
- b) Add a new virtual network interface by selecting **Add**.

XenServer uses the virtual network interface to connect to the physical network on the host. Be sure to select the network that corresponds with the network the virtual machine requires. To add a physical network, see *Setting Up Networks for the Pool*

10. 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.

11. Follow the OS installation screens and make your selections.
12. After the OS installation completes and the VM reboots, install the XenServer Tools.

Install XenServer Tools

XenServer Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer Tools consists of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. XenServer Tools must be installed on each VM in order for the VM to have a fully supported configuration. A VM functions without them, but performance is hampered. XenServer Tools also enable certain functions and features, including cleanly shutting down, rebooting, suspending and live migrating VMs.

Warning:

Install XenServer Tools for each Windows VM. Running Windows VMs without XenServer Tools is *not* supported.

To install XenServer Tools:

1. Select the VM in the Resources pane, right-click, and then click **Install XenServer Tools** on the shortcut menu. Alternatively, on the VM menu, click **Install XenServer Tools**.

Or

On the **General** tab of the VM, click **Install I/O drivers and Management Agent**.

Note:

When you install XenServer Tools on your VM, you are installing both I/O drivers (PV drivers) and the Management Agent

2. If AutoPlay is enabled for the VM's CD/DVD drive, installation will start automatically after a few moments. The process installs the I/O drivers and the Management Agent, and reboots the VM as required.
3. If AutoPlay is not enabled, the XenServer Tools installer displays the installation options. Click **Install XenServer Tools** to continue with the installation. The XenServer Tools ISO ([guest-tools.iso](#)) is mounted on the VM's CD/DVD drive.
4. Click **Run setup.exe** to begin XenServer Tools installation and restart the VM when prompted to complete the installation process.

After you have installed the XenServer Tools, you can customize your VM by installing applications and performing any other configurations. If you want to create multiple VMs with similar specifications, you can do so quickly by making a template from the existing VM. Use that template to create VMs. For more information, see [Creating VM Templates](#).

Migrate running VMs between hosts in a pool

Using XenMotion (live migration), you can move a running VM from one host to another in the same pool, and with virtually no service interruption. Where you decide to migrate a VM to depends on how you configure the VM and pool.

To migrate a running VM:

1. On the **Resources** pane, select the VM that you want to move.

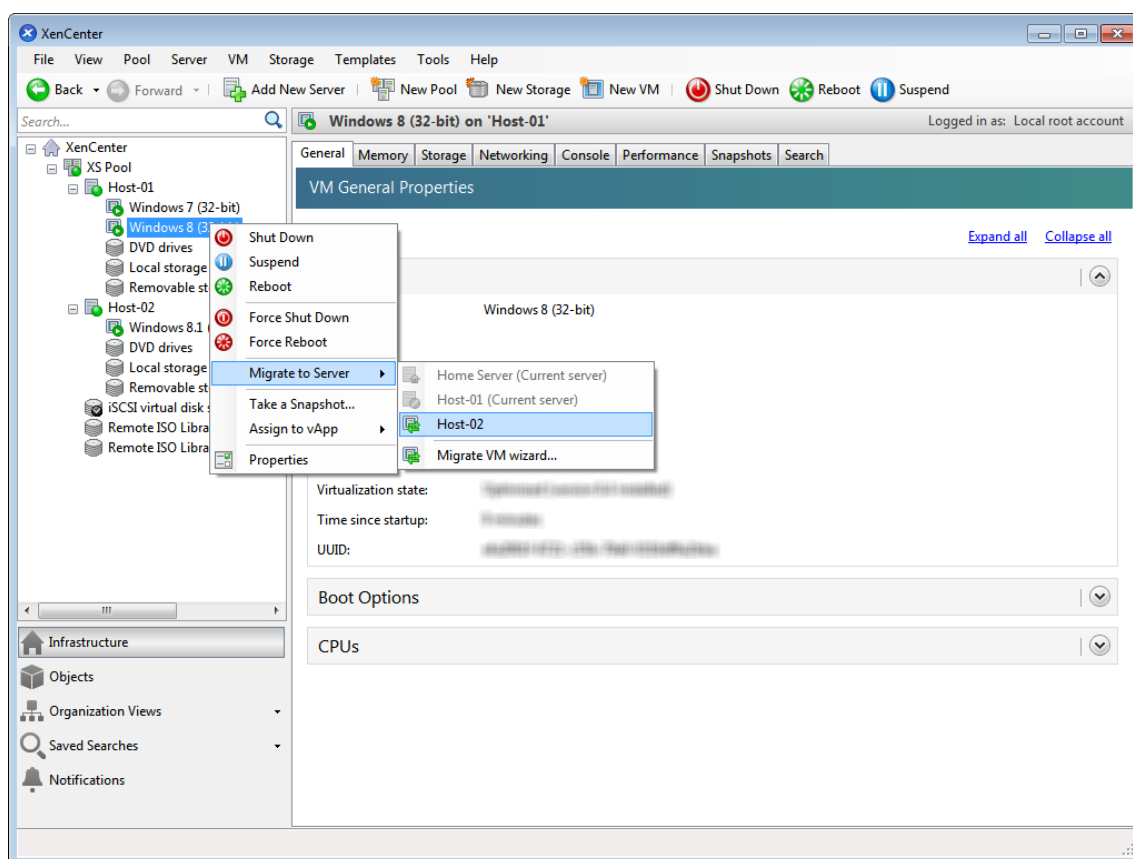
Note:

Ensure that the VM you migrate does not have local storage.

2. Right-click the VM icon, point to **Migrate to Server**, and then select the new VM host.

Tip:

You can also drag the VM onto the target host.



3. The migrated VM displays under the new host in the **Resources** pane.

Create VM templates

There are various ways to create a VM template from an existing Windows VM, each with its individual benefits. This section focuses on two methods: converting an existing VM into a template, and creating a template from a snapshot of a VM. In both cases, the VM template preserves the customized configuration of the original VM or VM snapshot. The template can then be used to create new, similar VMs quickly. This section demonstrates how to make new VMs from these templates.

Before you create a template from an existing VM or VM snapshot, Citrix Systems, Inc. recommends that you run the Windows utility **Sysprep** on the original VM. In general, running **Sysprep** prepares an operating system for disk cloning and restoration. Windows OS installations include many unique elements per installation (including Security Identifiers and computer names). These elements must stay unique and not be copied to new VMs. If copied, confusion and problems are likely to arise. Running **Sysprep** avoids these problems by allowing the generation of new, unique elements for the new VMs.

Note:

Running **Sysprep** may not be as necessary for basic deployments or test environments as it is for production environments.

For more information about **Sysprep**, see your Windows documentation. The detailed procedure of running this utility can differ depending on the version of Windows installed.

Create a VM template from an existing VM

To create a VM template from an existing VM:

Warning:

When you create a template from an existing VM, the new template replaces the original VM. The VM no longer exists.

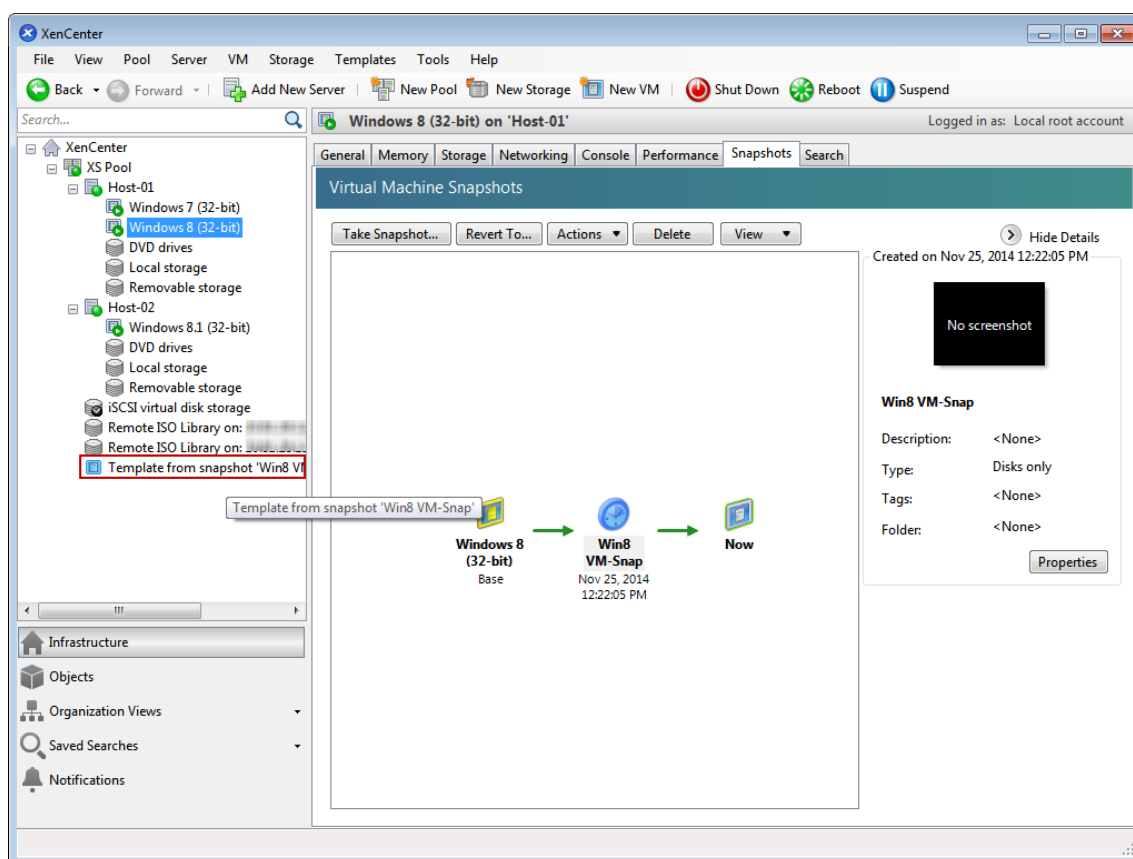
1. Shut down the VM that you want to convert.
2. On the **Resources** pane, right-click the VM, and select **Convert to Template**.
3. Click **Convert** to confirm.

Once you create the template, the new VM template appears in the **Resources** pane, replacing the existing VM.

Create a VM template from a VM snapshot

To create a template from a snapshot of a VM:

1. On the **Resources** pane, select the VM. Click the **Snapshots** tab, and then **Take Snapshot**.
2. Enter a name and an optional description of the new snapshot. Click **Take Snapshot**.
3. Once the snapshot finishes and the icon displays in the **Snapshots** tab, select the icon.



4. From the **Actions** list, choose **Save as a Template**.
5. Enter a name for the template, and then click **Create**.

Create VMs from a VM template

To create a VM from a customized VM template:

1. On the XenCenter **Resources** pane, right-click the template, and select **New VM** wizard.

The **New VM** wizard opens.

2. Follow the **New VM** wizard to create a VM from the selected template.

Note:

When the wizard prompts you for an OS installation media source, select the default and continue.

The new VM appears in the **Resources** pane.

If you are using a template created from an existing VM, you can also choose to select **Quick Create**. This option does not take you through the **New VM** wizard. Instead this option instantly creates and provisions a new VM using all the configuration settings specified in your template.

Technical overview

October 5, 2018

XenServer is an industry leading, open-source platform for cost-effective desktop, server, and cloud virtualization infrastructures. XenServer enables organizations of any size or type to consolidate and transform compute resources into virtual workloads for today's data center requirements. Meanwhile, it ensures a seamless pathway for moving workloads to the cloud.

The key features of XenServer are:

- Consolidating multiple virtual machines (VMs) onto a physical server
- Reducing the number of separate disk images to be managed
- Allowing for easy integration with existing networking and storage infrastructures
- Enabling you to schedule zero downtime maintenance by using XenMotion to live migrate VMs between XenServer hosts
- Assuring availability of VMs by using high availability to configure policies that restart VMs on another server in case one fails
- Increasing portability of VM images, as one VM image works on a range of deployment infrastructures

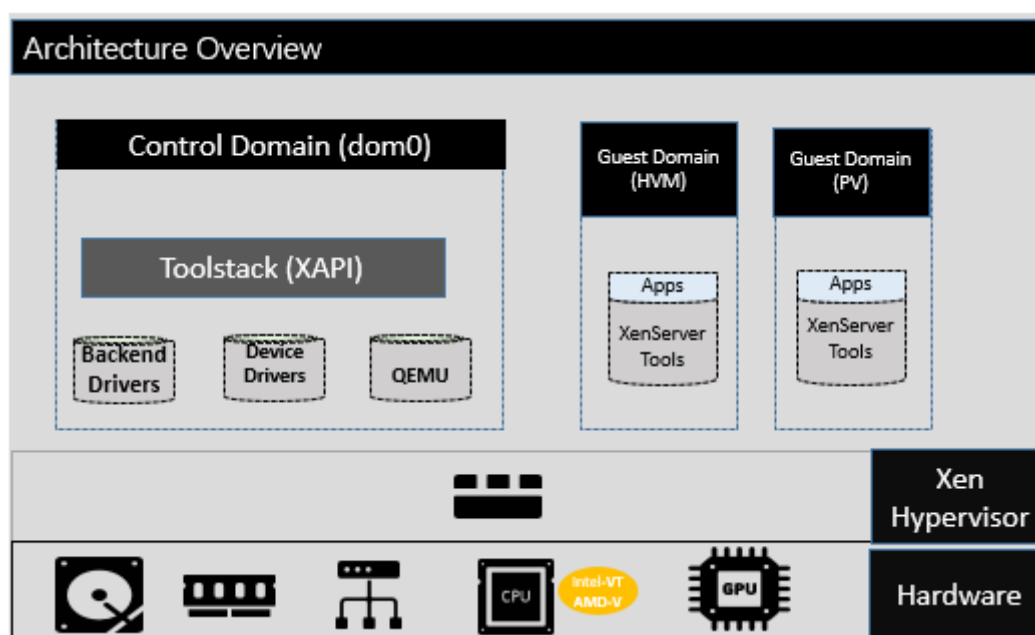
Virtualization and hypervisor

Virtualization, or to be more specific, hardware virtualization, is a method of running multiple independent VMs on a single physical computer. Software executed on these virtual machines is separated from the underlying hardware resources. It's a way of fully utilizing the physical resources available in modern powerful servers, which reduces the total cost of ownership (TCO) for server deployments.

A hypervisor is the basic abstraction layer of software. The hypervisor performs low-level tasks such as CPU scheduling and is responsible for memory isolation for resident VMs. The hypervisor abstracts the hardware for the VMs. The hypervisor has no knowledge of networking, external storage devices, video, and so on.

Key components

This section gives you a high-level understanding of how XenServer works. See the following illustration for the key components of XenServer:



Hardware

The hardware layer contains the physical server components, such as CPU, memory, network, and disk drives.

You need an Intel VT or AMD-V 64-bit x86-based system with one or more CPUs to run all supported guest operating systems. For more information about XenServer host system requirements, see [System requirements](#).

For a complete list of XenServer certified hardware and systems, see the [Hardware Compatibility List \(HCL\)](#).

Xen Hypervisor

The Xen Project hypervisor is an open-source type-1 or bare-metal hypervisor. It allows many instances of an operating system or different operating systems to run in parallel on a single machine (or host). Xen hypervisor is used as the basis for many different commercial and open-source applications, such as: server virtualization, Infrastructure as a Service (IaaS), desktop virtualization, security applications, embedded, and hardware appliances.

XenServer is based on the Xen Project hypervisor, with extra features and supports provided by Citrix. XenServer 7.6 uses version 4.7 of the Xen hypervisor.

Control domain

The **Control Domain**, also called Domain 0, or dom0, is a secure, privileged Linux VM that runs the XenServer management toolstack known as XAPI. This Linux VM is based on a CentOS 7.2 distribution. Besides providing XenServer management functions, dom0 also runs the physical device drivers for networking, storage, and so on. The control domain can talk to the hypervisor to instruct it to start or stop guest VMs.

Toolstack

The **Toolstack**, or XAPI is the software stack that controls VM lifecycle operations, host and VM networking, VM storage, and user authentication. It also allows the management of XenServer resource pools.

XAPI provides the publicly documented management API, which is used by all tools that manage VMs, and resource pools. For more information, see <https://developer-docs.citrix.com>.

Guest domain (VMs)

Guest domains are user-created virtual machines that request resources from dom0. The guest domain in XenServer supports full virtualization (HVM), paravirtualization (PV), and PV on HVM. For a detailed list of the supported distributions, see [Supported Guests, Virtual Memory, and Disk Size Limits](#).

Full virtualization

Full virtualization, or hardware-assisted virtualization uses virtualization extensions from the host CPU to virtualize guests. Fully virtualized guests do not require any kernel support. The guest is called a hardware virtual machine (HVM). HVM requires Intel VT or AMD-V hardware extensions for memory and privileged operations. XenServer uses Quick Emulator (QEMU) to emulate PC hardware, including BIOS, IDE disk controller, VGA graphic adaptor, USB controller, network adapter etc. To improve the performance of hardware-sensitive operations like disk or network access, HVM guests are installed with the XenServer tools. For more information, see PV on HVM.

HVM is commonly used when virtualizing an operating system such as Microsoft Windows where it is impossible to modify the kernel to make it virtualization aware.

Paravirtualization (PV)

Paravirtualization is an efficient and lightweight virtualization technique originally introduced by the Xen Project, and later adopted by other virtualization platforms. PV does not require virtualization

extensions from the host CPU. However, PV guests require a PV-enabled kernel and PV drivers, so the guests are aware of the hypervisor and can run efficiently without virtual emulated hardware. PV-enabled kernels exist for Linux, NetBSD, FreeBSD, and Open Solaris. For a list of supported distributions in PV mode, see [PV Linux distributions](#).

For a PV guest, Xen Hypervisor forwards the I/O operation requests to the control domain. The guest is aware of the hypervisor and sends privileged instructions to the hypervisor.

PV on HVM

PV on HVM is a mixture of paravirtualization and full hardware virtualization. The primary goal is to boost performance of HVM guests by using specially optimized Paravirtualized drivers. This mode allows you to take advantage of the x86 virtual container technologies in newer processors for improved performance. Network and storage access from these guests still operate in PV mode, using drivers building to the kernels.

Windows and some Linux distributions are available in PV on HVM mode in XenServer. For a list of supported Linux distributions using PV on HVM, see [HVM Linux distributions](#).

XenServer Tools

XenServer Tools, or guest tools provide high performance I/O services without the overhead of traditional device emulation. XenServer Tools consist of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent.

The I/O drivers contain front-end storage and network drivers, and low-level management interfaces. These drivers replace the emulated devices and provide high-speed transport between VMs and XenServer product family software.

The Management Agent, also known as the guest agent, is responsible for high-level virtual machine management features. It provides full functionality to XenCenter (for Windows VMs), including quiesced snapshots.

Notes:

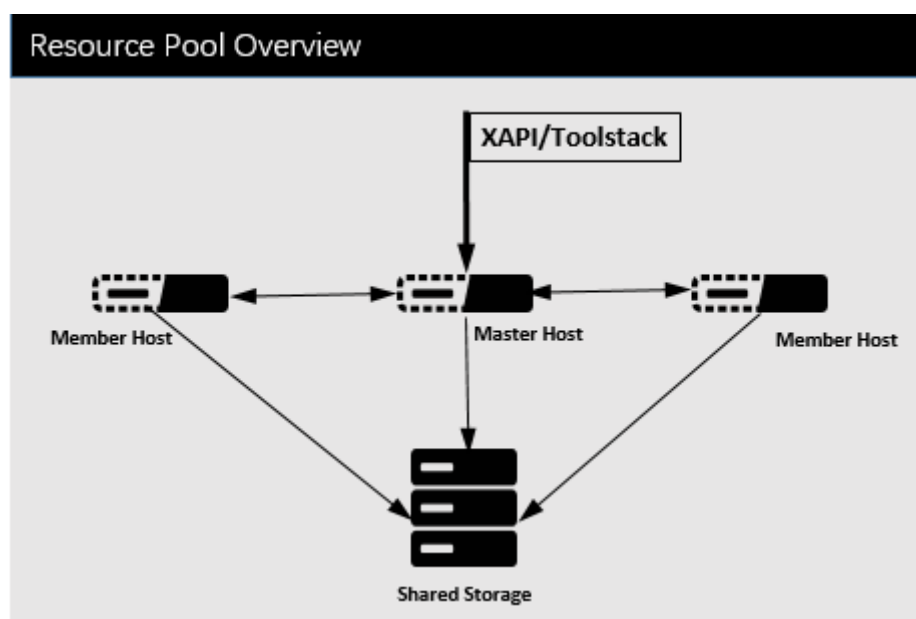
- XenServer Tools must be installed on each Windows VM in order for the VM to have a fully-supported configuration. A VM will function without the XenServer Tools, but performance will be significantly hampered when the I/O drivers (PV drivers) are not installed.
- For Windows VMs, XenServer Tools are called Windows guest tools, which include Windows PV drivers and the Management Agent.
- For Linux VMs, PV drivers are already included in the Xen Kernel.

For more information, see [XenServer Tools](#).

Key concepts

Resource pool

XenServer allows you to manage multiple servers and their connected shared storage as a single entity by using resource pools. Resource pools enable you to move and run virtual machines on different XenServer hosts. They also allow all servers to share a common framework for network and storage. A pool may contain up to 64 servers running the same version of XenServer software, at the same patch level, and with broadly compatible hardware. For more information, see [Hosts and resource pools](#).



XenServer resource pool adopts a master/slave architecture, implemented by XAPI. XAPI calls are forwarded from the pool master to pool members. Pool members make DB RPCs against the pool master. The master host is responsible for co-ordination and locking resources within the pool, and processes all control operations. Member hosts talk to the master through HTTP and XMLRPC, but they can talk to each other (over the same channel) to:

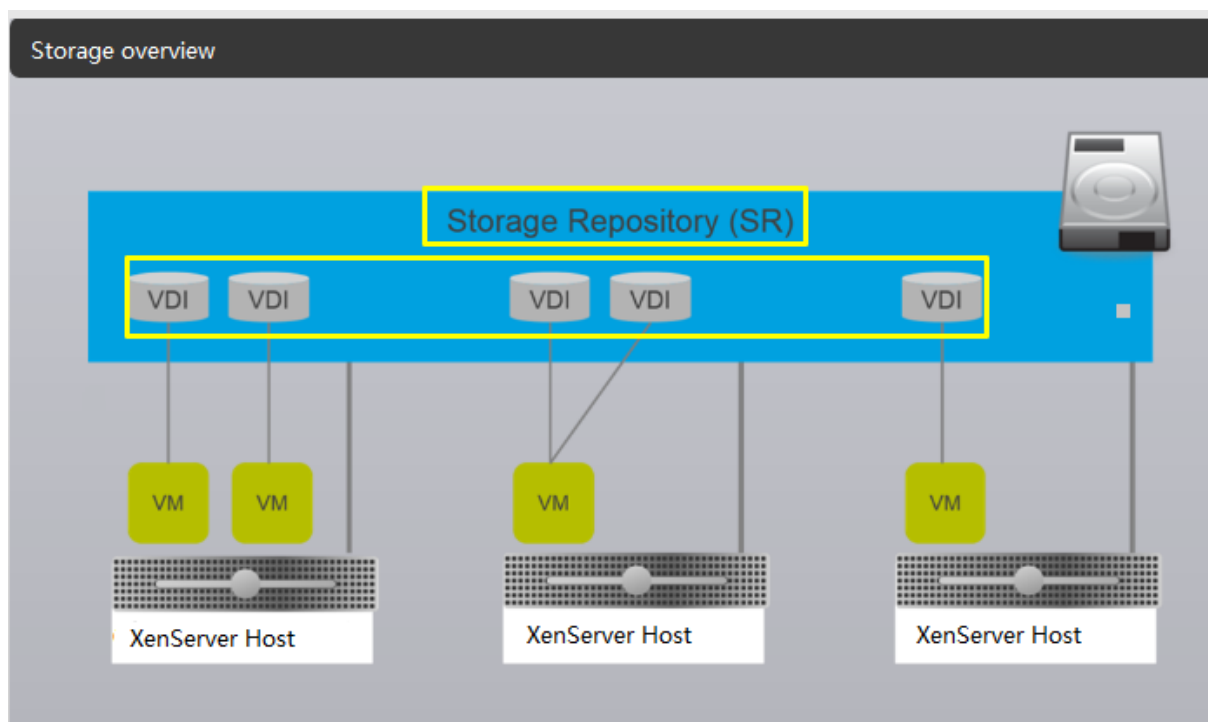
- Transfer VM memory images (VM migration)
- Mirror disks (storage migration)

Storage repository

XenServer storage targets are called storage repositories (SRs). A storage repository stores Virtual Disk Images (VDIs), which contains the contents of a virtual disk.

SRs are flexible, with built-in support for IDE, SATA, SCSI, and SAS drives that are locally connected, and iSCSI, NFS, SAS, and Fibre Channel remotely connected. The SR and VDI abstractions allow ad-

vanced storage features such as thin provisioning, VDI snapshots, and fast cloning to be exposed on storage targets that support them.



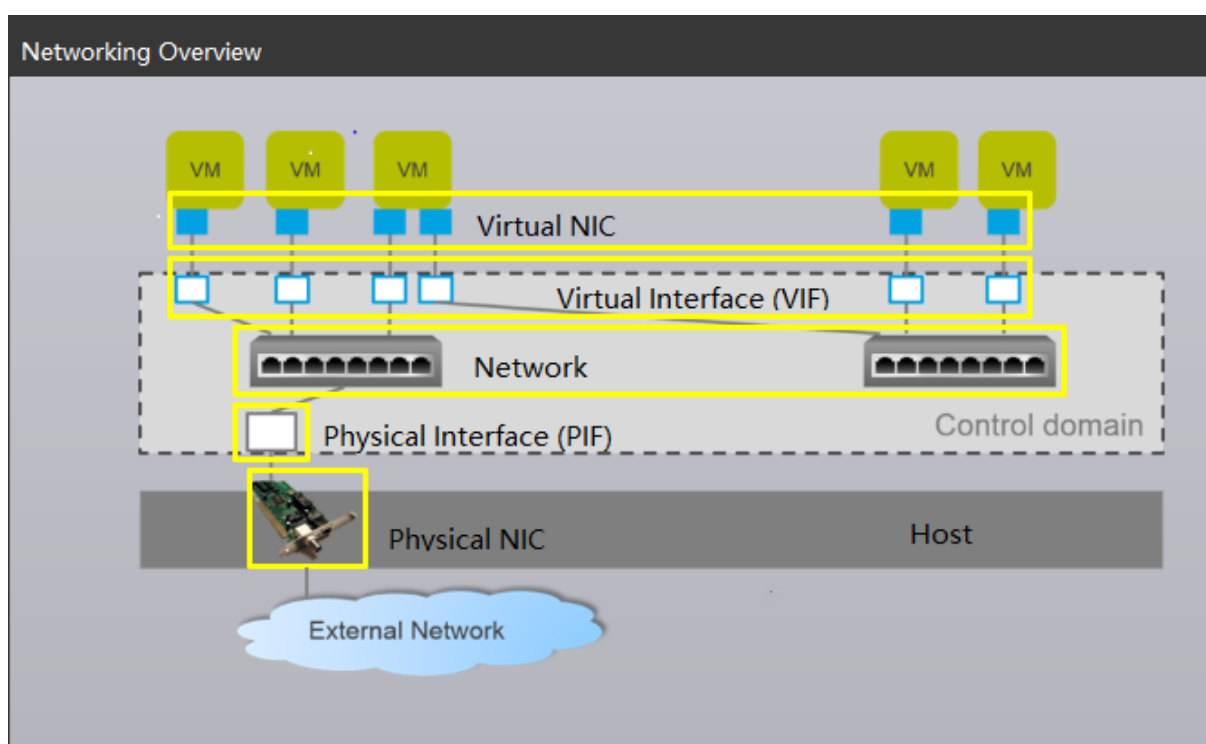
Each XenServer host can use multiple SRs and different SR types simultaneously. These SRs can be shared between hosts or dedicated to particular hosts. Shared storage is pooled between multiple hosts within a defined resource pool. A shared SR must be network accessible to each host. All hosts in a single resource pool must have at least one shared SR.

For more information about how to operate with SRs, see [Configure storage](#).

Networking

On an architecture level, there are three types of server-side software objects to represent networking entities. These objects are:

- A **PIF**, which is a software object used within in dom0 and represents a physical NIC on a host. PIF objects have a name and description, a UUID, the parameters of the NIC that they represent, and the network and server they are connected to.
- A **VIF**, which is a software object used within in dom0 and 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 used to route network traffic on a network host. Network objects have a name and description, a UUID, and the collection of VIFs and PIFs connected to them.



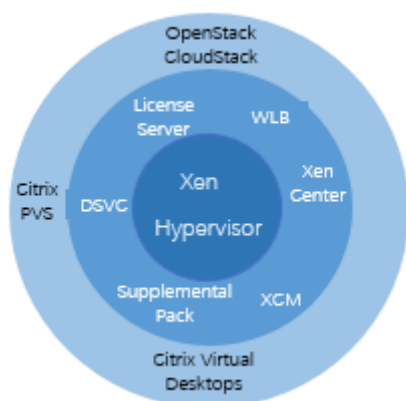
XenServer management APIs allow following operations:

- Configuration of networking options
- Control over the NIC to be used for management operations
- Creation of advanced networking features such as virtual local area networks (VLANs) and NIC bonds

For more information about how to manage networks on XenServer, see [Networking](#).

Related add-ons and applications

While Xen Hypervisor works at the very core level, there are XenServer specific add-ons related hypervisor-agnostic applications and services available to make the virtualization experience complete.



- **XenCenter**

A windows GUI client for VM management, implemented based on the management API. XenCenter provides a rich user experience to manage multiple XenServer hosts, resource pools, and the entire virtual infrastructure associated with them.

- **Workload Balancing (WLB)**

An appliance that balances your pool by relocating virtual machines onto the best possible servers for their workload in a resource pool. For more information, see [Workload balancing \(/en-us/xenserver/current-release/vswitch-controller.html\)](/en-us/xenserver/current-release/vswitch-controller.html).

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

A Debian based appliance that is used to create Open Flow rules that are XAPI aware. The implementation consists of the following:

- A virtualization-aware switch (the vSwitch) running on each XenServer and the vSwitch Controller.
- A centralized server that manages and coordinates the behavior of each individual vSwitch to provide the appearance of a single vSwitch.

For more information, see [vSwitch and controller](#).

- **Citrix Licensing Server**

A Linux based appliance that XenCenter contacts to request a license for the specified server.

- **XenServer Conversion Manager (XCM)**

An virtual appliance with a console that enables users to convert existing VMware virtual machines into XenServer virtual machines, with comparable networking and storage connectivity. For more information, see [Conversion manager](#).

- **Measured Boot Supplemental Pack**

A supplemental pack that enables customers to measure key components of their XenServer hosts at boot time, and provides APIs that enable remote attestation solutions to securely collect these measurements. For more information, see [Measured Boot Supplemental Pack](#).

- **Citrix Provisioning**

Provisioning services that support PXE boot from common images. Used widely with Citrix Virtual Desktops and Citrix Virtual Apps. For more information, see [Provisioning](#).

- **Citrix Virtual Desktops**

A Virtual Desktop Infrastructure (VDI) product specialized to Windows desktops. Citrix Virtual Desktops uses XAPI to manage XenServer in a multi-host pool configuration. For more information, see [Citrix Virtual Apps and Desktops](#).

- **OpenStack/CloudStack**

Open-source software for building public/private clouds. Uses the management API to control XenServer. For more information, see <https://www.openstack.org/> and <https://cloudstack.apache.org/>

Licensing

September 11, 2018

XenServer 7.6 is available in the following editions:

- Enterprise
- Standard
- Free (Unlicensed)

The **Standard** edition is our entry-level commercial offering. It has a range of features for customers who want a robust and high performing virtualization platform, but don't require the premium features of Enterprise Edition. Meanwhile, they still want to benefit from the assurance of comprehensive Citrix Support and Maintenance.

The **Enterprise** edition is our premium offering, optimized for desktop, server, and cloud workloads. In addition to the features available in the Standard edition, the Enterprise Edition offers the following features:

- Automated Windows VM driver updates
- Automatic updating of the Management Agent
- Support for SMB storage
- Direct Inspect APIs
- Dynamic Workload Balancing
- GPU virtualization with NVIDIA GRID and Intel GVT-g

- VMware vSphere to XenServer conversion utilities
- Intel Secure Measured Boot (TXT)
- Export pool resource data
- In-memory read caching
- PVS-Accelerator
- Automated Updates using XenCenter
- XenServer live patching
- AMD MxGPU
- Enablement for Citrix Virtual Desktops tablet mode
- Changed block tracking
- IGMP snooping
- USB passthrough
- SR-IOV network support
- Thin provisioning for shared block storage devices

Customers who have purchased Citrix Virtual Apps or Citrix Virtual Desktops have an entitlement to XenServer, which includes all the features listed previously.

The **Free** edition provides a reduced set of features and is not eligible for Citrix Support and Maintenance. Hosts that are running the Free edition of XenServer are labeled as “Unlicensed” in XenCenter.

For more information, see the [XenServer Feature Matrix](#).

XenServer uses the same licensing process as other Citrix products, and as such requires a valid license to be installed on a License Server. You can download the License Server from [Citrix Licensing](#). XenServer (other than through the Citrix Virtual Apps and Desktops licenses) is licensed on a *per-socket* basis. Allocation of licenses is managed centrally and enforced by a standalone Citrix License Server, physical or virtual, in the environment. After applying a per socket license, XenServer displays as *XenServer Per-Socket Edition*.

Note:

Mixed pools of licensed and unlicensed hosts behave as if all hosts were unlicensed.

Unlicensed hosts are subject to restrictions. For more information, see [Other Questions](#).

Licensing steps overview

You need the following items to license XenServer Enterprise or Standard Edition:

- A XenServer License
- A Citrix License Server
- A XenServer host
- XenCenter

The following steps provide an overview of the process:

1. Install Citrix License Server or import the Citrix License Server Virtual Appliance into a XenServer host.
2. Download a license file
3. Add the license file to the Citrix License Server
4. Using XenCenter, enter the License Server details and apply them to hosts in your resource pool

For more information about Citrix Licensing, see the [Citrix Licensing documentation](#).

Licensing XenServer

Q: Where can I purchase a XenServer license?

A: You can purchase a XenServer License from <http://citrix.com/buy>.

Q: How do I apply a XenServer license?

A: XenServer requires a License Server. After licensing XenServer, you are provided with a .LIC license access code. Install this license access code on either:

- A Windows server running the Citrix License Server software
or
- The Citrix License Server Virtual Appliance.

When you assign a license to a XenServer host, XenServer contacts the specified Citrix License Server and requests a license for the specified servers. If successful, a license is checked out and the License Manager displays information about the license the hosts are licensed under.

For instructions on applying a XenServer license to a Citrix License Server Virtual Appliance, see [CTX200159 – How to Apply a XenServer License File to Citrix License Server Virtual Appliance \(CLSVA\)](#).

Q: How many licenses do I need to license my resource pool?

A: XenServer is licensed on a *per-CPU socket* basis. For a pool to be considered licensed, all XenServer hosts in the pool must be licensed. XenServer only counts populated CPU sockets.

You can use the Citrix License Server to view the number of available licenses displayed in the *License Administration Console Dashboard*.

Q: Do I need a per-socket license for sockets that are not populated?

A: No, only populated CPU sockets are counted toward the number of sockets to be licensed.

Q: Do I lose my Virtual Machine (VM) when my license expires?

A: No, you do not lose any VMs or their data.

Q: What happens if I have a licensed pool and the License Server becomes unavailable?

A: If your license has not expired and the License Server is unavailable, you receive a *grace* period of 30 days at the licensing level that was applied previously.

Q: I am upgrading to XenServer 7.6 from a previous XenServer version with a per socket license; do I have to do anything?

A: No. You can upgrade your hosts to XenServer 7.6 Enterprise Edition using the previously purchased per socket licenses, provided Customer Success Services is valid at least until May 16, 2018.

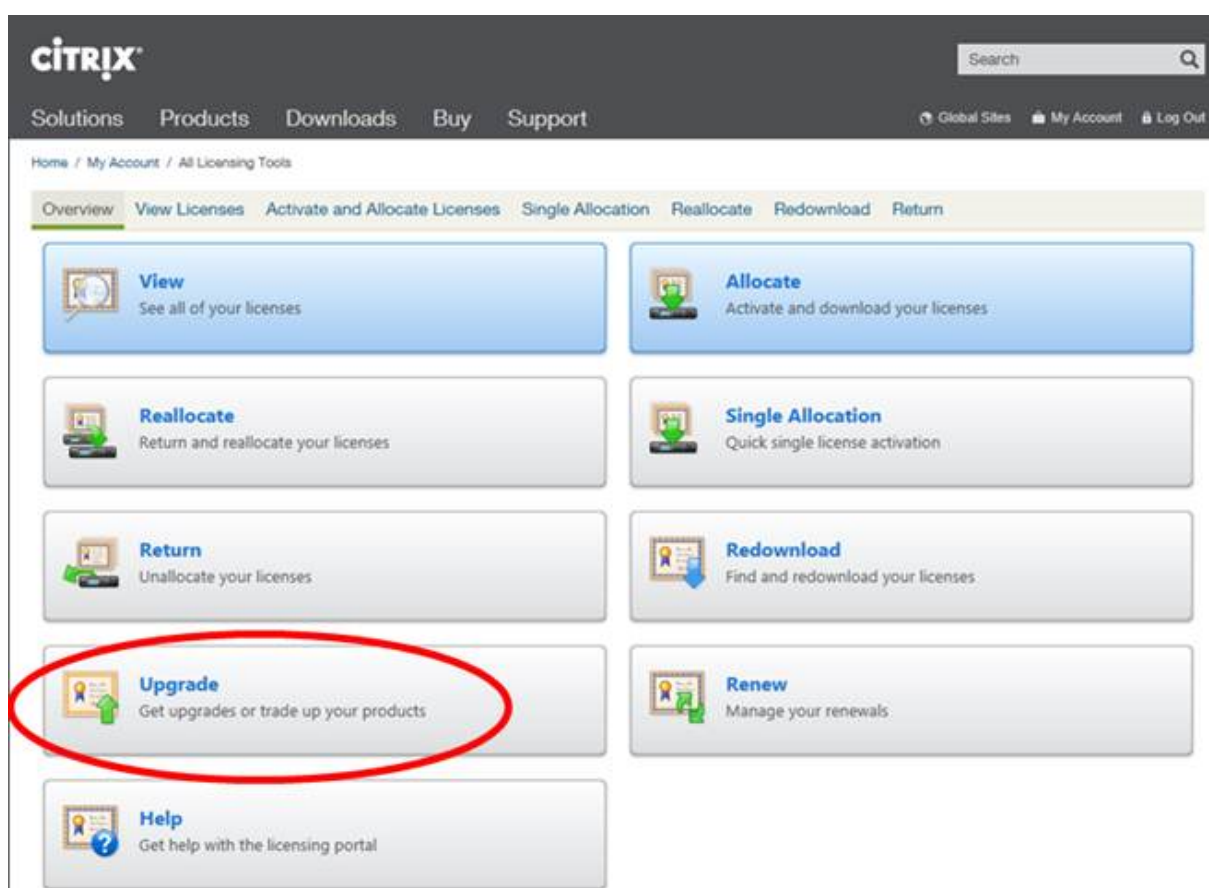
If you have renewed your Customer Success Services after the original purchase, you might need to refresh the license file on the License Server to ensure it displays the Customer Success Services eligibility.

Q: I am moving from XenServer 7.5 unlicensed edition to XenServer 7.6. Do I have to do anything?

A: No. You can upgrade or update your hosts to XenServer 7.6. You remain ineligible for support and premium features are inaccessible until an appropriate license is applied.

Q: I am a Citrix Virtual Apps and Desktops customer moving from XenServer 7.5 to XenServer 7.6. Do I have to do anything?

A: No. Citrix Virtual Apps or Citrix Virtual Desktops customers can update to XenServer 7.6 seamlessly. Your existing installed Citrix Virtual Apps or Citrix Virtual Desktops license grants you entitlement to XenServer without requiring any other changes.



Q: I am a Citrix Service Provider licensed for Citrix Virtual Apps and Desktops. Can I use this license for XenServer when I upgrade to XenServer 7.6?

A: Yes. XenServer 7.6 supports your license. With this license, you can use all of the premium features provided by the Enterprise Edition of XenServer. To apply this license to your pools, first upgrade or update all hosts within the pool to run XenServer 7.6.

Q: I am customer with a Citrix Virtual Apps and Desktops Service subscription. Am I entitled to use XenServer 7.6?

A: Yes. If you have a Citrix Virtual Apps and Desktops Service subscription that enables the use of on-premises Desktops and Apps, you are entitled to use XenServer to host these Desktops and Apps.

Download a license through the licensing management tool. Install this license on your License Server to use on-premises XenServer with your Citrix Virtual Apps and Desktops Service subscription.

With this license you can use all of the same premium features as with an on-premises Citrix Virtual Apps and Desktops entitlement. To apply this license to your pools, first upgrade all hosts within the pool to run XenServer 7.6.

Q: What are the constraints on the use of the XenServer Enterprise Edition advanced virtualization management capabilities delivered as part of Citrix Virtual Apps and Desktops?

A: Every edition of Citrix Virtual Apps and Desktops has access to XenServer Enterprise Edition advanced virtualization management features. A complete list of all features enabled by a Citrix Virtual Apps or Citrix Virtual Desktops license can be found in the XenServer Feature Matrix.

XenServer entitlements permit virtualization of any infrastructure required to deliver Citrix Virtual Apps or Citrix Virtual Desktops feature components. These features must be accessed exclusively by Citrix Virtual Apps or Citrix Virtual Desktops licensed users or devices.

Extra infrastructure support servers, such as Microsoft domain controllers and SQL servers are also covered by this entitlement, providing they are deployed in the same XenServer resource pool as the Citrix Virtual Apps or Citrix Virtual Desktops infrastructure covered by this license, and providing those support servers are used to support the Citrix Virtual Apps or Citrix Virtual Desktops infrastructure only.

The XenServer entitlement in the Citrix Virtual Apps or Citrix Virtual Desktops license cannot be used for XenServer pools that don't host Citrix Virtual Apps or Citrix Virtual Desktops infrastructure or Virtual Deliver Agents (VDAs). You also cannot use this entitlement for hosting virtual machines not covered by the permissions above. XenServer must be purchased separately for these uses.

Citrix License Servers

Q: Which License Servers can I use with XenServer?

A: You can either use the Citrix License Server software version 11.14 or later (on a server running Microsoft Windows), or the Linux-based Citrix License Server virtual appliance.

Q: How do I import my license onto the Citrix License Server?

A: For information on importing a license file, see the [Licensing documentation](#) on the Citrix Product Documentation website.

- [Install licenses by using Citrix Licensing Manager](#)
- [Import license files by using the Licensing Administration Console](#)
- [Install license files by using the command line](#)

Q: Can I run the License Server on my XenServer pool?

A: Yes. You can install the Citrix License Server software on a Windows VM or import the Linux-based Citrix License Server virtual appliance. For ease of deployment, the Citrix License Server software is

pre-installed on this virtual appliance, and it can run as a VM in your XenServer pool.

XenServer operates with a 'grace' license until the License Server is able to boot. This behavior means, after you have licensed the XenServer hosts in your pool, and you reboot the host that has the Citrix License Server running on it, a grace period is applied to that host until the appliance is restarted.

Q: Can I use the Windows version of the Citrix License Server with XenServer?

A: Yes.

Q: Can I install Licenses for other Citrix products on a Citrix License Server virtual appliance, or on the Citrix License Server software installed on Windows?

A: Yes, you can license other Citrix products using the Citrix License Server virtual appliance or through the Citrix License Server software installed on Windows. For more information, see [Licensing](#) on the [Citrix Product Documentation](#) website.

Licensing a XenServer pool

Q: How do I apply a license to all the hosts using XenCenter?

A: Follow this procedure to apply a license:

1. On the **Tools** menu, click **License Manager**.
2. Select the Pool or Hosts you would like to license, and then click **Assign License**.
3. In the **Apply License** dialog, specify the **Edition** type to assign to the host, and type the host-name or IP address of the License Server

Q: Can I apply a license without using XenCenter?

A: Yes, you can use the xe CLI. Run the host-apply-edition command. For example, enter the following to license a host:

```
1 xe host-apply-edition edition=enterprise-per-socket|desktop-plus |  
   desktop|standard-per-socket  
2  
3 license-server-address=<*licenseserveraddress* host-uuid=<*uuidofhost*  
4  
5 license-server-port=<*licenseserverport*
```

To license a pool, use the pool-apply-edition command. For example:

```
1 xe pool-apply-edition edition=enterprise-per-socket|desktop-plus|  
   desktop|standard-per-socket\  
2  
3 license-server-address=<*licenseserveraddress*> pool-uuid=<*uuidofpool  
   *>\  
4  
5 license-server-port=<*licenseserverport*>\  
6
```

Q: How can I discover the license status of my hosts and pools?

A: XenCenter displays the license type of a server or pool.

To see the license type of a server or pool, select that server or pool in the tree view. XenCenter displays the license status in the title bar for that server or pool, after the server or pool name.

Mixed pools of licensed and unlicensed hosts behave as if all hosts were unlicensed. In the tree view, XenCenter displays unlicensed pools with a warning triangle icon.

Other questions**Q: How do I get a license to evaluate XenServer?**

A: You do not need a license to evaluate XenServer. You can use XenServer in an unlicensed state. However, you do not have access to premium features. In addition, you are not eligible for Citrix Support or maintenance.

You can get a trial license to try the Enterprise Edition features. For more information, see [Get started](#).

Q: Can I use XenServer without a license?

A: If you use XenServer in an unlicensed state (Free edition), you are not eligible for Citrix Support or maintenance. In addition, the following features are restricted and require a license:

- Pools of more than three hosts

Note:

This restriction does not impact existing pools that contain three or more hosts until you attempt to add another host to the pool

- High Availability
- Dynamic Memory Control

- Storage Motion
- Role-Based Access Control
- GPU Passthrough
- Site Recovery Manager
- Active Directory Integration
- Rolling Pool Upgrade

You can get a trial license to try XenServer Enterprise Edition. For more information, see [Getting started with XenServer](#).

More information

- For more information about the XenServer 7.6 release, see [XenServer 7.6 Release Notes](#).
- To access XenServer 7.6 product documentation, see [XenServer 7.6 Product Documentation](#).
- For an overview of the XenServer product, see [Technical Overview](#).
- [CTX200159 – How to Apply a XenServer License File to Citrix License Server Virtual Appliance \(CLSVA\)](#).
- Raise any non-technical issues with XenServer including, Customer Success Services program support, licensing, administrative support, and order confirmation through [Citrix Customer Service](#).

Install

April 1, 2019

This section contains procedures to guide you through the installation, configuration, and initial operation of XenServer. 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 XenServer hosts on physical servers.

XenServer 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, XenServer can run on a wide variety of hardware and storage devices. However, Citrix recommends that you use certified device drivers.

For more information, see the [Hardware Compatibility List \(HCL\)](#).

Important:

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

Before you start

Before installing XenServer 7.6, consider the following factors:

- Which release stream of XenServer do you want to use?
- What is the appropriate installation method?
- What are the system requirements?

XenServer release streams

XenServer releases are in one of following release streams: Current Release (CR) or Long Term Service Release (LTSR). XenServer 7.6 is a Current Release. When you choose whether to install a version of XenServer from the CR stream or the LTSR stream, consider the following:

- How often do you want to update your version of XenServer?
- Do you prefer a stable feature set or the latest feature set?

Current Release

Current Releases of XenServer enable you to consume new features at the earliest possible opportunity. New versions of XenServer from the CR stream are released each quarter. If you are on the CR stream, you must regularly adopt new CRs to remain in support. Most issues discovered in XenServer CR are fixed in a subsequent current release. Security issues are fixed in hotfixes that can be applied to the CR.

If you have XenServer 7.5 or 7.4 installed, you must update to XenServer 7.6 to continue to receive support.

Long Term Service Release

Long Term Service Releases of XenServer guarantee stability in terms of the feature set within XenServer. New versions of XenServer from the LTSR stream are released every two years and are supported for up to 10 years. Any issues in XenServer LTSR are fixed in hotfixes or cumulative updates that can be applied to the XenServer LTSR.

If you currently have XenServer 7.1 Cumulative Update 2 LTSR installed, you can upgrade to the XenServer Current Release stream to take advantage of its new features.

Installation methods

XenServer 7.6 is provided in the following forms:

- As an update that can be applied to the previous CR of XenServer
- As a base installation that can be used to upgrade an earlier version of XenServer or to create a fresh installation

The file that you use to get XenServer 7.6 depends on the existing version XenServer that is installed.

Existing version of XenServer	How to get XenServer 7.6	ISO File to use
None	Fresh installation	Base Installation ISO
7.5, 7.4	Update	Updates ISO
7.1 Cumulative Update 2, 7.0	Upgrade	Base Installation ISO

Fresh installation

If you are creating a fresh installation of XenServer 7.6:

- Use the **XenServer 7.6 Base Installation ISO** file.
You can download this file from the [download site](#)
- Review the information in [System Requirements](#), [Licensing](#), and Install the XenServer host before installing XenServer.

Update

If you are updating a previous current release of XenServer 7.4 or 7.5 to XenServer 7.6:

- Use the **XenServer 7.6 Update ISO** file.
You can download this file from the [download site](#)
- Review the information in [Update](#) before updating XenServer.

Upgrade

If you are upgrading from XenServer 7.1 Cumulative Update 2 or 7.0 to XenServer 7.6:

- Use the **XenServer 7.6 Base Installation ISO** file.

You can download this file from the [download site](#)

- Review the information in [System Requirements](#) and [Upgrading from an existing version](#) before upgrading XenServer.

Install locations

Install the XenServer host by using one of the following methods:

- From a CD

You can download the installer (ISO file format) and burn it to a CD.

To download the installer, visit the [downloads](#) page.

The main installation file contains the basic packages required to set up XenServer on your host and install XenCenter on your Windows computer.

- 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](#).

- Install XenServer to a remote disk on a SAN to enable boot from SAN

For details, see [Boot From SAN](#).

Supplemental packs

You can install any required supplemental pack after installing XenServer. Download the supplemental pack (filename.iso) 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](#).

Upgrades

The installer presents the option to upgrade when it detects a previously installed version of XenServer. 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.

Important:

Upgrading requires careful planning and attention. For detailed information about upgrading individual XenServer hosts and pools, see [Upgrading from an existing version](#).

Install the XenServer host

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.

Warning:

Installing XenServer overwrites data on any hard drives that you select to use for the installation. Back up data that you want to preserve before proceeding.

To install or upgrade the XenServer host:

1. Boot the computer from the installation CD or, if applicable, network-boot from your TFTP server.
2. Following the initial boot messages and the Welcome to XenServer screen, select your keymap (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.

3. The Welcome to XenServer Setup screen is displayed.

XenServer 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.

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

Note:

Before enabling your XenServer host 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 XenServer host cannot find traffic that is on VLAN 0.

Warning:

Occasionally, booting a XenServer host 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.

4. The XenServer EULA is displayed. Use the Page Up and Page Down keys to scroll through and read the agreement. Select **Accept EULA** to proceed.
5. 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 XenServer, it offers the option to upgrade. For information about upgrading your XenServer host, see [Upgrading from an existing version](#).
 - *Restore:* If the installer detects a previously created backup installation, it offers the option to restore XenServer from the backup.

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

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

8. Select your installation media source.

To install from a CD, choose **Local media**. To install by using network, select **HTTP** or **FTP** or **NFS**. Choose **OK** to proceed.

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

- a) If the computer has multiple NICs, select one of them to be used to access the XenServer installation media files. Choose **OK** to proceed.
- b) 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.
- c) Provide VLAN ID if you have your installation media present in a VLAN network.
- d) 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.

- 9. 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.
- 10. Set and confirm a root password, which XenCenter uses to connect to the XenServer host. You also use this password (with user name “root”) to log into **xsconsole**, the system configuration console.
- 11. 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.

- 12. 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, XenServer hosts must have static IP addresses or be DNS addressable. When using DHCP, ensure that a static DHCP reservation policy is in place.

- 13. 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 XenServer host 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.

14. 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.
15. Specify how you want the server to determine local time: using NTP or manual time entry. Make your selection, and choose **OK** to proceed.
16. 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**.

Note:

XenServer assumes that the time setting in the BIOS of the server is the current time in UTC.

17. Select **Install XenServer**.

If you elected to set the date and time manually, you are prompted to do so during the installation. Once set, choose **OK** to proceed.

18. If you are installing from CD, the next screen asks if you want to install any supplemental packs from a CD. 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 XenServer installation CD, and insert the supplemental pack CD. 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 CD (if installing from CD) and select **OK** to reboot the server.

After the server reboots, XenServer 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 XenServer host.

Install XenCenter

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

The XenCenter installation media is bundled with the XenServer installation media. You can also download the latest version of XenCenter from the [download page](#).

To install XenCenter:

1. Before installing XenCenter, be sure to uninstall any previous version.
2. Launch the installer.

If installing from the XenServer installation CD:

- a) Insert the CD into the DVD drive of the computer which you want to run XenCenter.
 - b) Open the `client_install` folder on the CD. Double-click `XenCenter.msi` to begin the installation.
3. Follow the Setup wizard, which allows you to modify the default destination folder and then to install XenCenter.

Connect XenCenter to the XenServer host

To connect XenCenter to the XenServer host:

1. Launch XenCenter. The program opens to the **Home** tab.
2. Click the **Add New Server** icon.
3. Enter the IP address of the XenServer host in the **Server** field. Type the root user name and password that you set during XenServer 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

August 15, 2018

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

- One or more XenServer hosts with local storage
- Pools of XenServer hosts with shared storage:
 - Multiple XenServer hosts with shared NFS storage
 - Multiple XenServer hosts with shared iSCSI storage

XenServer hosts with local storage

The simplest deployment of XenServer is to run VMs on one or more XenServer hosts with local storage.

Note:

XenMotion live migration of VMs between XenServer hosts is only available when they share storage. However, Storage XenMotion 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 XenServer hosts

High-level procedure

1. Install the XenServer host software on the servers.
2. Install XenCenter on the systems.
3. Connect XenCenter to the XenServer hosts.

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

Pools of XenServer hosts with shared storage

A *pool* comprises multiple XenServer host installations, bound together as a single managed entity. When combined with shared storage, a pool enables VMs to be started on *any* XenServer host in the

pool that has sufficient memory. The VMs can then dynamically be moved between hosts while running (XenMotion) with minimal downtime. If an individual XenServer host 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. XenServer 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 XenServer. 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

This following sections step through setting up two common shared storage solutions – NFS and iSCSI – for a pool of XenServer hosts. 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 the XenCenter Help or [Hosts and Resource Pools](#).

XenServer hosts 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 XenServer hosts
- A server exporting a shared directory over NFS

High-level procedure

1. Install the XenServer host software on the servers.
2. Install XenCenter on the systems.
3. Connect XenCenter to the XenServer hosts.
4. Create your pool of XenServer hosts.

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, XenServer hosts 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 XenServer hosts 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 XenServer host in the pool.
2. Create the storage repository on *server:/path* by entering the following:

```
1 xe sr-create content-type=user type=nfs name-label=sr_name= \  
2 shared=true device-config:server=server \  
3 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:

```
1 xe pool-param-set uuid=pool_uuid \  
2      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.

XenServer hosts 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 XenServer hosts
- A server providing a shared directory over iSCSI

High-level procedure

1. Install the XenServer host software on the servers.
2. Install XenCenter on the Windows systems.
3. Connect XenCenter to the XenServer hosts.
4. Create your pool of XenServer hosts.
5. Configure the iSCSI storage.
6. If necessary, enable multiple initiators on your iSCSI device.
7. If necessary, configure the iSCSI IQN for each XenServer host.
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 XenServer hosts to be able to see and access the iSCSI target LUN. Both the iSCSI target and each iSCSI initiator on each XenServer host must have a valid and **unique** iSCSI Qualified Name (IQN). For configuration details, it is best to see your vendor documentation.

Configuring an iSCSI IQN for each XenServer host

Upon installation, XenServer automatically attributes a unique IQN to each host. If you must adhere to a local administrative naming policy, you can change the IQN by entering the following on the host console:

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

Or, you can use the xe CLI by entering the following:

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

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

Warning:

When you create XenServer 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 XenServer host 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 XenServer 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:

```
1 xe sr-create name=label=name_for_sr \  
2     host-uuid=host_uuid device-config:target=  
3     iscsi_server_ip_address \  
4     device-config:targetIQN=iscsi_target_iqn device-config:SCSIid=  
5     scsi_id \  
6     content-type=user type=lvmoiscsi shared=true \  
7
```

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:

```
1 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

April 1, 2019

Citrix provides upgrade and update capabilities that you can use to move from some earlier versions of XenServer to XenServer 7.6. Using the upgrade or update capability enables you to apply XenServer 7.6 without having to complete a full installation process. When you upgrade or update, XenServer 7.6 retains your VMs, SRs, and configuration.

- You can upgrade from XenServer 7.1 Cumulative Update 2 (LTSR) or 7.0 to XenServer 7.6 by using the **Base Installation ISO**. This section describes how to upgrade to XenServer 7.6.

Note:

Upgrading from XenServer 7.1 to XenServer 7.6 is not supported. Ensure that the latest

Cumulative Update is applied to XenServer 7.1 before attempting to upgrade.

- This Current Release (CR) of XenServer can be applied to previous supported XenServer Current Releases (7.5 and 7.4) as an update by using the **Update ISO**. A CR that is available as an update can be applied in the same way that hotfixes are applied. For more information, see [Update your hosts](#).
- For all other versions of XenServer, you cannot upgrade to XenServer 7.6 directly. You can either first upgrade to a later version of XenServer and then upgrade or update that version to 7.6, or you can perform a clean installation using the **Base Installation ISO**. For more information, see [Install](#).

Note:

To retain VMs from your previous installation of XenServer, export the VMs and import them into your clean installation of XenServer 7.6. VMs exported from any supported version of XenServer can be imported into XenServer 7.6. For more information, see [Import and export VMs](#).

This section describes how to upgrade XenServer by using XenCenter or the xe CLI. It guides you through upgrading your XenServer hosts - both pooled and standalone - automatically (using the XenCenter Rolling Pool Upgrade wizard) and manually.

Important:

- Upgrading XenServer hosts, and particularly a pool of XenServer hosts, 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. For example, when upgrading to XenServer 7.6, use XenCenter issued with XenServer 7.6. Using earlier versions of XenCenter to upgrade to a newer version of XenServer is not supported.
- 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](#).
- If you are upgrading to the latest version from XenServer 6.5 Service Pack 1 or earlier, the ordering and naming of the NICs is different. To work around this change, you can change the order of the NICs during installation. For more information, see [CTX135809 - How to Change Order of NICs in XenServer](#).

Rolling pool upgrades

XenServer 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 XenServer host 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 XenMotion is not supported with rolling pool upgrades.

You can perform a rolling pool upgrade using XenCenter or the xe CLI. When using XenCenter, Citrix recommends 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 XenServer hosts as you perform the rolling pool upgrade manually.

The Rolling Pool Upgrade wizard is available for XenServer Enterprise Edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer 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 XenServer hosts by using the XenCenter Rolling Pool Upgrade wizard

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

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 XenServer. 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 XenServer 7.6 to upgrade from any supported version of XenServer to XenServer 7.0 and later.

Note:

Rolling Pool Upgrade using XenCenter is only available for XenServer Enterprise Edition customers or those customers who have access to XenServer 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 XenServer 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.

Before you upgrade

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

- Download and install XenCenter issued with XenServer 7.6 from the [XenServer Product Download](#) page. Using earlier versions of XenCenter to upgrade to a newer version of XenServer is not supported.
- Citrix strongly recommends 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.

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.

To upgrade XenServer hosts by using the 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 CD/DVD or using network boot (using existing infrastructure)

Note:

If you choose **Manual Mode**, you must run the XenServer 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 XenServer 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 XenServer 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 XenServer pool.

- XenServer 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.

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 XenServer hosts by using the xe CLI

Important:

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 XenServer hosts running an older version of XenServer to one running the same version or higher. For example, from version 7.0 to version 7.1 or from version 7.1 to version 7.6. You **cannot** migrate VMs from an upgraded host to one running an older version of XenServer. For example, from version 7.6 to version 7.1. Be sure to allow for space on your XenServer hosts accordingly.
- Citrix strongly advises against running a mixed-mode pool (one with multiple versions of XenServer 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.
- Citrix strongly recommends 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 XenServer host to a host running an older version of XenServer.

Before you begin your rolling pool upgrade

- If you are using XenCenter, upgrade XenCenter to the latest version. The newer version of XenCenter correctly controls older versions of XenServer hosts.
- Empty the CD/DVD drives of the VMs in the pool. For details and instructions, see *Before Upgrading a Single XenServer Host*.
- 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 XenServer.

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 are 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 XenServer installation media and method of your choice (such as, installation CD or network). Follow the XenServer installation procedure (see [Install](#)) until the installer offers you the option to upgrade. **Choose to upgrade.**

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. On the pool master, start or resume any shutdown or suspended VMs. Migrate any VMs that you want back to the pool master.
6. Select the next XenServer host in your upgrade path. Disable the host.
7. Ensure that no VMs are running on the host. Shut down, suspend or migrate VMs to other hosts in the pool.
8. Shut down the host.
9. 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 XenServer on the host, and then join it, as a new host, to the pool using the `pool-join` command.

10. On the host, start or resume any shutdown or suspended VMs. Migrate any VMs that you want back to the host.
11. Repeat Steps 6–10 for the rest of the hosts in the pool.
12. After each host in the pool has been upgraded, it is important to upgrade the XenServer Tools on all VMs. For more information, see [Manage VMs](#).

Note:

Running older versions of the XenServer Tools on newer XenServer installations is not supported, except during the upgrade process.

If you are upgrading through multiple versions of XenServer, ensure that all upgrades have been applied before updating the XenServer Tools on your VMs. Do not update the XenServer Tools to interim versions.

Upgrade a single XenServer host by using the xe CLI

Before you upgrade a single XenServer host

Before upgrading a standalone XenServer host, 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 XenServer host. In addition, you must ensure that the VM is not attached to any physical CD/DVD drive on the XenServer host 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:

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

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

```
1 uuid ( R0) : abae3997-39af-2764-04a1-ffc501d132d9
2 vm-uuid ( R0): 340a8b49-866e-b27c-99d1-fb41457344d9
3 vm-name-label ( R0): VM02_DemoLinux
4 vdi-uuid ( R0): a14b0345-b20a-4027-a233-7cbd1e005ede
5 empty ( R0): false
6 device ( R0): xvdd
7
8 uuid ( R0) : ec174a21-452f-7fd8-c02b-86370fa0f654
9 vm-uuid ( R0): db80f319-016d-0e5f-d8db-3a6565256c71
10 vm-name-label ( R0): VM01_DemoLinux
11 vdi-uuid ( R0): a14b0345-b20a-4027-a233-7cbd1e005ede
12 empty ( R0): false
13 device ( R0): 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:

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

Upgrade a single XenServer host by using the xe CLI

To upgrade a single XenServer host by using the xe CLI:

1. Disable the XenServer host that you want to upgrade by typing the following:

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

When the XenServer host 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 XenServer 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. Restart any shutdown VMs, and resume any suspended VMs.

Update your hosts

April 16, 2019

Updates can often be applied with minimal service interruption. Citrix recommends that customers use XenCenter to apply all updates. If you are updating a XenServer 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 XenServer and XenCenter updates and new versions. Any Alerts are displayed in the **Notifications** pane.

Types of update

Citrix releases the following types of updates for XenServer:

- **Current Releases (CRs)**, which are full releases of XenServer from the CR stream. CRs can be applied as updates to the supported versions of XenServer from the CR stream.

- **Hotfixes**, which generally supply bug fixes to one or more specific issues. Hotfixes are provided for XenServer releases in the Long Term Service Release (LTSR) and Current Release (CR) streams and for earlier supported releases that are not part of either stream.
- **Cumulative Updates**, which contain previously released hotfixes and may contain support for new guests and hardware. Cumulative updates are applied to XenServer releases from the Long Term Service Release (LTSR) stream.

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

Current Releases

XenServer 7.6 is a Current Release of XenServer. The following table shows which previous versions of XenServer you can apply XenServer 7.6 to as an update:

Version	Apply XenServer 7.6 as an update?
XenServer 7.5 CR	Yes
XenServer 7.4 CR	Yes
XenServer 7.1 Cumulative Update 2 LTSR	No
XenServer 7.0	No

For those versions of XenServer that cannot have XenServer 7.6 applied as an update, instead use the Base Installation ISO and upgrade your existing installation.

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 XenServer 7.6 as an update to an existing XenServer installation that uses the legacy disk partition layout, the update might fail with insufficient space. If this failure occurs, create a fresh installation of XenServer 7.6 instead.

Hotfixes

Citrix might release hotfixes for XenServer 7.6 that provide fixes for specific issues.

Hotfixes for XenServer 7.6 are made available from the [Citrix Knowledge Center](#). Citrix recommends that customers regularly check the Knowledge Center for new updates. Alternatively,

you can subscribe to email alerts for updates to XenServer by registering for an account at <http://www.citrix.com/support/>.

Hotfixes on the latest CR is available to all XenServer customers. However, hotfixes on previous CRs 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 XenServer. 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.

XenServer 7.6 is a Current Release. No Cumulative Updates are provided for this release.

Prepare a pool for an update

Updates to XenServer 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 XenServer systems.

Important:

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

- (Applies to XenServer 7.6 hotfixes only) All hosts in the pool must be running XenServer 7.6 before you apply the hotfix.
- Back up your data before applying an update. For backup procedures, see [Disaster recovery and backup](#).
- 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. Schedule 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 XenServer hosts.

- After applying a Cumulative Update or Current Release to all hosts in a pool, update the XenServer Tools on all VMs. For more information, see [Manage VMs](#).

If you upgrade or update through multiple versions of XenServer, do not update the XenServer Tools until you have finished all updates.

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 XenServer Host](#).
- 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 Citrix 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 XenServer and XenCenter updates. Click **Refresh** to check manually for available updates.
- If the **Updates** tab cannot find any updates because 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 can be applied to the servers and the updates that are 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 XenServer
 - 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 update prechecks, to ensure that the pool is in a valid configuration state. The wizard also checks whether the hosts must be rebooted after the update is applied and displays the result. The **Install Update** wizard also checks whether a live patch is available for the hotfix and if 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 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 XenServer hosts by using the xe CLI

To update a pool of XenServer 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:

```
1 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. XenServer assigns the update file a UUID, which this command prints. Note the UUID.

Tip:

After an update file has been uploaded to the XenServer host, you can use the `update-list` and `update-param-list` commands to view information about the file.

3. If XenServer 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 XenServer.

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

```
1 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:

```
1 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 operation 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:

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

Here, `-s` refers to the hostname. XenServer assigns the update file a UUID, which this command prints. Note the UUID.

Tip:

After an update file has been uploaded to the XenServer host, you can use the `update-list` and `update-param-list` commands to view information about the update file.

4. If XenServer 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:

```
1 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](#) section.

Note:

The Automated Updates feature is available for XenServer Enterprise Edition customers, or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For more information, see [Licensing](#).

Note:

The Automated Updates feature is available for XenServer Enterprise 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 from Citrix 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 Citrix 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** section in XenCenter Help.
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 XenServer

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

XenServer customers who deploy XenServer hosts 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:

XenServer Live Patching is available for XenServer Enterprise Edition customers, or those cus-

tomers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To learn more about XenServer 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 live patch** — Some hotfixes that update 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 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:

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

- To disable Live Patching, run the following command:

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

Troubleshoot the installation

August 13, 2018

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 XenServer 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, Citrix Technical Support requests that you capture the log file from your host. 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:

```
1 /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.

Boot from SAN environments

September 5, 2018

Boot-from-SAN environments offer several advantages, including high performance, redundancy, and space consolidation. In these environments, the boot disk is on a remote SAN and not on the local host. The host communicates with the SAN through a host bus adapter (HBA). The HBA's BIOS contains the instructions that enable the host to find the boot disk.

Boot from SAN depends on SAN-based disk arrays with either hardware Fibre Channel or HBA iSCSI adapter support on the host. For a fully redundant boot from SAN environment, you must configure multiple paths for I/O access. To do so, ensure that the root device has multipath support enabled. For information about whether multipath is available for your SAN environment, consult your storage vendor or administrator. If you have multiple paths available, you can enable multipathing in your XenServer deployment upon installation.

Warning:

Boot-from-SAN settings are *not* inherited during the upgrade process. When upgrading using the ISO or network-boot, follow the same instructions as used in the installation process below to ensure that `multipath` is correctly configured.

To install XenServer to a remote disk on a SAN with multipathing enabled:

1. On the Welcome to XenServer screen, press **F2**.
2. At the boot prompt, enter `multipath`

The XenServer installation process configures the XenServer host, which boots from a remote SAN with multipathing enabled.

To enable file system multipathing using PXE or UEFI installation, add `device_mapper_multipath=yes` to your configuration file. The following is an example configuration:

```
1 default xenserver
2 label xenserver
3     kernel mboot.c32
4     append /tftpboot/xenserver/xen.gz dom0_max_vcpus=1-2 \
5     dom0_mem=1024M,max:1024M com1=115200,8n1 \
6     console=com1,vga --- /tftpboot/xenserver/vmlinuz \
7     xencons=hvc console=hvc0 console=tty0 \
8     device_mapper_multipath=yes \
9     install --- /tftpboot/xenserver/install.img
```

For additional information on storage multipathing in your XenServer environment, see [Storage](#).

Software-boot-from-iSCSI for Cisco UCS

The Software-boot-from-iSCSI feature enables customers to install and boot XenServer from SAN using iSCSI. Using this feature, XenServer can be installed to, booted from, and run from a LUN provided by an iSCSI target. The iSCSI target is specified in the iSCSI Boot Firmware Table. This capability allows the root disk to be attached through iSCSI.

XenServer supports the following features for Software-boot-from-iSCSI:

- Host installation through PXE-boot
- Cisco UCS vNIC

Software-boot-from-iSCSI has been tested in Legacy BIOS and UEFI boot mode by using Cisco UCS vNICs and Power Vault, NetApp, and EqualLogic arrays. Other configurations might work, however, they have not been validated.
- Jumbo Frames (MTU=9000) configured with the Cisco UCS manager
- Cisco UCS line-rate limiting
- Untagged VLANs
- Networks using the vSwitch back-end
- LVHDoiSCSI SRs and NFS SRs on the same or different SAN/NAS
- Multipathing of the iSCSI root disk
- Compatibility with common XenServer (Network, Maintenance) operations

Requirements

- The primary management interface (IP addressable) and the network for VM traffic, must use separate interfaces.
- Storage (iSCSI targets) must be on a separate Layer 3 (IP) network to all other network interfaces with IP addresses on the host.
- Storage must be on the same subnet as the storage interface of the XenServer host.

Install XenServer by using CD media

Perform the following steps to install XenServer using a CD:

1. Access the boot menu; at the `boot:` prompt enter `menu.c32`
2. Use the cursor keys to select an installation option:
 - For a single path LUN, select **install**
 - For a multipathed LUN, select **multipath**
3. Press the tab key.

Edit the line ending with the following:

```
1 --- /install.img
```

4. Using the cursor keys, edit this line to read:

```
1 use_ibft --- /install.img
```

5. Press **Enter**.

XenServer host installation proceeds as normal.

Install XenServer by using PXE

Perform the following steps to install XenServer using PXE:

Note:

Ensure that you add the keyword **use_ibft** in the kernel parameters. If multipathing is required, you must add **device_mapper_multipath=enabled**.

The following example shows PXE configuration for a single LUN:

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc console=
  tty0
5 console=hvc0 use_ibft --- XS/install.img
```

The following example shows PXE configuration for a multipathed LUN:

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc console=
  tty0
5 console=hvc0 use_ibft device_mapper_multipath=enabled --- XS/install.
  img
```

Network boot installations

September 5, 2018

XenServer supports booting hosts using the UEFI mode. UEFI mode provides a rich set of standardized facilities to the bootloader and operating systems. This feature allows XenServer to be more easily installed on hosts where UEFI is the default boot mode.

The following section contains information about setting up your TFTP and NFS, FTP, or HTTP servers to enable PXE and UEFI booting of XenServer host installations. It then describes how to create an XML answer file, which allows you to perform unattended installations.

Configure your PXE and UEFI environment for XenServer installation

Before you set up the XenServer installation media, configure your TFTP and DHCP servers. The following sections contain information on how to configure your TFTP server for PXE and UEFI booting. Consult your vendor documentation for general setup procedures.

Note:

XenServer 6.0 moved from MBR disk partitioning to GUID Partition Table (GPT). Some third-party PXE deployment systems might attempt to read the partition table on a machine's hard disk *before* deploying the image to the host.

If the deployment system isn't compatible with GPT partitioning scheme and the hard disk has

previously been used for a version of XenServer that uses GPT, the PXE deployment system might fail. A workaround for this failure is to delete the partition table on the disk.

In addition to the TFTP and DHCP servers, you require an NFS, FTP, or HTTP server to house the XenServer installation files. These servers can co-exist on one, or be distributed across different servers on the network.

Additionally, each XenServer host that you want to PXE boot must have a PXE boot-enabled Ethernet card.

The following steps assume that the Linux server you are using has RPM support.

Configure your TFTP server for PXE boot

1. In the `/tftpboot` directory, create a directory called `xenserver`
2. Copy the `mboot.c32` and `pxelinux.0` files from the `/usr/lib/syslinux` directory to the `/tftpboot` directory.

Note:

Citrix strongly recommends using `mboot.c32` and `pxelinux.0` files from the same source (for example, from the same XenServer ISO).

3. From the XenServer installation media, copy the files `install.img` (from the root directory), `vmlinux`, and `xen.gz` (from the `/boot` directory) to the new `/tftpboot/xenserver` directory on the TFTP server.
4. In the `/tftpboot` directory, create a directory called `pxelinux.cfg`.
5. In the `pxelinux.cfg` directory, create your configuration file called `default`.

The content of this file depends on how you want to configure your PXE boot environment. Two sample configurations are listed below. The first example configuration starts an installation on any machine that boots from the TFTP server. This installation requires manual responses. The second example configuration is for an unattended installation.

Note:

The following examples show how to configure the installer to run on the physical console, `tty0`. To use a different default, ensure that the console you want to use is the rightmost.

```
1  default xenserver
2  label xenserver
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5          dom0_mem=1024M,max:1024M com1=115200,8n1 \
6          console=com1,vga --- /tftpboot/xenserver/vmlinux \
```

```

7      xencons=hvc console=hvc0 console=tty0 \
8      --- /tftpboot/xenserver/install.img

```

A sample configuration that performs an unattended installation using the answer file at the URL specified:

Note:

To specify which network adapter to use to retrieve the answer file, include the `answerfile_device=ethX` or `answerfile_device=MAC` parameter and specify either the Ethernet device number or the MAC address of the device.

```

1  default xenserver-auto
2  label xenserver-auto
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5              dom0_mem=1024M,max:1024M com1=115200,8n1 \
6              console=com1,vga --- /tftpboot/xenserver/vmlinuz \
7              xencons=hvc console=hvc0 console=tty0 \
8              answerfile=http://pxehost.example.com/answerfile \
9              install --- /tftpboot/xenserver/install.img

```

For more information about PXE configuration file contents, see the [SYSLINUX](#) website.

Configure your TFTP server for UEFI boot

To configure your TFTP server for UEFI boot:

1. In the `/tftpboot` directory, create a directory called `EFI/xenserver`.
2. Configure your DHCP server to provide `/EFI/xenserver/grubx64.efi` as the boot file.
3. Create `grub.cfg` file. For example:
 - For an installation that requires manual responses to installation prompts:

```

1  menuentry "XenServer Install (serial)" {
2
3      multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
4          watchdog \
5          dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
6          module2 /EFI/xenserver/vmlinuz console=hvc0
7          module2 /EFI/xenserver/install.img
8  }

```

- For an unattended installation that uses an answer file:

```
1 menuentry "XenServer Install (serial)" {
2
3     multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
4     watchdog \
5     dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
6     module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
7     answerfile_device=eth0 answerfile=ftp://ip_address/
8     path_to_answerfile install
9     module2 /EFI/xenserver/install.img
10 }
```

For more information about using an answer file, see *Creating an answer file for unattended PXE and UEFI installation*.

4. Copy `grub.cfg` file to `/tftpboot/EFI/xenserver` directory on the TFTP server.
5. From the XenServer installation media, copy the files `grubx64.efi`, `install.img` (from the root directory), `vmlinuz`, and `xen.gz` (from the `/boot` directory) to the new `/tftpboot/EFI/xenserver` directory on the TFTP server.

For details for your specific operating system, see your server operating system manual. The information here is a guide that can be used for Red Hat, Fedora, and some other RPM-based distributions.

To set up the XenServer installation media on an HTTP, FTP or NFS server:

1. On the server, create a directory from which the XenServer installation media can be exported via HTTP, FTP, or NFS.
2. Copy the entire contents of the XenServer installation media to the newly created directory on the HTTP, FTP, or NFS server. This directory is your installation repository.

Note:

When copying the XenServer installation media, ensure that you copy the file `.treeinfo` to the newly created directory.

To prepare the destination system:

1. Start the system and enter the Boot menu (**F12** in most BIOS programs).
2. Select to boot from your Ethernet card.
3. The system then PXE boots from the installation source you set up, and the installation script starts. If you have set up an answer file, the installation can proceed unattended.

Install Supplemental Packs during XenServer installation

Supplemental Packs are used to modify and extend the capabilities of XenServer by installing software into the control domain (Dom0). For example, an OEM partner might want to ship XenServer with a set of management tools that require SNMP agents to be installed. Users can add supplemental packs either during initial XenServer installation, or at any time afterwards.

When installing supplemental packs during XenServer installation, unpack each supplemental pack into a separate directory.

Facilities also exist for OEM partners to add their supplemental packs to the XenServer installation repositories to allow automated factory installations.

Create an answer file for unattended PXE and UEFI installation

To perform installations in an unattended fashion, create an XML answer file. Here is an example answer file:

```
1 <?xml version="1.0"?>
2   <installation srtype="ext">
3     <primary-disk>sda</primary-disk>
4     <guest-disk>sdb</guest-disk>
5     <guest-disk>sdc</guest-disk>
6     <keymap>us</keymap>
7     <root-password>mypassword</root-password>
8     <source type="url">http://pxehost.example.com/xenserver/</source>
9     <post-install-script type="url">
10      http://pxehost.example.com/myscripts/post-install-script
11    </post-install-script>
12    <admin-interface name="eth0" proto="dhcp" />
13    <timezone>Europe/London</timezone>
14  </installation>
```

Contain all nodes within a root node named *installation*.

Note:

To enable thin provisioning, specify an `srtype` attribute as `ext`. If this attribute is not specified, the default local storage type is LVM. Thin provisioning sets the local storage type to EXT3 and enables local caching for Citrix Virtual Desktops to work properly. For more information, see [Storage](#).

The following is a summary of the elements. All node values are text, unless otherwise stated. Required elements are indicated.

<primary-disk>**Required?** Yes

Description: The name of the storage device where the control domain is installed. This element is equivalent to the choice made on the *Select Primary Disk* step of the manual installation process.

Attributes: You can specify a `guest-storage` attribute with possible values `yes` and `no`.

For example: `<primary-disk guest-storage="no">sda</primary-disk>`

The default value is `yes`. If you specify `no`, you can automate an installation scenario where no storage repository is created. In this case, specify no guest-disk keys.

<guest-disk>**Required?** No

Description: The name of a storage device to be used for storing guests. Use one of these elements for each extra disk.

Attributes: None

<keymap>**Required?** Yes

Description: The name of the keymap to use during installation. `<keymap>us</keymap>` The default value, `us` is considered if you do not specify a value for this element.

Attributes: None

You can also perform automated upgrades by changing the answer file appropriately. Set the `mode` attribute of the installation element to `upgrade`, specify the disk on which the existing installation lives with the `existing-installation` element. Leave the `primary-disk` and `guest-disk` elements unspecified. For example:

```
1 <?xml version="1.0"?>
2   <installation mode="upgrade">
3     <existing-installation>sda</existing-installation>
4     <source type="url">http://pxehost.example.com/xenserver/</
      source>
5     <post-install-script type="url">
6       http://pxehost.example.com/myscripts/post-install-script
7     </post-install-script>
8   </installation>
```


Host partition layout

March 12, 2019

XenServer 7.0 introduced a new host disk partition layout. By moving log files to a larger, separate partition, XenServer can store more detailed logs for a longer time. This feature improves the ability to diagnose issues. Simultaneously, the new partition layout relieves demands on Dom0's root disk and avoids potential space issues due to log file disk space consumption. The new layout contains the following partitions:

- 18 GB XenServer host control domain (dom0) partition
- 18 GB backup partition
- 4 GB logs partition
- 1 GB swap partition
- 0.5 GB UEFI boot partition

In XenServer 6.5 and earlier releases, the 4 GB control domain (dom0) partition was used for all dom0 functions, including swap and logging. Customers who do not use remote syslog or who used with third-party monitoring tools and supplemental packs found the size of the partition to be limited. XenServer eliminates this issue and provides a dedicated 18 GB partition to dom0. In addition, a larger partition dedicated to dom0 reduces demand on the dom0 root disk which can offer significant performance improvements.

The introduction of the 4 GB dedicated log partition eliminates scenarios where excessive logging filled up the dom0 partition and affected the behavior of the host. This partition also enables customers to retain a detailed list of logs for a longer time, improving the ability to diagnose issues.

The partition layout also contains a dedicated 500 MB partition required for UEFI boot.

Note:

If you install XenServer with the new partition layout described above, ensure that you have a disk that is at least 46 GB in size.

To install XenServer on smaller devices, you can do a clean installation of XenServer using the legacy DOS partition layout. A small device is one that has more than 12 GB but less than 46 GB disk space. For more information, see [Installing on Small Devices](#).

Important:

We recommend that you allocate a minimum of 46 GB disk space and install XenServer using the new GPT partition layout.

Upgrade to the new partition layout

When upgrading to XenServer 7.6 from XenServer 6.5 or earlier version using XenCenter, the host partition layout is upgraded to the new layout, provided:

- There is at least 46 GB of disk space on the local SR
- There are no VDIs present on the local SR
- You use XenCenter issued with XenServer 7.6 to perform a Rolling Pool Upgrade (RPU) to XenServer 7.6

Warning:

Customers cannot upgrade to the new host partition layout using xe CLI.

During the upgrade process, the RPU wizard checks for VDIs on the local SR. If there are any virtual disks (VDIs) present during the upgrade process, the wizard prompts you to move the VDI. Move VDIs on the local SR to a shared SR and then restart the upgrade process to continue with the new layout. If the VDIs cannot be moved or the local SR has insufficient space (less than 46 GB), the upgrade proceeds with the old partition layout. 0.5 GB of disk space is allocated from the dom0 partition to UEFI boot.

Restore the old partition layout

If you plan to restore XenServer from version 7.6 to version 6.x, the host partition layout reverts to the 6.x layout.

Legacy partition layouts

- XenServer 5.6 Service Pack 2 and earlier used DOS partition tables to separate the root file system and backups from the local storage.
- XenServer 6.0 introduced GUID partition tables to separate root file system, backup and local storage.
- Installing XenServer 7.6 on machines with a required initial partition that must be preserved continues to use the DOS partitioning scheme.

The following table lists the installation and upgrade scenarios and the partition layout that is applied after these operations:

Operation	Number of partitions before upgrade	Number of partitions after installation/upgrade	Partition table type
Clean installation with at least 46 GB of primary disk space	N/A	6	New GPT
Clean installation with <code>disable-gpt</code> with a minimum of 12 GB of primary disk space	N/A	3 (or 4 if there is a utility partition)	DOS
Clean installation on a machine with a utility partition	N/A	3 (or 4 if there is a utility partition)	DOS
Upgrading from XenServer 6.x with VMs on local SR or with less than 46 GB of primary disk space	3	4	Old GPT
Upgrading from XenServer 6.x without VMs on local SR or with more than 46 GB of primary disk space	3	6	New GPT
Upgrading from XenServer 6.x DOS partition (and utility partition, if any)	3 (or 4 if there is a utility partition)	3 (or 4 if there is a utility partition)	DOS

Install on small devices

August 13, 2018

XenServer enables customers with smaller devices to install XenServer 7.6 using the legacy DOS partition layout. A small device is one that has more than 12 GB but less than 46 GB of disk space. The legacy DOS partition layout includes:

- 4 GB Boot partition

- 4 GB Backup partition
- SR partition (if present on the local disk)

To install XenServer on small devices, you must add `disable-gpt` to the dom0 parameters. You can use `menu.c32` to add the parameter to dom0.

Note:

The installer preserves any utility partition that exists on the host before the installation process.

Important:

We recommend that you allocate a minimum of 46 GB disk space and install XenServer using the new GPT partition layout. For more information, see [Host Partition Layout](#).

Hosts and resource pools

March 22, 2019

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.

XenServer hosts and resource pools overview

A *resource pool* comprises multiple XenServer host 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* XenServer host which has sufficient memory. The VMs can then be dynamically moved among XenServer hosts while running with a minimal downtime (XenMotion). If an individual XenServer host suffers a hardware failure, the administrator can restart failed VMs on another XenServer host 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 XenServer 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 XenServer hosts, 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 XenServer 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, XenServer 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.

XenServer hosts 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 XenServer host to run a VM and to move a VM between XenServer hosts dynamically. If possible create a pool after shared storage is available. Citrix recommends 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. See [Manage networking](#) for details on how to dedicate a storage NIC from the CLI.

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 XenServer hosts *host1* and *host2* into a resource pool by using the CLI

1. Open a console on XenServer host *host2*.
2. Command XenServer host *host2* to join the pool on XenServer host *host1* by issuing the command:

```
1 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 XenServer host `host1`. The `password` must be the administrator password set when XenServer host `host1` was installed.

XenServer hosts 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`:

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

Create heterogeneous resource pools

XenServer 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:

Note:

The CPUs of XenServer hosts 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.

XenServer 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, XenServer 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 XenServer host in the pool.
2. Create the storage repository on server:/path by issuing the command

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

`device-config:server` is the hostname 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 XenServer host in the pool. Any XenServer hosts 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:

```
1 xe pool-list
```

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

```
1 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. See [Storage repository formats](#) for information about creating other types of shared storage.

Remove XenServer hosts from a resource pool

Note:

Before removing any XenServer host 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 XenServer hosts 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

```
1 xe host-list
```

3. Eject the required host from the pool:

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

The XenServer host 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 XenServer hosts 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 XenServer hosts. The VMs do not start until the virtual disks associated with them have been changed to point at shared storage seen by other XenServer hosts 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 XenServer hosts 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 XenServer hosts 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 XenServer host in the pool. You can do this by placing the XenServer host in to Maintenance mode using XenCenter. See the XenCenter Help for details.

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:

Citrix highly recommends rebooting all XenServer hosts before installing an update and then verifying their configuration. Some configuration changes only take effect when XenServer 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:

```
1 xe host-disable uuid=XenServer_host_uuid
2 xe host-evacuate uuid=XenServer_host_uuid
```

This command disables the XenServer host and then migrate any running VMs to other XenServer hosts in the pool.

2. Perform the desired maintenance operation.
3. Enable the XenServer host when the maintenance operation is complete:

```
1 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 XenServer Enterprise Edition customers, or those who have access to XenServer 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 XenServer host.

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 XenServer host 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 XenServer 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.

- **Hewlett-Packard Integrated Lights-Out (iLO).** To use XenServer with iLO, you must enable iLO on the host and connect interface to the network. For more information, see HP's iLO documentation.
- A custom script based on the management API that enables you to turn the power on and off through XenServer. 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, a DRAC or iLO 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 XenServer).

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:

```
1 xe host-set-power-on-mode host=<host uuid>\
2 power-on-mode=("wake-on-lan",
3 "iLO", "DRAC", "custom")
4 power-on-config=key:value
5
6
7 For iLO and DRAC the keys are 'power_on_ip'{
8 #prnmN7008A }
9 , 'power_on_user'{
10 #prnmN70090 }
11 , 'power_on_password_secret'{
12 #prnmN70096 }
13 . Use 'power_on_password_secret'{
14 #prnmN7009C }
```

```
15    to specify the password if you are using the secret feature. For more
      information, see [Secrets](/en-us/xenserver/current-release/
      command-line-interface.html#secrets).
```

To turn on hosts remotely by using the CLI

Run the command:

```
1  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 XenServer computers remotely. However, you can also create custom scripts for iLO, 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 XenServer 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 XenServer. Alternatively, you can specify it in XenCenter and use the XenCenter UI features to interact with it.

The XenServer API is documented in the document, the XenServer Management API, which is available from the Citrix 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 {#host.power_on_mode}

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:

```
1  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
 - “iLO”: Lets you specify HP iLO.
 - “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 iLO and DRAC.
- **Possible values:**
 - If you configured iLO or 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 iLO or DRAC is configured.
 - * “power_on_user”: The iLO or 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 XenServer 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` {#prnmN8012E}, `remote_host` {#prnmN80134}, and `power_on_config` {#prnmN8013A} in all custom scripts.

The result appears when the script is unsuccessful.

```
1 import XenAPI
2 def custom(session,remote_host,
3 power_on_config):
4 result="Power On Not Successful"
5 for key in power_on_config.keys():
6 result=result+' '
7 key=' '+key+' '
8 value=' '+power_on_config[key]
9 return result
```

Note:

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

Communicate with XenServer hosts and resource pools

XenServer uses TLS protocols to encrypt management API traffic. Any communication between XenServer and management API clients (or appliances) now uses TLS 1.2 protocol by default. However, if the management API client or the appliance does not communicate using TLS 1.2, earlier protocols may be used for communication.

XenServer uses the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

XenServer also enables you to configure your host or resource pool to allow communication through **TLS 1.2 only**. This option allows communication between XenServer and management API clients (or appliances) using the TLS 1.2 protocol. The TLS 1.2 only option uses cipher suite `TLS_RSA_WITH_AES_128_CBC_SHA256`.

Warning:

Select the **TLS 1.2 only** option after you ensure that all management API clients and appliances that communicate with the XenServer pool are compatible with TLS 1.2.

Clustered pools

September 5, 2018

Clustering provides extra features that are required for resource pools that use GFS2 SRs. For more information about GFS2, see [Configure storage](#).

A cluster is a pool of XenServer hosts that are more closely connected and coordinated than non-clustered pools. The hosts in the cluster maintain constant communication with each other on a selected network. All hosts in the cluster are aware of the state of every host in the cluster. This host coordination enables the cluster to control access to the contents of the GFS2 SR.

Quorum

Each host in a cluster must always be in communication with at least half of hosts in the cluster (including itself). This state is known as a host having quorum.

The quorum value for an odd-numbered pool is half of one plus the total number of hosts in the cluster: $(n+1)/2$. The quorum value for an even-numbered pool is half the total number of hosts in the cluster: $n/2$.

For an even-numbered pool, it is possible for the running cluster to split exactly in half. The running cluster decides which half of the cluster self-fences and which half of the cluster has quorum. When an even-numbered clustered pool powers up from a cold start, $(n/2)+1$ hosts must be available before the hosts have quorum. After the hosts have quorum, the cluster becomes active.

If a host does not have quorum, that host self-fences.

Self-fencing

If a host detects that it does not have quorum, it self-fences within a few seconds. When a host self-fences, it restarts immediately. All VMs running on the host are killed because the host does a hard shutdown. In a clustered pool that uses high availability, XenServer restarts the VMs according to their restart configuration on other pool members. The host that self-fenced restarts and attempts to rejoin the cluster.

If the number of live hosts in the cluster becomes less than the quorum value, all the remaining hosts lose quorum.

In an ideal scenario, your clustered pool always has more live hosts than are required for quorum and XenServer never fences. To make this scenario more likely, consider the following recommendations when setting up your clustered pool:

- Ensure that you have good hardware redundancy.
- Use a dedicated bonded network for the cluster network. Ensure that the bonded NICs are on the same L2 segment. For more information, see [Networking](#).
- Configure storage multipathing between the pool and the GFS2 SR. For more information, see [Storage multipathing](#).
- Configure high availability on the clustered pool. In clustered pools, the heartbeat SR must be a GFS2 SR. For more information, see [High availability](#).

Create a clustered pool

Before you begin, ensure the following prerequisites are met:

- All XenServer hosts in the clustered pool must have at least 2 GiB of control domain memory.
- All hosts in the cluster must use static IP addresses for the cluster network.
- Citrix recommends that you use clustering only in pools containing at least three hosts, as pools of two hosts are sensitive to self-fencing the entire pool.
- If you have a firewall between the hosts in your pool, ensure that hosts can communicate on the cluster network using the following ports:
 - TCP: 8892, 21064
 - UDP: 5404, 5405

For more information, see [Communication Ports Used by Citrix Technologies](#).

- If you are clustering an existing pool, ensure that high availability is disabled. You can enable high availability again after clustering is enabled.

You can set up clustering on your pool by using XenCenter. For more information, see the XenCenter Help.

To use the xe CLI to create a clustered pool:

1. Create a resource pool.

For more information, see [Hosts and resource pools](#).

2. Create a bonded network or choose an existing bonded network to use as the clustering network.

For more information, see [Networking](#).

3. Open a console on a XenServer host in your pool.
4. For every PIF that belongs to this network, set `disallow-unplug=true`:

```
1 xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

5. Enable clustering on your pool:

```
1 xe cluster-pool-create network-uuid=<network_uuid>
```

Manage your clustered pool

When managing your clustered pool, the following practices can decrease the risk of the pool losing quorum.

Ensure that hosts are shut down cleanly

When a host is cleanly shut down, it is temporarily removed from the cluster until it is started again. While the host is shut down, it does not count toward the quorum value of the cluster. The host absence does not cause other hosts to lose quorum.

However, if a host is forcibly or unexpectedly shut down, it is not removed from the cluster before it goes offline. This host does count toward the quorum value of the cluster. Its shutdown can cause other hosts to lose quorum.

Use maintenance mode

Before doing something on a host that might cause that host to lose quorum, put the host into maintenance mode. When a host is in maintenance mode, running VMs are migrated off it to another host in the pool. Also, if that host was the pool master, that role is passed to a different host in the pool. If your actions cause a host in maintenance mode to self-fence, you don't lose any VMs or lose your XenCenter connection to the pool.

Hosts in maintenance mode still count towards the quorum value for the cluster.

You can only change the IP address of a host that is part of a clustered pool when that host is in maintenance mode. Changing the IP address of a host causes the host to leave the cluster. When the IP address has been successfully changed, the host rejoins the cluster. After the host rejoins the cluster, you can take it out of maintenance mode.

Recover hosts that have self-fenced or are offline

It is important to recover hosts that have self-fenced. While these cluster members are offline, they count towards the quorum number for the cluster and decrease the number of cluster members that are contactable. This situation increases the risk of a subsequent host failure causing the cluster to lose quorum and shut down completely.

Having offline hosts in your cluster also prevents you from performing certain actions. In a clustered pool, every member of the pool must agree to every change of pool membership before the change can be successful. If a cluster member is not contactable, XenServer prevents operations that change cluster membership (such as host add or host remove).

Mark hosts as dead

If one or more offline hosts cannot be recovered, you can mark them as dead to the cluster. Marking hosts as dead removes them permanently from the cluster. After hosts are marked as dead, they no longer count towards the quorum value.

Constraints

- Clustered pools only support up to 16 hosts per pool.
- If a network has been used for both management and clustering, you cannot separate the management network without recreating the cluster.
- Using DHCP is highly discouraged, as a dynamic IP address change on a live cluster can expose the cluster to a rare chance of data loss.
- Changing the IP address of the cluster network by using XenCenter requires clustering and GFS2 to be temporarily disabled.
- Do not change the bonding of your clustering network while the cluster is live and has running VMs. This action can cause the cluster to fence.

Manage users

January 4, 2019

Defining users, groups, roles and permissions allows you to control who has access to your XenServer hosts and pools and what actions they can perform.

When you first install XenServer, a user account is added to XenServer automatically. This account is the local super user (LSU), or root, which XenServer authenticates locally.

The LSU, or root, is a special user account intended for system administration and has all permissions. In XenServer, the LSU is the default account at installation. XenServer 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 XenServer 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, XenServer does not assign newly created user accounts RBAC roles automatically. Therefore, these accounts do not have any access to the XenServer 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 XenServer users log on to a pool using their Windows domain credentials.

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 XenServer maps to an entity on your directory server (either a user or a group). When you enable external authentication, XenServer checks the credentials used to create a session against the local root credentials (in case your directory server is unavailable) 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 XenServer CLI uses slightly different terminology to refer to Active Directory and user account features:

XenCenter Term	XenServer CLI Term
Users	Subjects
Add users	Add subjects

Active Directory authentication in the XenServer environment

Even though XenServer is Linux-based, XenServer lets you use Active Directory accounts for XenServer user accounts. To do so, it passes Active Directory credentials to the Active Directory domain controller.

When you add Active Directory to XenServer, Active Directory users and groups become XenServer 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 XenServer. 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 XenServer) 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 XenServer, 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

XenServer supports use of Active Directory servers using Windows 2008 or later.

To authenticate Active Directory for XenServer hosts, you must use the same DNS server for both the Active Directory server (configured to allow for interoperability) and the XenServer host.

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 XenServer host. Alternatively, you can set the values in the PIF objects or use the installer when a manual static configuration is used.

Citrix recommends using DHCP to assign hostnames. Do not assign the hostnames `localhost` or `linux` to hosts.

Warning:

XenServer host names must be unique throughout the XenServer deployment.

Note the following:

- XenServer labels its AD entry on the AD database using its hostname. If two XenServer hosts with the same hostname are joined to the same AD domain, the second XenServer overwrites the AD entry of the first XenServer. The overwriting occurs regardless of whether the hosts belong to the same or different pools. This can cause the AD authentication on the first XenServer to stop working.

You can use the same host name in two XenServer hosts, as long as they join different AD domains.

- The XenServer hosts 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 XenServer 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 XenServer Active Directory integration uses the Kerberos protocol to communicate with the Active Directory servers. Therefore, XenServer 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 XenServer hosts must be synchronized with the clocks on your Active Directory server. When XenServer 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 XenServer 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`.
- XenServer uses PowerBroker Identity Services (PBIS) to authenticate the AD user in the AD server, and to encrypt communications with the AD server.

How does XenServer 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.

```
1 xe pool-enable-external-auth auth-type=AD \  
2   service-name=full-qualified-domain \  
3   config:user=username \  
4   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 XenServer hosts, use the following approaches to set up your DNS:

1. Set up your domain DNS suffix search order for resolving non-FQDN entries:

```
1  xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \  
2  "other-config:domain=suffix1.com suffix2.com suffix3.com"
```

2. Configure the DNS server to use on your XenServer hosts:

```
1  xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \  
2  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:

```
1  xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
```

Note:

External authentication is a per-host property. However, Citrix recommends that you enable and disable external authentication on a per-pool basis. A per-pool setting allows XenServer to deal with failures that occur when enabling authentication on a particular host. XenServer 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:

```
1  xe pool-disable-external-auth
```

User authentication

To allow a user access to your XenServer host, 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 XenServer, 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 number of users in the Active Directory group must not exceed 500.

To add an AD subject to XenServer:

```
1 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. :

```
1 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:

```
1 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:

```
1 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 XenServer host or pool:

```
1 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 that is in the subject list does not 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 help 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:

```
1 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=xendrt\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:

```
1 xe session-subject-identifier-logout subject-identifier=subject_id
```

Leave an AD domain

Warning:

When you leave the domain (that is, disable Active Directory authentication and disconnect a pool or server from its domain), any users who authenticated to the pool or server with Active Directory credentials are disconnected.

Use XenCenter to leave an AD domain. See the XenCenter help for more information. 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. For information on how to delete disabled host entries, see the [Microsoft Support article](#).

Role-based access control

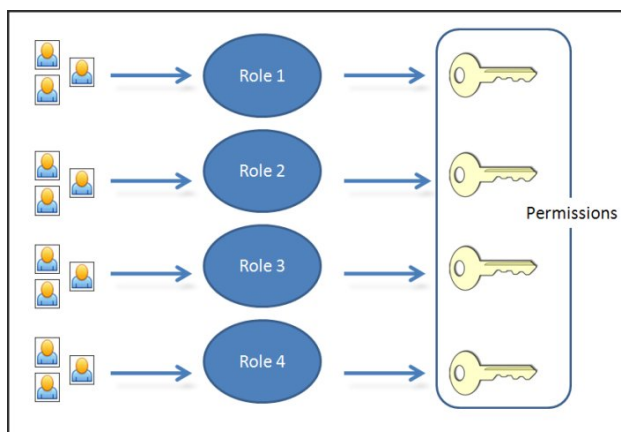
September 5, 2018

Role Based Access Control (RBAC) feature in XenServer allows you to assign users, roles, and permissions to control who has access to your XenServer and what actions they can perform. The XenServer RBAC system maps a user (or a group of users) to defined roles (a named set of permissions). The roles have associated XenServer 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. XenServer 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, XenServer 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 XenServer. The LSU is authenticated through XenServer 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 XenServer 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

February 12, 2019

Roles

XenServer 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.

- *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 XenServer, you must first assign a role to the newly created user before they can use the account. XenServer **does not** automatically assign a role to the newly created user. As a result, these accounts do not have any access to XenServer 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 per- missions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
Assign/modif roles	X					
Log in to (physical) server consoles (through SSH and XenCenter)	X					
Server backup/re- store	X					
Import/export OVF/OVA packages and disk images	X					
Set cores per socket	X	X	X	X		

Role per- missions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
Convert virtual machines using XenServer Conversion Manager	X					
Switch-port locking	X	X				
Multipathing	X	X				
Log out active user connec- tions	X	X				
Create and dismiss alerts	X	X				
Cancel task of any user	X	X				
Pool man- agement	X	X				
XenMotion	X	X	X			
Storage XenMotion	X	X	X			
VM advanced operations	X	X	X			
VM cre- ate/destroy operations	X	X	X	X		
VM change CD media	X	X	X	X	X	
VM change power state	X	X	X	X	X	

Role per- missions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
View VM consoles	X	X	X	X	X	
XenCenter view man- agement operations	X	X	X	X	X	
Cancel own tasks	X	X	X	X	X	X
Read audit logs	X	X	X	X	X	X
Connect to pool and read all pool metadata	X	X	X	X	X	X
Configure virtual GPU	X	X				
View virtual GPU config- uration	X	X	X	X	X	X
Access the config drive (CoreOS VMs only)	X					
Container manage- ment	X					
Scheduled Snapshots (Add/Re- move VMs to existing Snapshots Schedules)	X	X	X			

Role per- missions	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator	Read Only
Scheduled Snapshots (Add/Modi- fy/Delete Snapshot Schedules)	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 configura- tion	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 XenServer Conversion Manager:

- Convert VMware VMs to XenServer VMs

This permission lets the user convert workloads from VMware to XenServer by copying batches of VMware VMs to XenServer 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 XenServer cancel an in-progress task initiated by any user.

Pool management:

- Set pool properties (naming, default SRs)
- 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 slaves
- 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.

XenMotion:

- Migrate VMs from one host to another host when the VMs are on storage shared by both hosts

Storage XenMotion:

- 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 XenServer 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 XenServer 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

Container management:

- Start
- Stop
- Pause
- Resume
- Access information about the container

Scheduled Snapshots:

- Add VMs to existing snapshot schedules
- Remove VMs from existing snapshot schedules
- Add snapshot schedules
- Modify snapshot schedules
- Delete snapshot schedules

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 XenServer Enterprise 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:

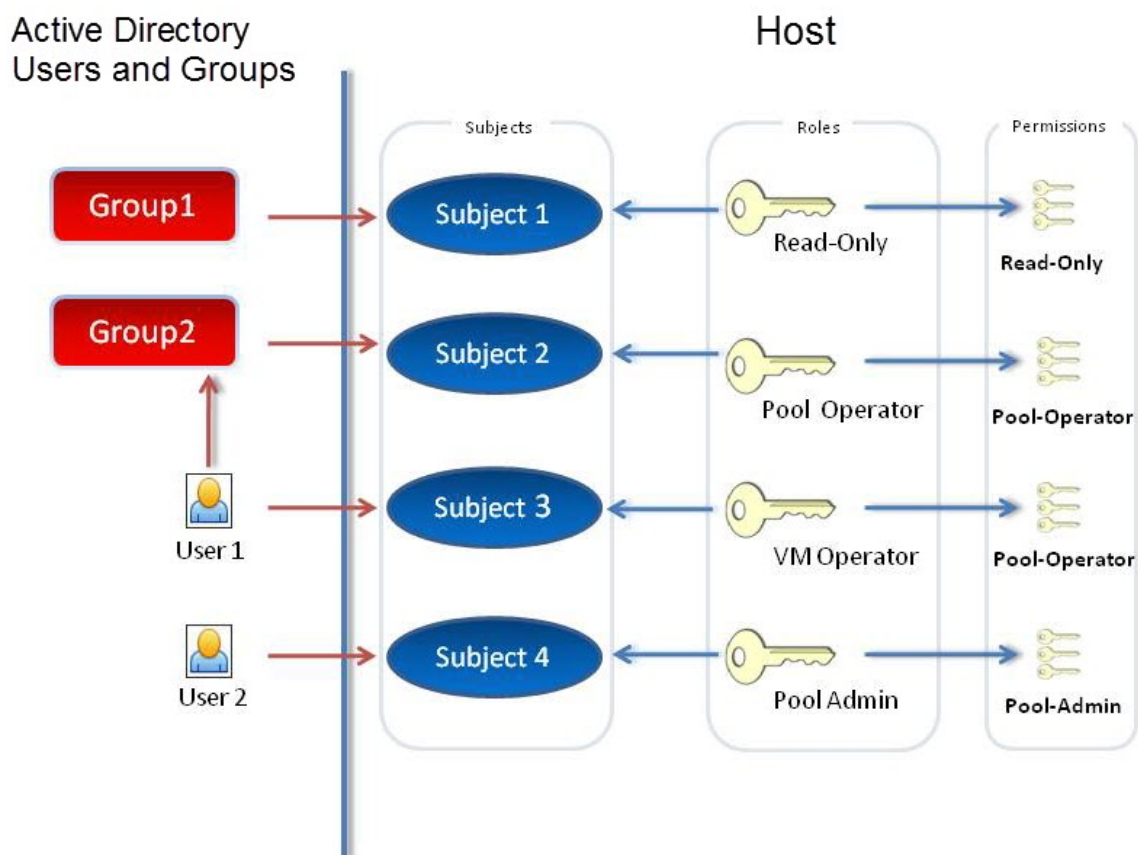
- View the status of PVS-Accelerator

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 XenServer 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. XenServer 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

September 5, 2018

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:

```
1 uuid( RO): 0165f154-ba3e-034e-6b27-5d271af109ba
2 name ( RO): pool-admin
3 description ( RO): The Pool Administrator role has full access to all
```



```
4 features and settings, including accessing Dom0 and managing subjects,
5 roles and external authentication
6
7 uuid ( RO): b9ce9791-0604-50cd-0649-09b3284c7dfd
8 name ( RO): pool-operator
9 description ( RO): The Pool Operator role manages host- and pool-wide
   resources,
10 including setting up storage, creating resource pools and managing
   patches, and
11 high availability (HA).
12
13 uuid( RO): 7955168d-7bec-10ed-105f-c6a7e6e63249
14 name ( RO): vm-power-admin
15 description ( RO): The VM Power Administrator role has full access to
   VM and
16 template management and can choose where to start VMs and use the
   dynamic memory
17 control and VM snapshot features
18
19 uuid ( RO): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
20 name ( RO): vm-admin
21 description ( RO): The VM Administrator role can manage VMs and
   templates
22
23 uuid ( RO): fb8d4ff9-310c-a959-0613-54101535d3d5
24 name ( RO): vm-operator
25 description ( RO): The VM Operator role can use VMs and interact with
   VM consoles
26
27 uuid ( RO): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
28 name ( RO): read-only
29 description ( RO): The Read-Only role can log in with basic read-only
   access
```

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:

```
1 xe subject-list
```

This command returns a list of XenServer users, their uuid, and the roles they are associated with:

```
1  uuid ( R0): bb6dd239-1fa9-a06b-a497-3be28b8dca44
2  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2244
3  other-config (MRO): subject-name: example01\user_vm_admin; subject-upn:
   \
4  user_vm_admin@XENDT.NET; subject-uid: 1823475908; subject-gid:
   1823474177; \
5  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2244; subject-
   gecos: \
6  user_vm_admin; subject-displayname: user_vm_admin; subject-is-group:
   false; \
7  subject-account-disabled: false; subject-account-expired: false; \
8  subject-account-locked: false; subject-password-expired: false
9  roles (SR0): vm-admin
10
11  uuid ( R0): 4fe89a50-6a1a-d9dd-afb9-b554cd00c01a
12  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2245
13  other-config (MRO): subject-name: example02\user_vm_op; subject-upn: \
14  user_vm_op@XENDT.NET; subject-uid: 1823475909; subject-gid:
   1823474177; \
15  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2245; \
16  subject-gecos: user_vm_op; subject-displayname: user_vm_op; \
17  subject-is-group: false; subject-account-disabled: false; \
18  subject-account-expired: false; subject-account-locked: \
19  false; subject-password-expired: false
20  roles (SR0): vm-operator
21
22  uuid ( R0): 8a63fbf0-9ef4-4fef-b4a5-b42984c27267
23  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2242
24  other-config (MRO): subject-name: example03\user_pool_op; \
25  subject-upn: user_pool_op@XENDT.NET; subject-uid: 1823475906; \
26  subject-gid: 1823474177; subject-s id:
27  S-1-5-21-1539997073-1618981536-2562117463-2242; \
28  subject-gecos: user_pool_op; subject-displayname: user_pool_op; \
29  subject-is-group: false; subject-account-disabled: false; \
30  subject-account-expired: false; subject-account-locked: \
31  false; subject-password-expired: false
32  roles (SR0): pool-operator
```

To add a subject to RBAC

To enable existing AD users to use RBAC, create a subject instance within XenServer, either for the AD user directly, or for the containing groups:

Run the following command to add a new subject instance:

```
1 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:

```
1 xe subject-role-add uuid=subject uuid role-uuid=role_uuid
```

Or

```
1 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:

```
1 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:

```
1 xe subject-role-remove uuid=subject uuid role-name= \  
2 role_name_to_remove  
3 xe subject-role-add uuid=subject uuid role-name= \  
4 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).

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.

```
1 xe audit-log-get \[since=timestamp\] filename=output filename
```

To obtain all audit records from the pool

Run the following command:

```
1 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:

```
1 xe audit-log-get since=2009-09-24T17:56:20.530Z \  
2 filename=/tmp/auditlog-pool-actions.out
```

To obtain audit records of the pool since a precise minute timestamp

Run the following command:

```
1 xe audit-log-get since=2009-09-24T17:56Z \  
2 filename=/tmp/auditlog-pool-actions.out
```

Configure networking

October 8, 2018

This section provides an overview of XenServer 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 XenServer. Follow the instructions in vSwitch networks to configure the Linux network stack.

If you are already familiar with XenServer networking concepts, you can skip ahead to [Manage networking](#) for information about the following sections:

- Create networks for standalone XenServer hosts
- Create private networks across XenServer hosts
- Create networks for XenServer hosts that are configured in a resource pool
- Create VLANs for XenServer hosts, either standalone or part of a resource pool
- Create bonds for standalone XenServer hosts
- Create bonds for XenServer hosts 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

XenServer 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:

XenServer 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

When used with a controller appliance, vSwitch networks support open flow and provide extra functionality such as Access Control Lists (ACL). The controller appliance for the XenServer vSwitch is called the vSwitch Controller. The vSwitch Controller lets you monitor your networks through a GUI. The vSwitch Controller:

- 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. For more information, see [vSwitch and Controller](#).

To determine what networking stack is configured, run the following command:

```
1 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:

```
1 network_backend: openvswitch
```

When the Linux bridge is configured as the network stack, the output appears as follows:

```
1 network_backend: bridge
```

To revert to the Linux network stack, run the following command:

```
1 xe-switch-network-backend bridge
```

Restart your host after running this command.

Warning:

The Linux network stack is not open-flow enabled, does not support Cross Server Private Networks. The XenServer vSwitch Controller does not manage the Linux network stack.

XenServer networking overview

This section describes the general concepts of networking in the XenServer environment.

XenServer 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 XenServer:

- **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.
- **Cross-Server Private networks** extend the single server private network concept to allow VMs on different hosts to communicate with each other by using the vSwitch.

Note:

Some networking options have different behaviors when used with standalone XenServer hosts 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 XenServer host 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 XenServer host, 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. XenServer hosts 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 XenServer VLAN features to connect guest virtual network interfaces (VIFs) to specific VLANs. In this case, the XenServer host performs the VLAN tagging/untagging functions for the guest, which is unaware of any VLAN configuration.

XenServer VLANs are represented by additional PIF objects representing VLAN interfaces corresponding to a specified VLAN tag. You can connect XenServer 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 XenServer hosts, either standalone or part of a resource pool, see [Creating VLANs](#).

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 XenServer 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:

XenServer 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

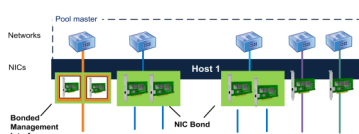
NIC bonds, sometimes also known as NIC teaming, improve XenServer host resiliency and bandwidth by enabling administrators to configure two or more NICs together. NIC bonds logically function as one network card and all bonded NICs share MAC address.

If one NIC in the bond fails, the host's network traffic is automatically redirected through the second NIC. XenServer supports up to eight bonded networks.

XenServer 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. XenServer 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. XenServer supports bonding the following types of NICs together:

- **NICs (non-management).** You can bond NICs that XenServer 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, Citrix recommends configuring multipathing instead of NIC bonding as described in the Designing XenServer 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 XenServer, An additional PIF represents a NIC bond. XenServer NIC bonds completely subsume the underlying physical devices (PIFs).

Notes:

- Creating a bond that contains only one NIC is not supported.
- 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. XenServer 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

XenServer 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

XenServer 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:

```
1 xe bond-param-get uuid=bond_uuid param-name=links-up
```

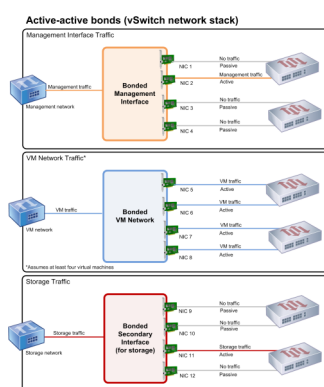
XenServer checks the status of links in bonds approximately every five seconds. Therefore, if more links in the bond fail in the five-second window, the failure is not logged until the next status check.

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.



XenServer can only send traffic over two or more NICs when there is more than one MAC address associated with the bond. XenServer 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. XenServer balances the control domain's traffic the same way as it balances VM traffic.

Traffic balancing

XenServer 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.

XenServer 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, XenServer 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 XenServer 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 XenServer 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 slave (interface) is tracked over a given period. If a packet to be sent contains a new source MAC address, it is assigned to the slave interface with the lowest utilization. Traffic is rebalanced at regular intervals.

Each MAC address has a corresponding load and XenServer 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:

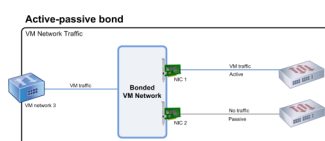
Active-active bonding does not require switch support for EtherChannel or 802.3ad (LACP).

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 XenServer. 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

XenServer 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:

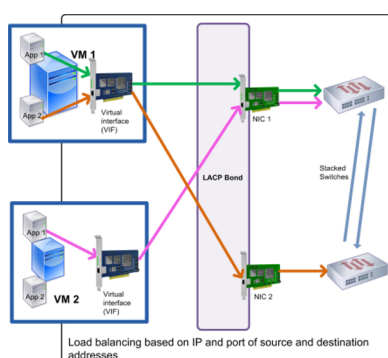
You configure settings for outgoing and incoming traffic separately on the host and the switch: the configuration does not have to match on both sides.

Load balancing based on IP and port of source and destination addresses.

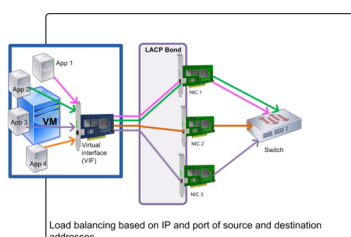
This hashing type is the default LACP bonding hashing algorithm. If there is a variation in the source or destination IP or port numbers, traffic from one guest can be distributed over two links.

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.



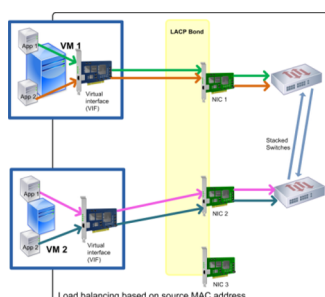
Configuring LACP bonding based on IP and port of source and destination address is beneficial when you want to balance the traffic of two different applications on the same VM. For example, when only one virtual machine is configured to use a bond of three NICs.



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. XenServer 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.

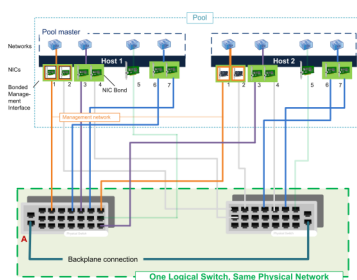
Use stacked switches when you want to connect bonded NICs to multiple switches and you configured the LACP bonding mode. The term 'stacked switches' is used to describe configuring multiple

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.

- XenServer 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 XenServer host 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 following 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 XenServer 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 XenServer host 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 XenServer 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:

```
1 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:

```
1 xe pif-unplug uuid=<uuid of bond master PIF>
2
3 xe pif-plug uuid=<uuid of bond master PIF>
```

Manage networking

October 4, 2018

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.

Cross-server private networks

Previous versions of XenServer allowed you to create single-server private networks that allowed VMs running on the same host to communicate with each other. The *cross-server private network* feature, which extends the single-server private network concept to allow VMs on different hosts to communicate with each other. Cross-server private networks combine the same isolation properties of a single-server private network but with the additional ability to span hosts across a resource pool. This combination enables use of VM agility features such as XenMotion live migration for VMs with connections to cross-server private networks.

Cross-server private networks are isolated. VMs that are not connected to the private network cannot sniff or inject traffic to the network. This happens even when they are on the same physical host with VIFs connected to a network on the same underlying physical network device (PIF). VLANs provide a similar functionality. However, unlike VLANs, cross-server private networks provide isolation without requiring configuration of a physical switch fabric, by using the Generic Routing Encapsulation (GRE) IP tunneling protocol.

Private networks provide the following benefits without requiring a physical switch:

- The isolation properties of single-server private networks
- The ability to span a resource pool, enabling VMs connected to a private network to live on multiple hosts within the same pool
- Compatibility with features such as XenMotion

Create Cross-Server Private Networks on a management interface or a secondary interface, as they require an IP addressable NIC. You can use any IP-enabled NIC as the underlying network transport. If you select to put cross-server private network traffic on a secondary interface, this secondary interface **must** be on a separate subnet.

If any management or secondary interfaces are on the same subnet, traffic is routed incorrectly.

Notes:

To create a cross-server private network, the following conditions must be met:

- All of the hosts in the pool must be using XenServer 6.0 or greater.
- All of the hosts in the pool must be using the vSwitch for the networking stack.
- The vSwitch Controller must be running and you must have added the pool to it. (The pool must have a vSwitch Controller configured that handles the initialization and configuration tasks required for the vSwitch connection.)
- You must create the cross-server private network on a NIC configured as a management interface. This can be the management interface or a secondary interface (IP-enabled PIF) you configure specifically for this purpose, provided it is on a separate subnet.

For more information on configuring the vSwitch, see [vSwitch and Controller](#). For UI-based procedures for configuring private networks, see the XenCenter Help.

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 the XenCenter Help.

Open the XenServer host text console.

Create the network by using the `network-create` command, which returns the UUID of the newly created network:

```
1 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 XenServer hosts 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 XenServer hosts in a pool. PIFs on the individual hosts are connected to

pool-wide networks based on device name. For example, all XenServer hosts 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 XenServer host in the pool.

If one XenServer host 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 XenServer host console.

Create a network for use with the VLAN. The UUID of the new network is returned:

```
1 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:

```
1 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.

```
1 xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
```

Attach VM VIFs to the new network. See [Creating networks in a standalone server](#) for details.

Create NIC bonds on a standalone host

Citrix recommends using XenCenter to create NIC bonds. For instructions, see the XenCenter Help.

This section describes how to use the xe CLI to bond NIC interfaces on XenServer hosts that are not in a pool. For information on using the xe CLI to create NIC bonds on XenServer hosts 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. From XenServer 6.0 onwards, the management interface is automatically moved to the bond PIF.

Use the `network-create` command to create a network for use with the bonded NIC. The UUID of the new network is returned:

```
1 xe network-create name-label=bond0
```

Use the `pif-list` command to determine the UUIDs of the PIFs to use in the bond:

```
1 xe pif-list
```

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:

```
1 xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,/  
2 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`:

```
1 xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1, /  
2 pif_uuid_2,pif_uuid_3,pif_uuid_4 /  
3 mode=balance-slb | active-backup | lACP
```

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, XenServer 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 XenServer host to a non-bonded configuration, the `bond-destroy` command automatically configures the primary-slave 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 slave.

The term primary-slave refers to the PIF that the MAC and IP configuration was copied from when creating the bond. When bonding two NICs, the primary slave 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:

```
1 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, Citrix recommends using XenCenter to create NIC bonds. For more information, see the XenCenter Help.

This section describes using the xe CLI to create bonded NIC interfaces on XenServer hosts 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 heartbeating 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:

```
1 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:

```
1 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:

```
1 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 heartbeating 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 sec-

ondary interface. (The IP-enabled NIC XenServer 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:

```
1 xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
```

Set the PIF's disallow-unplug parameter to true:

```
1 xe pif-param-set disallow-unplug=true uuid=pif-uuid
2
3 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 XenServer 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 XenServer 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. See the XenCenter Help for details.

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. Any VM network traffic sent through an SR-IOV VF bypasses the vSwitch. Therefore, it is not possible to create ACLs or view Quality of Service (QoS).
- 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:

```
1  ## 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:

```
1  ## VFs-param: max_vfs
2  ## VFs-maxvfs-by-default: 7
3  ## VFs-maxvfs-by-user: 4
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, Citrix recommends 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 on the vSwitch Controller, or in XenServer (using the CLI or XenCenter).

vSwitch

Configuration methods:

- **vSwitch Controller** This is the preferred method of setting the maximum transmission rate on a VIF when the vSwitch is the networking stack. When using the vSwitch stack, the XenCenter Quality of Service option is not available.
- **xe commands** It is possible to set the Quality of Service transmit rate using the commands in the example that follows. However, the preferred method is through the vSwitch Controller UI, which provides more finely grained control.

Linux bridge

Configuration Methods Available:

- **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.

Important:

When vSwitch is configured as the networking stack, it is possible to configure a QoS value inadvertently on the vSwitch Controller *and* inside the XenServer host. In this case, XenServer limits

the outgoing traffic using the lowest rate that you set.

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:

```
1 xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
2 xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
```

Note:

If you are using the vSwitch Controller, Citrix recommends setting the transmission rate limit in the vSwitch Controller instead of this CLI command. For directions on setting the QoS rate limit in the vSwitch Controller, see [vSwitch and Controller](#).

Change networking configuration options

This section discusses how to change the networking configuration of your XenServer host. 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:

```
1 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 XenServer host, use the `pif-reconfigure-ip` command. For example, for a PIF with a static IP:

```
1 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

XenServer hosts 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 `pbid-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. :

```
1 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 XenServer hosts in the pool are visible:

```
1 xe host-list
```

Changing the IP address of the master XenServer host 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:

```
1 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:

```
1 xe pool-recover-slaves
```

Management interface

When XenServer 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.

```
1 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.

```
1 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*:

```
1 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.

```
1 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.

```
1 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.

```
1 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 XenServer host in the usual manner. Then, after restarting the server, run the `xe` CLI command `pif-scan` to cause a new PIF object to be created for the new NIC.

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:

```
1 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:

```
1 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 [XenServer Changed Block Tracking Guide](#).

Use switch port locking

The XenServer 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 XenServer administrator has specified it can use
- Intercepting, spoofing, or disrupting the traffic of other VMs

Requirements

- The XenServer 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 XenServer 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 the vSwitch controller and other 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 XenServer 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

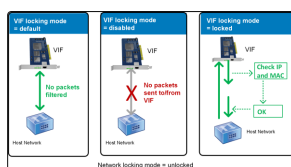
The switch-port locking feature lets you control packet filtering at one or more of two levels:

- **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 XenServer 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 XenServer 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`, XenServer 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`, XenServer applies a filtering rule so that the VIF drops all traffic.

-`default-locking-mode=unlocked`, XenServer 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.** XenServer 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.

XenServer lets you type IPv6 addresses when the Linux bridge is active. However, XenServer 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, XenServer lets all IPv6 traffic pass through the VIF. If you do not specify any IPv6 addresses, XenServer 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, XenServer 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:

```
1 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:

```
1 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:

```
1 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:

```
1 xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list  
  of ipv4-addresses
```

- Specify the IPv6 IP address. For example:

```
1 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:

```
1 xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated  
  list of ipv4-addresses
```

- Specify the IPv6 IP address to delete. For example:

```
1 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 XenServer 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:

```
1 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, XenServer 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:

```
1 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 XenServer network to determine how packets are filtered, as described in the previous section *How switch-port locking works*.

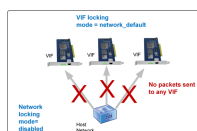
Specifically, a network's `default-locking-mode` setting determines how new VIFs with default settings behave. Whenever a VIF's `locking-mode` is set to `default`, the VIF refers to the network-locking mode (`default-locking-mode`) to determine if and how to filter packets traveling through the VIF:

- **Unlocked.** When the network `default-locking-mode` parameter is set to `unlocked`, XenServer 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`, XenServer 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:

```
1 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:

```
1 xe network-param-get uuid=network-uuid param-name=default-locking-mode
```

OR

```
1 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 XenServer 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:

```
1 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:

```
1 xe network-param-set uuid=network-uuid default-locking-mode=unlocked
```

Troubleshoot networking

August 13, 2018

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:

```
1 xe pif-list device=eth0
```

Next, set the following parameter on the PIF to disable TX offload:

```
1 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, XenServer host 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 XenMotion.

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, Citrix advises customers to 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
<code>-m, --master</code>	Optional	IP address of the Pool Master's management interface. Defaults to the last known Pool Master's IP address.
<code>--device</code>	Optional	Device name of the management interface. Defaults to the device name specified during installation.

Parameter	Required/Optional	Description
<code>-mode=static</code>	Optional	Enables the following four networking parameters for static IP configuration for the management interface. If not specified, networking is configured using DHCP.
<code>-ip</code>	Required, if mode=static	IP address for the host's management interface. Only valid if mode=static.
<code>-netmask</code>	Required, if mode=static	Netmask for the management interface. Only valid if mode=static.
<code>-gateway</code>	Optional	Gateway for the management interface. Only valid if mode=static.
<code>-dns</code>	Optional	DNS Server for the management interface. Only valid if mode=static.
<code>-vlan</code>	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:

```
1 xe-reset-networking
```

To reset networking for Static IP configuration:

```
1 xe-reset-networking --mode= static --ip=ip-address \
2   --netmask=netmask --gateway=gateway \
3   --dns=dns
```

To reset networking for DHCP configuration if another interface became the management interface

after initial setup:

```
1 xe-reset-networking --device=device-name
```

To reset networking for Static IP configuration if another interface became the management interface after initial setup:

```
1 xe-reset-networking --device=device-name --mode=static \  
2   --ip=ip-address --netmask=netmask \  
3   --gateway=gateway --dns=dns
```

To reset networking for management interface on VLAN:

```
1 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:

```
1 xe-reset-networking
```

To reset networking for DHCP if the Pool Master's IP address was changed:

```
1 xe-reset-networking --master=master-ip-address
```

To reset networking for Static IP configuration, assuming the Pool Master's IP address didn't change:

```
1 xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \  
2   --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:

```
1 xe-reset-networking --device=device-name --master=master-ip-address
```

Configure storage

February 26, 2019

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:

- IDE
- SATA
- SCSI
- SAS

Remotely connected:

- iSCSI
- NFS
- SAS
- Fibre Channel

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.

SR commands provide operations for creating, destroying, resizing, cloning, connecting and discovering the individual VDIs that they contain.

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 XenServer host 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. All servers in a single resource pool must have at least one shared SR in common.

CLI operations to manage storage repositories are described in [SR commands](#).

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 XenServer. VDIs are persistent, on-disk objects that exist independently of XenServer hosts. 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)

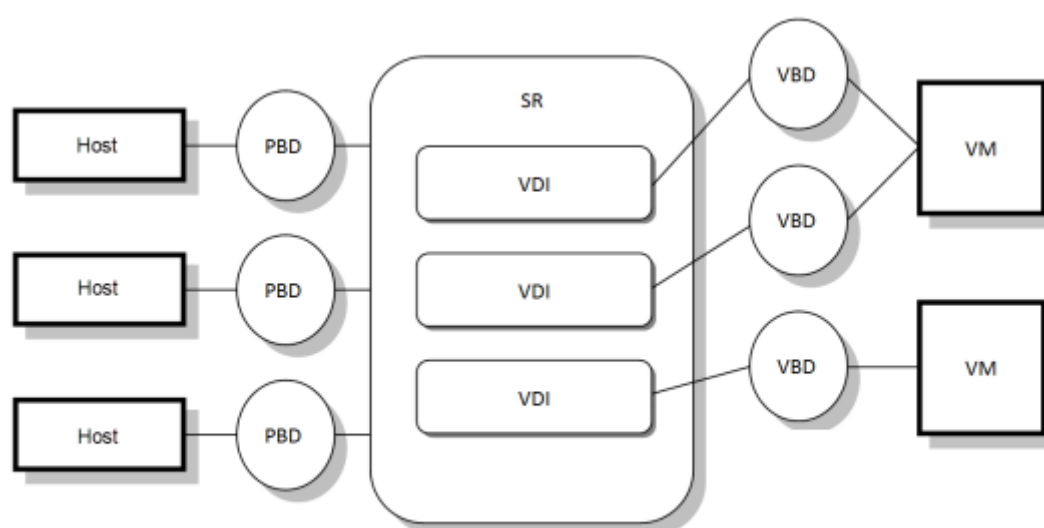
Physical block devices represent the interface between a physical server and an attached SR. PBDs are connector objects that allow a given SR to be mapped to a host. PBDs store the device configuration fields that are used to connect to and interact with a given storage target. For example, NFS device configuration includes the IP address of the NFS server and the associated path that the XenServer host mounts. PBD objects manage the run-time attachment of a given SR to a given XenServer host. 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 XenServer 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 (EXT type SR) or a shared NFS target (NFS type SR).

VDI types

For most 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. For GFS2 SRs, QCOW2 VDIs are created.

To check if a VDI was created with `type=raw`, check its `sm-config` map. The `sr-param-list` and `vd-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:

```
1 xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size  
  \  
2   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, XenServer 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. XenServer 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

March 29, 2019

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 XenServer 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 XenServer 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, NFS, GFS2) support full thin provisioning, including for virtual disks that are active.

Warning:

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.

The maximum supported VDI sizes are:

Storage Repository Format	Maximum VDI size
EXT3	2 TiB
LVM	2 TiB
NFS	2 TiB
LVMoFCOE	2 TiB
LVMoiSCSI	2 TiB
LVMoHBA	2 TiB
GFS2 (with iSCSI or HBA)	2 TiB

Local LVM

The Local LVM type presents disks within a locally attached Volume Group.

By default, XenServer 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.

LVM performance considerations

The snapshot and fast clone functionality for LVM-based SRs comes with an inherent performance overhead. When optimal performance is required, XenServer supports creation of VDIs in the *raw*

format in addition to the default VHD format. The XenServer snapshot functionality is not supported on raw VDIs.

Non-transportable snapshots that use the default Windows VSS provider work on any type of VDI.

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.

```
1 xe sr-create host-uuid=valid_uuid content-type=user \  
2 name-label="Example Local LVM SR" shared=false \  
3 device-config:device=/dev/sdb type=lvm
```

Local EXT3

Using EXT3 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, 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 EXT SRs must be configured using the XenServer CLI.

Creating a local EXT3 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 ext SR on `/dev/sdb`, use the following command:

```
1 xe sr-create host-uuid=valid_uuid content-type=user \
2   name-label="Example Local EXT3 SR" shared=false \
3   device-config:device=/dev/sdb type=ext
```

udev

The `udev` type represents devices plugged in using the `udev` device manager as VDIs.

XenServer 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 XenServer host. The other is for a USB device plugged into a USB port of the XenServer host. 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:

```
1 xe sr-create host-uuid=valid_uuid content-type=iso \
2   type=iso name-label="Example ISO SR" \
3   device-config:location=nfs server:path
```

Citrix recommends that you use SMB version 3.0 to mount ISO SR on Windows file server. Version 3.0 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 1.0 using the following command:

```
1 xe sr-create content-type=iso type=iso shared=true device-config:
   location=valid location
2 device-config:username=username device-config:cifspassword=password
3 device-config:type=cifs device-config:vers=Choose either 1.0 or 3.0
   name-label="Example ISO SR"
```


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

XenServer 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 XenMotion: VMs can be started on any XenServer host 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.

XenServer host 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.

XenServer hosts 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 XenServer host 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 XenServer host IQN value can be adjusted using XenCenter, or using the CLI with the following command when using the iSCSI software initiator:

```
1 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 XenServer host 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?
<code>SCSIid</code>	The SCSI bus ID of the destination LUN	Yes

Run the following command to create a shared FCoE SR:

```
1 xe sr-create type=lvmofoe \
2 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 XenServer host, 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.

```
1 /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
```

2. Add a persistent iSCSI target to port 0 of the HBA.

```
1 /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. Citrix recommends 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 XenServer host 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:

```
1 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.

Create a shared LVM over iSCSI SR by using the Software iSCSI initiator

Device-config parameters for LVMoiSCSI SRs:

Parameter Name	Description	Required?
<code>target</code>	The IP address or hostname of the iSCSI filer that hosts the SR	Yes
<code>targetIQN</code>	The IQN target address of iSCSI filer that hosts the SR	Yes
<code>SCSIid</code>	The SCSI bus ID of the destination LUN	Yes

Parameter Name	Description	Required?
<code>chapuser</code>	The user name to be used for CHAP authentication	No
<code>chappassword</code>	The password to be used for CHAP authentication	No
<code>port</code>	The network port number on which to query the target	No
<code>usediscoverynumber</code>	The specific iSCSI record index to use	No
<code>incoming_chapuser</code>	The user name that the iSCSI filter uses to authenticate against the host	No
<code>incoming_chappassword</code>	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.

```
1 xe sr-create host-uuid=valid_uuid content-type=user \
2 name-label="Example shared LVM over iSCSI SR" shared=true \
3 device-config:target=target_ip= device-config:targetIQN=target_iqn= \
4 device-config:SCSIid=scsi_id \
5 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?
<code>SCSIid</code>	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 XenServer host 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 XenServer host 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.

```
1  xe sr-probe type=lvmohba \  
2  host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31  
3  Error code: SR_BACKEND_FAILURE_90  
4  Error parameters: , The request is missing the device parameter, \  
5  <?xml version="1.0" ?>  
6  <Devlist>  
7      <BlockDevice>  
8          <path>  
9              /dev/disk/by-id/scsi-360a9800068666949673446387665336f  
10         </path>  
11         <vendor>  
12             HITACHI  
13         </vendor>  
14         <serial>  
15             730157980002  
16         </serial>  
17         <size>  
18             80530636800  
19         </size>  
20         <adapter>  
21             4  
22         </adapter>  
23         <channel>
```

```

24         0
25     </channel>
26     <id>
27         4
28     </id>
29     <lun>
30         2
31     </lun>
32     <hba>
33         qla2xxx
34     </hba>
35 </BlockDevice>
36 <Adapter>
37     <host>
38         Host4
39     </host>
40     <name>
41         qla2xxx
42     </name>
43     <manufacturer>
44         QLogic HBA Driver
45     </manufacturer>
46     <id>
47         4
48     </id>
49 </Adapter>
50 </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.

```

1 xe sr-create host-uuid=valid_uuid \
2   content-type=user \
3   name-label="Example shared LVM over HBA SR" shared=true \
4   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

Thin provisioning better utilizes the available storage by allocating disk storage space to VDI as 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).

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

- If you want increased space efficiency, as 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, as the images of individual VMs will then typically utilize even less space.
- If you use snapshots, as each snapshot is an image and each image is now sparse.

The shared GFS2 type represents disks as in a filesystem created on an iSCSI or HBA LUN. To use shared GFS2 storage, the XenServer resource pool must be a clustered pool. Enable clustering on your pool before creating a GFS2 SR. For more information, see [Clustered pools](#).

SRs of type GFS2 can be created and managed using the xe CLI or XenCenter.

VDIs stored on a GFS2 SR are stored in the QCOW2 image format.

Note:

Shared GFS2 storage currently has the following constraints:

- You cannot resize the backing LUN.
- VM migration with storage XenMotion is not supported for VMs whose VDIs are on a GFS2 SR.
- The FCoE protocol is not supported with GFS2 SRs.
- Trim/unmap is not supported on GFS2 SRs.
- Performance metrics are not available for GFS2 SRs and disks on these SRs.
- Changed block tracking is not supported for VDIs stored on GFS2 SRs.

Create a shared GFS2 over iSCSI SR by using the Software iSCSI initiator

Device-config parameters for GFS2 SRs:

Parameter Name	Description	Required?
<code>provider</code>	The block provider implementation. In this case, <code>iscsi</code> .	Yes
<code>target</code>	The IP address or hostname of the iSCSI filer that hosts	Yes
<code>targetIQN</code>	The IQN target of iSCSI filer that hosts the SR	Yes
<code>SCSIid</code>	Device SCSI ID	Yes

To create a shared GFS2 SR on a specific LUN of an iSCSI target, run the following command on a host in your clustered pool:

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
2 device-config:provider=iscsi device-config:targetIQN=target_iqns \
3 device-config:target=portal_address device-config:SCSIid=scsci_id
```

If the iSCSI target is not reachable while GFS2 filesystems are mounted, some hosts in the clustered pool might fence.

Create a shared GFS2 over HBA SR

Device-config parameters for GFS2 SRs:

Parameter name	Description	Required?
<code>provider</code>	The block provider implementation. In this case, <code>hba</code> .	Yes
<code>SCSIid</code>	Device SCSI ID	Yes

To create a shared GFS2 SR on a specific LUN of an HBA target, run the following command on a host in your clustered pool:

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
2 device-config:provider=hba device-config:SCSIid=device_scsi_id
```

NFS and SMB

Shares on NFS servers (that support NFSv4 or NFSv3) or on SMB servers (that support SMB 3.0) can be used immediately as an SR for virtual disks. VDI's are stored in the Microsoft VHD format only. Additionally, as these SRs can be shared, VDI's stored on shared SRs allow:

- VMs to be started on any XenServer hosts in a resource pool
- VM migrate between XenServer hosts in a resource pool using XenMotion (without noticeable downtime)

Important:

- Support for SMB 3.0 is limited to the ability to connect to a share using the 3.0 protocol. Extra features like Transparent Failover depend on feature availability in the upstream Linux kernel and are not supported in XenServer 7.6.
- For NFSv4, only the authentication type `AUTH_SYS` is supported.
- SMB storage is available for XenServer Enterprise Edition customers, or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement.

VDI's 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 VDI's 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 XenServer 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 VDI's.

XenServer 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. XenServer 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. XenServer hosts do not enforce that the space required for VDIs on file-based SRs is present.

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 XenServer 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 XenServer 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?
<code>server</code>	IP address or hostname of the NFS server	Yes
<code>serverpath</code>	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:

```
1 xe sr-create content-type=user \
2 name-label="shared NFS SR" shared=true \
3 device-config:server=192.168.1.10 device-config:serverpath=/export1
  type=nfs \
```

```
4 nfsversion="3", "4"
```

To create a non-shared NFS SR, run the following command:

```
1 xe sr-create host-uuid=host_uuid content-type=user \
2 name-label="Non-shared NFS SR" \
3 device-config:server=192.168.1.10 device-config:serverpath=/export1
  type=nfs \
4 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.

Note:

SMB SR has been tested against Network Appliance storage running OnTap 8.3 and Windows Server 2012 R2.

Device-config parameters for SMB SRs:

Parameter Name	Description	Required?
<code>server</code>	Full path to share on server	Yes
<code>username</code>	User account with RW access to share	Optional
<code>password</code>	Password for the user account	Optional

For example, to create a shared SMB SR on 192.168.1.10:/share1, use the following command:

```
1 xe sr-create content-type=user \
2 name-label="Example shared SMB SR" shared=true \
3 device-config:server=//192.168.1.10/share1 \
4 device-config:username=valid_username device-config:password=
  valid_password type=smb
```

To create a non-shared SMB SR, run the following command:

```
1 xe sr-create host-uuid=host_uuid content-type=user \
2 name-label="Non-shared SMB SR" \
3 device-config:server=//192.168.1.10/share1 \
```

```
4 device-config:username=valid_username device-config:password=
  valid_password type=smb
```

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.

XenServer hosts 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 XenServer host. 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:

XenServer 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.

Manage storage repositories

October 11, 2018

This section covers creating storage repository types and making them available to your XenServer host. 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 XenServer host. 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 help.

Note:

Local SRs of type `lvm` and `ext3` 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 XenServer host 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:

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10
2
3 Error code: SR_BACKEND_FAILURE_96
4 Error parameters: , The request is missing or has an incorrect target
   IQN parameter, \
5 <?xml version="1.0" ?>
```

```
6 <iscsi-target-iqn>
7   <TGT>
8     <Index>
9       0
10    </Index>
11    <IPAddress>
12      192.168.1.10
13    </IPAddress>
14    <TargetIQN>
15      iqn.192.168.1.10:filer1
16    </TargetIQN>
17  </TGT>
18 </iscsi-target-iqn>
```

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.

```

1  xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
2  device-config:targetIQN=iqn.192.168.1.10:filer1
3
4  Error code: SR_BACKEND_FAILURE_107
5  Error parameters: , The SCSIId parameter is missing or incorrect, \
6  <?xml version="1.0" ?>
7  <iscsi-target>
8      <LUN>
9          <vendor>
10             IET
11          </vendor>
12          <LUNid>
13             0
14          </LUNid>
15          <size>
16             42949672960
17          </size>
18          <SCSIid>
19             14945540000000000000000000000000000000000000b70200000f000000
20          </SCSIid>
21      </LUN>
22  </iscsi-target>

```

Probing the same target and supplying all three parameters returns a list of SRs that exist on the LUN, if any.

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
2 device-config:targetIQN=192.168.1.10:filer1 \
```

```
3 device-config:SCSIid=1494554000000000000000000000000020000000b70200000f000000
4
5 <?xml version="1.0" ?>
6 <SRlist>
7     <SR>
8         <UUID>
9             3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
10        </UUID>
11        <Devlist>
12            /dev/disk/by-id/scsi-1494554000000000000000000000000020000000
13                b70200000f000000
14        </Devlist>
15    </SR>
16</SRlist>
```

The following parameters can be probed for each SR type:

SR type	The <code>device-config</code> parameters, in order of dependency	Can be probed?	Required for <code>sr-create</code> ?
lvm <code>iscsi</code>	<code>target</code>	No	Yes
	<code>chapuser</code>	No	No
	<code>chappassword</code>	No	No
	<code>targetIQN</code>	Yes	Yes
	<code>SCSIid</code>	Yes	Yes
<code>lvmohba</code>	<code>SCSIid</code>	Yes	Yes
NetApp	<code>target</code>	No	Yes
	<code>username</code>	No	Yes
	<code>password</code>	No	Yes
	<code>chapuser</code>	No	No
	<code>chappassword</code>	No	No
	<code>aggregate</code>	No (see note 1)	Yes
	<code>FlexVols</code>	No	No
	<code>allocation</code>	No	No
	<code>asis</code>	No	No
<code>nfs</code>	<code>server</code>	No	Yes

SR type	The <code>device-config</code> parameters, in order of dependency	Can be probed?	Required for <code>sr-create</code> ?
	<code>serverpath</code>	Yes	Yes
<code>lvm</code>	<code>device</code>	No	Yes
<code>ext</code>	<code>device</code>	No	Yes
<code>EqualLogic</code>	<code>target</code>	No	Yes
	<code>username</code>	No	Yes
	<code>password</code>	No	Yes
	<code>chapuser</code>	No	No
	<code>chappassword</code>	No	No
	<code>storagepool</code>	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 XenServer host, 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 XenServer host:

```
1 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 XenServer host database and deletes the SR contents from the physical disk:

```
1 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 XenServer host database but leaves the actual SR content intact on the physical media:

```
1 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 XenServer hosts to activate the SR.

The following example introduces an SR of type `lvmoiscsi`.

1. Probe the existing SR to determine its UUID:

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \  
2 device-config:targetIQN=192.168.1.10:filer1 \  
3 device-config:SCSIid=1494554000000000000000000000000020000000  
   b70200000f000000
```

2. Introduce the existing SR UUID returned from the `sr-probe` command. The UUID of the new SR is returned:

```
1 xe sr-introduce content-type=user name-label="Example Shared LVM  
   over iSCSI SR"  
2 shared=true uuid=valid_sr_uuid type=lvmoiscsi
```

3. Create a PBD to accompany the SR. The UUID of the new PBD is returned:

```
1 xe pbd-create type=lvmoiscsi host-uuid=valid_uuid sr-uuid=  
   valid_sr_uuid \  
2 device-config:target=192.168.0.1 \  
3 device-config:targetIQN=192.168.1.10:filer1 \  
4 device-config:SCSIid=1494554000000000000000000000000020000000  
   b70200000f000000
```

4. Plug the PBD to attach the SR:

```
1 xe pbd-plug uuid=pbd_uuid
```

5. Verify the status of the PBD plug. If successful, the `currently-attached` property is true:

```
1 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 XenServer host. Live LUN Expansion allows you to increase the size of the LUN without any VM downtime.

After adding more capacity to your storage array, enter,

```
1 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**. For more information, press **F1** to display the XenCenter help.

Warnings:

- It is not possible to shrink or truncate LUNs. Reducing the LUN size on the storage array can lead to data loss.
- LUN resize is not supported for GFS2 SRs.

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.
- VDIs with more than one snapshot cannot be migrated.

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.

```
1 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.

```
1 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 XenServer 7.6.
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:

```
1 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. 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. Citrix recommends that you schedule this work outside of peak array demand hours.

Automatically reclaim space when deleting snapshots

When deleting snapshots with XenServer, 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 EXT 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 EXT 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:

```
1 xe host-call-plugin host-uuid=host-UUID \  
2   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:

```
1 xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea \  
   \
```

```
2 plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2  
c2d-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:

Citrix recommends 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 XenServer 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.

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:

```
1 xe sr-param-set other-config:scheduler=noop|cfq|anticipatory|deadline \  
2 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:

```
1 xe vbd-param-set uuid=vbd_uuid qos_algorithm_type=ionice
2 xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:sched=rt
3 xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:class=5
4 xe sr-param-set uuid=sr_uuid other-config:scheduler=cfq
5 xe pbd-plug uuid=pbd_uuid
```

Storage multipathing

August 15, 2018

Dynamic multipathing support is available for Fibre Channel and iSCSI storage back-ends. You can enable multipathing in XenCenter or on the xe CLI.

Important:

Before attempting to enable multipathing, verify that multiple targets are available on your storage server. For example, an iSCSI storage back-end queried for `sendtargets` on a given portal returns multiple targets, as in the following example:

```
1 iscsiadm -m discovery --type sendtargets --portal 192.168.0.161
2 192.168.0.161:3260,1 iqn.strawberry:litchie
3 192.168.0.204:3260,2 iqn.strawberry:litchie
```

Unplug all PBDs on the host:

```
1 xe pbd-unplug uuid=pbd_uuid
```

Set the host's `other-config:multipathing` parameter:

```
1 xe host-param-set other-config:multipathing=true uuid=host_uuid
```

Set the host's `other-config:multipathhandle` parameter to `dmp`:

```
1 xe host-param-set other-config:multipathhandle=dmp uuid=host_uuid
```

If there are existing SRs on the host running in single path mode but that have multiple paths:

- Migrate or suspend any running guests with virtual disks in affected the SRs
- Unplug and replug the PBD of any affected SRs to reconnect them using multipathing:

```
1 xe pbd-plug uuid=pbd_uuid
```

To disable multipathing, first unplug your VBDs, 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 XenServer 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 XenServer. 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:

```
1 mpathutil list
```

```
2
3  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 XenServer. 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.

IntelliCache

September 5, 2018

Note:

This feature is only supported when using XenServer with Citrix Virtual Desktops.

Intellicache is not supported for VMs using a GFS2 SR.

Using XenServer with *IntelliCache* makes hosted Virtual Desktop Infrastructure deployments more cost-effective by enabling you to use a combination of shared storage and local storage. It is of particular benefit when many Virtual Machines (VMs) all share a common OS image. The load on the storage array is reduced and performance is enhanced. In addition, network traffic to and from shared storage is reduced as the local storage caches the master image from shared storage.

IntelliCache works by caching data from a VMs parent VDI in local storage on the VM host. This local cache is then populated as data is read from the parent VDI. When many VMs share a common parent VDI, a VM can use the data read into the cache from another VM. Further access to the master image on shared storage is not required.

A thin provisioned, local SR is required for IntelliCache. Thin provisioning is a way of optimizing the use of available storage. This approach allows you to make more use of local storage instead of shared storage. It relies on on-demand allocation of blocks of data. In other approaches, all blocks are allocated up front.

Important:

Thin Provisioning changes the default local storage type of the host from LVM to EXT3. Thin Provisioning **must be** enabled in order for Citrix Virtual Desktops local caching to work properly.

Thin Provisioning allows the administrator to present more storage space to the VMs connecting to the Storage Repository (SR) than is available on the SR. There are no space guarantees, and allocation of a LUN does not claim any data blocks until the VM writes data.

Warning:

Thin provisioned SRs may run out of physical space, as the VMs within can grow to consume disk capacity on demand. IntelliCache VMs handle this condition by automatically falling back to shared storage when the local SR cache is full. Do not mix traditional virtual machines and IntelliCache VMs on the same SR, as IntelliCache VMs can grow quickly in size.

IntelliCache deployment

IntelliCache must be enabled either during host installation or be enabled manually on a running host using the CLI.

Citrix recommends that you use a high performance local storage device to ensure the fastest possible data transfer. For example, use a Solid State Disk or a high performance RAID array. Consider both data throughput and storage capacity when sizing local disks. The shared storage type, used to host the source Virtual Disk Image (VDI), must be NFS or EXT based.

Enable on host installation

To enable IntelliCache during host installation, on the **Virtual Machine Storage** screen, select **Enable thin provisioning**. This option selects the host's local SR to be the one to be used for the local caching of VM VDIs.



Convert an existing host to use thin provisioning

To delete an existing LVM based local SR, and replace it with a thin provisioned EXT3 based SR, enter the following commands.

Warning:

These commands remove your existing local SR, and VMs on the SR are permanently deleted.

```
1 localsr='xe sr-list type=lvm host=hostname params=uuid --minimal'
2 echo localsr=$localsr
3 pbd='xe pbd-list sr-uuid=$localsr params=uuid --minimal'
4 echo pbd=$pbd
5 xe pbd-unplug uuid=$pbd
6 xe pbd-destroy uuid=$pbd
7 xe sr-forget uuid=$localsr
8 sed -i "s/'lvm'/'ext'/" /etc/firstboot.d/data/default-storage.conf
9 rm -f /etc/firstboot.d/state/10-prepare-storage
10 rm -f /etc/firstboot.d/state/15-set-default-storage
11 service firstboot start
12 xe sr-list type=ext
```

To enable local caching, enter the following commands:

```
1 xe host-disable host=hostname
2 localsr='xe sr-list type=ext host=hostname params=uuid --minimal'
3 xe host-enable-local-storage-caching host=hostname sr-uuid=$localsr
4 xe host-enable host=hostname
```

VM boot behavior

There are two options for the behavior of a VM VDI when the VM is booted:

1. Shared Desktop Mode

On VM boot, the VDI is reverted to the state it was in at the previous boot. All changes while the VM is running are lost when the VM is next booted.

Select this option if you plan to deliver standardized desktops to which users cannot make permanent changes.

2. Private Desktop Mode

On VM boot, the VDI is in the state it was left in at the last shutdown.

Select this option if you plan to allow users to make permanent changes to their desktops.

VM caching behavior settings

The VDI flag `allow-caching` dictates the caching behavior:

Shared desktop mode

For shared desktops, the `on-boot` option is `reset` and the `allow-caching` flag is `true`. New VM data is written only to local storage. There are no writes to shared storage. This approach means that the load on shared storage is reduced. However the VM cannot be migrated between hosts.

Private desktop mode

For private desktops, the `on-boot` option is set to `persist` and the `allow-caching` flag is set to `true`. New VM data is written to both local and shared storage. Reads of cached data do not require I/O traffic to shared storage so the load on shared storage is reduced. VM Migration to another host is permitted and the local cache on the new host is populated as data is read.

Implementation details and troubleshooting

Q: Is IntelliCache compatible with XenMotion and High Availability?

A: You can use XenMotion and High Availability with IntelliCache when virtual desktops are in Private mode, that is when `on-boot=persist`

Warning:

A VM cannot be migrated if any of its VDIs have caching behavior flags set to `on-boot=reset` and `allow-caching=true`. Migration attempts for VMs with these properties fail.

Q: Where does the local cache live on the local disk?

A: The cache lives in a Storage Repository (SR). Each host has a configuration parameter (called `local-cache-sr`) indicating which (local) SR is to be used for the cache files. Typically, this SR is an EXT type SR. When you run VMs with IntelliCache, you see files inside the SR with names `uuid.vhdcache`. This file is the cache file for the VDI with the given UUID. These files are not displayed in XenCenter – the only way of seeing them is by logging into dom0 and listing the contents of `/var/run/sr-mount/sr-uuid`

Q: How do I specify a particular SR for use as the cache?

A: The host object field `local-cache-sr` references a local SR. You can view its value by running the following command:

```
1 xe sr-list params=local-cache-sr,uuid,name-label
```

This field is set either:

- After host installation, if you have chosen “Enable thin provisioning” option in the host installer, or
- By executing `xe host-enable-local-storage-caching host=host sr-uuid=sr`. The command requires the specified host to be disabled. Shut down the VMs when you use this command.

The first option uses the EXT type local SR and is created during host installation. The second option uses the SR that is specified on the command-line.

Warning:

These steps are only necessary for users who have configured more than one local SR.

Q: When is the local cache deleted?

A: A VDI cache file is only deleted when the VDI itself is deleted. The cache is reset when a VDI is attached to a VM (for example on VM start). If the host is offline when you delete the VDI, the SR synchronization that runs on startup garbage collects the cache file.

Note:

The cache file is not deleted from the host when a VM migrates to a different host or is shut down.

Storage read caching

September 5, 2018

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 XenServer Enterprise Edition customers.

Storage Read Caching is also available for customers who access XenServer through their Citrix Virtual Desktops and Citrix Virtual Apps entitlement.

Enable and disable read caching

For file-based SRs, such as NFS and EXT3 SR types, read-caching is enabled by default. Read-caching is disabled for all other SRs.

To disable read caching for a specific SR, run the following command:

```
1 xe sr-param-set uuid=sr-uuid other-config:o_direct=true
```

Limitations

- Read caching is available only for NFS and EXT3 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 XenServer'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 XenServer host, open a local shell and log on as root.

To set the size of the read cache, run the following command:

```
1 /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 MB:

```
1 /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:

```
1 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 752 MB

	Total	Used	Free	Shared	Buffer	Cached
Mem	594	486	108	0	149	78
-/+ buffers/ cache		258	336			
Swap	511	49	462			

What Range of Values Can be Used?

As the XenServer Control Domain (dom0) is 64-bit, large values can be used, for example 32768 MB. Citrix recommends that you do not set the initial value to be lower than 752 MB, as it can cause the host to fail to boot.

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 XenServer 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.

PVS-Accelerator

February 6, 2019

The XenServer PVS-Accelerator feature offers extended capabilities for customers using XenServer with Citrix Provisioning. Citrix Provisioning is a popular choice for image management and hosting for Citrix Virtual Apps and Desktops. PVS-Accelerator dramatically improves the already excellent combination of XenServer and Citrix Provisioning. Some of the benefits that this new feature provides include:

- **Data locality:** Use the performance and locality of memory, SSD, and NVM devices for read requests, while substantially reducing network utilization.
- **Improved end-user experience:** Data locality enables a reduction in the read I/O latency for cached target devices (VMs), further accelerating end-user applications.
- **Accelerated VM boots and boot storms:** Reduced read I/O-latency and improved efficiency can accelerate VM boot times and enable faster performance when many devices boot up within a narrow time frame.

- **Simplified scale-out by adding more hypervisor hosts:** Fewer Citrix Provisioning servers may be needed as the storage load is efficiently dispersed across all XenServer hosts. Peak loads are handled using the cache within originating hosts.
- **Reduced TCO and simplified infrastructure requirements:** Fewer Citrix Provisioning servers means a reduction in hardware and license requirements, in addition to reduced management overhead. Freed up capacity is available for workloads.

Note:

PVS-Accelerator is available for XenServer Enterprise Edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To use the PVS-Accelerator feature, upgrade the License Server to version 11.14.

How does PVS-Accelerator work

PVS-Accelerator employs a Proxy mechanism that resides in the Control Domain (dom0) of XenServer. When this feature is enabled, Citrix Provisioning targets device (VM) read requests are cached directly on the XenServer host machine. These requests are cached in physical memory or a storage repository. When subsequent VMs on that XenServer host make the same read request, the virtual disk is streamed directly from cache, not from the Citrix Provisioning server. Removing the need to stream from the Citrix Provisioning server reduces network utilization and processing on the server considerably. This approach results in a substantial improvement in VM performance.

Enable PVS-Accelerator

Customers must complete the following configuration settings in XenServer and in Citrix Provisioning to enable the PVS-Accelerator feature:

1. Install the PVS-Accelerator Supplemental Pack on each XenServer host in the pool. The supplemental pack is available to download from the [XenServer Product Downloads](#) page. You can install the supplemental pack using XenCenter or the xe CLI. For information about installing a supplemental pack using XenCenter, see the XenCenter Help. For CLI instructions, see the [XenServer Supplemental Packs and the DDK Guide](#).
2. Configure PVS-Accelerator in XenServer by using XenCenter or the xe CLI. This configuration includes adding a Citrix Provisioning site and specifying the location for Citrix Provisioning cache storage.
 - For CLI instructions, see *Configuring PVS-Accelerator in XenServer by using the CLI* in the following section.
 - For information about configuring PVS-Accelerator using XenCenter, see the XenCenter Help.

3. After configuring PVS-Accelerator in XenServer, complete the cache configuration for the PVS Site using the PVS UI. For detailed instructions, see [Completing the cache configuration in Citrix Provisioning](#).

Configure PVS-Accelerator in XenServer by using the CLI

1. Run the following command to create a Citrix Provisioning site configuration on XenServer:

```
1 PVS_SITE_UUID=$(xe pvs-site-introduce name=label=My PVS Site)
```

2. For each host in the pool, specify what cache to use. You can choose to store the cache on a storage repository (SR) or in the Control Domain Memory.

Configure cache storage on a storage repository

Consider the following characteristics when choosing a storage repository (SR) for cache storage:

Advantages:

- Most recently read data is cached in the memory on a best effort basis. Accessing the data can be as fast as using the Control Domain memory.
- The cache can be much larger when it is on an SR. The cost of the SR space is typically a fraction of the cost of the memory space. Caching on an SR can take more load off the Citrix Provisioning server.
- You don't have to modify the Control Domain memory setting. The cache automatically uses the memory available in the Control Domain and never causes the Control Domain to run out of memory.

Disadvantages:

- If the SR is slow and the requested data isn't in the memory tier, the caching process can be slower than a remote Citrix Provisioning server.

Perform the following steps to configure cache storage on a Storage Repository:

1. Run the following command to find the UUID of the SR that to use for caching:

```
1 xe sr-list name=label=Local storage host=host-name-label --  
minimal)
```

2. Create the cache-storage.

```
1 xe pvs-cache-storage-create host=host-name-label pvs-site-uuid  
=PVS_SITE_UUID  
2 sr-uuid=SR_UUID size=10GiB
```

Note:

When selecting a Storage Repository (SR), the feature uses up to the specified cache size on the SR. It also implicitly uses available Control Domain memory as a best effort cache tier.

Configuring cache storage in the control domain memory

Consider the following characteristics when choosing the Control Domain memory for cache storage:

Advantages:

Using memory means consistently fast Read/Write performance when accessing or populating the cache.

Disadvantages:

- Hardware must be sized appropriately as the RAM used for cache storage is not available for VMs.
- Control Domain memory must be extended **before** configuring cache storage.

Note:

If you choose to store the cache in the Control Domain memory, the feature uses up to the specified cache size in Control Domain memory. This option is only available after extra memory has been assigned to the Control Domain. For information about increasing the Control Domain memory, see [Change the amount of memory allocated to the control domain](#).

After you increase the amount of memory allocated to the Control Domain of the host, the additional memory can be explicitly assigned for PVS-Accelerator.

Perform the following steps to configure cache storage in the Control Domain memory:

1. Run the following command to find the UUID of the host to configure for caching:

```
1 xe host-list name-label=host-name-label --minimal
```

2. Create an SR of the special type `tmpfs`:

```
1 xe sr-create type=tmpfs name-label=MemorySR host-uuid=
  HOST_UUID device-config:uri=""
```

3. Run the following command to create the cache storage:

```
1 xe pvs-cache-storage-create host-uuid=HOST_UUID
2 pvs-site-uuid=PVS_SITE_UUID sr-uuid=SR_UUID size=1GiB
```

Where `SR_UUID` is the UUID of the SR created in step b

Complete the cache configuration in Citrix Provisioning

After configuring PVS-Accelerator in XenServer, perform the following steps to complete the cache configuration for the Citrix Provisioning site.

In the Citrix Provisioning Administrator Console, use the Citrix Virtual Desktops Setup Wizard or the Streaming VM Wizard (depending on your deployment type) to access the Proxy capability. Although both wizards are similar and share many of the same screens, the following differences exist:

- The **Citrix Virtual Desktops Setup Wizard** is used to configure VMs running on XenServer hypervisor that is controlled using Citrix Virtual Desktops.
- The **Streaming VM Wizard** is used to create VMs on a host. It does not involve Citrix Virtual Desktops.

Launch the Citrix Provisioning Administrator Console:

1. Navigate to the Citrix Provisioning site.
2. Select the Citrix Provisioning site, right-click to expose a contextual menu.
3. Choose the appropriate wizard based on the deployment. Select the option **Enable PVS-Accelerator for all Virtual Machines** to enable the PVS-Accelerator feature.
4. If you are enabling virtual disk caching for the first time, the **XenServer** screen appears on the Streamed Virtual Machine Setup wizard. It displays the list of all Citrix Provisioning sites configured on XenServer that have not yet been associated with a Citrix Provisioning site. Using the list, select a Citrix Provisioning site to apply PVS-Accelerator. This screen is not displayed when you run the wizard for the same Citrix Provisioning site using the same XenServer host.
5. Click **Next** to complete the caching configuration.
6. Click **Finish** to provision Citrix Virtual Desktops or Streamed VMs and associate the selected Citrix Provisioning site with the PVS Accelerator in XenServer. When this step is complete, the **View PVS Servers** button in the **PVS-Accelerator configuration** window is enabled in XenCenter. Clicking the **View PVS Servers** button displays the IP addresses of all PVS Servers associated with the Citrix Provisioning site.

Caching operation

Consider the following when using the PVS-Accelerator feature:

- The PVS-Accelerator user interfaces in XenCenter and Citrix Provisioning are only exposed if the PVS-Accelerator supplemental pack is installed.

- Citrix Provisioning target devices are aware of their proxy status. No additional configuration is required once the capability is installed.
- In environments where multiple Citrix Provisioning servers are deployed with the same VHD, but have different file system timestamps, data might be cached multiple times. Due to this limitation, Citrix recommends using VHDX format, rather than VHD for virtual disks.
- After you start a VM with PVS-Accelerator enabled, the caching status for the VM is displayed in XenCenter:
 - In the **PVS** tab of the pool or the host
 - In the **General** tab for the VM
- Customers can confirm the correct operation of the PVS-Accelerator using RRD metrics on the host's **Performance** tab in XenCenter. For more information, see [Monitor and manage your deployment](#).

Important:

- PVS-Accelerator requires Citrix Provisioning 7.13 or later.
- PVS-Accelerator is available for XenServer Enterprise Edition customers or those customers who have access to XenServer through their Citrix Virtual Desktops and Citrix Virtual Apps entitlement.
- PVS-Accelerator requires License Server 11.14.
- PVS-Accelerator uses capabilities of OVS and is therefore not available on hosts that use Linux Bridge as the network back-end.
- PVS-Accelerator works on the first virtual network interface (VIF) of a cached VM. Therefore, connect the first VIF to the Citrix Provisioning storage network for caching to work.
- PVS-Accelerator can currently not be used on network ports which enforce that IPs are bound to certain MAC addresses. This switch functionality might be called “IP Source Guard” or similar. In such environments, PVS targets fail to boot with error ‘Login request time out!’ after enabling PVS-Accelerator.

The PVS-Accelerator functionality caches:

- **Reads** from virtual disks but not writes or reads from a write cache
- **Based on image versions.** Multiple VMs share cached blocks when they use the same image version
- Devices with any **non-persistent** write cache type
- Virtual disks with the **access mode Standard Image**. It does not work for virtual disks with the access mode Private Image
- Devices that are marked as **type Production or Test**. Devices marked as type Maintenance are not cached

PVS-Accelerator CLI operations

The following section describes the operations that customers can perform when using PVS-Accelerator using the CLI. Customers can also perform these operations using XenCenter. For more information, see XenCenter Help.

View Citrix Provisioning server addresses and ports configured by Citrix Provisioning

PVS-Accelerator works by optimizing the network traffic between a VM and the Citrix Provisioning server. When completing the configuration on the Citrix Provisioning server, the Citrix Provisioning server populates the `pvs-server` objects on XenServer with their IPs and ports. PVS-Accelerator later uses this information to optimize specifically the traffic between a VM and its Citrix Provisioning servers. The configured Citrix Provisioning servers can be listed using the following command:

```
1 xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
```

Configure a VM for caching

PVS-Accelerator can be enabled for the VM by using any of the following tools:

- Citrix Provisioning CLI
- Citrix Virtual Desktops Setup Wizard
- Streamed VM Setup Wizard
- XenCenter
- The xe CLI

The xe CLI configures PVS-Accelerator by using the VIF of a VM. It creates a Citrix Provisioning proxy that links the VM's VIF with a Citrix Provisioning site.

To configure a VM:

1. Find the first VIF of the VM to enable caching on it:

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --  
minimal)
```

2. Create the Citrix Provisioning proxy

```
1 xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
```


Disable caching for a VM

PVS-Accelerator can be disabled for a VM by destroying the Citrix Provisioning proxy that links the VM's VIF with a `pvs-site`.

1. Find the first VIF of the VM:

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --minimal)
```

2. Find the Citrix Provisioning proxy of the VM:

```
1 PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
```

3. Destroy the Citrix Provisioning proxy:

```
1 xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
```

Remove the PVS-Accelerator storage for a host or a site

To remove the PVS-Accelerator storage for a host or a site:

1. Find the host for which you would like to destroy the storage:

```
1 HOST_UUID=$(xe host-list name=label=HOST_NAME --minimal)
```

2. Find the uuid of the object:

```
1 PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=$HOST_UUID --minimal)
```

3. Destroy the object:

```
1 xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
```

Forget the PVS-Accelerator configuration for a site

To forget the PVS-Accelerator configuration for a site:

1. Find the Citrix Provisioning site:

```
1 PVS_SITE_UUID=$(xe pvs-site-list name=label=My PVS Site)
```

2. Run the following command to forget the Citrix Provisioning site:

```
1 xe pvs-site-forget uuid=$PVS_SITE_UUID
```

Graphics overview

February 27, 2019

This section provides an overview of XenServer's virtual delivery of 3D professional graphics applications and workstations. The offerings include GPU Pass-through (for NVIDIA, AMD and Intel GPUs) and hardware-based GPU sharing with NVIDIA GRID™ vGPU™, AMD MxGPU™, and Intel GVT-g™.

GPU Pass-Through

In a virtualized system, most of the physical system components are shared. These components are represented as multiple virtual instances to multiple clients by the hypervisor. A pass-through GPU is not abstracted at all, but remains one physical device. Each hosted virtual machine (VM) gets its own dedicated GPU, eliminating the software abstraction and the performance penalty that goes with it.

XenServer allows you to assign a physical GPU (in the XenServer host) to a Windows or HVM Linux VM running on the same host. This GPU Pass-Through feature is intended for graphics power users, such as CAD designers.

Shared GPU

Shared GPU allows one physical GPU to be used by multiple VMs concurrently. Because a portion of a physical GPU is used, performance is greater than emulated graphics, and there is no need for one card per VM. This feature enables resource optimization, boosting the performance of the VM. The graphics commands of each virtual machine are passed directly to the GPU, without translation by the hypervisor.

Licensing note

Graphics Virtualization is available for XenServer Enterprise Edition customers, or customers who have access to XenServer through their Virtual Apps and Desktops entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For more information, see [Licensing](#).

Vendor support

The following table lists GPU and shared GPU support for guests:

	GPU for Windows VMs	GPU for HVM Linux VMs	Shared GPU For Windows VMs	Virtual GPU for Linux VMs
AMD	YES		YES	
Intel	YES		YES	
NVIDIA	YES	YES	YES	YES

You might need a vendor subscription or a license depending on the graphics card used.

vGPU XenMotion

vGPU XenMotion enables a VM that uses a virtual GPU to perform XenMotion, Storage XenMotion, or VM Suspend. VMs with vGPU XenMotion capabilities can be migrated to avoid downtime.

To use vGPU XenMotion, your VM must run on a graphics card that supports this feature and has the supported drivers from the GPU vendor installed.

The following restrictions apply when using vGPU XenMotion:

- XenMotion of VMs from the previous versions of XenServer is not supported.
- XenMotion is not compatible with GPU Pass-through.
- VMs must have the appropriate vGPU drivers installed to be supported with any vGPU XenMotion features. The in-guest drivers must be installed for all guests using vGPU.
- Reboot and shutdown operations on a VM are not supported while a migration is in progress. These operations can cause the migration to fail.
- Linux VMs are not supported with any vGPU XenMotion features.
- Live migration by the Workload Balancing appliance is not supported for vGPU-enabled VMs. The Workload Balancing appliance cannot capacity plan for VMs that have a vGPU attached.
- Making disk and memory snapshots are not supported.
- After migrating a VM using vGPU XenMotion, the guest VNC console might become corrupted. Use ICA, RDP, or another network-based method for accessing VMs after a vGPU XenMotion has been performed.
- VDI migration uses XenMotion, therefore requires enough vGPU space on the host to make a copy of the vGPU instance on the host. If the physical GPUs are fully used, VDI migration might not be possible.

Vendor support

The following table lists support for vGPU XenMotion:

	GPRU for Windows VMs	GPU for HVM Linux VMs	Shared GPU for Windows VMs	Virtual GPU for Linux VMs
NVIDIA			YES	

For more information about the graphics cards that support this feature, see the vendor-specific sections of this guide. Customers might need a vendor subscription or a license depending on the graphics card used.

Guest support and constraints

XenServer 7.6 supports the following guest operating systems for virtual GPU.

NVIDIA vGPU

Windows guests:

- Windows 7 (32-bit/64-bit)
- Windows 8.1 (32-bit/64-bit)
- Windows 10 (64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)

HVM Linux guests:

- RHEL 7.x
- CentOS 7.x
- Oracle Linux 7.x
- Scientific Linux 7.x
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 18.04

AMD MxGPU

Windows guests:

- Windows 7 SP1 (64-bit)
- Windows 10 (64-bit)
- Windows Server 2016 (64-bit)

Intel GVT-g

Windows guests:

- Windows 7 (32-bit/64-bit)
- Windows 8.1 (32-bit/64-bit)
- Windows 10 (64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)

Constraints

- XenServer supports only one GPU per VM.
- VMs with a virtual GPU are not supported with Dynamic Memory Control.
- XenServer automatically detects and groups identical physical GPUs across hosts in the same pool. If assigned to a group of GPUs, a VM can be started on any host in the pool that has an available GPU in the group.
- All graphics solutions (NVIDIA vGPU, Intel GVT-d, Intel GVT-G, AMD MxGPU, and vGPU pass-through) can be used in an environment that makes use of high availability. However, VMs that use these graphics solutions cannot be protected with high availability. These VMs can be restarted on a best-effort basis while there are hosts with the appropriate free resources.

Prepare host for graphics

October 4, 2018

This section provides step-by-step instructions on how to prepare XenServer for supported graphical virtualization technologies. The offerings include NVIDIA GRID vGPU, AMD MxGPU, and Intel GVT-d and GVT-g.

NVIDIA GRID vGPU

NVIDIA GRID vGPU enables multiple Virtual Machines (VM) to have simultaneous, direct access to a single physical GPU. It uses NVIDIA graphics drivers deployed on non-virtualized Operating Systems.

GRID physical GPUs can support multiple virtual GPU devices (vGPUs). To provide this support, the physical GPU must be under the control of NVIDIA's GRID Virtual GPU Manager running in XenServer Control Domain (dom0). The vGPUs can be assigned directly to VMs.

VMs use GRID virtual GPUs like a physical GPU that the hypervisor has passed through. An NVIDIA driver loaded in the VM provides direct access to the GPU for performance critical fast paths. It also provides a paravirtualized interface to the GRID Virtual GPU Manager.

NVIDIA GRID is compatible with the HDX 3D Pro feature of Citrix Virtual Apps and Desktops. For more information, see [HDX 3D Pro](#).

Licensing note

NVIDIA vGPU is available for XenServer Enterprise Edition customers, or customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For more information, see [Licensing](#).

Depending on the NVIDIA graphics card used, you might need NVIDIA subscription or a license.

For information on licensing NVIDIA cards, see the [NVIDIA website](#).

Available NVIDIA GRID vGPU types

NVIDIA GRID cards contain multiple Graphics Processing Units (GPU). For example, TESLA M10 cards contain four GM107GL GPUs, and TESLA M60 cards contain two GM204GL GPUs. Each physical GPU can host several different types of virtual GPU (vGPU). vGPU types have a fixed amount of frame buffer, number of supported display heads and maximum resolutions, and are targeted at different classes of workload.

For a list of the most recently supported NVIDIA cards, see the [Hardware Compatibility List](#) and the [NVIDIA product information](#).

Note:

The vGPUs hosted on a physical GPU at the same time **must all be of the same type**. However, there is no corresponding restriction for physical GPUs on the same card. This restriction is automatic and can cause unexpected capacity planning issues.

For example, a TESLA M60 card has two physical GPUs, and can support 11 types of vGPU:

- GRID M60-1A
- GRID M60-2A
- GRID M60-4A
- GRID M60-8A

- GRID M60-0B
- GRID M60-1B
- GRID M60-0Q
- GRID M60-1Q
- GRID M60-2Q
- GRID M60-4Q
- GRID M60-8Q

In the case where you start both a VM that has vGPU type M60-1A and a VM that has vGPU type M60-2A:

- One physical GPU only supports M60-1A instances
- The other only supports M60-2A instances

You cannot start any M60-4A instances on that single card.

NVIDIA GRID system requirements

- NVIDIA GRID card:
 - For a list of the most recently supported NVIDIA cards, see the [Hardware Compatibility List](#) and the [NVIDIA product information](#).
- Depending on the NVIDIA graphics card used, you might need an NVIDIA subscription or a license. For more information, see the [NVIDIA product information](#).
- XenServer Enterprise Edition (or access to XenServer through a Citrix Virtual Apps and Desktops entitlement).
- A server capable of hosting XenServer and NVIDIA GRID cards.
- NVIDIA GRID vGPU software package for XenServer, consisting of the GRID Virtual GPU Manager for XenServer, and NVIDIA drivers.
- To run Citrix Virtual Desktops with VMs running NVIDIA vGPU, you also need: Citrix Virtual Desktops 7.6 or later, full installation.

Note:

Review the NVIDIA GRID Virtual GPU User Guide (Ref: DU-06920-001) available from the [NVIDIA website](#). Register with NVIDIA to access these components.

vGPU XenMotion

XenServer enables the use of XenMotion, Storage XenMotion, and the ability to suspend and resume for NVIDIA GRID vGPU-enabled VMs.

To use the vGPU XenMotion, Storage XenMotion, or Suspend features, satisfy the following requirements:

- An NVIDIA GRID card, Maxwell family or later.
- An NVIDIA GRID Virtual GPU Manager for XenServer with XenMotion enabled. For more information, see the NVIDIA Documentation.
- A Windows VM that has NVIDIA XenMotion-enabled vGPU drivers installed.

vGPU XenMotion enables the use of XenMotion within a pool, XenMotion between pools, Storage XenMotion, and Suspend/Resume of vGPU-enabled VMs.

Preparation overview

1. Install XenServer
2. Install the NVIDIA GRID Virtual GPU Manager for XenServer
3. Restart the XenServer host

Installation on XenServer

XenServer is available for download from the [XenServer Downloads](#) page.

Install the following:

- **XenServer Base Installation ISO**
- **XenCenter Windows Management Console**

For more information, see [Install](#).

Licensing note

vGPU is available for XenServer Enterprise Edition customers, or customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For more information, see [Licensing](#).

Depending on the NVIDIA graphics card used, you might need NVIDIA subscription or a license. For more information, see [NVIDIA product information](#).

For information about licensing NVIDIA cards, see the [NVIDIA website](#).

Install the NVIDIA GRID vGPU Manager for XenServer

Install the NVIDIA GRID vGPU Software that is available from [NVIDIA](#). The NVIDIA GRID software consists of:

- GRID vGPU Manager
(For example: NVIDIA-vGPU-XenServer-7.2-367.64.x86_64.rpm)
- Windows Display Driver (The Windows display driver depends on the Windows version)
(For example: 369.71_grid_win10_server2016_64bit_international.exe)

The *GRID vGPU Manager* runs in the XenServer Control Domain (dom0). It is provided as either a supplemental pack or an RPM file. For more information about installation, see the User Guide included in the NVIDIA GRID vGPU Software.

Note:

The Update, RPM names, and versions are examples and are different in your environment.

The Update can be installed in one of the following methods:

- Use XenCenter (**Tools > Install Update > Select update or supplemental pack from disk**)
- Use the xe CLI command `xe-install-update`.

The Update is named `NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.iso` or similar.

Note:

If you are installing the GRID vGPU Manager using an RPM file, ensure that you copy the RPM file to dom0 and then install.

1. Use the rpm command to install the package:

```
1 [root@xenserver ~]# rpm -iv NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.rpm
2 Preparing packages for installation...
3 NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64
4 [root@xenserver ~]
```

2. Restart the XenServer host:

```
1 [root@xenserver ~]# shutdown -r now
2 Broadcast message from root (pts/1) Mon May 09 13:05:31 2016):
3 [root@xenserver ~]
```

3. After you restart the XenServer host, verify that the GRID package has been installed and loaded correctly by checking the NVIDIA kernel driver:

```

1 [root@xenserver ~]#lsmod |grep nvidia
2 nvidia                8152994 0
3 i2c_core               20294 2 nvidia,i2c_i801
4 [root@xenserver ~]#

```

4. Verify that the NVIDIA kernel driver can successfully communicate with the GRID physical GPUs in your host. Run the `nvidia-smi` command to produce a listing of the GPUs in your platform similar to:

```

1 [root@xenserver ~]# nvidia-smi
2
3 Thu Jan 26 13:48:50 2017
4 +-----+
5 NVIDIA-SMI 367.64 Driver Version: 367.64
6 -----+-----+
7 GPU Name Persistence-M| Bus-Id Disp.A | Volatile Uncorr. ECC
8 Fan Temp Perf Pwr:Usage/Cap| Memory-Usage | GPU-Util Compute M
9 .|
10 =====+=====+=====
11 | 0 Tesla M60 On | 0000:05:00.0 Off| Off |
12 | N/A 33C P8 24W / 150W | 7249MiB / 8191MiB | 0%
13 | Default |
14 +-----+-----+-----+
15 | 1 Tesla M60 On | 0000:09:00.0 Off| Off |
16 | N/A 36C P8 24W / 150W | 7249MiB / 8191MiB | 0%
17 | Default |
18 +-----+-----+-----+
19 | 2 Tesla M60 On | 0000:85:00.0 Off| Off |
20 | N/A 36C P8 23W / 150W | 19MiB / 8191MiB | 0%
21 | Default |
22 +-----+-----+-----+
23 | 3 Tesla M60 On | 0000:89:00.0 Off| Off |
24 | N/A 37C P8 23W / 150W | 14MiB / 8191MiB | 0%
25 | Default |
26 +-----+-----+-----+
27
28 +-----+
29 Processes: GPU Memory |

```

```

24 | GPU      PID  Type  Process name      Usage  |
25 | =====
26 | No running compute processes found |
27 +-----
28 [root@xenserver ~]#

```

Note:

When using NVIDIA vGPU with XenServer hosts that have more than 768 GB of RAM, add the parameter `iommu=dom0-passthrough` to the Xen command line:

- a) Run the following command in the control domain (Dom0):

```
1 /opt/xensource/libexec/xen-cmdline - -set-xen iommu=dom0-
  passthrough
```

- b) Restart the host.

AMD MxGPU

AMDs MxGPU enables multiple Virtual Machines (VM) to have direct access to a portion of a single physical GPU, using Single Root I/O Virtualization. The same AMD graphics driver deployed on non-virtualized operating systems can be used inside the guest.

VMs use MxGPU GPUs in the same manner as a physical GPU that the hypervisor has passed through. An AMD graphics driver loaded in the VM provides direct access to the GPU for performance critical fast paths.

For more information about using AMD MxGPU with XenServer, see the [AMD Documentation](#).

Licensing note

MxGPU is available for XenServer Enterprise Edition customers, or customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website [here](#). For detailed information on Licensing, see XenServer Licensing FAQ on the [Citrix Product Documentation](#) website.

Available AMD MxGPU vGPU types

AMD MxGPU cards can contain multiple GPUs. For example, S7150 cards contain one physical GPU and S7150x2 cards contain two GPUs. Each physical GPU can host several different types of virtual GPU

(vGPU). vGPU types split a physical GPU into a pre-defined number of vGPUs. Each of these vGPUs has an equal share of the frame buffer and graphics processing abilities. The different vGPU types are targeted at different classes of workload. vGPU types that split a physical GPU into fewer pieces are more suitable for intensive workloads.

Note:

The vGPUs hosted on a physical GPU at the same time **must all be of the same type**. However, there is no corresponding restriction on physical GPUs on the same card. This restriction is automatic and can cause unexpected capacity planning issues.

AMD MxGPU system requirements

- AMD FirePro S7100-series GPUs
- XenServer Enterprise Edition (or access to XenServer through a Citrix Virtual Desktops/Citrix Virtual Apps entitlement)
- A server capable of hosting XenServer and AMD MxGPU cards. The list of servers validated by AMD can be found on [the AMD website](#).
- AMD MxGPU host drivers for XenServer. These drivers are available from [the AMD download site](#).
- AMD FirePro in-guest drivers, suitable for MxGPU on XenServer. These drivers are available from [the AMD download site](#).
- To run Citrix Virtual Desktops with VMs running AMD MxGPU, you also need Citrix Virtual Desktops 7.13 or later, full installation.
- System BIOS configured to support SR-IOV and the MxGPU configured as the secondary adapter

Preparation overview

1. Install XenServer
2. Install the AMD MxGPU host drivers for XenServer
3. Restart the XenServer host

Installation on XenServer

XenServer is available for download from the [XenServer Downloads](#) page.

Install the following:

- **XenServer 7.6 Base Installation ISO**

- **XenCenter 7.6 Windows Management Console**

For more information about installation, see the [XenServer Installation Guide](#).

Install the AMD MxGPU host driver for XenServer

Complete the following steps to install the host driver.

1. The update that contains the driver can be installed by using XenCenter or by using the xe CLI.
 - To install by using XenCenter, go to **Tools > Install Update > Select update or supplemental pack from disk**
 - To install by using the xe CLI, copy the update to the host and run the following command in the directory where the update is located:

```
1 xe-install-supplemental-pack mxgpu-1.0.5.amd.iso
```

2. Restart the XenServer host.
3. After restarting the XenServer host, verify that the MxGPU package has been installed and loaded correctly. Check whether the `gim` kernel driver is loaded by running the following commands in the XenServer host console:

```
1 modinfo gim
2 modprobe gim
```

4. Verify that the `gim` kernel driver has successfully created MxGPU Virtual Functions, which are provided to the guests. Run the following command:

```
1 lspci | grep "FirePro S7150"
```

The output from the command shows Virtual Functions that have the “S7150V” identifier.

5. Use the GPU tab in XenCenter to confirm that MxGPU Virtual GPU types are listed as available on the system.

After the AMD MxGPU drivers are installed, the **Passthrough** option is no longer available for the GPUs. Instead use the **MxGPU.1** option.

Create a MxGPU enabled VM

Before configuring a VM to use MxGPU, install the VM. Ensure that AMD MxGPU supports the VM operating system. For more information, see [Guest support and constraints](#).

After the VM is installed, complete the configuration by following the instructions in [Create vGPU enabled VMs](#).

Intel GVT-d and GVT-g

XenServer supports Intel's virtual GPU (GVT-g), a graphics acceleration solution that requires no additional hardware. It uses the Intel Iris Pro feature embedded in certain Intel processors, and a standard Intel GPU driver installed within the VM.

Intel GVT-d and GVT-g are compatible with the HDX 3D Pro features of Citrix Virtual Apps and Desktops. For more information, see [HDX 3D Pro](#).

Note:

Because the Intel Iris Pro graphics feature is embedded within the processors, CPU-intensive applications can cause power to be diverted from the GPU. As a result, you might not experience full graphics acceleration as you do for purely GPU-intensive workloads.

Intel GVT-g system requirements and configuration

To use Intel GVT-g, your XenServer host must have the following hardware:

- A CPU that has Iris Pro graphics. This CPU must be listed as supported for Graphics on the [Hardware Compatibility List](#)
- A motherboard that has a graphics-enabled chipset. For example, C226 for Xeon E3 v4 CPUs or C236 for Xeon E3 v5 CPUs.

Note:

Ensure that you restart the hosts when switching between Intel GPU pass-through (GVT-d) and Intel Virtual GPU (GVT-g).

When configuring Intel GVT-g, the number of Intel virtual GPUs supported on a specific XenServer host depends on its GPU bar size. The GPU bar size is called the 'Aperture size' in the BIOS. Citrix recommends that you set the Aperture size to 1,024 MB to support a maximum of seven virtual GPUs per host.

If you configure the Aperture size to 256 MB, only one VM can start on the host. Setting it to 512 MB can result in only three VMs being started on the XenServer host. An Aperture size higher than 1,024 MB is not supported and **does not** increase the number of VMs that start on a host.

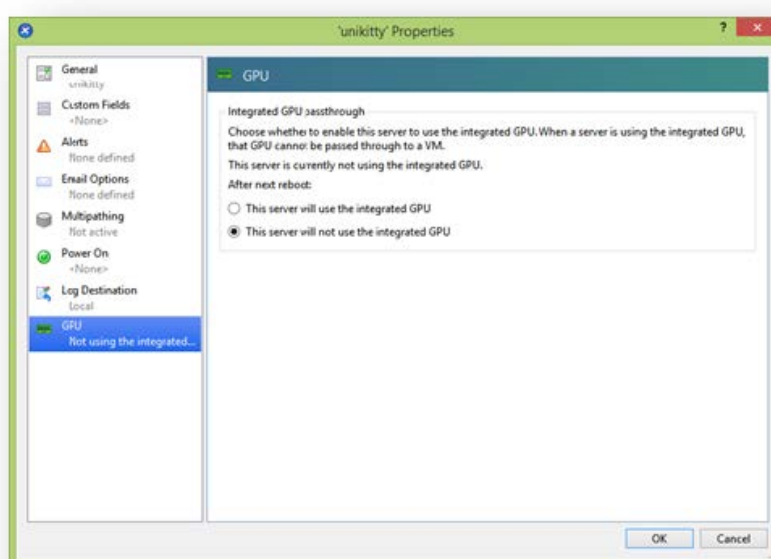
Enable Intel GPU Pass-Through

XenServer supports the GPU Pass-Through feature for Windows 7 and Windows 8.1 (32-/64-bit) VMs using an Intel integrated GPU device. For more information on supported hardware, see the [Hardware Compatibility List](#).

When using Intel GPU on Intel servers, the XenServer host's Control Domain (dom0) has access to the integrated GPU device. In such cases, the GPU is available for pass-through. To use the Intel GPU Pass-through feature on Intel servers, disable the connection between dom0 and the GPU before passing through the GPU to the VM.

To disable this connection, complete the following steps:

1. On the **Resources** pane, choose the XenServer host.
2. On the **General** tab, click **Properties**, and in the left pane, click **GPU**.
3. In the **Integrated GPU passthrough** section, select **This server will not use the integrated GPU**.



This step disables the connection between dom0 and the Intel integrated GPU device.

4. Click **OK**.
5. Restart the XenServer host for the changes to take effect.

The Intel GPU is now visible on the GPU type list during new VM creation, and on the VM's **Properties** tab.

Note:

The XenServer host's external console output (for example, VGA, HDMI, DP) will not be available after disabling the connection between dom0 and the GPU.

Create vGPU enabled VMs

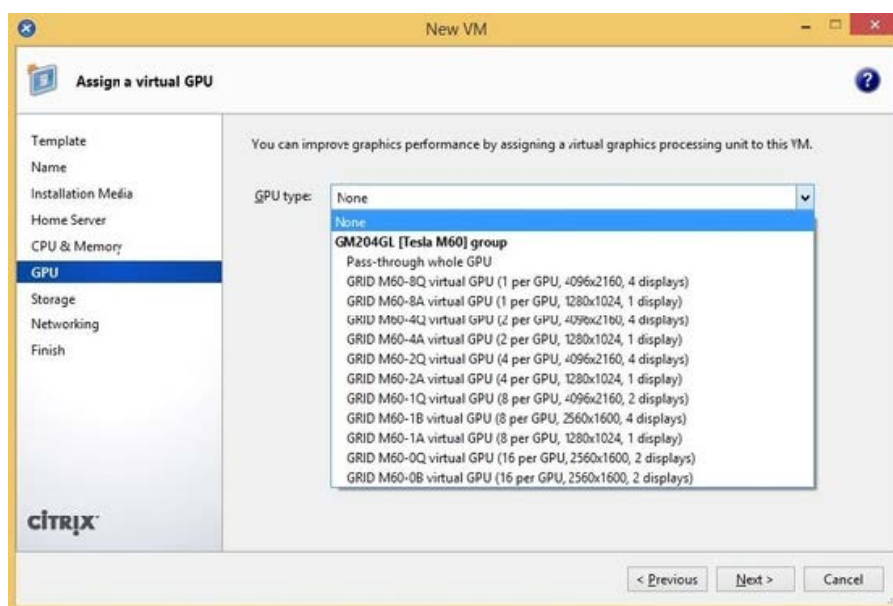
August 13, 2018

This section provides step-by-step instructions on how to create a virtual GPU or GPU pass-through enabled VM.

Note:

If you are using the Intel GPU Pass-through feature, first see the section *Enabling Intel GPU Pass-through* for more configuration, and then complete the following steps.

1. Create a VM using XenCenter. Select the host on the Resources pane and then select **New VM** on the VM menu.
2. Follow the instructions on the **New VM** configuration and select the **Installation Media, Home Server, CPU, and Memory**.
3. GPU-enabled servers display a **GPU** configuration page:



4. From the **GPU Type** list, select either **Pass-through whole GPU**, or a virtual GPU type. Unavailable virtual GPU types are grayed-out.
5. Click **Next** to configure **Storage** and then **Networking**.
6. After you complete your configuration, click **Create Now**.

Install the XenServer Tools

1. Install the XenServer Tools

Without the optimized networking and storage drivers provided by the XenServer Tools, remote graphics applications running on GRID vGPU do **not** deliver maximum performance.

- a) Select the VM in the **Resources** pane, right-click, and then click **Install XenServer Tools** on the shortcut menu. Alternatively, on the **VM** menu, click **Install XenServer Tools**.
- b) Click **Install XenServer Tools** on the message dialog to go to the VM's console and begin the installation.
- c) If Autoplay is enabled for the VM's CD/DVD drive, installation is started automatically after a few moments. This process installs the I/O drivers and the Management Agent. Restart the VM when prompted to get your VM to an optimized state. If Autoplay is not enabled, the XenServer Tools installer displays the installation options. Click **Install XenServer Tools** to continue with the installation. This operation mounts the XenServer Tools ISO (guest-tools.iso) on the VM's CD/DVD drive.
- d) Click **Run setup.exe** to begin XenServer Tools installation and restart the VM when prompted to get your VM to an optimized state.

Install the in-guest drivers

When viewing the VM console in XenCenter, the VM typically boots to the desktop in VGA mode with 800 x 600 resolution. The standard Windows screen resolution controls can be used to increase the resolution to other standard resolutions. (Control Panel > Display > Screen Resolution)

Note:

When using GPU Pass-Through or MxGPU, we recommend that you install the in-guest drivers through RDP or VNC over the network. That is, not through XenCenter.

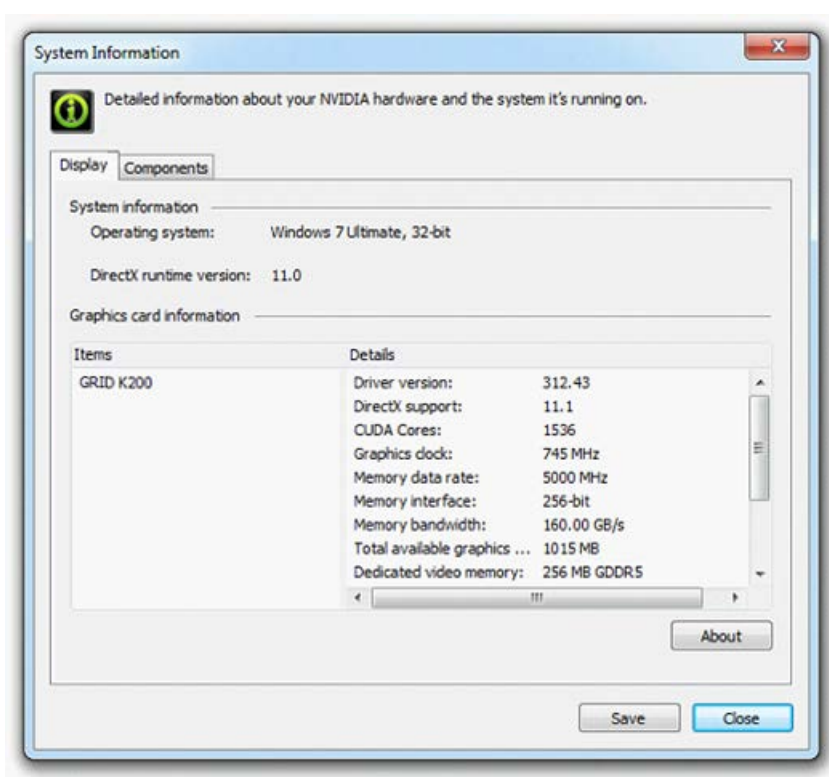
Install the NVIDIA drivers

To enable vGPU operation (as for a physical NVIDIA GPU), install NVIDIA drivers into the VM.

The following section provides an overview of the procedure. For detailed instructions, see the NVIDIA User Guides.

1. Start the VM. In the **Resources** pane, right-click on the VM, and click **Start**.
During this start process, XenServer dynamically allocates a vGPU to the VM.
2. Follow the Windows operating system installation screens.
3. After the operating system installation completes, restart the VM.
4. Install the appropriate driver for the GPU inside the guest. The following example shows the specific case for in guest installation of the NVIDIA GRID drivers.

5. Copy the 32-bit or 64-bit NVIDIA Windows driver package to the VM, open the zip file, and run setup.exe.
6. Follow the installer steps to install the driver.
7. After the driver installation has completed, you might be prompted to reboot the VM. Select **Restart Now** to restart the VM immediately, alternatively, exit the installer package, and restart the VM when ready. When the VM starts, it boots to a Windows desktop.
8. To verify that the NVIDIA driver is running, right-click on the desktop and select **NVIDIA Control Panel**.
9. In the NVIDIA Control Panel, select **System Information**. This interface shows the GPU Type in use by the VM, its features, and the NVIDIA driver version in use:

**Note:**

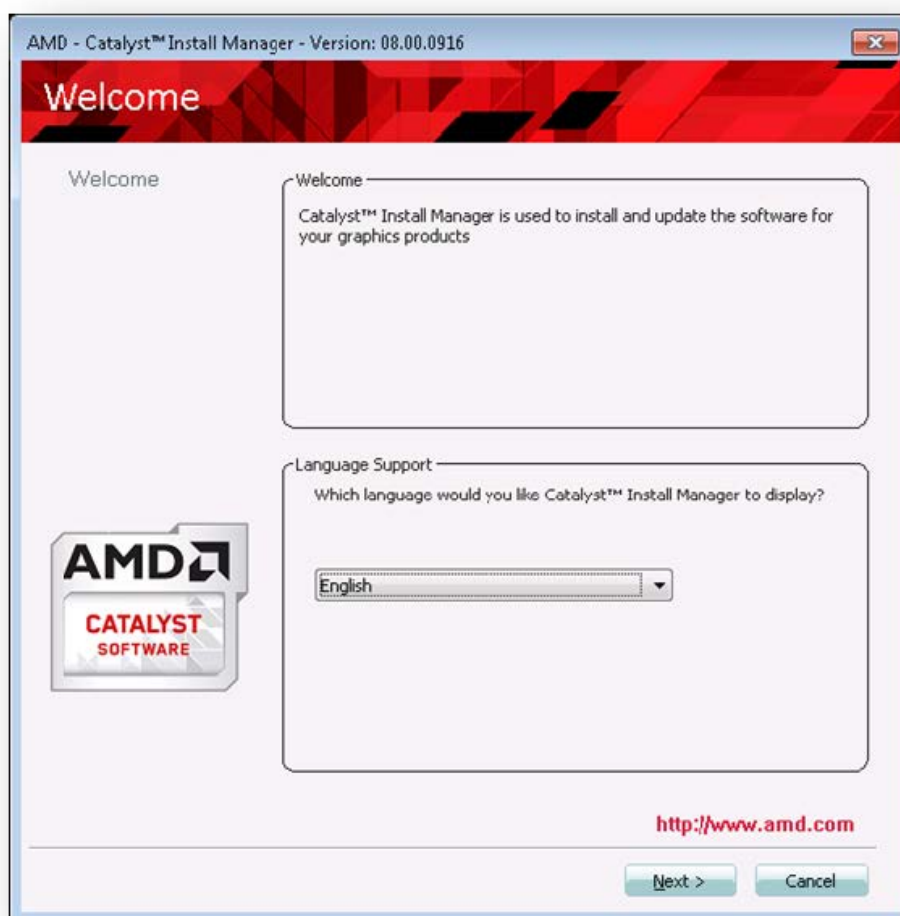
Depending on the NVIDIA graphics card used, you might need an NVIDIA subscription or a license. For more information, see the [NVIDIA product information](#).

The VM is now ready to run the full range of DirectX and OpenGL graphics applications supported by the GPU.

Install the AMD drivers

To enable GPU operation, install AMD drivers into the VM.

1. Start the VM. In the **Resources** pane, right-click on the VM, and click **Start**.
During this boot process, XenServer dynamically allocates a GPU to the VM.
2. Follow the Windows operating system installation screens.
3. After the operating system installation completes, restart the VM.
4. Copy the 32-bit or 64-bit AMD Windows drivers (AMD Catalyst Install Manager) to the VM.
5. Run the AMD Catalyst Install Manager; select your **Destination Folder**, and then click **Install**.

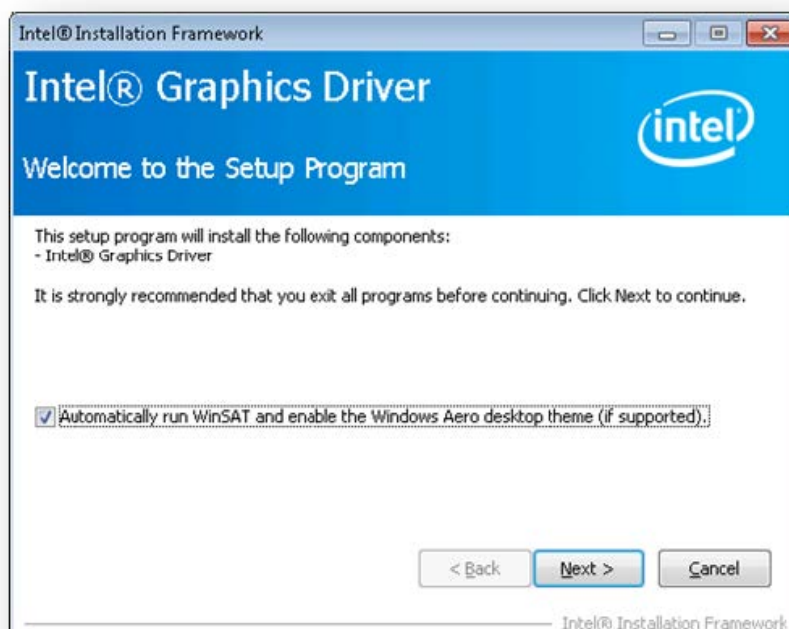


6. Follow the installer steps to install the driver.
7. To complete the installation, restart your VM.
8. After the VM restarts, check that graphics are working correctly. Open the **Windows Device Manager**, expand **Display adapters**, and ensure that the AMD Graphics Adapter does not have any warning symbols.

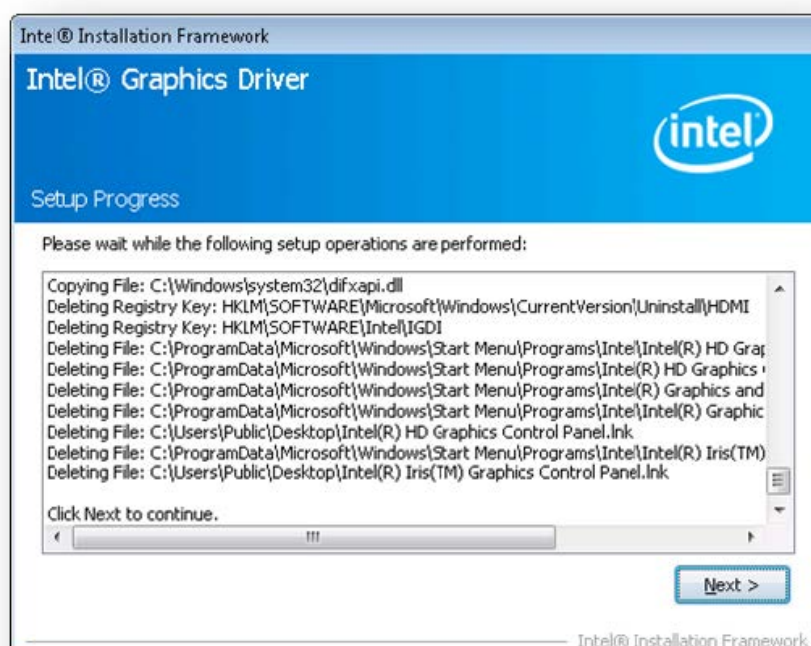
Install the Intel drivers

To enable GPU operation, install Intel drivers into the VM.

1. Start the **VM**. In the **Resources** pane, right-click on the VM, and click **Start**.
During this boot process, XenServer dynamically allocates a GPU to the VM.
2. Follow the Windows operating system installation screens.
3. After the operating system installation completes, reboot the VM.
4. Copy the 32-bit or 64-bit Intel Windows driver (Intel Graphics Driver) to the VM.
5. Run the **Intel Graphics Driver** setup program
6. Select **Automatically run WinSAT**, and then click **Next**.



7. To accept the License Agreement, click **Yes**, and on the Readme File Information screen, click **Next**.
8. Wait until the setup operations complete. When you are prompted, click **Next**.



9. To complete the installation, you are prompted to restart the VM. Select **Yes**, I want to restart this computer now, and click **Finish**.
10. After the VM restarts, check that graphics are working correctly. Open the Windows Device Manager, expand **Display adapters**, and ensure that the Intel Graphics Adapter does not have any warning symbols.

Note:

You can obtain the latest drivers from the [Intel website](#).

Memory usage

August 14, 2018

Two components contribute to the memory footprint of the XenServer host. 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 XenServer management toolstack (XAPI). Besides providing XenServer 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:

Host Memory (GB)	Control Domain Memory Allocated (MB)
20–24	752
24–48	2048
48–64	3072
64–1024	4096

Note:

The amount reported in the XenServer 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 reduce the memory allocated to the Control Domain to lower than the default 752 MB on hosts with smaller memory (less than 16 GB). However, Citrix recommends that you **do not reduce the dom0 memory below 400 MB**.

1. On the XenServer host, open a local shell and log on as root.
2. Type the following:

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<nn>M
```

Where <nn> represents the amount of memory, in MB, to be allocated to dom0.

3. Restart the XenServer host using XenCenter or the `reboot` command on the xsconsole.

When the host restarts, on the xsconsole, run the `free` command to verify the new memory settings.

Warning:

Increasing the amount of memory allocated to the Control Domain results in less memory being available to VMs.

You can increase the amount of memory allocated to the Control Domain beyond the amount shown in the *Control domain memory* table. However, you must do this operation under the guidance of Citrix Support.

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:

```
1 xe host-list uuid=host_uuid params=memory-free
2 xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
```

Monitor and manage your deployment

September 5, 2018

XenServer provides detailed monitoring of performance metrics, including 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.

XenServer 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 go 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 XenServer performance

Customers can monitor the performance of their XenServer hosts 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
<code>avgqu_sz_<sr-uuid-short></code>	Average I/O queue size (requests).	At least one plugged VBD in SR <code><sr-uuid-short></code> on the host	<code>sr-uuid-short</code> Queue Size
<code>cpu<cpu>-C<cstate></code>	Time CPU <code>cpu</code> spent in C-state <code>cstate</code> in milliseconds.	C-state exists on CPU	CPU <code>cpu</code> C-state <code>cstate</code>
<code>cpu<cpu>-P<pstate></code>	Time CPU <code>cpu</code> spent in P-state <code>pstate</code> in milliseconds.	P-state exists on CPU	CPU <code>cpu</code> P-state <code>pstate</code>
<code>cpu<cpu></code>	Utilization of physical CPU <code>cpu</code> (fraction). Enabled by default.	CPU <code>cpu</code> exists	CPU <code>cpu</code>
<code>cpu_avg</code>	Mean utilization of physical CPUs (fraction). Enabled by default.	None	Average CPU
<code>inflight_<sr-uuid-short></code>	Number of I/O requests currently in flight. Enabled by default.	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Inflight Requests
<code>io_throughput_read_<sr-uuidshort></code>	Data read from SR (MiB/s).	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Read Throughput
<code>io_throughput_write_<sr-uuidshort></code>	Data written to the SR (MiB/s).	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Write Throughput
<code>io_throughput_total_<sr-uuidshort></code>	All SR I/O (MiB/s).	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Total Throughput

Metric Name	Description	Condition	XenCenter Name
<code>iops_read_<sr-uuid-short></code>	Read requests per second.	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Read IOPS
<code>iops_write_<sr-uuid-short></code>	Write requests per second.	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Write IOPS
<code>iops_total_<sr-uuid-short></code>	I/O requests per second.	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Total IOPS
<code>iowait_<sr-uuid-short></code>	Percentage of the time waiting for I/O.	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> IO Wait
<code>latency_<sr-uuid-short></code>	Average I/O latency (milliseconds).	At least one plugged VBD in SR <code>sr</code> on the host	<code>sr</code> Latency
<code>loadavg</code>	Domain0 load average. Enabled by default	None	Control Domain Load
<code>memory_free_kib</code>	Total amount of free memory (KiB). Enabled by default.	None	Free Memory
<code>memory_reclaimed</code>	Host memory reclaimed by squeeze (B).	None	Reclaimed Memory
<code>memory_reclaimed_max</code>	Host memory available to reclaim with squeeze (B).	None	Potential Reclaimed Memory
<code>memory_total_kib</code>	Total amount of memory (KiB) in the host. Enabled by default.	None	Total Memory

Metric Name	Description	Condition	XenCenter Name
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 Statefile 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)
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

Metric Name	Description	Condition	XenCenter Name
<code>pvsaccelerator_eviction_rate</code>	Bytes per second evicted from the cache	PVSAccelerator Enabled	PVS-Accelerator eviction rate
<code>pvsaccelerator_read_rate</code>	Reads per second served from the cache	PVSAccelerator Enabled	PVS-Accelerator hit rate
<code>pvsaccelerator_read_miss_rate</code>	Reads per second that cannot be served from the cache	PVSAccelerator Enabled	PVS-Accelerator miss rate
<code>pvsaccelerator_traffic_clients</code>	Bytes per second sent by cached PVS clients	PVSAccelerator Enabled	PVS-Accelerator observed network traffic from clients
<code>pvsaccelerator_traffic_servers</code>	Bytes per second sent by cached PVS servers	PVSAccelerator Enabled	PVS-Accelerator observed network traffic from servers
<code>pvsaccelerator_read_rate_observed</code>	Reads per second observed by the cache	PVSAccelerator Enabled	PVS-Accelerator observed read rate
<code>pvsaccelerator_traffic_saved</code>	Bytes per second sent by PVSAccelerator instead of the PVS server	PVSAccelerator Enabled	PVS-Accelerator saved network traffic
<code>pvsaccelerator_space_utilization</code>	Percentage of space used by PVSAccelerator on this host, compared to the total size of the cache storage	PVSAccelerator Enabled	PVS-Accelerator space utilization
<code>sr_<sr>_cache_size</code>	Size in bytes of the IntelliCache SR. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Size
<code>sr_<sr>_cache_hits</code>	Cache hits per second. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Hits

Metric Name	Description	Condition	XenCenter Name
<code>sr_<sr>_cache_misses</code>	Cache misses per second. Enabled by default.	IntelliCache Enabled	IntelliCache Cache Misses
<code>xapi_allocation_ki</code>	Memory (KiB) allocation done by the XAPI daemon. Enabled by default.	None	Agent Memory Allocation
<code>xapi_free_memory_ki</code>	Free memory (KiB) available to the XAPI daemon. Enabled by default.	None	Agent Memory Free
<code>xapi_healthcheck/latency_health</code>	Turn-around time in seconds of the latest XAPI status monitoring call on the local host. Disabled by default	High availability Enabled	XenServer Healthcheck Latency
<code>xapi_live_memory_ki</code>	Live memory (KiB) used by XAPI daemon. Enabled by default.	None	Agent Memory Live
<code>xapi_memory_usage_</code>	Total memory (KiB) allocated used by XAPI daemon. Enabled by default.	None	Agent Memory Usage

Available VM metrics

Metric Name	Description	Condition	XenCenter Name
<code>cpu<cpu></code>	Utilization of vCPU <code>cpu</code> (fraction). Enabled by default	vCPU <code>cpu</code> exists	CPU

Metric Name	Description	Condition	XenCenter Name
<code>memory</code>	Memory currently allocated to VM (Bytes). Enabled by default	None	Total Memory
<code>memory_target</code>	Target of VM balloon driver (Bytes). Enabled by default	None	Memory target
<code>memory_internal_free</code>	Memory used as reported by the guest agent (KiB). Enabled by default	None	Free Memory
<code>runstate_fullrun</code>	Fraction of time that all vCPUs are running.	None	vCPUs full run
<code>runstate_fullcontention</code>	Fraction of time that all vCPUs are runnable (that is, waiting for CPU)	None	vCPUs full contention
<code>runstate_concurrency</code>	Fraction of time that some vCPUs are running and some are runnable	None	vCPUs concurrency hazard
<code>runstate_blocked</code>	Fraction of time that all vCPUs are blocked or offline	None	vCPUs idle
<code>runstate_partialrun</code>	Fraction of time that some vCPUs are running, and some are blocked	None	vCPUs partial run
<code>runstate_partialcontention</code>	Fraction of time that some vCPUs are runnable and some are blocked	None	vCPUs partial contention
<code>vbd_<vbd>_write</code>	Writes to device <code>vbd</code> in bytes per second. Enabled by default	VBD <code>vbd</code> exists	Disk <code>vbd</code> Write

Metric Name	Description	Condition	XenCenter Name
<code>vbd_<vbd>_read</code>	Reads from device <code>vbd</code> in bytes per second. Enabled by default.	VBD <code>vbd</code> exists	Disk <code>vbd</code> Read
<code>vbd_<vbd>_write_latency</code>	Writes to device <code>vbd</code> in microseconds.	VBD <code>vbd</code> exists	Disk <code>vbd</code> Write Latency
<code>vbd_<vbd>_read_latency</code>	Reads from device <code>vbd</code> in microseconds.	VBD <code>vbd</code> exists	Disk <code>vbd</code> Read Latency
<code>vbd <vbd>_iops_read</code>	Read requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> Read IOPs
<code>vbd <vbd>_iops_write</code>	Write requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> Write IOPS
<code>vbd <vbd>_iops_total</code>	I/O requests per second.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> Total IOPS
<code>vbd <vbd>_iowait</code>	Percentage of time waiting for I/O.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> IO Wait
<code>vbd <vbd>_inflight</code>	Number of I/O requests currently in flight.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> Inflight Requests
<code>vbd <vbd>_avgqu_sz</code>	Average I/O queue size.	At least one plugged VBD for non-ISO VDI on the host	Disk <code>vbd</code> Queue Size
<code>vif_<vif>_rx</code>	Bytes per second received on virtual interface number <code>vif</code> . Enabled by default.	VIF <code>vif</code> exists	<code>vif</code> Receive
<code>vif_<vif>_tx</code>	Bytes per second transmitted on virtual interface <code>vif</code> . Enabled by default.	VIF <code>vif</code> exists	<code>vif</code> Send

Metric Name	Description	Condition	XenCenter Name
<code>vif_<vif>_rx_errors</code>	Receive errors per second on virtual interface <code>vif</code> . Enabled by default.	VIF <code>vif</code> exists	<code>vif</code> Receive Errors
<code>vif_<vif>_tx_errors</code>	Transmit errors per second on virtual interface <code>vif</code> . Enabled by default.	VIF <code>vif</code> exists	<code>vif</code> Send Errors

Note:

The value of `<XenCenter-pif-name>` can be any of the following:

NIC <code><pif></code>	If <code><pif></code> contains <code>pif_eth#</code> , where <code>##</code> is 0–9
<code><pif></code>	If <code><pif></code> contains <code>pif_eth#.</code> <code>##</code> or <code>pif_xenbr##</code> or <code>pif_bond##</code>
<code><Internal> Network <pif></code>	If <code><pif></code> contains <code>pif_xapi##</code> , (note that <code><Internal></code> appears as is)
TAP <code><tap></code>	If <code><pif></code> contains <code>pif_tap##</code>
xapi Loopback	If <code><pif></code> contains <code>pif_lo</code>

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 XenServer Tools (paravirtualized drivers) 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 Help 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:

```
1 name_label: cpu0-C1
2 name_description: Proportion of time CPU 0 spent in C-state 1
3 enabled: true
4 standard: true
5 min: 0.000
6 max: 1.000
7 units: Percent
```

Enable a specific metric

Most metrics are enabled and collected by default, to enable those metrics that are not, enter the following:

```
1 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:

```
1 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:

```
1 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:

```
1 xe vm-data-source-list vm=vm_name
```

Use RRDs

XenServer 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 XenServer are:

- AVERAGE
- MIN
- MAX

RRDs exist for individual VMs (including dom0) and the XenServer host. 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 XenServer RRDs, see the [XenServer Software Development Kit Guide](#).

Analyze RRDs using HTTP

You can download RRDs over HTTP from the XenServer host 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.

```
1 wget http://server/host_rrd?session_id=OpaqueRef:SESSION_HANDLE>
```

Download a VM RRD.

```
1 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.

For detailed information on how to use XenServer RRDs with HTTP, see the xenserver.org.

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:

```
1 man rrd2csv
```

Or

```
1 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:

```
1 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 XenServer to generate alerts based on any of the available Host or VM Metrics. In addition, XenServer provides preconfigured alarms 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
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 XenServer host 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 XenServer host 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 the XenCenter help.

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	XenServer 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.

Name	Priority/Severity	Description
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_overcommitted	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.

Name	Priority/Severity	Description
host_sync_data_failed	3	Failed to synchronize XenServer performance statistics.
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:** XenServer expects a newer version but can still connect to the current version
- **XenCenter out of date:** XenCenter is too old to connect to XenServer
- **XenServer out of date:** XenServer is an old version that the current XenCenter cannot connect to
- **License expired alert:** XenServer license has expired
- **Missing IQN alert:** XenServer uses iSCSI storage but the host IQN is blank
- **Duplicate IQN alert:** XenServer 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 XenServer 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`:

```
1 xe vm-param-set uuid=vm_uuid other-config:perfmon=\
2
3 '<config>
4   <variable>
5     <name value="cpu_usage"/>
6     <alarm_trigger_level value="0.5"/>
7   </variable>
8 </config>'
```

Note:

You can use multiple variable nodes.

After setting the new configuration, use the following command to refresh `perfmon` for each host:

```
1 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 alarm will be disabled after an alarm 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 alarm (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 alarm 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_xxxxxxx (where xxxxxxxx is the first eight characters of the SR-UUID).

Note:

SR Throughput: Storage throughput alerts must be configured on the SR rather than the host.
For example:

```

1 xe sr-param-set uuid=sr_uuid other-config:perfmon=\
2 '<config>
3   <variable>
4     <name value="sr_io_throughput_total_per_host"/>
5     <alarm_trigger_level value="0.01"/>
6   </variable>
7 </config>'

```

Generic example configuration

The following example shows a generic configuration:

```

1 <config>
2   <variable>
3     <name value="NAME_CHOSEN_BY_USER"/>
4     <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALARM"/>
5     <alarm_trigger_period value="
6       RAISE_ALARM_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
7     <alarm_priority value="PRIORITY_LEVEL"/>
8     <alarm_trigger_sense value="HIGH_OR_LOW"/>
9     <alarm_auto_inhibit_period value="
10      MINIMUM_TIME_BETWEEN_ALARMS_FROM_THIS_MONITOR"/>
11     <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
12     <rrd_regex value="REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
13   </variable>
14   ...
15 </variable>
16   ...
17 </config>

```

Configure email alerts

You can configure XenServer to send email notifications when XenServer hosts 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:

```
1 xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.bloggs@domain.tld
2 xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.domain.tld[:port]
```

You can also specify the minimum value of the priority (known as 'severity' in XenCenter) field in the message before the email is sent:

```
1 xe pool-param-set uuid=pool_uuid other-config:mail-max-priority=level
```

The default priority level is 4.

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 hostname to the FQDN so this address is used when connecting to your mail server.

To configure performance alert mail language:

```
1 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 XenServer 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:

```
1 root=postmaster
2 authUser=<username>
3 authPass=<password>
4 mailhub=<server address>:<port>
```

Note:

This configuration file is used for all alerts generated by XenServer hosts.

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:

```
1 NAME
2     ssmtp.conf - ssmtp configuration file
3
4 DESCRIPTION
5     ssmtp reads configuration data from /etc/ssmtp/ssmtp.conf The file
6     contains keyword-argument pairs, one per line. Lines starting with '#'
7     and empty lines are interpreted as comments.
8
9     The possible keywords and their meanings are as follows (both are case-
```

```
10 insensitive):
11
12     Root
13     The user that gets all mail for userids less than 1000. If blank,
14     address rewriting is disabled.
15
16     Mailhub
17     The host to send mail to, in the form host | IP_addr port [:
18     port]. The default port is 25.
19
20     RewriteDomain
21     The domain from which mail seems to come. For user authentication.
22
23     Hostname
24     The full qualified name of the host. If not specified, the host
25     is queried for its hostname.
26
27     FromLineOverride
28     Specifies whether the From header of an email, if any, may over
29     -
30     ride the default domain. The default is "no".
31
32     UseTLS
33     Specifies whether smtp uses TLS to talk to the SMTP server.
34     The default is "no".
35
36     UseSTARTTLS
37     Specifies whether smtp does a EHLO/STARTTLS before starting
38     SSL
39     negotiation. See RFC 2487.
40
41     TLSCert
42     The file name of an RSA certificate to use for TLS, if required
43     .
44
45     AuthUser
46     The user name to use for SMTP AUTH. The default is blank, in
47     which case SMTP AUTH is not used.
48
49     AuthPass
50     The password to use for SMTP AUTH.
51
52     AuthMethod
53     The authorization method to use. If unset, plain text is used.
54     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. See the XenCenter Help for more information.

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. See the XenCenter Help for more information.

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

October 4, 2018

This section provides an overview of how to create Virtual Machines (VMs) using templates. It also explains other preparation methods, including physical to virtual conversion (P2V), 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](#).

XenServer supports guests with any combination of IPv4 or IPv6 configured addresses.

Types of virtual machines

In XenServer VMs can operate in one of two modes:

- Paravirtualized (PV): The virtual machine kernel uses specific code which is aware it is running on a hypervisor for managing devices and memory.
- Fully virtualized (HVM): 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. XenServer 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. XenServer 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 XenServer can be used in newer versions of XenServer. However, templates created in newer versions of XenServer are not compatible with older versions of XenServer. If you created a VM template by using XenServer 7.6, 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.

Physical-to-virtual conversion

Physical to Virtual Conversion (P2V) is the process that converts an existing Windows operating system on a physical server to a virtualized instance of itself. The conversion includes the file system, configuration, and so on. This virtualized instance is then transferred, instantiated, and started as a VM on the XenServer host.

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.

XenServer 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 XenServer host that is in another resource pool.

For details and procedures on importing and exporting VMs, see [Importing and Exporting VMs](#).

XenServer Tools

XenServer Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer Tools consists of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. Install XenServer Tools on each Windows VM for that VM to have a fully supported configuration, and to be able to use the xe CLI or XenCenter. The version of XenServer Tools installed on the VM must be the same as the latest available version installed on the XenServer host. For example, some hotfixes include an updated XenServer Tools ISO that updates the version installed on the host.

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 XenServer product family software. While installing of a Windows operating system, XenServer uses traditional device emulation to present a standard IDE controller and a standard network card to the VM. This emulation allows Windows to install by using 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. These functions include quiesced snapshots.

You must install XenServer Tools on each Windows VM for the VM to have a fully supported configuration. The version of XenServer Tools installed on the VM must be the same as the version installed on the XenServer host. A VM functions without the XenServer Tools, but performance is hampered when the I/O drivers (PV drivers) are not installed. You must install XenServer Tools 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 XenMotion or Storage XenMotion)
- Create quiesced snapshots or snapshots with memory (checkpoints), or revert to snapshots
- Adjust the number of vCPUs on a running Linux VM (Windows VMs require a reboot for this change to take effect)

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 XenServer Tools (I/O drivers and the Management Agent) 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. Click the **Install I/O drivers and Management Agent** link to install the I/O drivers from the XenServer Tools ISO.

Note:

I/O drivers are automatically installed on a Windows VM that can receive updates from Windows Update. For more information, see [Updating XenServer Tools](#).

Management Agent installed (not installed): This field displays whether or not the Management Agent is installed on the VM. Click the **Install I/O drivers and Management Agent** link to install the Management Agent from the XenServer Tools ISO.

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 installer on the XenServer Tools ISO.

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. Click the link to install XenServer Tools. For Linux VMs, clicking the status link switches to the VM's console and loads the XenServer Tools ISO. You can then mount the ISO and manually run the installation, as described in [Installing XenServer Tools](#).

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 XenServer product family.

XenServer product family virtual device support

The current version of the XenServer 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 XenServer [Hardware Compatibility List](#).

VM block devices

In the para-virtualized (PV) Linux case, block devices are passed through as PV devices. XenServer does not attempt to emulate SCSI or IDE, but instead provides a more suitable interface in the virtual environment. This interface is in the form of `xvd*` devices. It is also sometimes possible to get an `sd*` device using the same mechanism, where the PV driver inside the VM takes over the SCSI device namespace. This behavior is not desirable so it is best to use `xvd*` where possible for PV guests. The `xvd*` devices are the default for Debian and RHEL.

For Windows or other fully virtualized guests, XenServer emulates an IDE bus in the form of an `hd*` device. When using Windows, installing the XenServer Tools installs a special I/O driver that works in a similar way to Linux, except in a fully virtualized environment.

Windows VMs

November 13, 2018

Installing Windows VMs on the XenServer host 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. Installing the Windows operating system
3. Installing the XenServer Tools (*I/O drivers and the Management Agent*)

Warning:

Citrix only support Windows VMs when the VMs have the XenServer Tools installed. For more information, see XenServer Tools.

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.

Note:

VM templates for Windows XP, Windows Server 2003, and Windows Vista do not exist in XenServer 7.6. If you want to create a VM with one of these Windows versions, use the 'Legacy Windows' template. Run `xenlegacy.exe` from the XenServer Tools ISO to install XenServer Tools on such VMs.

This advice reflects Microsoft's decision to end extended support for these guests. If a support incident concerning Windows XP or Windows Server 2003 requires escalation, you are asked to upgrade to a supported guest operating system. Technical workarounds might be limited or not possible for customers on unsupported guest operating systems.

The available Windows templates are listed below:

Template Name	Description
Citrix XenApp on Windows Server 2008 (32-bit)	Used to install Windows Server 2008 SP2 (32-bit). All editions are supported. This template is specially tuned to optimize Citrix XenApp performance.
Citrix XenApp on Windows Server 2008 (64-bit)	Used to install Windows Server 2008 SP2 (64-bit). All editions are supported. This template is specially tuned to optimize Citrix XenApp performance.
Citrix XenApp on Windows Server 2008 R2 (64-bit)	Used to install Windows Server 2008 R2 and Windows Server 2008 R2 SP1 (64-bit). All editions are supported. This template is specially tuned to optimize Citrix XenApp performance.

Template Name	Description
Windows 7 (32-bit)	Used to install Windows 7 and Windows 7 SP1 (32-bit).
Windows 7 (64-bit)	Used to install Windows 7 and Windows 7 SP1 (64-bit).
Windows 8.1 (32-bit)	Used to install Windows 8.1 (32-bit). (See note)
Windows 8.1 (64-bit)	Used to install Windows 8.1 (64-bit). (See note)
Windows 10 (32-bit)	Used to install Windows 10.
Windows 10 (64-bit)	Used to install Windows 10 (64-bit).
Windows Server 2008 (32-bit)	Used to install Windows Server 2008 SP2 (32-bit). All editions are supported.
Windows Server 2008 (64-bit)	Used to install Windows Server 2008 SP2 (64-bit). All editions are supported.
Windows Server 2008 R2 (64-bit)	Used to install Windows Server 2008 R2 and Windows Server 2008 R2 SP1 (64-bit). All editions are supported.
Windows Server 2012 (64-bit)	Used to install Windows Server 2012 (64-bit).
Windows Server 2012 R2 (64-bit)	Used to install Windows Server 2012 R2 (64-bit).
Windows Server 2016 (64-bit)	Used to install Windows Server 2016 or Windows Server Core 2016 (64-bit)

Note:

Windows 8 is no longer supported. Users who install Windows 8 are upgraded to Windows 8.1.

Warning:

Experimental guest operating systems have received limited testing, might not be present in future product releases, and must not be enabled on production systems. Citrix may not respond to support requests regarding experimental features.

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 XenServer host, 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.

Create a VM by using XenCenter

Note:

The following procedure provides an example of creating Windows 7 (32-bit) VM. The default values may vary depending on the operating system that you choose.

**** To create a Windows 7 (32-bit) 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 XenServer 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.

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.

- a) Choose the default installation source option (DVD drive)
- b) Insert the disk into the DVD drive of the XenServer host
- c) Choose **Next** to proceed.

XenServer 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. 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, XenServer 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, WLB nominates the best server for the VM by analyzing XenServer resource pool metrics and by recommending optimizations.
- If a VM has a virtual GPU 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.

6. 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 may also choose to modify the defaults. Click **Next** to continue.
7. Assign a virtual GPU. The New VM wizard prompts you to assign a dedicated GPU or a virtual GPU 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.
8. 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**.

9. 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**.

10. 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.

11. Follow the OS installation screens and make your selections.

12. After the OS installation completes and the VM reboots, install the XenServer Tools.

Install XenServer Tools

XenServer has a simpler mechanism to install and update XenServer Tools (I/O drivers and the Management Agent) on Windows VMs.

XenServer Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer Tools consists of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. XenServer Tools must be installed on each Windows VM in order for the VM to have a fully supported configuration. A VM functions without them, but performance is significantly hampered.

Note:

To install XenServer Tools on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.

To install XenServer Tools:

1. Select the VM in the **Resources** pane, right-click, and then click **Install XenServer Tools** on the shortcut menu. Alternatively, on the **VM** menu, click **Install XenServer Tools**, or on the **General** tab of the VM, click **Install I/O drivers and Management Agent**.

Note:

When you install XenServer Tools on your VM, you are installing both I/O drivers (PV drivers) and the Management Agent.

2. If AutoPlay is enabled for the VM's CD/DVD drive, installation will start automatically after a few moments. The process installs the I/O drivers and the Management Agent. Restart the VM when prompted to get your VM to an optimized state.
3. If AutoPlay is not enabled, click **Install XenServer Tools** to continue with the installation. This action mounts the XenServer Tools ISO (`guest-tools.iso`) on the VM's CD/DVD drive.

When prompted, select one of the following options to choose what happens with the XenServer Tools ISO:

- Click **Run Setup.exe** to begin the XenServer Tools installation. This action opens the **XenServer Windows Management Agent Setup** wizard. Follow the instructions on the wizard to get your VM to an optimized state and perform any actions that are required to complete the installation process. When you install XenServer Tools using this method, the Management Agent is configured to get updates automatically. However, the management agent update mechanism does not automatically update the I/O drivers. This behavior is the default. If you prefer to change the default behavior, install XenServer Tools using the following method:

- Click **Open folders to view files** and then run `Setup.exe` from the CD Drive. This option opens the **XenServer Windows Management Agent Setup** wizard and lets you customize the XenServer Tools installation and the Management Agent update settings.
- 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 **XenServer Windows Management Agent Setup** wizard displays the default 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**.

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 XenServer Tools installation process.
- When prompted, perform any actions that are required to complete the installation process and click **Finish** to exit the wizard.

Note:

I/O drivers are automatically installed on a Windows VM that can receive updates from Windows Update. However, we recommend that you install the XenServer Tools package to install the Management Agent, and to maintain supported configuration.

To install the I/O drivers and the Management Agent on many Windows VMs, install `managementagentx86.msi` or `managementagentx64.msi` using your preferred MSI installation tool. These files can be found on the XenServer Tools ISO.

Customers who install the XenServer Tools or the Management Agent through RDP may 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 XenServer Tools silently and to prevent the system from rebooting, run one of the following commands:

```
1 Msiexec.exe /package managementagentx86.msi /quiet /norestart
2 Msiexec.exe /package managementagentx64.msi /quiet /norestart
```

Or

```
1 Setup.exe /quiet /norestart
```

A non-interactive, but non-silent installation can be obtained by running:

```
1 Msiexec.exe managementagentx86.msi /passive
2 Msiexec.exe managementagentx64.msi /passive
```

Or

```
1 Setup.exe /passive
```

For interactive, silent, and passive installations, following the next system restart there might be several automated reboots before the XenServer Tools 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 XenServer Tools are installed by default in the `C:\Program Files\Citrix\XenTools` directory on the VM.

Notes:

- To install XenServer Tools 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 XenServer Tools can cause the friendly name and identifier of some network adapters to change. Any software which is configured to use a particular adapter may have to be reconfigured following XenServer Tools 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:

```
1 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:

```
1 xe-mount-iso-sr path_to_iso_sr
```

3. List all of the available ISOs:

```
1 xe cd-list
```

4. Insert the specified ISO into the virtual CD drive of the specified VM:

```
1 xe vm-cd-add vm=vm_name cd-name=iso_name device=3
```

5. Start the VM and install the operating system:

```
1 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 and reinstalling XenServer Tools.

Upgrades to VMs are typically required when moving to a newer version of XenServer. Note the following limitations when upgrading your VMs to a newer version of XenServer:

- Before migrating Windows VMs using XenMotion, you must upgrade the XenServer Tools on each VM.
- Suspend/Resume operation is not supported on Windows VMs until the XenServer Tools are upgraded.
- The use of certain antivirus and firewall applications can crash Windows VMs, unless the XenServer Tools are upgraded.

Warning:

Before updating Windows operating systems, uninstall the XenServer Tools. If they are present during the attempt to update, the update fails.

Windows installation disks typically provide an upgrade option when you boot them on a server which has an earlier version of Windows already installed.

You can update the operating system of Windows VMs in a similar way.

To uninstall the XenServer Tools:

1. From the **Start** button, select **Control Panel**.
2. Select **Programs**, and then select **Programs and Features**.
3. Select all of the following items (the list depends on your operating system and the version of XenServer Tools installed on your VM):
 - XenServer Windows Management Agent
 - Citrix Tools for Virtual Machines
 - XenServer Tools Installer
 - XenServer Windows Guest Agent
 - XenServer Xen Windows x64 PV Drivers
 - XenServer Xen Windows x86 PV Drivers
 - XenServer VSS Provider
4. Select **Uninstall**.

This choice removes the XenServer Tools. When the operation completes, a message is displayed. Click **OK** to close the message box.

After the operating system update is complete, reinstall the XenServer Tools just as you would after installing a fresh Windows VM.

Reinstall XenServer Tools

The XenServer Tools are available in XenCenter on the built-in `guest-tools.iso`. On the **VM** menu, select **Install XenServer Tools**. This option attaches the CD image containing the XenServer Tools to the VM.

If AutoPlay is enabled for the VM's CD/DVD drive, installation will start automatically after a few moments. The process installs the I/O drivers and the Management Agent. Restart the VM when prompted to get your VM to an optimized state.

If AutoPlay is not enabled, the XenServer Tools installer displays the installation options. Click **Install XenServer Tools** to continue with the installation. This option mounts the XenServer Tools ISO (`guest-tools.iso`) on the VM's CD/DVD drive. Click **Run setup.exe** to begin XenServer Tools installation and restart the VM when prompted to get your VM to an optimized state.

Update XenServer Tools

XenServer 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.

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.

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 XenServer 7.6 Enterprise Edition, or have access to XenServer through Citrix Virtual Apps and Desktops entitlement.
- You have created a Windows VM using XenCenter issued with XenServer 7.6

Important: VMs imported from earlier versions of XenServer **are not** capable of receiving I/O drivers from Windows Update.

- 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 2016 does not support using Windows Update to install or update the I/O drivers. Instead use the installer on the XenServer Tools ISO.

Note:

Customers can also receive I/O driver updates automatically through the automatic Management Agent update mechanism. You can configure this setting during XenServer Tools installation. For more information, see *Installing XenServer Tools*.

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

XenServer enables you to update the Management Agent automatically on both new and existing Windows VMs. By default, XenServer 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 XenServer Tools 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 XenServer 7.6 Enterprise Edition, or have access to XenServer through Citrix Virtual Apps and Desktops entitlement.
- You have installed XenServer Tools issued with XenServer 7.0 or higher
- The Windows VM has access to the Internet

Important:

Updates to XenServer Tools can also be issued through the standard XenServer update (hotfix) mechanism. Such hotfixes contain updates to both I/O drivers and the Management Agent. There is no licensing restriction to update XenServer Tools issued as a hotfix.

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

XenServer enables you to use command line to manage the automatic updating of the I/O drivers and the Management Agent. You can run `setup.exe` or `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 XenServer Tools using `setup.exe` or `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 as non-persistent.

Argument	Values	Description
ALLOWAUTOUPDATE	YES/NO	Allow/disallow auto updating of the Management Agent
ALLOWDRIVERINSTALL	YES/NO	Allow/disallow the XenServer Tools 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:

```
1 setup.exe /passive /forcerestart ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
2 ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Or

```
1 msixexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES  
  ALLOWDRIVERINSTALL=NO \  
2 ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Redirect the Management Agent updates

XenServer 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:

1. Download the TSV file from <https://pvupdates.vmd.citrix.com/updates.latest.tsv>.
2. Download the Management Agent MSI files referenced in the TSV file.
3. Upload the MSI files to an internal web server that your VMs can access.
4. Update the TSV file to point to the MSI files on the internal web server.
5. Upload the TSV 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

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url  
  /d \  
2 url of the .tsv 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 .tsv 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:


```
1 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:

```
1 xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=  
   false
```

Modify the automatic I/O driver update settings

During XenServer Tools 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 XenServer Tools installation process, perform the following steps:

1. On the VM, open a command prompt as an administrator.
2. Run the following command:

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v \  
   \  
2 InstallDrivers /d YES/NO
```

To send anonymous usage information to Citrix:

During XenServer Tools 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 XenServer Tools installation process, perform the following steps:

1. On the VM, open a command prompt as an administrator.
2. Run the following command:

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \  
2 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 located 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 XenServer Tools.
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 XenServer. 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 XenServer Tools 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 XenServer Tools.

- 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 may 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 may 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 in 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 1 Gbps in Windows VMs. This speed is a hardcoded value and is not relevant in a virtual environment because the virtual NIC is connected to a virtual switch. The data rate is not limited by the advertised network speed.

Windows 7

Microsoft only supports the use of Windows 7 when Service Pack 1 is installed. For a Windows 7 VM to be supported on XenServer, ensure that SP1 or later is installed.

Windows 8

We no longer support Windows 8 guests. If you install a Windows 8 VM, it is upgraded to Windows 8.1.

Windows Server 2008 R2

Microsoft only supports the use of Windows Server 2008 R2 when Service Pack 1 is installed. For a Windows Server 2008 R2 VM to be supported on XenServer, ensure that SP1 or later is installed.

Linux VMs

April 17, 2019

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 Citrix 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 XenServer, 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 XenServer Tools immediately after installing the operating system. For more information, see [Install the Linux Guest Agent](#). For some operating systems, the XenServer Tools include a kernel specific to XenServer, which replaces the kernel provided by the vendor. Other operating systems, such as RHEL 5.x require you to install a specific version of a vendor-provided kernel.

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 XenServer Tools (recommended).
4. Configure the correct time and time zone on the VM and VNC as you would in a normal non-virtual environment.

XenServer supports the installation of many Linux distributions as VMs. There are three installation mechanisms:

- Installing from an internet repository
- Installing from a physical CD
- Installing from an ISO library

Warning:

The **Other install media** template is for advanced users who want to attempt to install VMs running unsupported operating systems. XenServer 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.

VMs created using the **Other install media** template are created as HVM guests. This behavior might mean that some Linux VMs use slower emulated devices rather than the higher perfor-

manage I/O drivers.

For information regarding specific Linux distributions, see Installation notes for Linux distributions.

PV Linux distributions

The supported PV Linux distributions are:

- Debian Squeeze 6 (32-/64-bit)
- Debian Wheezy 7 (32-/64-bit)
- Red Hat Enterprise Linux 5.x (32-/64-bit)
Supported provided you use the 5.4 or later kernel.
- Red Hat Enterprise Linux 6.x (32-/64-bit)
- CentOS 5.x (32-/64-bit)
- CentOS 6.x (32-/64-bit)
- Oracle Linux 5.x (32-/64-bit)
- Oracle Linux 6.x (32-/64-bit)
- Scientific Linux 6.6–6.9 (32-/64-bit)
- SUSE Linux Enterprise Server 11 SP3, SP4 (32-/64-bit)
- SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64-bit)
- SUSE Linux Enterprise Desktop 11 SP3 (64-bit)
- SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64-bit)
- Ubuntu 12.04 (32-/64-bit)
- NeoKylin Linux Advanced Server 6.5 (64-bit)
- Asianux Server 4.2 (64-bit)
- Asianux Server 4.4 (64-bit)
- Asianux Server 4.5 (64-bit)
- GreatTurbo Enterprise Server 12.2 (64-bit)
- NeoKylin Linux Security OS V5.0 (64-bit)

Other PV 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.

Notes:

- Running 32-bit PV Linux VMs on a host that has more than 128 GB of memory is not supported.
- XenServer hardware security features can reduce the overall performance of 32-bit PV VMs. If this issue impacts you, you can do one of the following things:
 - Run a 64-bit version of the PV Linux VM
 - Boot Xen with the `no-smep no-smap` option.

We do not recommend this option as it can reduce the depth of security of the host

HVM Linux distributions

These VMs can take advantage of the x86 virtual container technologies in newer processors for improved performance. Network and storage access from these guests still operate in PV mode, using drivers built-in to the kernels.

The supported HVM Linux distributions are:

- Debian Jessie 8 (32-/64-bit)
- Debian Stretch 9 (32-/64-bit)
- Red Hat Enterprise Linux 7.x (64-bit)
- CentOS 7.x (64-bit)
- Oracle Enterprise Linux 7.x (64-bit)
- Scientific Linux 7.x (64-bit)
- SUSE Linux Enterprise Server 12 SP3 (64-bit)
- SUSE Linux Enterprise Desktop 12 SP3 (64-bit)
- Ubuntu 14.04 (32-/64-bit)
- Ubuntu 16.04 (32-/64-bit)
- Ubuntu 18.04 (64-bit)
- CoreOS Stable (64-bit)
- Linx Linux V6.0 (64-bit)
- Linx Linux V8.0 (64-bit)
- Yinhe Kylin 4.0 (64-bit)

Other HVM 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 by installing from an internet repository

This section shows the xe CLI procedure for creating a Linux VM, using a Debian Squeeze example, by installing the OS from an internet repository.

1. Create a VM from the Debian Squeeze template. The UUID of the VM is returned:

```
1 xe vm-install template=template-name new-name-label=squeeze-vm
```

2. Specify the installation repository. This repository is a Debian mirror with the packages required to install the base system and the extra that you select during the Debian installer:

```
1 xe vm-param-set uuid=UUID other-config:install-repository=
  path_to_repository
```

An example of a valid repository path is <http://ftp.xx.debian.org/debian> where *xx* is your country code (see the Debian mirror list for a list of these codes). For multiple installations Citrix recommends using a local mirror or apt proxy to avoid generating excessive network traffic or load on the central repositories.

Note:

The Debian installer supports only HTTP and FTP apt repos. NFS is not supported.

3. Find the UUID of the network that you want to connect to. For example, if it is the one attached to *xenbr0*:

```
1 xe network-list bridge=xenbr0 --minimal
```

4. Create a VIF to connect the new VM to this network:

```
1 xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random
  device=0
```

5. Start the VM. It boots straight into the Debian installer:

```
1 xe vm-start uuid=UUID
```

6. Follow the Debian Installer procedure to install the VM in the configuration you require.
7. Install the guest agent and configure graphical display. For more information, see [Install the Linux Guest Agent](#).

Create a Linux VM by installing from a physical CD or DVD

This section shows the CLI procedure for creating a Linux VM, using a Debian Squeeze example, by installing the OS from a physical CD/DVD.

1. Create a VM from the Debian Squeeze template. The UUID of the VM is returned:

```
1 xe vm-install template=template-name new-name-label=vm-name
```

2. Get the UUID of the root disk of the new VM:

```
1 xe vbd-list vm-uuid=vm_uuid userdevice=0 params=uuid --minimal
```

3. Using the UUID returned, set the root disk not to be bootable:

```
1 xe vbd-param-set uuid=root_disk_uuid bootable=false
```

4. Get the name of the physical CD drive on the XenServer host:

```
1 xe cd-list
```

The result of this command gives you something like SCSI 0:0:0:0 for the `name-label` field.

5. Add a virtual CD-ROM to the new VM using the XenServer host CD drive `name-label` parameter as the `cd-name` parameter:

```
1 xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label" device=3
```

6. Get the UUID of the VBD corresponding to the new virtual CD drive:

```
1 xe vbd-list vm-uuid=vm_uuid type=CD params=uuid --minimal
```

7. Make the VBD of the virtual CD bootable:

```
1 xe vbd-param-set uuid=cd_drive_uuid bootable=true
```

8. Set the install repository of the VM to be the CD drive:

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=cdrom
```

9. Insert the Debian Squeeze installation CD into the CD drive on the XenServer host.
10. Open a console to the VM with XenCenter or an SSH terminal and follow the steps to perform the OS installation.
11. Start the VM. It boots straight into the Debian installer:

```
1 xe vm-start uuid=UUID
```

12. Install the guest utilities and configure graphical display. For more information, see [Install the Linux Guest Agent](#).

Create a Linux VM by installing from an ISO image

This section shows the CLI procedure for creating a Linux VM, by installing the OS from network-accessible ISO.

1. Run the command

```
1 xe vm-install template=template new-name-label=name_for_vm sr-uuid  
=storage_repository_uuid
```

This command returns the UUID of the new VM.

2. Find the UUID of the network that you want to connect to. For example, if it is the one attached to *xenbr0*:

```
1 xe network-list bridge=xenbr0 --minimal
```

3. Create a VIF to connect the new VM to this network:

```
1 xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random  
device=0
```

4. Set the `install-repository` key of the `other-config` parameter to the path of your network repository. For example, to use http://mirror.centos.org/centos/6/os/x86_64 as the URL of the vendor media:

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=http:  
//mirror.centos.org/centos/6/os/x86_64
```

5. Start the VM

```
1 xe vm-start uuid=vm_uuid
```

6. Connect to the VM console using XenCenter or VNC and perform the OS installation.

Network installation notes

The XenServer guest installer allows you to install an operating system from a network-accessible ISO image onto a VM. To prepare for installing from an ISO, make an exploded network repository of your vendor media (*not* ISO images). Export it over NFS, HTTP, or FTP so that it is accessible to the XenServer host administration interface.

The network repository must be accessible from the control domain of the XenServer host, normally using the management interface. The URL must point to the base of the CD/DVD image on the network server, and be of the form:

- **HTTP:** `http://<server>/<path>`
- **FTP:** `ftp://<server>/<path>`
- **NFS:** `nfs://<server>/<path>`
- **NFS:** `nfs:<server>/<path>`

See your vendor installation instructions for information about how to prepare for a network-based installation, such as where to unpack the ISO.

Note:

When using the NFS installation method from XenCenter, always use the `nfs://` style of path.

When creating VMs from templates, the XenCenter **New VM** wizard prompts you for the repository URL. When using the CLI, install the template as normal using `vm-install` and then set the `other-config:install-repository` parameter to the value of the URL. When the VM is then started, it begins the network installation process.

Warning:

When installing a new Linux-based VM, it is important to complete the installation and reboot it before performing any other operations on it. This process is analogous to not interrupting a Windows installation – which would leave you with a non-functional VM.

Advanced operating system boot parameters

When creating a VM, you can specify advanced operating system boot parameters using XenCenter or the xe CLI. Specifying advanced parameters can be helpful when you are, for example, configuring automated installations of paravirtualized guests. For example, you might use a Debian preseed or RHEL kickstart file as follows.

To install Debian by using a preseed file:

1. Create a preseed file. For information on creating preseed files, see the Debian documentation for details.
2. Set the kernel command-line correctly for the VM before starting it. Use the New VM wizard in XenCenter or execute an xe CLI command like the following:

```
1 xe vm-param-set uuid=uuid PV-args=preseed_arguments
```

To install RHEL by using a Kickstart File:**Note:**

A Red Hat Kickstart file is an automated installation method, similar to an answer file, you can use to provide responses to the RHEL installation prompts. To create this file, install RHEL manually.

The kickstart file is located in `/root/anaconda-ks.cfg`.

1. In XenCenter, choose the appropriate RHEL template.
2. Specify the kickstart file to use as a kernel command-line argument in the XenCenter New VM Wizard. Specify this value exactly as it would be specified in the PXE config file. For example:

```
1 ks=http://server/path ksdevice=eth0
```

3. On the command line, use `vm-param-set` to set the `PV-args` parameter to use a Kickstart file

```
1 xe vm-param-set uuid=vm_uuid PV-args="ks=http://server/path
ksdevice=eth0"
```

4. Set the repository location so XenServer knows where to get the kernel and `initrd` from for the installer boot:

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=http:
//server/path
```

Note:

To install using a kickstart file without the **New VM** wizard, you can add the appropriate argument to the **Advanced OS boot parameters** text box.

Install the Linux guest agent

Although all supported Linux distributions are natively paravirtualized (and don't need special drivers for full performance), XenServer includes 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 XenServer host. For more information, see [Update Linux kernels and guest utilities](#).

To install the guest agent:

1. The files required are present on the built-in `guest-tools.iso` CD image, or alternatively can be installed by selecting **VM** and then **Install XenServer Tools** option in XenCenter.
2. Mount the image onto the guest by running the command:

```
1 mount -o ro,exec /dev/disk/by-label/XenServer Tools /mnt
```

Note:

If mounting the image fails, you can locate the image by running the following:

```
1 blkid -t LABEL="XenServer Tools"
```

3. Execute the installation script as the root user:

```
1 /mnt/Linux/install.sh
```

4. Unmount the image from the guest by running the command:

```
1 umount /mnt
```

5. If the kernel has been upgraded, or the VM was upgraded from a previous version, reboot the VM now.

Note:

CD-ROM drives and ISOs attached to Linux Virtual Machines appear as devices, such as `/dev/xvdd` or `/dev/sdd`, instead of as `/dev/cdrom` as you might expect. This behavior is because they are not true CD-ROM devices, but normal devices. When you use either XenCenter or the CLI to eject the CD, it hot-unplugs the device from the VM and the device disappears. In Windows VMs, the behavior is different and the CD remains in the VM in an empty state.

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.

CentOS 5.x (32-/64-bit)

For a CentOS 5.x VM, ensure that the operating system uses the CentOS 5.4 kernel or later, which is available from the distribution vendor. Enterprise Linux kernel versions earlier than 5.4 contain issues that prevent XenServer VMs from running properly. Upgrade the kernel using the vendor's normal kernel upgrade procedure.

Red Hat Enterprise Linux 5.x (32-/64-bit)

For RHEL 5.x VMs, ensure that the operating system uses the RHEL 5.4 kernel (2.6.18-164.el5) or later, which is available from the distribution vendor.

Enterprise Linux kernel versions earlier than 5.4 contain issues that prevent XenServer VMs from running properly. Upgrade the kernel using the vendor's normal kernel upgrade procedure.

Red Hat Enterprise Linux* 7.x (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 XenServer, 1 GB RAM is sufficient.

Note:

This information applies to both Red Hat and Red Hat derivatives.

Oracle Linux 5.x (32-/64-bit)

For an OEL 5.x VM, ensure that the operating system uses the OEL 5.4 kernel or later, which is available from the distribution vendor. Enterprise

Linux kernel versions before 5.4 contain issues that prevent XenServer VMs from running properly. Upgrade the kernel using the vendor's normal kernel upgrade procedure.

For OEL 5.6 64-bit, the Unbreakable Enterprise Kernel (UEK) does not support the Xen platform. If you attempt to use UEK with this operating system, the kernel fails to boot properly.

Oracle Linux 6.9 (64-bit)

For OEL 6.9 VMs with more than 2 GB memory, set the boot parameter `crashkernel=no` to disable the crash kernel. The VM reboots successfully only when this parameter is set. If you use an earlier version of OEL 6.x, set this boot parameter before updating to OEL 6.9.

To set the parameter by using XenCenter, add it to the **Advanced OS boot parameters** field in the **Installation Media** page of the **New VM** wizard.

To modify an existing VM by using XenCenter, right-click on the VM and select **Properties > Boot Options > OS boot parameters**.

Debian 6.0 (Squeeze) (32-/64-bit)

When a private mirror is specified in XenCenter, this mirror is only used to retrieve the installer kernel. When the installer is running, you must enter again the address of the mirror to be used for package retrieval.

Debian 7 (Wheezy) (32-/64-bit)

When a private mirror is specified in XenCenter, this mirror is only used to retrieve the installer kernel. When the installer is running, you must enter again the address of the mirror to be used for package retrieval.

Asianux Server 4.5

Installation must be performed with a graphical installer. In the **Installation Media** tab, add “VNC” in the **Advanced OS boot parameters** field.

Linux Linux V6.0

Supports up to 6 vCPUs. To add disks to the Linux Linux V6.0 VMs, set the device ID greater than 3 using the following steps:

1. Get the usable device ID:

```
xe vm-param-get param-name=allowed-VBD-devices uuid=<VM uuid>
```

2. Use the ID in the list that is bigger than 3:

```
xe vbd-param-set userdevice=<Device ID> uuid=<VM uuid>
```

Yinhe Kylin 4.0

For guest tools installation, enable root user in the grub menu and install the guest tools as root user.

NeoKylin Linux Security OS V5.0 (64-bit)

By default NeoKylin Linux Security OS 5 (64-bit) disables settings in `/etc/init/control-alt-delete.conf`. Thus, you cannot use the `xe` command or XenCenter to reboot it. To resolve this issue, do one of the following:

- Specify the **force=1** option when running `xe` to reboot VM:

```
xe vm-reboot force=1 uuid=<vm uuid>
```

- Or, click **Force Reboot** button after clicking **Reboot** in XenCenter.
- Or, ensure that the following two lines are enabled in `/etc/init/control-alt-delete.conf` file of the guest OS:
`start on control-alt-delete`
`exec /sbin/shutdown -r now "Control-Alt-Delete pressed"`

By default **Selinux** is enabled in the OS. So, the user cannot log in into the VM through XenCenter. To resolve this issue, do the following:

1. Disable **Selinux** by adding `selinux=0` to **Boot Options** through XenCenter:
2. After accessing the VM, note the IP address of the VM.
3. After obtaining the IP address from the above step, use any third-party software (for example, Xshell) to connect to the VM and remove `selinux=0`.

Note:

You can access VM using XenCenter only if you disable `selinux`.

4. If you don't need access to VM using XenCenter, enable **Selinux** again by removing the options you previously added.

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, XenServer 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 Citrix recommends 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 not 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 `ethn` 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 1. Configure two virtual NICs when installing a VM
2 1. Shut down the VM
3 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 `Linux/install.sh` script from the built-in `guest-tools.iso` CD image (see [Install the Linux Guest Agent](#)).



For `yum`-enabled distributions CentOS 5.x, RHEL 5.x and higher, `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, Citrix recommends that you always rerun `Linux/install.sh`. This script automatically determines if your VM needs any updates and installs if necessary.

### Upgrade to Ubuntu 14.04, RHEL 7, and CentOS 7 guests

To upgrade *existing* Linux guests to versions that operate in **HVM** mode (for example, RHEL 7.x, CentOS 7.x, and Ubuntu 14.04), 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 XenServer host, open a local shell, log on as root, and enter the following command:

```
1 /opt/xensource/bin/pv2hvm vm_name
```

Or

```
1 /opt/xensource/bin/pv2hvm vm_uuid
```

Restart the VM to complete the process.

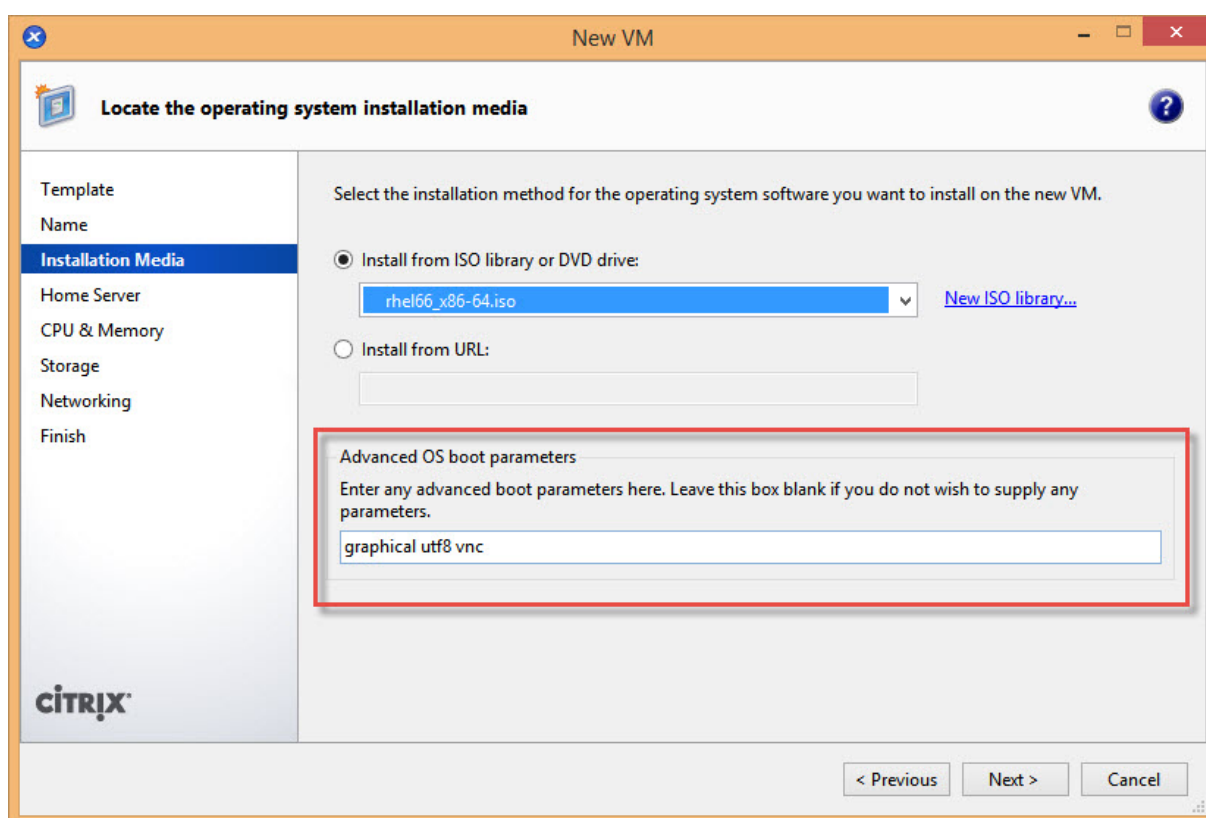
### Linux VM release notes

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:

```
1 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 5

XenServer requires that you run the RHEL 5.4 kernel or higher. Older kernels have the following known issues:

- RHEL 5.0 64-bit guest operating systems with their original kernels fail to boot on XenServer 7.6. Before attempting to upgrade the XenServer host to version 7.6, update the kernel to version 5.4 (2.6.18-164.el5xen) or later. If you run these guests and have already upgraded your host to XenServer 7.6, see [CTX134845](#) for information about upgrading the kernel.
- When resuming a suspended VM, allocations can be made that can cause swap activity that cannot be performed because the swap disk is still being reattached. This occurrence is rare. (Red Hat issue [429102](#)).
- If you are running RHEL 5.3 or 5.4 (32/64-bit), do not use Dynamic Memory Control (DMC) as

this feature can cause the guest to crash. If you want to use DMC, Citrix recommends that you upgrade to more recent versions of RHEL or CentOS. [EXT-54]

- In RHEL 5.3, sometimes when there are many devices attached to a VM, there is not enough time for all of these devices to connect. In this case, startup fails. [EXT-17]
- In RHEL 5.0–5.3, use of the XFS file system can lead to kernel panic under exceptional circumstances. Applying the Red Hat RHEL 5.4 kernel onwards resolves this issue. [EXT-16]
- In RHEL 5.2, 5.3, VMs may crash when a host has 64 GiB RAM or higher configured. Applying the Red Hat RHEL 5.4 kernel onwards resolves this issue. [EXT-30]
- In RHEL 5.0–5.3, the network driver contains an issue that can, in rare circumstances, lead to a kernel deadlock. Applying the Red Hat RHEL 5.4 kernel onwards resolves this issue. [EXT-45]

**Note:**

In previous releases, XenServer included a replacement RHEL 5 kernel that fixed critical issues that prevented RHEL 5 from running effectively as a virtual machine. Red Hat has resolved these issues in RHEL 5.4 and higher. Therefore, XenServer no longer includes a RHEL 5 specific kernel.

**Prepare a RHEL 5 guest for cloning**

To prepare a RHEL 5.x guest for cloning, edit `/etc/sysconfig/network-scripts/ifcfg-eth0` before converting the VM into a template and remove the `HWADDR` line. For more information, see [Prepare to clone a Linux VM](#).

**Note:**

Red Hat recommends the use of Kickstart to perform automated installations, instead of directly cloning disk images (see [Red Hat KB Article 1308](#)).

**Red Hat Enterprise Linux 6****Note:**

Red Hat Enterprise Linux 6.x also includes Red Hat Enterprise Linux Workstation 6.6 (64-bit) and Red Hat Enterprise Linux Client 6.6 (64-bit).

- The RHEL 6.0 kernel has a bug which affects disk I/O on multiple virtualization platforms. This issue causes VMs running RHEL 6.0 to lose interrupts. For more information, see Red Hat issues [681439](#), [603938](#), and [652262](#).
- Attempts to detach a Virtual Disk Image (VDI) from a running a RHEL 6.1 and 6.2 (32-/64-bit) VM, might be unsuccessful. These unsuccessful attempts result in a guest kernel crash with a `NULL pointer dereference at <xyz>` error message. Update the kernel to version 6.3 (2.6.32-238.el6) or later to resolve this issue. For more information, see [Red Hat issue 773219](#).

## **Red Hat Enterprise Linux 7**

After migrating or suspending the VM, RHEL 7.x guests might freeze during resume. For more information, see Red Hat issue [1141249](#).

## **CentOS 5**

For the list of CentOS 5.x release notes, see Red Hat Enterprise Linux 5.

## **CentOS 6**

For the list of CentOS 6.x release notes, see Red Hat Enterprise Linux 6.

## **CentOS 7**

For the list of CentOS 7.x release notes, see Red Hat Enterprise Linux 7.

## **Oracle Linux 5**

For the list of Oracle Linux 5.x release notes, see Red Hat Enterprise Linux 5.

## **Oracle Linux 6**

Oracle Linux 6.x guests installed on a host running versions earlier than v6.5, continue to run the Red Hat kernel following an upgrade to v6.5. To switch to the UEK kernel (the default with a clean installation), delete the `/etc/pygrub/rules.d/oracle-5.6` file in dom0. You can choose which kernel to use for an individual VM by editing the bootloader configuration within the VM.

For OEL 6.9 VMs with more than 2 GB memory, set the boot parameter `crashkernel=no` to disable the crash kernel. The VM only reboots successfully when this parameter is set. If you use an earlier version of OEL 6.x, set this boot parameter before updating to OEL 6.9. For more information, see *Installation notes for Linux distributions*

For the list of Oracle Linux 6.x release notes, see Red Hat Enterprise Linux 6.

## **Oracle Linux 7**

For the list of Oracle Linux 7.x release notes, see Red Hat Enterprise Linux 7.

## Scientific Linux 6

For the list of Scientific Linux 6.x release notes, see Red Hat Enterprise Linux 6.

## Scientific Linux 7

For the list of Scientific Linux 7.x release notes, see Red Hat Enterprise Linux 7.

## SUSE Linux Enterprise 12

SUSE Linux Enterprise 12 VMs are supported in the following modes by default:

PV mode:

- SUSE Linux Enterprise Desktop 12, 12 SP1, and 12 SP2
- SUSE Linux Enterprise Server 12, 12 SP1, and 12 SP2

HVM mode:

- SUSE Linux Enterprise Desktop 12 SP3
- SUSE Linux Enterprise Server 12 SP3

## 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:

```
1 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:

```
1 FORCE_PERSISTENT_NAMES=yes
```

To

```
1 FORCE_PERSISTENT_NAMES=no
```

3. Save the changes and reboot the VM.

For more information, see [Prepare to Clone a Linux VM](#).

## Ubuntu 12.04

Ubuntu 12.04 VMs with original kernel can crash during boot. To work around this issue, you can do one of the following actions:

- Create Ubuntu 12.04 VMs using the latest install media supported by the vendor
- Update an existing VM to the latest version using in-guest update mechanism

## Ubuntu 14.04

Attempts to boot a PV guest can cause the guest to crash with the following error: `kernel BUG at /build/buildd/linux-3.13.0/arch/x86/kernel/paravirt.c:239!`. This error is caused when improperly calling a non-atomic function from interrupt context. Update the linux-image package to version 3.13.0-35.62 to fix this issue. For more information, see Ubuntu Launchpad [1350373](#).

## Configure VM memory

February 27, 2019

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 XenServer 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 Help.

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)?

XenServer 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, XenServer attempts to reclaim memory by automatically reducing the current memory allocation of running VMs within their defined memory ranges. XenServer attempts to reclaim memory even when the server is full.

**Note:**

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. XenServer 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 XenServer 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 XenServer 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. XenServer *guarantees* always to assign each VM memory within its specified DMR when using DMC.

## **The concept of static range**

Many Operating Systems that XenServer supports do not fully ‘understand’ the notion of dynamically adding or deleting memory. As a result, XenServer 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 XenServer. 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 XenServer.

**Note:**

Citrix recommends 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, XenServer 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. XenServer 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. XenServer 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. XenServer 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 XenServer to repartition host memory dynamically in response to changing numbers of guests, or changing host memory pressure. XenServer 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 XenServer takes care of the rest.

## Memory constraints

XenServer allows administrators to use all memory control operations with any guest operating system. However, XenServer enforces the following memory property ordering constraint for all guests:

0 `memory-static-min` `memory-dynamic-min` `memory-dynamic-max` `memory-static-max`

XenServer 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, Citrix supports only certain guest memory configurations for each supported operating system. The range of supported configurations depends on the guest operating system in use. XenServer 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, Citrix advises 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:

```
1 xe vm-list
```

2. Note the uuid, and then run the command `param-name=memory-static`

```
1 xe vm-param-get uuid=uuid param-name=memory-static-{
2 min,max }
```

For example, the following displays the static maximum memory properties for the VM with the uuid beginning ec77:

```
1 xe vm-param-get uuid= \
2 ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
3 param-name=memory-static-max;
4 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:

```
1 xe vm-list
```

2. Note the uuid, and then run the command `param-name=memory-dynamic`:

```
1 xe vm-param-get uuid=uuid param-name=memory-dynamic-{
2 min,max }
```

For example, the following displays the dynamic maximum memory properties for the VM with uuid beginning ec77

```
1 xe vm-param-get uuid= \
2 ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
3 param-name=memory-dynamic-max;
4 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:

```
1 xe vm-memory-static-range-set uuid=uuid min=valuemax=value
```

Update the dynamic memory range of a virtual machine:

```
1 xe vm-memory-dynamic-range-set \
2 uuid=uuid min=value \
3 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. XenServer adjusts the guest's memory allocation to meet the target you specify. For example:

```
1 xe vm-target-set target=value vm=vm-name
```

Update all memory limits (static and dynamic) of a virtual machine:

```
1 xe vm-memory-limits-set \
2 uuid=uuid \
3 static-min=value \
4 dynamic-min=value \
5 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:

Citrix advises not to 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:

```
1 xe vm-list
```

2. Note the uuid, and then use the command `memory-dynamic-{ min,max } =value`

```
1 xe vm-param-set uuid=uuidmemory-dynamic-{
2 min,max }
3 =value
```

The following example changes the dynamic maximum to 128 MB:

```
1 xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-
 dynamic-max=128MiB
```

## Migrate VMs

September 5, 2018

You can migrate running VMs by using *XenMotion* and *Storage XenMotion* and move a VM's Virtual Disk Image (VDI) without any VM downtime.

### XenMotion and Storage XenMotion

The following sections describe the compatibility requirements and limitations of XenMotion and Storage XenMotion.

#### XenMotion

XenMotion is available in all versions of XenServer. This feature enables you to move a running VM from one host to another host, when the VM's disks are on storage shared by both hosts. Pool maintenance features such as high availability and Rolling Pool Upgrade (RPU) can automatically move VMs by using XenMotion. These features allow for workload leveling, infrastructure resilience, and the upgrade of server software, without any VM downtime.

**Note:**

Storage can only be shared between hosts in the same pool. As a result VMs can only be migrated to hosts in the same pool.

Virtual GPU and Intel GVT-g are not compatible with XenMotion, Storage XenMotion, or VM Suspend. However, VMs using GPU Pass-through or vGPU can still be started any host that has the appropriate resources. For information about NVIDIA vGPU compatibility with these features, see [Graphics](#).

**Storage XenMotion****Notes:**

- Do not use Storage XenMotion in Citrix Virtual Desktops deployments.
- Storage XenMotion cannot be used on VMs that have changed block tracking enabled. Disable changed block tracking before attempting Storage XenMotion.
- Storage XenMotion cannot be used on VMs whose VDIs are on a GFS2 SR.

Storage XenMotion additionally allows VMs to be moved from one host to another, where the VMs are not on storage shared between the two hosts. As a result, VMs stored on local storage can be migrated without downtime and VMs can be moved from one pool to another. This feature enables system administrators to:

- Rebalance VMs between XenServer pools (for example from a development environment to a production environment).
- Upgrade and update standalone XenServer hosts without any VM downtime.
- Upgrade XenServer host hardware.

**Note:**

Moving a VM from one host to another preserves the VM *state*. The state information includes information that defines and identifies the VM and the historical performance metrics, such as CPU and network usage.

**Compatibility requirements**

When migrating a VM with XenMotion or Storage XenMotion, VM and the target host must meet the following compatibility requirements for the migration to proceed:

- The target host must have the same or a more recent version of XenServer installed as the source host.

- XenServer Tools must be installed on each Windows VM that you want to migrate. The version of XenServer Tools installed on the VM must be the same as the version installed on the target XenServer host.
- Storage XenMotion only: If the CPUs on the source and target host are different, the target CPU must provide at least the entire feature set as the source CPU. So, it is unlikely to be possible to move a VM between, for example, AMD and Intel processors.
- Storage XenMotion only: VMs with more than one snapshot cannot be migrated.
- VMs with checkpoint cannot be migrated.
- Storage XenMotion only: VMs with more than six attached VDIs cannot be migrated.
- The target host must have sufficient spare memory capacity or be able to free sufficient capacity using Dynamic Memory Control. If there is not enough memory, the migration fails to complete.
- Storage XenMotion only: The target storage must have enough free disk space available for the incoming VMs. The free space required can be three times the VDI size (without snapshots). If there is not enough space, the migration fails to complete.

### Limitations and caveats

XenMotion and Storage XenMotion are subject to the following limitations and caveats:

- VMs using PCI pass-through cannot be migrated.
- VM performance is reduced during migration.
- For Storage XenMotion, pools protected by high availability, disable high availability before attempting VM migration.
- Time to completion of VM migration depends on the memory footprint of the VM and its activity. In addition, the size of the VDI and its storage activity affects VMs being migrated with Storage XenMotion.
- IPv6 Linux VMs require a Linux Kernel greater than 3.0.

### Migrate a VM using XenCenter

1. In the Resources pane, select the VM and do one of the following:
  - To migrate a running or suspended VM using XenMotion or Storage XenMotion, on the **VM** menu, click **Migrate to Server** and then **Migrate VM wizard**. This action opens the **Migrate VM** wizard.
  - To move a stopped VM: On the **VM** menu, select **Move VM**. This action opens the **Move VM** wizard.

2. From the **Destination** list, select a standalone server or a pool.
3. From the **Home Server** list, select a server to assign as the home server for the VM and click **Next**.
4. In the **Storage** tab, specify the storage repository where you would like to place the migrated VM's virtual disks, and then click **Next**.
  - The **Place all migrated virtual disks on the same SR** radio button is selected by default and displays the default shared SR on the destination pool.
  - Click **Place migrated virtual disks onto specified SRs** to specify an SR from the **Storage Repository** list. This option allows you to select different SR for each virtual disk on the migrated VM.
5. From the **Storage network** list, select a network on the destination pool that is used for the live migration of the VM's virtual disks. Click **Next**.

**Note:**

Due to performance reasons, it is recommended that you do not use your management network for live migration.

6. Review the configuration settings and click **Finish** to start migrating the VM.

## 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

- Do not use Storage XenMotion in Citrix Virtual Desktops deployments.
- IPv6 Linux VMs require a Linux Kernel greater than 3.0.
- If you perform live VDI migration on a VM that has a vGPU, vGPU XenMotion is used. The host must have enough vGPU space to make a copy of the vGPU instance on the host. If the pGPUs are fully employed, VDI migration may not be possible.

### To move virtual disks

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.

## Import and export VMs

March 29, 2019

XenServer 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 XenServer 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 XenServer. 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 XenServer XVA format.

When importing and exporting VMs, a temporary VM – the Transfer VM – is used to perform the import/export of OVF/OVA packages and disk images. Configure networking settings for the Transfer VM in the XenCenter Import and Export wizards. For more information, see The Transfer VM.

You can also use the xe CLI to import VMs from and export them to XenServer 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. |
| XenServer 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 <code>.xva</code> .                                                 |
| XenServer XVA Version 1 format           | XVA Version 1 is the original format specific to Xen-based hypervisors. This format packages an individual VM as a single file archive, including a descriptor and disk images. Its file name extension is <code>ova.xml</code> .                 |

### Which format to use?

Consider using OVF/OVA format to:

- Share XenServer 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:

- Share VMs with versions of XenServer earlier than 6.0
- 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. XenServer 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 XenServer host 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, Citrix recommends 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 XenServer, 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, with the extension `.checksum`.

**Important:**

If a VM is exported from the XenServer host and then imported into another XenServer host 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.

**XVA version 1 format**

XVA Version 1 is the original format specific to Xen-based hypervisors. This format packages an individual VM as a single file archive, including a descriptor and disk images. Its file name extension is `ova.xml`.

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 one file for each 1 GB chunk of the disk image. The base name of each file includes the chunk number in decimal. It contains one block of the disk image in raw binary format, compressed with `gzip`.

**Important:**

If a VM is exported from the XenServer host and then imported into another XenServer host with a different CPU type, it might 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 XenServer, you might have to configure the VM before it boots properly on the XenServer host.

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 XenServer. 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 XenServer 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 XenServer 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.

**The Transfer VM**

The Transfer VM is a built-in VM that only runs during the import or export of a virtual disk image. It is used to transfer its contents between the disk image file location and the XenServer storage reposi-

tory.

One Transfer VM runs for each import or export of a disk image. When importing or exporting a virtual appliance with more than one disk image, only one disk image transfers at a time.

Running one Transfer VM has the following requirements:

|                |                                                                                      |
|----------------|--------------------------------------------------------------------------------------|
| Virtual CPU    | 1                                                                                    |
| Virtual Memory | 256 MB                                                                               |
| Storage        | 8 MB                                                                                 |
| Network        | Reachable by the XenServer host; static or dynamic IP address (dynamic, recommended) |

The default transfer protocol is iSCSI. In which case, the Transfer VM requires an iSCSI Initiator on the XenServer host. An alternate transfer protocol is RawVDI.

#### To use the RawVDI transfer protocol:

1. Back up the `XenCenterMain.exe.config` file, which is located in the installation folder.
2. Using a text editor, open the `XenCenterMain.exe.config` file.
3. Add the following section group to the `configSection`:

```

1 <sectionGroup name="applicationSettings"
2 type="System.Configuration.ApplicationSettingsGroup, System,
3 Version=2.0.0.0,
4 Culture=neutral, PublicKeyToken=b77a5c561934e089" >
5 <section name="XenOvfTransport.Properties.Settings"
6 type="System.Configuration.ClientSettingsSection, System,
7 Version=2.0.0.0,
8 Culture=neutral, PublicKeyToken=b77a5c561934e089"
9 requirePermission="false"/>
10 </sectionGroup>

```

4. To the end of the file, add the following section:

```

1 <applicationSettings>
2 <XenOvfTransport.Properties.Settings>
3 <setting name="TransferType" serializeAs="String"> <value>
4 UploadRawVDI</value>
5 </setting>
6 </XenOvfTransport.Properties.Settings>

```

```
6 </applicationSettings>
```

5. Save the `XenCenterMain.exe.config` file.

**Note:**

If XenCenter fails to start properly, then check that the new section group and section were added correctly.

## 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](#).
- It is necessary to configure networking for the Transfer VM used to perform the import process. For more information, see [The Transfer VM](#).

**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 on XenServer](#).

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 :

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 XenServer host.

To select a host or pool, choose from the **Import VM(s)** to list.

To assign each VM a home XenServer host, 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 XenServer, select the **Use Operating System Fixup** check box. Select an ISO SR where the Fixup ISO can be copied so that XenServer can access it. For more information about this feature, see Operating system fixup.

Click **Next** to continue.

9. 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:

```
1 xe vm-param-set uuid=VM uuid platform:device_id=0002
```

2. Set the `platform` parameter to `viridian=true`. For example:

```
1 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 XenServer 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 XenServer host.

To select a host or pool, choose from the **Import VM(s)** to list.

To assign each VM a home XenServer host, 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 XenServer, select the Use Operating System Fixup check box. Select an ISO SR where the Fixup ISO can be copied so that XenServer can access it. For more information about this feature, see Operating system fixup.

Click **Next** to continue.

8. 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 2008 and later, set the `platform` parameter to `device_id=0002`. For example:

```
1 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:

```
1 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`) or XVA Version 1 format (`ova.xml`). 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 XenServer host, enter the following:

```
1 xe vm-import -h hostname -u root -pw password \
2 filename=pathname_of_export_file
```

To import the VM to a different SR on the target XenServer host, add the optional `sr-uuid` parameter:

```
1 xe vm-import -h hostname -u root -pw password \
2 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**:

```
1 xe vm-import -h hostname -u root -pw password \
2 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.

- a) 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.

- b) To add a digital signature to the package, select the **Sign the OVF package** check box, browse to locate a certificate. Enter the private key associated with the certificate in the **Private key password** field.

When a signed package is imported, the user can verify the identity of the creator by using the public key to validate the digital signature. Use an X.509 certificate that you created from a Trusted Authority and exported as either a `.pem` or `.pfx` file. The certificate must contain the signature of the manifest file and the certificate used to create that signature.

- c) 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.
- d) 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. 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. Citrix recommends exporting a VM to a machine other than the XenServer host, 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:

```
1 xe vm-export -h hostname -u root -pw password vm=vm_name \
2 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.

## Bromium Secure Platform

September 6, 2018

XenServer 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

XenServer 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 7 SP1 (32-bit and 64-bit), 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, XenServer does not support and prevents the use of the following features:

- Any form of VM motion (for example: XenMotion, Storage XenMotion).
- 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 XenServer Enterprise Edition or have access to XenServer through Citrix Virtual Apps and Desktops entitlement.

## Configuration

To prepare your XenServer 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:

- a) VM='xe vm-list name-label='vm\_name' -minimal'
- b) `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.

## Container management

September 6, 2018

XenServer includes two new features to enhance deployments of Docker Containers on XenServer

- Support for CoreOS Linux VMs and configuring Cloud Config Drives
- Container Management for CoreOS, Debian 8, Ubuntu 14.04, and RHEL/CentOS/OEL 7
- Preview of Container Management for Windows Server Containers on Windows Server 2016 Technology Preview

CoreOS is a minimalist Linux distribution which has become popular for hosting Docker applications. The CoreOS Cloud Config Drive allows the customization of various operating system configuration options. When Container Management is enabled on a VM, XenServer becomes aware of any Docker containers running in the VM.

### **Note:**

For information on how to install CoreOS guests, configure Cloud-Config parameters, and manage Docker containers, see the XenCenter Help. Press **F1** or click **Help**.

The Container Management Supplemental Pack enables XenServer to take the following actions:

- Query the VMs
- Interact with Cloud Config Drives
- Discover application containers
- Display application containers within XenCenter's Infrastructure view.

XenCenter also enables interaction with the containers to allow for start, stop and pause operations, and other monitoring capabilities. For more information, see Container Management Supplemental Pack.

## What is Docker

Docker is an open platform for developers and system administrators to build, ship, and run distributed applications. A Docker container comprises just the application and its dependencies. It

runs as an isolated process in user space on the host operating system, sharing the kernel and base filesystem with other containers. For more information, see <https://www.docker.com/whatisdocker>.

**Note:**

The XenServer Container Management feature complements, but not does replace the Docker environment. You can use one of the many Docker management tools available to manage individual Docker Engine instances in the VMs.

## Container Management Supplemental Pack

The Container Management Supplemental Pack provides:

**Monitoring and Visibility:** allows you to see which VMs are in use for Docker hosting, and which containers on the VM are running.

**Diagnostics:** access is provided to basic container information such as forwarded network ports, and originating Docker image name. This feature can help accelerate investigations into problems where either the infrastructure and applications layers maybe impacted.

**Performance:** gives insight into which containers are running on that VM. Depending on the information provided by the operating system, it provides information on the processes and applications running on the container, and the CPU resource consumed.

**Control Applications:** enables you to use XenCenter to start, stop, and pause (if supported by the operating system) application containers enabling rapid termination of problematic applications.

**Note:**

XenServer supports installing Supplemental Packs using XenCenter. For information on how to install a supplemental pack using XenCenter, see the XenCenter Help. If you would prefer to install using the xe CLI, see the [XenServer Supplemental Packs and the DDK guide](#).

## Manage Docker containers by using XenCenter

This section contains information on managing your CoreOS VMs using XenCenter. To manage CoreOS VMs, complete the following steps:

1. Install or upgrade your host to XenServer 7.6.
2. Install the XenCenter shipped with XenServer 7.6.
3. Install the Container Management Supplemental pack available from the [Citrix website](#).
4. Create a CoreOS VM and include a config drive for the VM.

When you create a CoreOS VM in XenCenter, the **New VM** wizard prompts you to specify cloud-config parameters for your VM. The config drive provides user data for the VM instance. If you are planning to use XenServer to manage containers running inside the VM, create a config drive.

By default, XenCenter includes a predefined set of parameters on the Cloud-Config Parameters page. You can modify these parameters based on your requirements. For detailed information about supported configuration parameters, see the CoreOS documentation.

**Warning:**

Container Management may not work if you do not create a config drive for the VM.

5. Enable container management for the VM. You can update this setting on the VM's **Properties** tab in XenCenter.

**Note:**

If you migrate a Container Managed VM between pools, Container Management stops working for the VM. This behavior is because Container Management is implemented using a pool-specific key. To enable Container Management functionality again for the VM, update the Cloud Config Drive configuration in the VM preferences.

## Manage containers on other Linux guests

CoreOS VMs that are created with the default Cloud Config Drive configuration are automatically prepared for Container Management. Just only need to enable the feature. Other Linux guests can be prepared manually. This feature is supported for Debian 8, Ubuntu 14.04, and RHEL/CentOS/OEL 7.x VMs only.

To prepare a Linux guest manually:

1. Ensure that the VM has XenServer Tools installed, and that the VM network is configured as described in Network Requirements and Security.
2. Install Docker, Ncat and SSHD inside the VM.

For Ubuntu 14.04: `apt-get install docker.io nmap openssh-server`

For RHEL/CentOS/OEL 7.x: `yum install docker nmap openssh-server`

3. Enable autostart for docker.service:

```
systemctl enable docker.service
```

4. Start docker.service

```
systemctl start docker.service
```

Use a non-root user for container management. Add the user to the 'docker' group to provide access to Docker.

5. Prepare the VM for container management; run the following command on the control domain (dom0) on one of the hosts in the pool:

```
xscontainer-prepare-vm -v vm_uuid -u username
```

Where `vm_uuid` is the VM to be prepared, and `username` is the user name on the VM that the Container Management uses for management access.

The preparation script guides you through the process and automatically enables container management for this VM.

**Note:**

If you migrate a Container Managed VM between pools, Container Management stops working for the VM. This behavior is because Container Management is implemented using a pool-specific key. To enable Container Management functionality again for the VM, run the `xscontainer-prepare-vm` command again on the VM. Even after running this command, the original XenServer pool might keep access to the VM.

## Access the Docker Container console and logs

For Linux VMs, XenCenter enables customers to access the container console and view logs to manage and monitor applications running on Docker containers. To access the container console and logs using XenCenter:

1. Select the container in the **Resources** pane.
2. On the **Container General Properties** section, click **View Console** to view the container console. To see the console logs, click **View Log**. This action opens an SSH client on the machine running XenCenter.
3. When prompted, log into the SSH client using the VM user name and password.

**Note:**

Customers can automate the authentication process by configuring their public/private SSH keys. See the following section for details.

## Automate the authentication process (optional)

When accessing the container console and logs, customers are required to enter the login credentials of the VM to authenticate SSH connections. However, customers can automate the authentication process to avoid entering the credentials manually. Follow the instructions below to configure the automatic authentication process:

1. Generate a public/private key pair.

2. Add the public SSH key to the user directory on the VM running the container.
  - For containers running on a CoreOS VM, add the public key to the **Cloud-Config Parameters** section on the VM's **General** tab in XenCenter.
  - For containers running on Ubuntu 14.04, RHEL/CentOS/Oracle Linux 7, and Debian 8, manually add the public key to `~/.ssh/authorized_keys`.
3. Add the private SSH key to the `%userprofile%` directory on the machine running XenCenter and rename the key as `ContainerManagement.ppk`.

## Manage Windows Server Containers

Windows Server Containers are part of the Windows Server 2016 guest operating system. They allow the encapsulation of Windows applications by isolating processes into their own namespace. XenServer Container Management supports monitoring and managing Windows Server Containers on Windows Server 2016 guest operating systems.

### Note:

Windows Server 2016 VMs must be configured with one or more static IP addresses for TLS communication, as TLS server certificates are bound to certain IP addresses.

To prepare Windows Server Containers for Container Management:

1. Ensure that the VM has XenServer Tools installed, and that the VM network is configured as described in Network Requirements and Security.
2. Install Windows Server Container support inside the VM as described in [Microsoft Documentation](#). Windows Server Containers are not Hyper-V Containers.
3. Create a file called `daemon.json` in the folder `C:\ProgramData\docker\config` with the contents:

```

1 {
2
3 "hosts": ["tcp://0.0.0.0:2376", "npipe://"],
4 "tlsverify": true,
5 "tlscacert": "C:\ProgramData\docker\certs.d\ca.pem",
6 "tlscert": "C:\ProgramData\docker\certs.d\server-cert.pem"
7 ,
8 "tlskey": "C:\ProgramData\docker\certs.d\server-key.pem"
9 }
```

4. Prepare the VM for container management; run one of the following commands on the control domain (dom0) on one of the hosts in the pool:

**Option 1** (for single-user VMs): Have XenServer generate TLS certificates for this VM.

**Important:**

This option is only safe where only a single user has access to the VM. The TLS server and client keys are injected into the VM using a virtual CD. This information can be copied by malicious users during the preparation.

```
1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls --generate-
 certs
```

Where *vm\_uuid* is the VM to be prepared. Follow the on-screen instructions to complete the process of preparing Windows Server Containers. It involves interacting with dom0 and the VM.

**Option 2:** To configure XenServer with externally generated TLS certificates

```
1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls \
2 --client-cert client_cert --client-key client_key --ca-cert
 ca_cert
```

Where *vm\_uuid* is the VM to be prepared, *client\_cert* is the TLS client certificate, *client\_key* is the TLS client key, and *ca\_cert* is the CA certificate. This option assumes that Docker is already configured for TLS inside the VM.

## Network requirements and security

**Important:**

For container management to work, it may be necessary to relax security requirements regarding network isolation.

For maximum security of virtualization environments, Citrix recommends that administrators partition the network by isolating XenServer's management network (with XenServer Control Domain) from the VMs.

Enabling container management requires a route between these two networks, which increases the risk of malicious VMs attacking the management network (that is, dom0). To mitigate the risk of allowing traffic between VM and the management network, we advise the configuration of firewall rules to allow only trusted sources to initiate a connection between the two networks.

Do not use this feature in production in the following cases:

- If this recommended network configuration doesn't match your risk profile
- If you lack the necessary network or firewall expertise to secure this route sufficiently for your specific use-case



## Network partitioning and firewalls

As with other VMs, do not connect container managed VMs directly to XenServer's management network to provide necessary isolation.

For Container Management to work, managed VMs have to be reachable from the XenServer's Control Domain (dom0). To monitor containers on Linux-based operating systems, the networking topology and firewalls must allow outbound SSH connections from dom0 to Container Managed VMs. To monitor Windows Server Containers, the networking topology and firewalls must allow outbound Docker TLS (destination TCP port 2376) connections from dom0 to Container Managed VMs.

To mitigate the risk of allowing traffic between VM and the management network, pass all traffic through an external stateful firewall. This firewall must be manually set up and configured by an expert according to your specific business and security requirement.

The following section contains an example configuration:

To secure connections between the networks:

- Prevent all connections between the XenServer management network (that is including dom0) and the VM network (that is including container managed VMs) either way.

Add exceptions for enabling Container Management:

- To monitor Linux-based operating system, allow dom0 to have outbound SSH (TCP port 22) connections (both NEW and ESTABLISHED) to Container Managed VMs.
- To monitor Windows Server containers, allow dom0 to have outbound Docker TLS (TCP port 2376) connections (both NEW and ESTABLISHED) to Container Managed VMs.
- Allow Container Managed VMs to reply to (ESTABLISHED) SSH and Docker TLS connections initiated by dom0.

## Authentication on Linux-based operating systems

XenServer's Container Management uses a pool-specific 4096-bit private/public RSA-key-pair to authenticate on Container Managed VMs. The private key is stored in the XenServer Control Domain (dom0). The respective public-key is registered in Container Managed VMs during the preparation, either using the Cloud Config Drive or `~user/.ssh/authorized_keys` file. As usual with all private/public key-pairs, the private key must be kept securely, as it allows for password-less access to all Container Managed VMs. This access includes both currently managed VMs and VMs managed in the past.

XenServer's Container Management attempts to reach Container Managed VMs through any of the IP addresses advertised by the XenServer Tools running inside the VM. After an initial connection, XenServer stores the public key of container managed VMs and validates that the key matches on

any subsequent connection. Ensure that only the Container Managed VM can be contacted through its advertised IP (using IP Source Guard or similar means). If the network topology cannot ensure this behavior, Citrix recommends that administrators confirm the SSH hostkey that the Container Management obtained when making the first connection to the VM.

The key can be accessed by using the following command:

```
1 xe vm-param-get-uuid=vm_uuid param-name=other-config /
2 param-key=xscontainer-sshhostkey
```

*vm\_uuid* is the UUID of the VM

## Authentication for Windows Server Containers

XenServer uses SSL or TLS to monitor and control Windows Server Containers. In this instance XenServer acts as the SSL/TLS client, and Windows Server VMs act as the SSL/TLS server. Keys are stored in both Dom0 and the VM.

### Important:

- The client key must be kept securely, as it allows for password-less access to Docker on the VM
- The server key must be kept securely, as it serves to authenticate the monitoring connection to the VM

When XenServer Container Management generates TLS certificates and keys by using the `-generate -certs` option, temporary CA, server, and client certificates are generated for a specific pool and VM. Certificates use sha256 hash and are valid for up to 2\*365 days. After this time, repeat the preparation. The TLS connection is always established using a AES128-SHA cipher.

## Notes

When using XenServer Container Management and Docker, be aware of the following behaviors:

- Renaming a container does not trigger the Container Management view to update. Additionally on Ubuntu 14.04 the pause or unpause of a container from outside XenCenter doesn't trigger the view to update. This behavior can mean that XenServer might not show the current (renamed/-paused/unpaused) container-status. The underlying cause is that the view only gets refreshed following Docker event notifications. As a workaround, the refresh can be triggered by performing an action (that is, start or stop) on an unrelated container on the same VM.

## vApps

September 5, 2018

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**.

See the XenCenter Help for more information. Press **F1** or click **Help** to display the XenCenter Help.

## 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 of 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 of 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

September 5, 2018

Citrix provides a fully functional installation of a Demo Linux Virtual Appliance, based on a CentOS 5.5 distribution.

The appliance is available for download, in a single [xva](#) file from the [XenServer 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 allows you to deploy a VM quickly and simply. You can use this appliance to test XenServer product features such as XenMotion, Dynamic Memory Control, and high availability. XenServer Tools are preinstalled in the Demo Linux Virtual Appliance. The appliance also includes pre-configured networking connectivity and 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 [XenServer Download](#) page.

1 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.

1. In the **Resources** pane, select a host or a Pool, then right-click and select **Import**. The Import Wizard is displayed.
2. Click **Browse** and navigate to the location of the downloaded Demo Linux Virtual Appliance `xva` file on your computer.
3. Click **Next**.
4. Select the target XenServer host or pool, then click **Next**.
5. Select a storage repository on which to create the virtual appliance's disk, then click **Next**.
6. 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 command to send ping packets to Google and back:

```
1 ping -c 10 google.com
```

Other installed networking tools include `ifconfig`, `netstat`, and `tracert`.

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 use 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 help.

## Advanced notes for virtual machines

October 4, 2018

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:

```
1 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:

```
1 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 shut-down/start or reboot.

### Make the ISO library available to XenServer hosts

To make an ISO library available to XenServer hosts, 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:

```
1 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:

```
1 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:

```
1 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.

## Windows Volume Shadow Copy Service (VSS) provider

The Windows tools also include a VSS provider for XenServer that is used to quiesce the guest filesystem in preparation for a VM snapshot. The VSS provider is installed as part of the PV driver installation, but is not enabled by default.

### To enable the Windows XenServer VSS provider:

1. Install the Windows PV drivers.
2. Navigate to the directory where the drivers are installed (by default `c:\Program Files\Citrix\XenTools`, or the value of `HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\Install_dir` in the Windows Registry).
3. Double-click the `install-XenProvider.cmd` command to activate the VSS provider.

#### Notes:

- The VSS provider is automatically uninstalled when the PV drivers are uninstalled. Enable the VSS provider again when it is installed again. They can be uninstalled separately from the PV drivers by using `uninstall-XenProvider.cmd` in the same directory.
- Using VSS snapshots on GFS2 SRs is not supported.

## 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 XenServer 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 XenServer Tools. 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** (Windows 7).
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. Citrix recommends 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. XenServer uses the hardware clock setting of the VM to synchronize the VM. XenServer does not use the system clock setting of the VM.

When performing suspend and resume operations or using XenMotion, ensure that you have up-to-date XenServer Tools installed. XenServer Tools 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

The time handling behavior of Linux VMs in XenServer depends on whether the VM is a PV guest or an HVM guest.

In addition to the behavior defined by XenServer, 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](#).

## Time handling in PV Linux VMs

There are two *wall-clock* behaviors for paravirtualized Linux distributions – *dependent* and *independent*.

**Dependent wall-clock:** The system clocks in PV Linux VMs are synchronized to the clock running on the control domain, and cannot be independently altered. This mode is convenient, as only the control domain has to run the Network Time Protocol (NTP) service to keep accurate time across all VMs.

**Independent wall-clock:** System clocks in PV Linux VMs are **not** synchronized to the clock running on the control domain and can be altered. When the VM starts, the control domain time is used to set the initial time of the system clock.

Some PV Linux VMs can use the `independent_wallclock` setting to change the wall-clock behavior of the VM.

The following table lists wallclock behavior for PV Linux VMs:

| Guest OS                                  | Default wall-clock behavior | Is <code>independent_wallclock</code> setting available? |
|-------------------------------------------|-----------------------------|----------------------------------------------------------|
| CentOS 5.x (32-/64-bit)                   | Dependent                   | Yes                                                      |
| CentOS 6.x (32-/64-bit)                   | Independent                 |                                                          |
| Red Hat Enterprise Linux 5.x (32-/64-bit) | Dependent                   | Yes                                                      |
| Red Hat Enterprise Linux 6.x (32-/64-bit) | Independent                 |                                                          |
| Oracle Linux 5.x (32-/64-bit)             | Dependent                   | Yes                                                      |
| Oracle Linux 6.x (32-/64-bit)             | Independent                 |                                                          |
| Scientific Linux 6.x (32-/64-bit)         | Independent                 |                                                          |
| SLES 11 SP3, SP4 (32-/64-bit)             | Independent                 | Yes (No-op)                                              |
| SLES 12 SP1, SP2 (64-bit)                 | Independent                 | Yes (No-op)                                              |

| Guest OS                                    | Default wall-clock behavior | Is <code>independent_wallclock</code> setting available? |
|---------------------------------------------|-----------------------------|----------------------------------------------------------|
| SLED 11 SP3, SP4 (64-bit)                   | Independent                 | Yes (No-op)                                              |
| SLED 12 SP1, SP2 (64-bit)                   | Independent                 | Yes (No-op)                                              |
| Debian 6 (32-/64-bit)                       | Independent                 |                                                          |
| Debian 7 (32-/64-bit)                       | Independent                 |                                                          |
| Ubuntu 12.04 (32-/64-bit)                   | Independent                 |                                                          |
| NeoKylin Linux Advanced Server 6.5 (64-bit) | Independent                 |                                                          |
| Asianux Server 4.2 (64-bit)                 | Dependent                   | Yes                                                      |
| Asianux Server 4.4 (64-bit)                 | Dependent                   | Yes                                                      |
| Asianux Server 4.5 (64-bit)                 | Dependent                   | Yes                                                      |
| GreatTurbo Enterprise Server 12.2 (64-bit)  | Dependent                   | Yes                                                      |
| NeoKylin Linux Security OS V5.0 (64-bit)    | Dependent                   | Yes                                                      |

For PV Linux VMs where the `independent_wallclock` setting is available, you can use this setting to define whether the VM has dependent or independent wallclock behavior.

#### Important:

Citrix recommends using the `independent_wallclock` setting to enable independent wall-clock behavior and running a reliable NTP service on the Linux VMs and the XenServer host.

#### To set individual Linux VMs to have independent wall-clock behavior:

1. From a root prompt on the VM, run the command: `echo 1 > /proc/sys/xen/independent_wallclock`
2. This setting can be persisted across reboots by changing the `/etc/sysctl.conf` configuration file and adding:

```
1 ## Set independent wall clock time
2 xen.independent_wallclock=1
```

3. As a third alternative, `independent_wallclock=1` can also be passed as a boot parameter to the VM.

#### To set individual Linux VMs to have dependent wall-clock behavior:

1. From a root prompt on the VM, run the command: `echo 0 > /proc/sys/xen/independent_wallclock`
2. This setting can be persisted across reboots by changing the `/etc/sysctl.conf` configuration file and adding:

```
1 ## Set independent wall clock time
2 xen.independent_wallclock=0
```

3. As a third alternative, `independent_wallclock=0` can also be passed as a boot parameter to the VM.

## HVM Linux VMs

Hardware clocks in HVM 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 the XenServer time handling behavior for HVM Linux VMs.

## Install HVM VMs from Reseller Option Kit (BIOS-locked) media

There are two types of HVM VMs: 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 XenServer BIOS strings.

#### Note:

If a VM doesn't have BIOS strings set when it starts, the standard XenServer 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.

### 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):

```
1 xe vm-install copy-bios-strings-from=host uuid \
2 template=template name sr-name=label=name of sr \
3 new-name-label=name for new VM
```

This command returns the UUID of the newly created VM.

For example:

```
1 xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786
 ef4 \
2 template="win7sp1" sr-name=label=Local\ storage \
3 new-name-label=newcentos
4 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:

```
1 xe vm-is-bios-customized uuid=VM uuid
```

For example:

```
1 xe vm-is-bios-customized \
2 uuid=7cd98710-bf56-2045-48b7-e4ae219799db
3 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`):

```
1 xe vm-install template=template name sr-name-label=name of sr \
2 new-name-label=name for new VM
```

This command returns the UUID of the newly created VM.

For example:

```
1 xe vm-install template="win7sp1" sr-name-label=Local\ storage \
2 new-name-label=newcentos \
3 7cd98710-bf56-2045-48b7-e4ae219799db
```

2. To set user-defined BIOS strings, run the following command before starting the VM for the first time:

```
1 xe vm-param-set uuid=VM_UUID bios-strings:bios-vendor=VALUE \
2 bios-strings:bios-version=VALUE bios-strings:system-manufacturer=
 VALUE \
3 bios-strings:system-product-name=VALUE bios-strings:system-version
 =VALUE \
4 bios-strings:system-serial-number=VALUE bios-strings:enclosure-
 asset-tag=VALUE
```

For example:

```
1 xe vm-param-set uuid=7cd98710-bf56-2045-48b7-e4ae219799db \
2 bios-strings:bios-vendor="vendor name" \
3 bios-strings:bios-version=2.4 \
4 bios-strings:system-manufacturer="manufacturer name" \
5 bios-strings:system-product-name="product name" \
6 bios-strings:system-serial-number="serial number" \
7 bios-strings:enclosure-asset-tag="asset tag"
```



```
5 bios-strings:system-product-name=guest1 \
6 bios-strings:system-version=1.0 \
7 bios-strings:system-serial-number="serial number" \
8 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)**

XenServer enables you to assign a physical GPU in the XenServer host 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 XenServer 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 XenMotion 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 XenServer host. 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 XenServer host and then restart the machine. Upon restart, XenServer 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:

```
1 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 XenServer host.

## 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:

```
1 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:

```
1 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, XenServer 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:

```
1 xe vgpu-list vm-uuid=uuid_of_vm
```

3. Detach the GPU from the VM by entering the following:

```
1 xe vgpu-destroy uuid=uuid_of_vgpu
```

4. Start the VM by using the `xe vm-start` command.

## Create ISO images

XenServer 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

```
1 dd if=/dev/cdrom of=/path/cding_filename.iso
```

This command takes some time. When the operation is completed successfully, you see something like:

```
1 1187972+0 records in
2 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**

September 5, 2018

VMs might not be set up to support Virtual Network Computing (VNC), which XenServer 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 Squeeze VMs**

#### **Note:**

Before enabling a graphical console on your Debian Squeeze VM, ensure that you have installed the Linux guest agent. For more information, see [Install the Linux Guest Agent](#).

The graphical console for Debian Squeeze 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 Squeeze 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):

```
1 apt-get install vnc4server
```

**Note:**

The Debian Squeeze Graphical Desktop Environment, which uses the Gnome Display Manager version 3 daemon, can take significant CPU time. Citrix strongly advises that customers uninstall the Gnome Display Manager `gdm3` package and install the `gdm` package as follows:

```
1 apt-get install gdm
2 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:

```
1 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:

```
1 [servers]
2 0=VNC
3 [daemon]
4 VTAllocation=false
5 [server-VNC]
6 name=VNC
7 command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/vncpass
 BlacklistTimeout=0
8 flexible=true
```

5. Restart GDM, and then wait for XenCenter to detect the graphical console:

```
1 /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:**

Configuring VNC  
for Red Hat VMs

Before setting up your Red Hat VMs for VNC, be sure that you have installed the Linux guest agent. For more information, see [Install the Linux Guest Agent](#).

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.

**Note:**

For information on enabling VNC for RHEL, CentOS, or OEL 6.x VMs, see [Enable VNC for RHEL, CentOS, or OEL 6 VMs](#).

**Determine the location of your VNC configuration file**

If you are using Red Hat Linux version 5.x, 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:

```
1 [server-VNC]
2 name=VNC Server
3 command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
 depth 16 \
4 -BlacklistTimeout 0
5 flexible=true
```

With configuration files on Red Hat Linux 5.x, 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 5.x or greater, 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 Runlevels](#).

## 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 5.x, 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:

```
1 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 6 VMs

If you are using Red Hat Linux version 6.x, 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**:

The default installation of Red Hat Enterprise Linux is a basic server install. You can optionally select a different set of software now.

- ☐ Basic Server
- ☐ Database Server
- ☐ Web Server
- ☐ Identity Management Server
- ☐ Virtualization Host
- ☒ Desktop
- ☐ Software Development Workstation
- ☐ Minimal

Please select any additional repositories that you want to use for software installation.

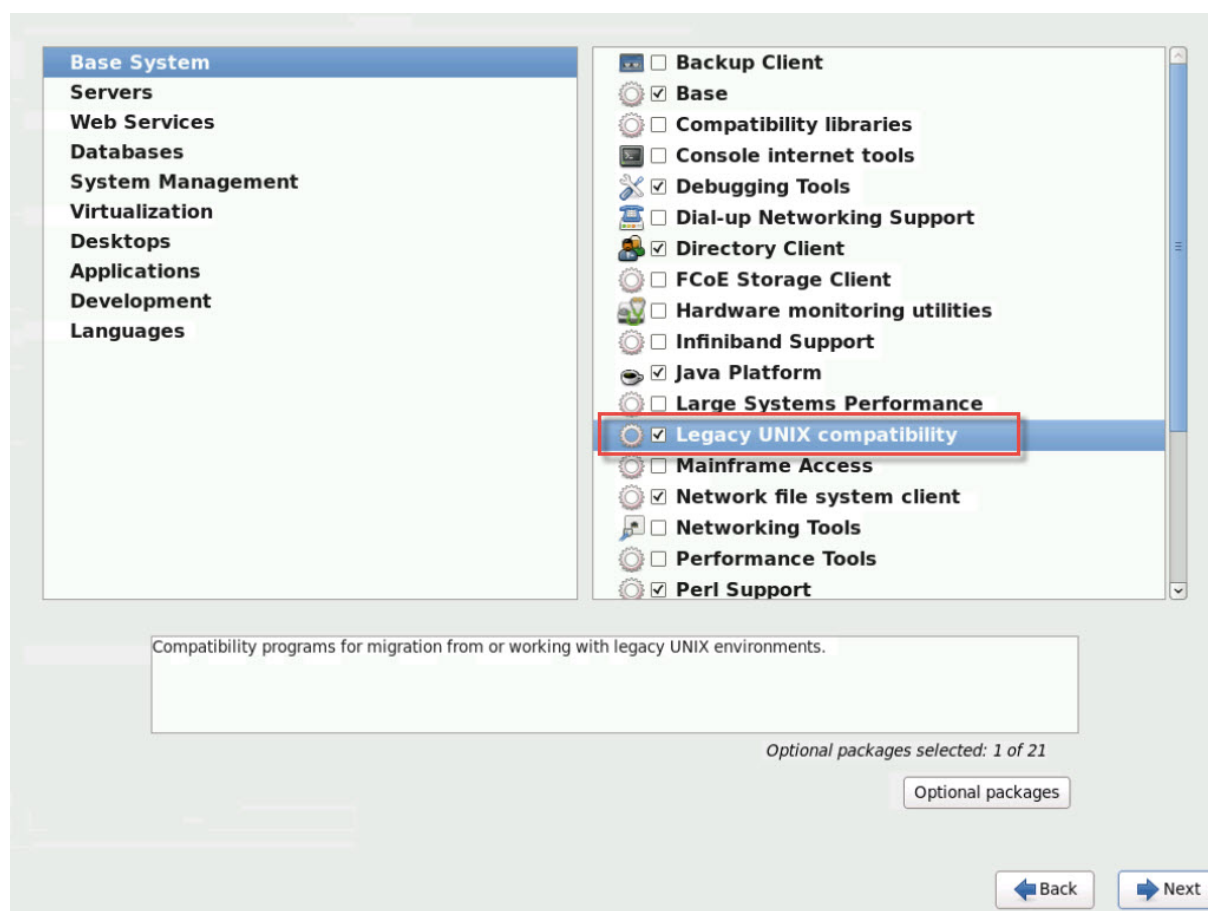
- ☐ High Availability
- ☐ Load Balancer
- ☒ Red Hat Enterprise Linux
- ☐ Resilient Storage

You can further customize the software selection now, or after install via the software management application.

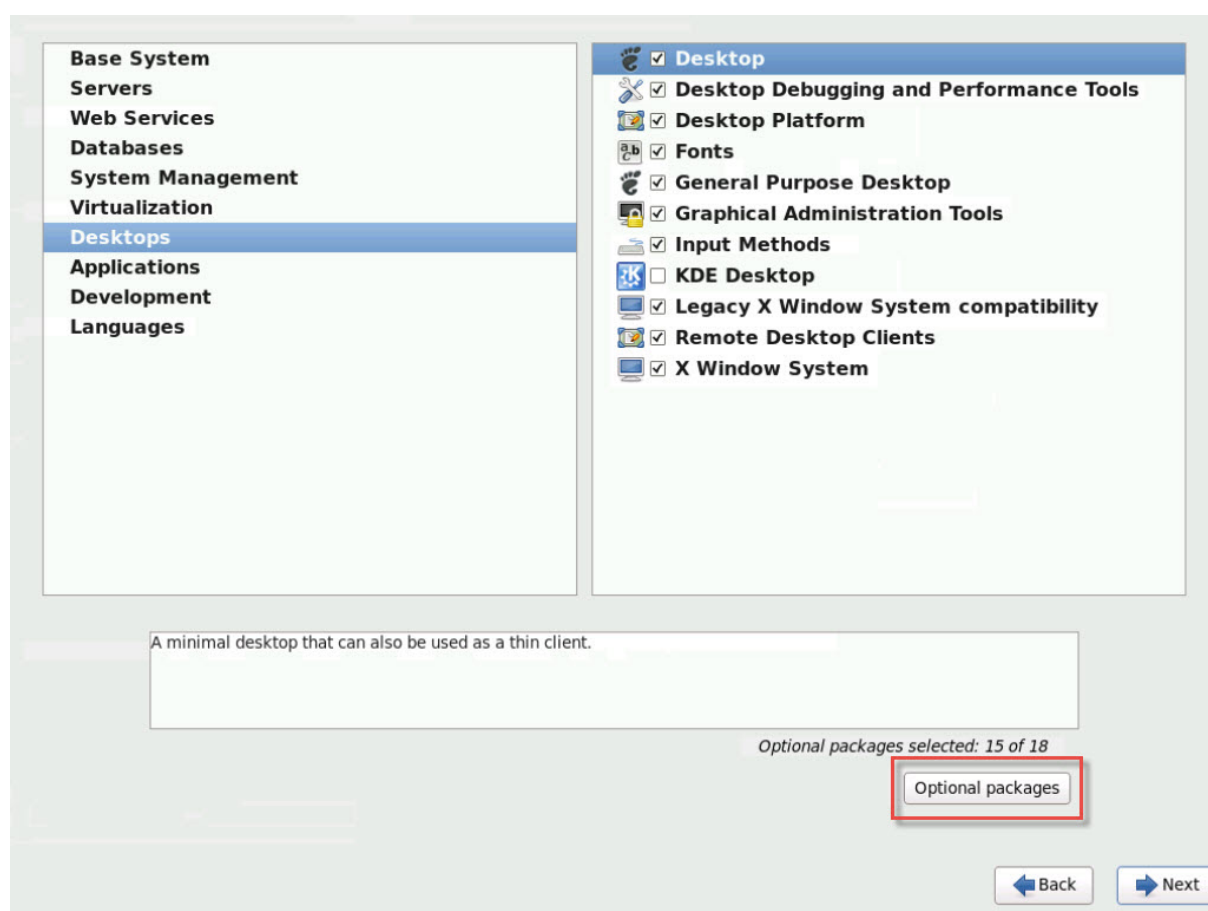
- ☐ Customize later
- ☒ Customize now



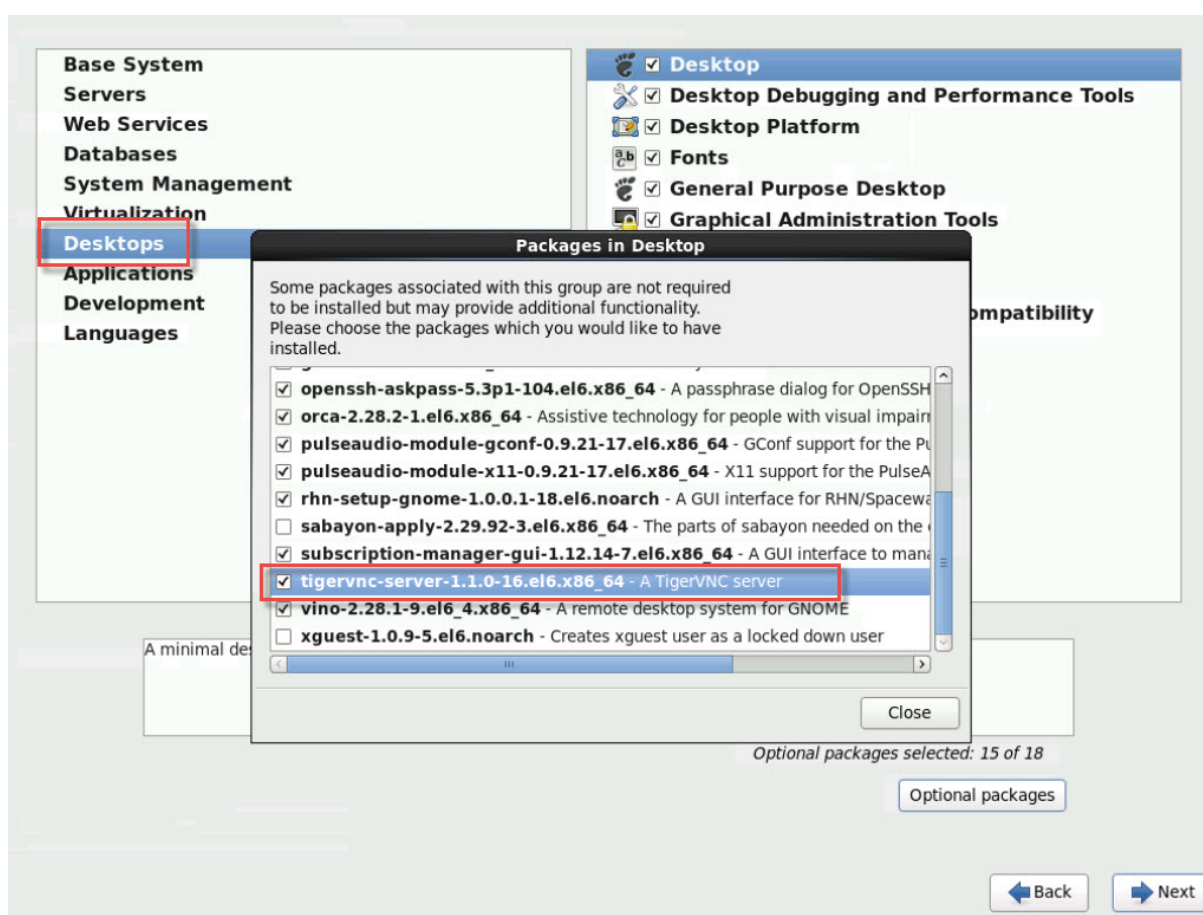
This action displays the Base System screen, ensure that **Legacy UNIX compatibility** is selected:



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 6.x VMs:

1. Open the GDM configuration file with your preferred text editor and add the following lines to the appropriate sections:

```

1 [security]
2 DisallowTCP=false
3
4 [xdmcp]
5 Enable=true

```

2. Create the file, `/etc/xinetd.d/vnc-server-stream`:

```

1 service vnc-server
2 {
3
4 id = vnc-server
5 disable = no
6 type = UNLISTED
7 port = 5900
8 socket_type = stream

```

```
9 wait = no
10 user = nobody
11 group = tty
12 server = /usr/bin/Xvnc
13 server_args = -inetd -once -query localhost -SecurityTypes
 None \
14 -geometry 800x600 -depth 16
15 }
```

3. Enter the following command to start the `xinetd` service:

```
1 # 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`:

```
1 -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

5. Enter the following command to restart `iptables`:

```
1 # service iptables restart
```

6. Enter the following command to restart `gdm`:

```
1 # telinit 3
2 # 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 runlevels](#).

## 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 Linux guest agent. See [Install the Linux Guest Agent](#) 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:

```
1 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:

```
1 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:

```
1 service vnc1
2 {
3
4 socket_type = stream
5 protocol = tcp
6 wait = no
7 user = nobody
8 server = /usr/X11R6/bin/Xvnc
9 server_args = :42 -inetd -once -query localhost -geometry 1024x768
 -depth 16
10 type = UNLISTED
11 port = 5901
12 }
```

3. Edit the `port` line to read

```
1 port = 5900
```

4. Save and close the file.
5. Restart the display manager and `xinetd` service with the following commands:

```
1 /etc/init.d/xinetd restart
2 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 Runlevels](#).

## 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:

```
1 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:

```
1 /etc/init.d/xinetd restart
2 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,

```
1 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:

```
1 /etc/init.d/xinetd restart
2 rcxdm restart
```

## Check runlevels

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:

```
1 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 re-boot to switch runlevels.

## Troubleshoot VM problems

November 14, 2018

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 XenServer Solution Provider and Citrix track and resolve the issue.

### Important:

Follow the troubleshooting information in this section only under the guidance of your XenServer Solution Provider or Citrix Support.

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                                         |
|-----------------------|-----------------------------------------------------|
| <code>preserve</code> | Leave the VM in a paused state. (For analysis)      |
| <code>restart</code>  | No core dump, just reboot VM. (This is the default) |
| <code>destroy</code>  | No core dump, leave VM halted.                      |

### To enable saving of Linux VM crash dumps:

1. On the XenServer host, determine the UUID of the desired VM by running the following command:

```
1 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:

```
1 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:

```
1 echo c | sudo tee /proc/sysrq-trigger
```

4. Execute the dump core command on dom0. For example, run:

```
1 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 XenServer host 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:

```
1 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:

```
1 xe-edit-bootloader -u linux_vm_uuid -p partition_number
```

Or, you can use the name-label as follows:

```
1 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.

## Configure high availability

September 5, 2018

High availability is a set of automatic features designed to plan for, and safely recover from issues which take down XenServer hosts or make them unreachable. For example, during physically disrupted networking or host hardware failures.

## Overview

High availability ensures that when a host becomes unreachable or unstable, VMs running on that host are shut down and restarted on another host. Shutting down and restarting VMs on another host avoids the VMs being started (manually or automatically) on a new host. At some point later, the original host is recovered. This scenario can lead two instances of the same VM running on different hosts, and a corresponding high probability of VM disk corruption and data loss.

When the pool master becomes unreachable or unstable, high availability can also recover administrative control of a pool. High availability ensures that administrative control is restored automatically without any manual intervention.

Optionally, high availability can also automate the process of restarting VMs on hosts which are known to be in a good state without manual intervention. These VMs can be scheduled for restart in groups to allow time to start services. It allows infrastructure VMs to be started before their dependent VMs (For example, a DHCP server before its dependent SQL server).

### Warning:

High availability can be used along with multipathed storage and bonded networking. Configure multipathed storage and bonded networking before attempting to set up high availability. Customers who do not set up multipathed networking and storage can see unexpected host reboot behavior (Self Fencing) when there is an infrastructure instability.

### Note:

All graphics solutions (NVidia vGPU, Intel GVT-d, Intel GVT-G, AMD MxGPU, and vGPU pass-through) can be used in an environment that makes use of high availability. However, VMs that use these graphics solutions cannot be protected with high availability. These VMs can be restarted on a best-effort basis while there are hosts with the appropriate free resources.

## Overcommitting

A pool is overcommitted when the VMs that are currently running cannot be restarted elsewhere following a user-defined number of host failures.

Overcommitting can happen if there is not enough free memory across the pool to run those VMs following a failure. However, there are also more subtle changes which can make high availability guarantees unsustainable: Changes to Virtual Block Devices (VBDs) and networks can affect which VMs can be restarted on which hosts. XenServer cannot check all potential actions and determine if they cause violation of high availability demands. However, an asynchronous notification is sent if high availability becomes unsustainable.

XenServer dynamically maintains a *failover plan* which details what to do when a set of hosts in a pool fail at any given time. An important concept to understand is the *host failures to tolerate* value, which

is defined as part of high availability configuration. The value of *host failures to tolerate* determines the number of failures that is allowed without any loss of service. For example, consider a resource pool that consists of 64 hosts and the tolerated failures is set to 3. In this case, the pool calculates a failover plan that allows any three hosts to fail and restart the VMs on other hosts. If a plan cannot be found, then the pool is considered to be *overcommitted*. The plan is dynamically recalculated based on VM lifecycle operations and movement. If changes, for example the addition on new VMs to the pool, cause your pool to become overcommitted, alerts are sent (either through XenCenter or email).

### Overcommitment warning

If any attempts to start or resume a VM cause the pool to be overcommitted, a warning alert is displayed. This warning appears in XenCenter and is also available as a message instance through the Xen API. If you have configured an email address, a message may also be sent to the email address. You can then cancel the operation, or proceed anyway. Proceeding causes the pool to become overcommitted. The amount of memory used by VMs of different priorities is displayed at the pool and host levels.

### Host fencing

Sometimes, a server can fail due to the loss of network connectivity or when a problem with the control stack is encountered. In such cases, the XenServer host self-fences to ensure the VMs are not running on two servers simultaneously. When a fence action is taken, the server restarts immediately and abruptly, causing all VMs running on it to be stopped. The other servers detect that the VMs are no longer running and the VMs are restarted according to the restart priorities assigned to them. The fenced server enters a reboot sequence, and when it has restarted it tries to rejoin the resource pool.

#### Note:

Hosts in clustered pools can also self-fence when they cannot communicate with more than half the other hosts in the resource pool. For more information, see [Clustered pools](#).

### Configuration requirements

#### Note:

Citrix recommends that you enable high availability only in pools that contain at least three XenServer hosts. For more information, see [CTX129721 - High Availability Behavior When the Heartbeat is Lost in a XenServer Pool](#).

To use the high availability feature, you need:

- Shared storage, including at least one iSCSI, NFS, or Fibre Channel LUN of size 356 MB or greater - the *heartbeat SR*. The high availability mechanism creates two volumes on the heartbeat SR:

4 MB heartbeat volume: Used for heartbeating.

256 MB metadata volume: To store pool master metadata to be used if there is a master failover.

**Notes:**

- For maximum reliability, Citrix recommends that you use a dedicated NFS or iSCSI storage repository as your high availability heartbeat disk. Do not use this storage repository for any other purpose.
  - If your pool is a clustered pool, your heartbeat SR must be a GFS2 SR.
  - Storage attached using either SMB or iSCSI when authenticated using CHAP cannot be used as the heartbeat SR.
  - When using a NetApp or EqualLogic SR, manually provision an NFS or iSCSI LUN on the array to use as the heartbeat SR.
- XenServer pool (this feature provides high availability at the server level within a single resource pool).
  - Static IP addresses for all hosts.

**Warning:**

If the IP address of a server changes while high availability is enabled, high availability assumes that the host's network has failed. The change in IP address can fence the host and leave it in an unbootable state. To remedy this situation, disable high availability using the `host-emergency -ha-disable` command, reset the pool master using `pool-emergency-reset-master`, and then re-enable high availability.

For a VM to be protected by high availability, it must be agile. It means the VM:

- Must have its virtual disks on shared storage. You can use any type of shared storage. iSCSI, NFS, or Fibre Channel LUN is only required for the storage heartbeat and can be used for virtual disk storage.
- Can use XenMotion
- Does not have a connection to a local DVD drive configured
- Has its virtual network interfaces on pool-wide networks

When high availability is enabled, Citrix strongly recommends using a bonded management interface on the servers in the pool and multipathed storage for the heartbeat SR.

If you create VLANs and bonded interfaces from the CLI, then they may not be plugged in and active despite being created. In this situation, a VM can appear to be not agile and it is not protected by high availability. You can use the CLI `pif-plug` command to bring up the VLAN and bond PIFs so

that the VM can become agile. You can also determine precisely why a VM is not agile by using the `xe diagnostic-vm-status` CLI command. This command analyzes its placement constraints, and you can take remedial action if necessary.

## Restart configuration settings

Virtual machines can be considered protected, best-effort, or unprotected by high availability. The value of `ha-restart-priority` defines whether a VM is treated as protected, best-effort, or unprotected. The restart behavior for VMs in each of these categories is different.

### Protected

High availability guarantees to restart a protected VM that goes offline or whose host goes offline, provided the pool isn't overcommitted and the VM is agile.

If a protected VM cannot be restarted when a server fails, high availability attempts to start the VM when there is extra capacity in a pool. Attempts to start the VM when there is extra capacity might now succeed.

`ha-restart-priority` Value: `restart`

### Best-effort

If the host of a best-effort VM goes offline, high availability attempts to restart the best-effort VM on another host. It makes this attempt only after all protected VMs have been successfully restarted. High availability makes only one attempt to restart a best-effort VM. If this attempt fails, high availability does not make further attempts to restart the VM.

`ha-restart-priority` Value: `best-effort`

### Unprotected

If an unprotected VM or the host it runs on is stopped, high availability does not attempt to restart the VM.

`ha-restart-priority` Value: Value is an empty string

#### Note:

High availability never stops or migrates a running VM to free resources for a protected or best-effort VM to be restarted.

If the pool experiences server failures and the number of tolerable failures drops to zero, the protected VMs are not guaranteed to restart. In such cases, a system alert is generated. If another failure occurs, all VMs that have a restart priority set behave according to the best-effort behavior.

## Start order

The start order is the order in which XenServer high availability attempts to restart protected VMs when a failure occurs. The values of the `order` property for each of the protected VMs determines the start order.

The `order` property of a VM is used by high availability and also by other features that start and shut down VMs. Any VM can have the `order` property set, not just the VMs marked as protected for high availability. However, high availability uses the `order` property for protected VMs only.

The value of the `order` property is an integer. The default value is 0, which is the highest priority. Protected VMs with an `order` value of 0 are restarted first by high availability. The higher the value of the `order` property, the later in the sequence the VM is restarted.

You can set the value of the `order` property of a VM by using the command-line interface:

```
1 xe vm-param-set uuid=VM_UUID order=int
```

Or in XenCenter, in the Start Options panel for a VM, set Start order to the required value.

## Enable high availability on your XenServer pool

You can enable high availability on a pool by using either XenCenter or the command-line interface. In either case, you specify a set of priorities that determine which VMs are given the highest restart priority when a pool is overcommitted.

### Warnings:

- When you enable high availability, some operations that compromise the plan for restarting VMs, such as removing a server from a pool, may be disabled. You can temporarily disable high availability to perform such operations, or alternatively, make VMs protected by high availability unprotected.
- If high availability is enabled, you cannot enable clustering on your pool. Temporarily disable high availability to enable clustering. You can enable high availability on your clustered pool. Some high availability behavior, such as self-fencing, is different for clustered pools. For more information, see [Clustered pools](#)

## Enable high availability by using the CLI

1. Verify that you have a compatible Storage Repository (SR) attached to your pool. iSCSI, NFS, or Fibre Channel SRs are compatible. For information about how to configure such a storage repository using the CLI, see [Manage storage repositories](#).
2. For each VM you want to protect, set a restart priority and start order. You can set the restart priority as follows:

```
1 xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
```

3. Enable high availability on the pool, and optionally, specify a timeout:

```
1 xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
 timeout in seconds
```

Timeout is the period during which networking or storage is not accessible by the hosts in your pool. If you do not specify a timeout when you enable high availability, XenServer uses the default 30 seconds timeout. If any XenServer host is unable to access networking or storage within the timeout period, it can self-fence and restart.

4. Run the command `pool-ha-compute-max-host-failures-to-tolerate`. This command returns the maximum number of hosts that can fail before there are insufficient resources to run all the protected VMs in the pool.

```
1 xe pool-ha-compute-max-host-failures-to-tolerate
```

The number of failures to tolerate determines when an alert is sent. The system recomputes a failover plan as the state of the pool changes. It uses this computation to identify the pool capacity and how many more failures are possible without loss of the liveness guarantee for protected VMs. A system alert is generated when this computed value falls below the specified value for `ha-host-failures-to-tolerate`.

5. Specify the number of failures to tolerate parameter. The value must be less than or equal to the computed value:

```
1 xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
```

## Remove high availability protection from a VM by using the CLI

To disable high availability features for a VM, use the `xe vm-param-set` command to set the `ha-restart-priority` parameter to be an empty string. Setting the `ha-restart-priority` parameter does not clear the start order settings. You can enable high availability for a VM again by setting the `ha-restart-priority` parameter to `restart` or `best-effort` as appropriate.



## Recover an unreachable host

If for some reason, a host cannot access the high availability state file, it is possible that a host may become unreachable. To recover your XenServer installation, you may have to disable high availability using the `host-emergency-ha-disable` command:

```
1 xe host-emergency-ha-disable --force
```

If the host was the pool master, it starts up as normal with high availability disabled. Pool members reconnect and automatically disable high availability. If the host was a pool member and cannot contact the master, you might have to take one of the following actions:

- Force the host to reboot as a pool master (`xe pool-emergency-transition-to-master`)

```
1 xe pool-emergency-transition-to-master uuid=host_uuid
```

- Tell the host where the new master is (`xe pool-emergency-reset-master`):

```
1 xe pool-emergency-reset-master master-address=new_master_hostname
```

When all hosts have successfully restarted, re-enable high availability:

```
1 xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
```

## Shutting down a host when high availability is enabled

Take special care when shutting down or rebooting a host to prevent the high availability mechanism from assuming that the host has failed. To shut down a host cleanly when high availability is enabled, `disable` the host, `evacuate` the host, and finally `shutdown` the host by using either XenCenter or the CLI. To shut down a host in an environment where high availability is enabled, run these commands:

```
1 xe host-disable host=host_name
2 xe host-evacuate uuid=host_uuid
3 xe host-shutdown host=host_name
```

## Shut down a VM protected by high availability

When a VM is protected under a high availability plan and set to restart automatically, it cannot be shut down while this protection is active. To shut down a VM, first disable its high availability protection and then execute the CLI command. XenCenter offers you a dialog box to automate disabling the protection when you select the **Shutdown** button of a protected VM.

**Note:**

If you shut down a VM from within the guest, and the VM is protected, it is automatically restarted under the high availability failure conditions. The automatic restart helps ensure that operator error doesn't result in a protected VM being left shut down accidentally. If you want to shut down this VM, disable its high availability protection first.

## Disaster recovery and backup

August 13, 2018

The XenServer Disaster Recovery (DR) feature allows you to recover virtual machines (VMs) and vApps from a failure of hardware which destroys a whole pool or site. For protection against single server failures, see [High availability](#).

**Note:**

You must be logged on with your *root* account or have the role of *Pool Operator* or higher to use the DR feature.

## Understanding XenServer DR

XenServer DR works by storing all the information required to recover your business-critical VMs and vApps on storage repositories (SRs). The SRs are then replicated from your primary (production) environment to a backup environment. When a protected pool at your primary site goes down, you can recover the VMs and vApps in that pool from the replicated storage recreated on a secondary (DR) site with minimal application or user downtime.

The **Disaster Recovery** settings in XenCenter can be used to query the storage and import selected VMs and vApps to a recovery pool during a disaster. When the VMs are running in the recovery pool, the recovery pool metadata is also replicated. The replication of the pool metadata allows any changes in VM settings to be populated back to the primary pool when the primary pool recovers. Sometimes, information for the same VM can be in several places. For example, storage from the primary site, storage from the disaster recovery site and also in the pool that the data is to be imported to. If XenCenter finds that the VM information is present in two or more places, it ensures that it uses only the most recent information.

The Disaster Recovery feature can be used with XenCenter and the xe CLI. For CLI commands, see [Disaster recovery commands](#).

**Tip:**

You can also use the Disaster Recovery settings to run test failovers for non-disruptive testing of

your disaster recovery system. In a test failover, all the steps are the same as failover. However, the VMs and vApps are not started up after they have been recovered to the disaster recovery site. When the test is complete, cleanup is performed to delete all VMs, vApps, and storage recreated on the DR site.

XenServer VMs consist of two components:

- Virtual disks that are being used by the VM, stored on configured storage repositories (SRs) in the pool where the VMs are located.
- Metadata describing the VM environment. This information is required to recreate the VM if the original VM is unavailable or corrupted. Most metadata configuration data is written when the VM is created and is updated only when you change the VM configuration. For VMs in a pool, a copy of this metadata is stored on every server in the pool.

In a DR environment, VMs are recreated on a secondary site using the pool metadata and configuration information about all VMs and vApps in the pool. The metadata for each VM includes its name, description and Universal Unique Identifier (UUID), and its memory, virtual CPU, and networking and storage configuration. It also includes VM startup options – start order, delay interval, high availability, and restart priority. The VM startup options are used when restarting the VM in a high availability or DR environment. For example, when recovering VMs during disaster recovery, VMs within a vApp are restarted in the DR pool in the order specified in the VM metadata, and using the specified delay intervals.

## **DR infrastructure requirements**

Set up the appropriate DR infrastructure at both the primary and secondary sites to use XenServer DR.

- Storage used for pool metadata *and* the virtual disks used by the VMs must be replicated from the primary (production) environment to a backup environment. Storage replication such as using mirroring varies between devices. Therefore, consult your storage solution vendor to handle Storage replication.
- After the VMs and vApps that you recovered to a pool on your DR site are up and running, the SRs containing the DR pool metadata and virtual disks must be replicated. Replication allows the recovered VMs and vApps to be restored back to the primary site (*failed back*) when the primary site is back online.
- The hardware infrastructure at your DR site does not have to match the primary site. However, the XenServer environment must be at the same release and patch level. In addition, sufficient resources must be configured in the target pool to allow all the failed over VMs to be recreated and started.

**Warning:**

The Disaster Recovery settings do not control any Storage Array functionality.

Users of the Disaster Recovery feature must ensure that the metadata storage is, in some way replicated between the two sites. Some Storage Arrays contain “Mirroring” features to achieve the replication automatically. If you use these features, you must disable the mirror functionality (“mirror is broken”) before restarting VMs on the recovery site.

**Deployment considerations**

Review the following steps before enabling Disaster Recovery.

**Steps to take before a disaster**

The following section describes the steps to take before disaster.

- Configure your VMs and vApps.
- Note how your VMs and vApps are mapped to SRs, and the SRs to LUNs. Take particular care with the naming of the `name_label` and `name_description` parameters. Recovering VMs and vApps from replicated storage is easier if the names of SRs capture how VMs and vApps are mapped to SRs, and SRs to LUNs.
- Arrange replication of the LUNs.
- Enable pool metadata replication to one or more SRs on these LUNs.
- Ensure that the SRs you are replicating the primary pool metadata to are attached to only one pool.

**Steps to take after a disaster**

The following section describes the steps to take after a disaster has occurred.

- Break any existing storage mirrors so that the recovery site has read/write access to the shared storage.
- Ensure that the LUNs you want to recover VM data from are not attached to any other pool, or corruption can occur.
- If you want to protect the *recovery* site from a disaster, you must enable pool metadata replication to one or more SRs on the recovery site.

## Steps to take after a recovery

The following section describes the steps to take after a successful recovery of data.

- Resynchronize any storage mirrors.
- On the recovery site, cleanly shut down the VMs or vApps that you want to move back to the primary site.
- On the primary site, follow the same procedure as for the failover in the previous section, to failback selected VMs or vApps to the primary
- To protect the primary site against future disaster - you must re-enable pool metadata replication to one or more SRs on the replicated LUNs.

## Enable Disaster Recovery

September 6, 2018

This section describes how to enable Disaster Recovery in XenCenter. Use the **Configure DR** option to identify storage repositories where the pool metadata, configuration information about all the VMs and vApps in the pool is stored. The metadata is updated whenever you change the VM or vApp configuration within the pool.

### Note:

You can enable Disaster Recovery only when using LVM over HBA or LVM over iSCSI. A small amount of space is required on this storage for a new LUN which contains the pool recovery information.

Before you begin, ensure that the SRs used for DR are attached only to the pool at the primary site. SRs used for DR must not be attached to the pool at the secondary site.

To configure Disaster Recovery, complete the following steps:

1. On the primary site, select the pool that you want to protect. From the **Pool** menu, point to **Disaster Recovery**, and then select **Configure**.
2. Select up to 8 SRs where the pool metadata can be stored. A small amount of space is required on this storage for a new LUN which contains the pool recovery information.

### Note:

Information for all VMs in the pool is stored, VMs do not need to be independently selected for protection.

3. Select **OK**. Your pool is now protected.

## Recover VMs and vApps during a disaster (Failover)

This section explains how to recover your VMs and vApps on the secondary (recovery) site.

1. In XenCenter select the secondary pool, and on the **Pool** menu, select **Disaster Recovery** and then **Disaster Recovery Wizard**.

The Disaster Recovery wizard displays three recovery options: **Failover**, **Failback**, and **Test Failover**. To recover on to your secondary site, select **Failover** and then select **Next**.

### Warning:

If you use Fibre Channel shared storage with LUN mirroring to replicate data to the secondary site, break the mirroring before attempting to recover VMs. Mirroring must be broken to ensure that the secondary site has Read/Write access.

2. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to recover.

By default, the list on this wizard page shows all SRs that are currently attached within the pool. To scan for more SRs, select **Find Storage Repositories** and then select the storage type to scan for:

- To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
- To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then type the target host, IQN, and LUN details.

When you have selected the required SRs in the wizard, select **Next** to continue.

3. Select the VMs and vApps that you want to recover. Select the appropriate **Power state after recovery** option to specify whether you want the wizard to start them up automatically when they have been recovered. Alternatively, you can start them up manually after failover is complete.

Select **Next** to progress to the next wizard page and begin failover prechecks.

4. The wizard performs several prechecks before starting failover. For example, to ensure that all the storage required by the selected VMs and vApps is available. If any storage is missing at this point, you can select **Attach SR** on this page to find and attach the relevant SR.

Resolve any issues on the prechecks page, and then select **Failover** to begin the recovery process.

5. A progress page displays the result of the recovery process for each VM and vApp. The Failover process exports the metadata for VMs and vApps from the replicated storage. Therefore, The time taken for Failover depends on the VMs and vApps you recover. The VMs and vApps are recreated in the primary pool, and the SRs containing the virtual disks are attached to the recreated VMs. If specified, the VMs are started.

6. When the failover is complete, select **Next** to see the summary report. Select **Finish** on the summary report page to close the wizard.

When the primary site is available, work through the Disaster Recovery wizard and select **Failback** to return to running your VMs on that site.

## Restore VMs and vApps to the primary site after disaster (Failback)

This section explains how to restore VMs and vApps from replicated storage. You can restore VMs and vApps back to a pool on your primary (production) site when the primary site comes back up after a disaster. To failback VMs and vApps to your primary site, use the Disaster Recovery wizard.

1. In XenCenter select the primary pool, and on the Pool menu, select **Disaster Recovery** and then **Disaster Recovery Wizard**.

The Disaster Recovery wizard displays three recovery options: **Failover**, **Failback**, and **Test Failover**. To restore VMs and vApps to your primary site, select Failback and then select **Next**.

### Warning:

When you use Fibre Channel shared storage with LUN mirroring to replicate data to the primary site, break the mirroring before attempting to restore VMs. Mirroring must be broken to ensure that the primary site has Read/Write access.

2. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to recover.

By default, the list on this wizard page shows all SRs that are currently attached within the pool. To scan for more SRs, choose **Find Storage Repositories** and then select the storage type to scan for:

- To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
- To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then type the target host, IQN, and LUN details.

When you have selected the required SRs in the wizard, select **Next** to continue.

3. Select the VMs and vApps that you want to restore. Select the appropriate **Power state after recovery** option to specify whether you want the wizard to start them up automatically when they have been recovered. Alternatively, you can start them up manually after failback is complete.

Select **Next** to progress to the next wizard page and begin failback prechecks.

4. The wizard performs several pre-checks before starting failback. For example, to ensure that all the storage required by the selected VMs and vApps is available. If any storage is missing at this point, you can select **Attach SR on this page** to find and attach the relevant SR.

Resolve any issues on the prechecks page, and then select **Failback** to begin the recovery process.

5. A progress page displays the result of the recovery process for each VM and vApp. The Failback process exports the metadata for VMs and vApps from the replicated storage. Therefore, Failback can take some time depending on the number of VMs and vApps you are restoring. The VMs and vApps are recreated in the primary pool, and the SRs containing the virtual disks are attached to the recreated VMs. If specified, the VMs are started.
6. When the failback is complete, select **Next** to see the summary report. Select **Finish** on the summary report page to close the wizard.

## Test failover

Failover testing is an essential component in disaster recovery planning. You can use the Disaster Recovery wizard to perform non-disruptive testing of your disaster recovery system. During a test failover operation, the steps are the same as for failover. However, instead of being started after they have been recovered to the DR site, the VMs and vApps are placed in a paused state. At the end of a test failover operation, all VMs, vApps, and storage recreated on the DR site are automatically deleted. After initial DR configuration, and after you make significant configuration changes in a DR-enabled pool, verify that failover works correctly by performing a test failover.

1. In XenCenter select the secondary pool, and on the **Pool** menu, select **Disaster Recovery** to open the **Disaster Recovery Wizard**.
2. Select **Test Failover** and then select **Next**.

### Note:

If you use Fibre Channel shared storage with LUN mirroring to replicate data to the secondary site, break the mirroring before attempting to recover data. Mirroring must be broken to ensure that the secondary site has Read/Write access.

3. Select the storage repositories (SRs) containing the pool metadata for the VMs and vApps that you want to recover.

By default, the list on this wizard page shows all SRs that are currently attached within the pool. To scan for more SRs, select **Find Storage Repositories** and then the storage type to scan for:

- To scan for all the available Hardware HBA SRs, select **Find Hardware HBA SRs**.
- To scan for software iSCSI SRs, select **Find Software iSCSI SRs** and then type the target host, IQN, and LUN details in the box.

When you have selected the required SRs in the wizard, select **Next** to continue.



4. Select the VMs and vApps that you want to recover then select **Next** to progress to the next page and begin failover prechecks.
5. Before beginning the test failover, the wizard performs several pre-checks. For example, to ensure that all the storage required by the selected VMs and vApps is available.

- **Check that storage is available.** If any storage is missing, you can select Attach SR on this page to find and attach the relevant SR.
- **Check that high availability is not enabled on the target DR pool.** High availability must be disabled on the secondary pool to avoid having the same VMs running on both the primary and DR pools. High availability must be disabled to ensure that it does not start the recovered VMs and vApps automatically after recovery. To disable high availability on the secondary pool, you can simply select **Disable HA** on the page. If high availability is disabled at this point, it is enabled again automatically at the end of the test failover process.

Resolve any issues on the pre-checks page, and then select **Failover** to begin the test failover.

6. A progress page displays the result of the recovery process for each VM and vApp. The Failover process recovers metadata for the VMs and vApps from the replicated storage. Therefore, Failover can take some time depending on the number of VMs and vApps you are recovering. The VMs and vApps are recreated in the DR pool, the SRs containing the virtual disks are attached to the recreated VMs.

The recovered VMs are placed in a paused state: they do not start up on the secondary site during a test failover.

7. After you are satisfied that the test failover was performed successfully, select Next in the wizard to have the wizard clean up on the DR site:
  - VMs and vApps that were recovered during the test failover are deleted.
  - Storage that was recovered during the test failover is detached.
  - If high availability on the DR pool was disabled at the prechecks stage to allow the test failover to take place, it is re-enabled automatically.

The progress of the cleanup process appears on the wizard.

8. Select **Finish** to close the wizard.

## vApps

September 5, 2018

A vApp is logical group of one or more related Virtual Machines (VMs). vApps can be started up as a single entity when there is a disaster. When a vApp is started, the VMs contained within the vApp start

in a user predefined order. The start order allows 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 example, during a software update. The VMs within the vApp do not have to reside on one host and are distributed within a pool using the normal rules. The vApp feature is useful in the Disaster Recovery (DR) situation. In a DR scenario, an Administrator may group all VMs on the same Storage Repository, or which relate to the same Service Level Agreement (SLA).

To group VMs together in a vApp follow the procedure:

1. Select the pool and, on the **Pool** menu, click **Manage vApps**.
2. Type a name for the vApp, and optionally a description, and then click **Next**.

You can choose any name you like, but an informative name is best. Although we recommend you to avoid having multiple vApps using the same name, it is not a requirement. XenCenter does not enforce any constraints regarding unique vApp names. It is not necessary to use quotation marks for names that include spaces.

3. Select which VMs to include in the new vApp, and then click **Next**.

You can use the search option to list only VMs with names that include the specified text string.

4. Specify the startup sequence for the VMs in the vApp, and then click **Next**.

**Start Order:** Specifies the order in which individual VMs are started within the vApp, allowing certain VMs to be restarted before others. VMs with a start order value of 0 (zero) are started first. VMs with a start order value of 1 are started next, and then the VMs with a value of 2, and so on.

**Attempt to start next VM after:** A delay interval that specifies how long to wait after starting the VM before attempting to start the next group of VMs in the startup sequence.

5. You can review the vApp configuration on the final page. Click **Previous** to go back and change any settings, or **Finish** to create the vApp.

#### **Note:**

A vApp can span multiple servers in a single pool, but cannot span across several pools.

## **Manage vApps in XenCenter**

The **Manage vApps** setting in XenCenter allows you to create, delete, and change vApps. It also enables you to start and shut down vApps, and import and export vApps within the selected pool. When you select a vApp in the list, the VMs it contains are listed in the details pane. For more information, see the XenCenter Help.

## Back up and restore hosts and VMs

March 29, 2019

Citrix recommends that, whenever possible, you leave the installed state of XenServer hosts unaltered. That is, do not install any additional packages or start additional services on XenServer hosts and treat them as appliances. The best way to restore, then, is to reinstall XenServer host software from the installation media. If you have multiple XenServer hosts, the best approach is to configure a TFTP server and appropriate answer files for this purpose. For more information, see [Network boot installations](#).

Citrix recommends that you use a backup solution offered by one of our certified partners. For more information, see [Citrix Ready Marketplace](#).

XenServer Enterprise Edition customers running XenServer 7.3 or a newer version can take advantage of the faster changed block only backup. For more information, see Citrix blog about [Changed Block Tracking backup APIs](#).

Citrix recommends that you frequently perform as many of the following backup procedures as possible to recover from possible server and software failure.

### To back up pool metadata:

1. Run the command:

```
1 xe pool-dump-database file-name=backup
```

2. To restore the database, run the command:

```
1 xe pool-restore-database file-name=backup dry-run=true
```

This command checks that the target machine has an appropriate number of appropriately named NICs, which is required for the backup to succeed.

### To back up host configuration and software:

1. Run the command:

```
1 xe host-backup host=host file-name=hostbackup
```

#### Notes:

- Do not create the backup in the control domain.
- The backup procedure can create a large backup file.

- To complete a restore, you must reboot to the original install CD.
- This data can only be restored to the original machine.

**To back up a VM:**

1. Ensure that the VM to be backed up is offline.
2. Run the command:

```
1 xe vm-export vm=vm_uuid filename=backup
```

**Note:**

This backup also backs up all of the VM data. When importing a VM, you can specify the storage mechanism to use for the backed-up data.

**Warning:**

The backup process can take longer to complete as it backs up all of the VM data.

**To back up VM metadata only:**

Run the command:

```
1 xe vm-export vm=vm_uuid filename=backup metadata=true
```

**Back up virtual machine metadata**

XenServer hosts use a database on each host to store metadata about VMs and associated resources such as storage and networking. When combined with SRs, this database forms the complete view of all VMs available across the pool. Therefore it is important to understand how to back up this database to recover from physical hardware failure and other disaster scenarios.

This section first describes how to back up metadata for single-host installations, and then for more complex pool setups.

**Back up single host installations**

Use the CLI to back up the pool database. To obtain a consistent pool metadata backup file, run `pool-dump-database` on the XenServer host and archive the resulting file. The backup file contains sensitive authentication information about the pool, so ensure it is securely stored.

To restore the pool database, use the `xe pool-restore-database` command from a previous dump file. If your XenServer host has died completely, then you must first do a fresh install, and then run the `pool-restore-database` command against the freshly installed XenServer host.

After you restore the pool database, some VMs may still be registered as being *Suspended*. However, if the storage repository with the suspended memory state defined in the `suspend-VDI-uuid` field, is a local SR, then the SR may not be available as the host has been reinstalled. To reset these VMs back to the *Halted* state so that they can start up again, use the `xe vm-shutdown vm=vm_name -force` command, or use the `xe vm-reset-powerstate vm=vm_name -force` command.

**Warning:**

XenServer preserves UUIDs of the hosts restored using this method. If you restore to a different physical machine while the original XenServer host is still running, duplicate UUIDs may be present. As a result, XenCenter refuses to connect to the second XenServer host. Pool database backup is not the recommended mechanism for cloning physical hosts. Use the automated installation support instead. For more information, see [Install](#).

## Back up pooled installations

In a pool scenario, the master host provides an authoritative database that is synchronously mirrored to all the pool member hosts. This process provides a level of built-in redundancy to a pool. Any pool member can replace the master because each pool member has an accurate version of the pool database. For more information on how to transition a member into becoming a pool master, see [Hosts and resource pools](#).

This level of protection may not be sufficient. For example, when shared storage containing the VM data is backed up in multiple sites, but the local server storage (containing the pool metadata) is not. To re-create a pool given a set of shared storage, you must first back up the `pool-dump-database` file on the master host, and archive this file. To restore this backup later on a brand new set of hosts:

1. Install a fresh set of XenServer hosts from the installation media, or if applicable, network boot from your TFTP server.
2. Use the `xe pool-restore-database` on the host designated to be the new master.
3. Run the `xe host-forget` command on the new master to remove the old member machines.
4. Use the `xe pool-join` command on the member hosts to connect them to the new pool.

## Back up XenServer hosts

This section describes the XenServer host control domain backup and restore procedures. These procedures do *not* back up the storage repositories that house the VMs, but only the privileged control domain that runs Xen and the XenServer agent.

**Note:**

The privileged control domain is best left as installed, without customizing it with other packages. Citrix recommends that you set up a network boot environment to install XenServer cleanly from the XenServer media as a recovery strategy. Typically, you do not need to back up the control domain, but we recommend that you save the pool metadata (see [Back up virtual machine metadata](#)). Consider this backup method as complementary to backing up the pool metadata.

Using the `xe` commands `host-backup` and `host-restore` is another approach that you can take. The `xe host-backup` command archives the active partition to a file you specify. The `xe host-restore` command extracts an archive created by `xe host-backup` over the currently inactive disk partition of the host. This partition can then be made active by booting off the installation CD and selecting to restore the appropriate backup.

After completing the steps in the previous section and rebooting the host, ensure that the VM metadata is restored to a consistent state. Run `xe pool-restore-database` on `/var/backup/pool-database-{ DATE }` to restore the VM metadata. This file is created by `xe host-backup` using `xe pool-dump-database` command before archiving the running filesystem, to snapshot a consistent state of the VM metadata.

**To back up your XenServer host:**

On a remote host with enough disk space, run the following command

```
1 xe host-backup file-name=filename -h hostname -u root -pw password
```

This command creates a compressed image of the control domain file system. The image is stored in the location specified by the `file-name` argument.

**To restore a running XenServer host:**

1. If you want to restore your XenServer host from a specific backup, run the following command while the XenServer host is up and reachable:

```
1 xe host-restore file-name=filename -h hostname -u root -pw
password
```

This command restores the compressed image back to the hard disk of the XenServer host which runs this command (not the host on which `filename` resides). In this context, “restore” may be a misnomer, as the word usually suggests that the backed-up state has been put fully in place. The restore command only unpacks the compressed backup file and restores it to its normal form. However, it is written to another partition (`/dev/sda2`) and does *not* overwrite the current version of the filesystem.

2. To use the restored version of the root filesystem, reboot the XenServer host using the XenServer installation CD and select the **Restore from backup** option.

After the restore from backup is completed, reboot the XenServer host and it will start up from the restored image.

3. Finally, restore the VM metadata using the following command:

```
1 xe pool-restore-database file-name=/var/backup/pool-database-* -h
 hostname -u root -pw password
```

#### Notes:

Restoring from a backup as described in this section does not destroy the backup partition.

### To restart a crashed XenServer host:

If your XenServer host has crashed and is not reachable, use the XenServer installation CD to do an upgrade install. When the upgrade install is complete, reboot the machine and ensure that your host is reachable with XenCenter or remote CLI.

Then proceed with backing up XenServer hosts as describes in this section.

## Back up VMs

Citrix recommends that you use a backup solution offered by one of our certified partners. For more information, see [Citrix Ready Marketplace](#).

XenServer Enterprise Edition customers running XenServer 7.3 or a newer version can take advantage of the faster changed block only backup. For more information, see Citrix blog about [Changed Block Tracking backup APIs](#).

## VM snapshots

September 5, 2018

XenServer provides a convenient mechanism that can take a snapshot of a VM storage and metadata at a given time. Where necessary, I/O is temporarily halted while the snapshot is being taken to ensure that a self-consistent disk image can be captured.

Snapshot operations result in a snapshot VM that is similar to a template. The VM snapshot contains all the storage information and VM configuration, including attached VIFs, allowing them to be exported and restored for backup purposes. Snapshots are supported on all storage types. However, for the LVM-based storage types the following requirements must be met:

- If the storage repository was created on a previous version of XenServer, it must have been upgraded
- The volume must be in the default format (you cannot take a snapshot of `type=raw` volumes)

The snapshot operation is a two-step process:

- Capturing metadata as a template.
- Creating a VDI snapshot of the disks.

Three types of VM snapshots are supported: regular, quiesced, and snapshot with memory

## **Regular snapshots**

Regular snapshots are crash consistent and can be performed on all VM types, including Linux VMs.

## **Quiesced snapshots**

Quiesced snapshots take advantage of the Windows Volume Shadow Copy Service (VSS) to generate application consistent point-in-time snapshots. The VSS framework helps VSS-aware applications (for example, Microsoft SQL Server) flush data to disk and prepare for the snapshot before it is taken.

Quiesced snapshots are therefore safer to restore, but can have a greater performance impact on a system while they are being taken. They may also fail under load so more than one attempt to take the snapshot may be required.

XenServer supports quiesced snapshots on:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32/64-bit)

Windows 8.1, Windows 8, Windows 7, Windows 2000, Windows XP, Windows 2003, and Windows Vista are not supported. For more information about quiesced snapshots, see *Advanced Notes for Quiesced Snapshots*.

## **Snapshots with memory**

In addition to saving the VMs memory (storage) and metadata, snapshots with memory also save the VMs state (RAM). This feature can be useful when you upgrade or patch software, but you also want the option to revert to the pre-change VM state (RAM). Reverting to a snapshot with memory, does not require a reboot of the VM.

You can take a snapshot with memory of a running or suspended VM via the management API, the xe CLI, or by using XenCenter.



## Create a VM snapshot

Before taking a snapshot, see the following information about any special operating system-specific configuration and considerations:

- [Prepare to clone a Windows VM by using Sysprep](#)
- [Prepare to clone a Linux VM](#)

First, ensure that the VM is running or suspended so that the memory status can be captured. The simplest way to select the VM on which the operation is to be performed is by supplying the argument `vm=name` or `vm=vm uuid`.

Run the `vm-snapshot` and `vm-snapshot-with-quietse` commands to take a snapshot of a VM.

```
1 xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
2 xe vm-snapshot-with-quietse vm=vm uuid new-name-label=vm_snapshot_name
```

## Create a snapshot with memory

Run the `vm-checkpoint` command, giving a descriptive name for the snapshot with memory, so that you can identify it later:

```
1 xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
```

When XenServer has completed creating the snapshot with memory, its uuid is displayed.

For example:

```
1 xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \
2 new-name-label=example_checkpoint_1
3 b3c0f369-59a1-dd16-ecd4-a1211df29886
```

A snapshot with memory requires at least 4 MB of disk space per disk, plus the size of the RAM, plus around 20% overhead. So a checkpoint with 256 MB RAM would require approximately 300 MB of storage.

### Note:

During the checkpoint creation process, the VM is paused for a brief period, and cannot be used during this period.

## To list all of the snapshots on your XenServer pool

Run the `snapshot-list` command:

```
1 xe snapshot-list
```

This command lists all of the snapshots in the XenServer pool.

### To list the snapshots on a particular VM

Get the uuid of the particular VM by running the `vm-list` command.

```
1 xe vm-list
```

This command displays a list of all VMs and their UUIDs. For example:

```
1 xe vm-list
2 uuid (RO): 116dd310-a0ef-a830-37c8-df41521ff72d
3 name-label (RW): Windows Server 2012 (1)
4 power-state (RO): halted
5
6 uuid (RO): 96fde888-2a18-c042-491a-014e22b07839
7 name-label (RW): Windows 2008 R2 (1)
8 power-state (RO): running
9
10 uuid (RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
11 name-label (RW): Control domain on host
12 power-state (RO): running
```

VMs can also be specified by filtering the full list of VMs on the values of fields.

For example, specifying `power-state=halted` selects all VMs whose power-state field is equal to 'halted'. Where multiple VMs are matching, the option `--multiple` must be specified to perform the operation. Obtain the full list of fields that can be matched by using the command `xe vm-list params=all`.

Locate the required VM and then enter the following:

```
1 xe snapshot-list snapshot-of=vm uuid
```

For example:

```
1 xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
```

This command lists the snapshots currently on that VM:

```
1 uuid (RO): d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
2 name-label (RW): Regular
```

```
3 name-description (RW):
4 snapshot_of (RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
5 snapshot_time (RO): 20090914T15:37:00Z
6
7 uuid (RO): 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef
8 name-label (RW): Snapshot with memory
9 name-description (RW):
10 snapshot_of (RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
11 snapshot_time (RO): 20090914T15:39:45Z
```

## Restore a VM to its previous state

Ensure that you have the uuid of the snapshot that you want to revert to, and then run the `snapshot -revert` command:

1. Run the `snapshot-list` command to find the UUID of the snapshot or checkpoint that you want to revert to:

```
1 xe snapshot-list
```

2. Note the uuid of the snapshot, and then run the following command to revert:

```
1 xe snapshot-revert snapshot-uuid=snapshot uuid
```

For example:

```
1 xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
 a1211df29886
```

After reverting a VM to a checkpoint, the VM is suspended.

### Notes:

- If there's insufficient disk space available to thickly provision the snapshot, you cannot restore to the snapshot until the current disk's state has been freed. If this issue occurs, retry the operation.
- It is possible to revert to any snapshot. Existing snapshots and checkpoints are not deleted during the revert operation.

## Delete a snapshot

Ensure that you have the UUID of the checkpoint or snapshot that you want to remove, and then run the following command:

1. Run the `snapshot-list` command to find the UUID of the snapshot or checkpoint that you want to revert to:

```
1 xe snapshot-list
```

2. Note the UUID of the snapshot, and then run the `snapshot-uninstall` command to remove it:

```
1 xe snapshot-uninstall snapshot-uuid=snapshot-uuid
```

3. This command alerts you to the VM and VDI that are deleted. Type `yes` to confirm.

For example:

```
1 xe snapshot-uninstall snapshot-uuid=1760561d-a5d1-5d5e-2be5-
 d0dd99a3b1ef
2 The following items are about to be destroyed
3 VM : 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef (Snapshot with memory)
4 VDI: 11a4aa81-3c6b-4f7d-805a-b6ea02947582 (0)
5 VDI: 43c33fe7-a768-4612-bf8c-c385e2c657ed (1)
6 VDI: 4c33c84a-a874-42db-85b5-5e29174fa9b2 (Suspend image)
7 Type 'yes' to continue
8 yes
9 All objects destroyed
```

If you only want to remove the metadata of a checkpoint or snapshot, run the following command:

```
1 xe snapshot-destroy snapshot-uuid=snapshot-uuid
```

For example:

```
1 xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
```

## Snapshot templates

### Create a template from a snapshot

You can create a VM template from a snapshot. However, its memory state is removed.

1. Use the command `snapshot-copy` and specify a `new-name-label` for the template:

```
1 xe snapshot-copy new-name-label=vm-template-name \
2 snapshot-uuid=uuid of the snapshot
```

For example:

```
1 xe snapshot-copy new-name-label=example_template_1
2 snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
```

**Note:**

This command creates a template object in the SAME pool. This template exists in the XenServer database for the current pool only.

2. To verify that the template has been created, run the command `template-list`:

```
1 xe template-list
```

This command lists all of the templates on the XenServer host.

### Export a snapshot to a template

When you export a VM snapshot, a complete copy of the VM (including disk images) is stored as a single file on your local machine. This file has a `.xva` file name extension.

1. Use the command `snapshot-export-to-template` to create a template file:

```
1 xe snapshot-export-to-template snapshot-uuid=snapshot-uuid \
2 filename=template- filename
```

For example:

```
1 xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16-
 ecd4-a1211df29886 \
2 filename=example_template_export
```

The VM export/import feature can be used in various different ways:

- As a convenient backup facility for your VMs. An exported VM file can be used to recover an entire VM in a disaster scenario.
- As a way of quickly copying a VM, for example, a special-purpose server configuration that you use many times. You simply configure the VM the way you want it, export it, and then import it to create copies of your original VM.
- As a simple method for moving a VM to another server.

For more information about the use of templates, see [Create VMs](#) and also the Managing VMs section in the XenCenter Help.

## Advanced notes for quiesced snapshots

### Note:

Do not forget to install the Xen VSS provider in the Windows guest to support VSS. This installation is done using the `install-XenProvider.cmd` script provided with the XenServer Tools. For more information, see [Windows VMs](#).

In general, a VM can only access VDI snapshots (not VDI clones) of itself using the VSS interface. A XenServer administrator can add an attribute of `snapmanager=true` to the VM `other-config` allows that VM to import snapshots of VDIs from other VMs.

### Warning:

This configuration opens a security vulnerability. Use it with care. With it, an administrator can attach VSS snapshots using an in-guest transportable snapshot ID as generated by the VSS layer to another VM for the purposes of backup.

*VSS quiesce timeout:* the Microsoft VSS quiesce period is set to a non-configurable value of 10 seconds. It is probable that a snapshot cannot complete in time. For example, if the XAPI daemon has queued extra blocking tasks such as an SR scan, the VSS snapshot may time out and fail. If this timeout happens, retry the operation.

### Note:

The more VBDs attached to a VM, the more likely it is that this timeout may be reached. Citrix recommends attaching no more than 2 VBDs to a VM to avoid reaching the timeout. However, there is a workaround to this problem. The probability of taking a successful VSS based snapshot of a VM with more than 2 VBDs can be increased when all VDIs for the VM are on different SRs.

*VSS snapshot all the disks attached to a VM:* to store all data available at the time of a VSS snapshot. The XAPI manager takes a snapshot of all disks and the VM metadata associated with a VM that you can take a snapshot of by using the XenServer storage manager API. If the VSS layer requests a snapshot of only a subset of the disks, a full VM snapshot is not taken.

*vm-snapshot-with-quiesce:* Produces bootable snapshot VM images: The XenServer VSS hardware provider makes snapshot volumes writable, including the snapshot of the boot volume.

*VSS snap of volumes hosted on dynamic disks in the Windows Guest:* The `vm-snapshot-with-quiesce` CLI and the XenServer VSS hardware provider do not support snapshots of volumes hosted on dynamic disks on the Windows VM.

### Note:

Do not forget to install the Xen VSS provider in the Windows guest to support VSS. This installation is done using the `install-XenProvider.cmd` script provided with the XenServer Tools. For more information, see [Windows VMs](#).

## Scheduled snapshots

The Scheduled Snapshots feature provides a simple backup and restore utility for your critical service VMs. Regular scheduled snapshots are taken automatically and can be used to restore individual VMs. Scheduled Snapshots work by having pool-wide snapshot schedules for selected VMs in the pool. When a snapshot schedule is enabled, Snapshots of the specified VM are taken at the scheduled time each hour, day, or week. Several Scheduled Snapshots may be enabled in a pool, covering different VMs and with different schedules. A VM can be assigned to only one snapshot schedule at a time.

XenCenter provides a range of tools to help you use this feature:

- To define a Scheduled Snapshot, use the **New snapshot schedule** wizard.
- To enable, disable, edit, and delete Scheduled Snapshots for a pool, use the **VM Snapshot Schedules** dialog box.
- To edit a snapshot schedule, open its **Properties** dialog box from the **VM Snapshot Schedules** dialog box.
- To revert a VM to a scheduled snapshot, select the snapshot on the **Snapshots** tab and revert the VM to it.

For more information about Scheduled Snapshots, see *XenCenter Help*.

## Cope with machine failures

September 5, 2018

This section provides details of how to recover from various failure scenarios. All failure recovery scenarios require the use of one or more of the backup types listed in [Backup](#).

### Member failures

In the absence of HA, master nodes detect the failures of members by receiving regular heartbeat messages. If no heartbeat has been received for 600 seconds, the master assumes the member is dead. There are two ways to recover from this problem:

- Repair the dead host (e.g. by physically rebooting it). When the connection to the member is restored, the master will mark the member as alive again.
- Shutdown the host and instruct the master to forget about the member node using the `xe host-forget` CLI command. Once the member has been forgotten, all the VMs which were running there will be marked as offline and can be restarted on other XenServer hosts. Note it is *very* important to ensure that the XenServer host is actually offline, otherwise VM data corruption might occur. Be careful not to split your pool into multiple pools of a single host by

using `xe host-forget`, since this could result in them all mapping the same shared storage and corrupting VM data.

**Warning:**

- If you are going to use the forgotten host as an active host again, perform a fresh installation of the XenServer software.
- Do not use `xe host-forget` command if HA is enabled on the pool. Disable HA first, then forget the host, and then re-enable HA.

When a member XenServer host fails, there may be VMs still registered in the *running* state. If you are sure that the member XenServer host is definitely down, use the `xe vm-reset-powerstate` CLI command to set the power state of the VMs to *halted*. See [vm-reset-powerstate](#) for more details.

**Warning:**

Incorrect use of this command can lead to data corruption. Only use this command if absolutely necessary.

Before you can start VMs on another XenServer host, you are also required to release the locks on VM storage. Each disk in an SR can only be used by one host at a time, so it is key to make the disk accessible to other XenServer hosts once a host has failed. To do so, run the following script on the pool master for each SR that contains disks of any affected VMs: `/opt/xensource/sm/resetvdis.py host_UUID SR_UUID master`

You need only supply the third string (“master”) if the failed host was the SR master MDASH pool master or XenServer host using local storage MDASH at the time of the crash.

**Warning:**

Be absolutely sure that the host is down before executing this command. Incorrect use of this command can lead to data corruption.

If you attempt to start a VM on another XenServer host before running the script above, then you will receive the following error message: `VDI <UUID> already attached RW`.

## Master failures

Every member of a resource pool contains all the information necessary to take over the role of master if required. When a master node fails, the following sequence of events occurs:

1. If HA is enabled, another master is elected automatically.
2. If HA is not enabled, each member will wait for the master to return.

If the master comes back up at this point, it re-establishes communication with its members, and operation returns to normal.



If the master is really dead, choose one of the members and run the command `xe pool-emergency-transition-to-master` on it. Once it has become the master, run the command `xe pool-recover-slaves` and the members will now point to the new master.

If you repair or replace the server that was the original master, you can simply bring it up, install the XenServer host software, and add it to the pool. Since the XenServer hosts in the pool are enforced to be homogeneous, there is no real need to make the replaced server the master.

When a member XenServer host is transitioned to being a master, you should also check that the default pool storage repository is set to an appropriate value. This can be done using the `xe pool-param-list` command and verifying that the `default-SR` parameter is pointing to a valid storage repository.

## Pool failures

In the unfortunate event that your entire resource pool fails, you will need to recreate the pool database from scratch. Be sure to regularly back up your pool-metadata using the `xe pool-dump-database` CLI command (see [pool-dump-database](#)).

To restore a completely failed pool:

1. Install a fresh set of hosts. Do not pool them up at this stage.
2. For the host nominated as the master, restore the pool database from your backup using the `xe pool-restore-database` command (see [pool-restore-database](#)).
3. Connect to the master host using XenCenter and ensure that all your shared storage and VMs are available again.
4. Perform a pool join operation on the remaining freshly installed member hosts, and start up your VMs on the appropriate hosts.

## Cope with failure due to configuration errors

If the physical host machine is operational but the software or host configuration is corrupted:

1. Run the following command to restore host software and configuration:

```
1 xe host-restore host=host file-name=hostbackup
```

2. Reboot to the host installation CD and select **Restore from backup**.

## Physical machine failure

If the physical host machine has failed, use the appropriate procedure listed below to recover.

**Warning:**

Any VMs running on a previous member (or the previous host) which have failed will still be marked as **Running** in the database. This is for safety– simultaneously starting a VM on two different hosts would lead to severe disk corruption. If you are sure that the machines (and VMs) are offline you can reset the VM power state to **Halted**:

```
1 xe vm-reset-powerstate vm=vm_uuid --force VMs can then be
 restarted using XenCenter or the CLI.
```

**To replace a failed master with a still running member:**

1. Run the following commands:  
  
xe pool-emergency-transition-to-master  
xe pool-recover-slaves
2. If the commands succeed, restart the VMs.

**To restore a pool with all hosts failed:**

1. Run the command:

```
1 xe pool-restore-database file-name=backup
```

**Warning:**

This command will only succeed if the target machine has an appropriate number of appropriately named NICs.

2. If the target machine has a different view of the storage (for example, a block-mirror with a different IP address) than the original machine, modify the storage configuration using the **pbd-destroy** command and then the **pbd-create** command to recreate storage configurations. See [pbd commands](#) for documentation of these commands.
3. If you have created a new storage configuration, use **pbd-plug** or Storage > Repair Storage Repository menu item in XenCenter to use the new configuration.
4. Restart all VMs.

**To restore a VM when VM storage is not available:**

1. Run the following command:

```
1 xe vm-import filename=backup metadata=true
```

2. If the metadata import fails, run the command:

```
1 xe vm-import filename=backup metadata=true --force
```

This command attempts to restore the VM metadata on a 'best effort' basis.

3. Restart all VMs.

## Troubleshooting

August 13, 2018

### 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 XenServer host, 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 Citrix Solution Provider and Citrix track and resolve the issue.

For information about troubleshooting XenServer installation issues, see [Troubleshoot the installation](#). For information about troubleshooting virtual machine issues, see [Troubleshoot VM problems](#).

#### Important:

Citrix recommends that you follow the troubleshooting information in this section solely under the guidance of your Citrix Solution Provider or Citrix Support.

In some support cases, serial console access is required for debug purposes. Therefore, when setting up your XenServer 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 or HP iLO 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 XenServer 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 XenServer systems based on the report that CIS generates.

## Requirements

To use the Health Check feature:

- All hosts in the pool must be running XenServer 7.6
- Connect to the XenServer pool using XenCenter shipped with XenServer 7.6
- 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 the XenCenter Help.

## XenServer host logs

XenCenter can be used to gather XenServer host 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 details, see the XenCenter Help.

Additionally, the XenServer host 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 Citrix 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 Citrix Support, use the `xe` command `host-crashdump-upload`. For a full description of this command and its optional parameters, see `host-crashdump-upload`.

**Important:**

XenServer host 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 XenServer host 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:

```
1 xe host-param-set uuid=BRAND_SERVER_host_uuid logging:
 syslog_destination=hostname
```

Run the command:

```
1 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 XenServer host**

If you have trouble connecting to the XenServer host with XenCenter, check the following:

- Is your XenCenter an older version than the XenServer host you are attempting to connect to?

The XenCenter application is backward-compatible and can communicate properly with older XenServer hosts, but an older XenCenter cannot communicate properly with newer XenServer hosts.

To correct this issue, install the XenCenter version that is the same, or newer, than the XenServer host version.

- Is your license current?

You can see the expiration date for your license access code in the XenServer host **General** tab under the **License Details** section in XenCenter.

For more information on licensing a host, see [Licensing](#).

- The XenServer host 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 XenServer host and the machine running the client software, ensure that it allows traffic from these ports.

## Integration overview

October 4, 2018

The XenServer-Nutanix Integration feature enables Citrix customers to reap Nutanix's hyper-converged infrastructure (HCI) benefits such as linear scalability and reduced complexity. This feature also allows Nutanix customers to deploy XenServer on the Nutanix HCI platform. You can take advantage of the mature, fully featured, and highly optimized integration of XenServer into the wider Citrix stack. That stack includes Citrix Virtual Apps and Desktops with both MCS and PVS, and App Disks. Additionally, Nutanix customers can also benefit from the unique selling points of XenServer such as:

- Leading graphics virtualization solution
- Automated delivery of I/O drivers through Windows Update
- Support for Containers
- PVS Read Cache
- Advanced threat detection using Direct Inspect APIs

Customers can use the Nutanix Prism web console to configure your storage and clusters (pools), and to monitor the HCI platform, including the VM storage. Managing the XenServer and performing VM lifecycle operations can be done using XenCenter.

**Notes:**

- XenServer-Nutanix Integration applies only to Nutanix servers, and to certified servers running the Nutanix stack. For a list of supported servers, see the [Hardware Compatibility List](#).
- This guide serves as an auxiliary document to complement the [XenServer on Nutanix Administration Guide](#).
- Every XenServer release requires a compatible Nutanix release to enable the XenServer-Nutanix Integration feature. For information about compatible releases, see the [XenServer on Nutanix Administration Guide](#).

**Compatibility requirements and caveats**

With the tight integration of Nutanix with XenServer, the following XenServer features do not apply to the Nutanix HCI deployments:

- **Storage XenMotion** - Storage XenMotion enables the movement of a VM's storage from one Storage Repository (SR) to another. However, Nutanix enables the aggregation of storage for an entire cluster.
- **Disaster Recovery (DR)** - The DR feature in XenServer is based on array-level mirroring that is not applicable in Nutanix deployments.
- **WLB Power Management** - Within HCI environments, the removal of any hardware has to be tightly managed. This removal is orchestrated through the Nutanix Prism UI, hence the Power Management feature in XenServer Workload Balancing (WLB) is not permissible for Nutanix deployments.
- **SRs** - HCIs mandate their own SR, simplifying the choice of SR type. Local, NFS, iSCSI, Hardware HBA, SMB/CIFS, and Software FCoE are not available. However, ISO libraries are supported.
- **IntelliCache** - The IntelliCache feature in XenServer does not apply as Nutanix storage already ensures data locality.
- **XenCenter Automated Updates** - The host-aggregated clustered storage requires that hosts are restarted in a specific sequence.

When using the XenCenter **Install Tools** wizard, the **Automated Updates** option is not available. Instead choose to **Download update or new version from Citrix** or to **Select update or supplemental pack from disk**.

After you have installed the updates, use the Nutanix Prism console to trigger a Rolling Pool Restart if a restart is required. This process ensures that the restarts occur in the correct sequence.

In addition, the following limitations also apply when using XenServer on Nutanix:

- The concept of 'cluster' in Nutanix maps to the concept of 'pool' in XenServer. This mapping means that the cluster size is limited to a maximum 64 hosts per cluster.
- High availability can only accommodate a single host failure (assuming there are at least three hosts in a cluster). This limit is only enforced in XenCenter.
- Customers must use OVS as the network back-end. Linux Bridge is not supported.
- The XenServer VSS provider that enables quiesced snapshots is not applicable as the integration is based on Nutanix native snapshot format.

## Configuration

Use the Nutanix Prism web console to configure storage and cluster infrastructure and to monitor the HCI platform, including the VM storage. Managing the XenServer and performing VM lifecycle operations can be done using XenCenter.

### Note:

Use the Nutanix Prism console to manage host membership in the cluster and pool. The options for pool-join and -eject are disabled on the XenServer user interfaces. This recommendation is because hosts in the XenServer pool must match the hosts in the Nutanix cluster.

The Nutanix software stack runs inside a privileged VM called the Controller VM (CVM) on each host. Similar to the XenServer Control Domain (dom0), the CVM domain is visible in CLI and in XenCenter on the **Nutanix CVM Console** tab of the host. The Controller VM is not displayed as a VM in XenCenter.

### To modify the memory allocated to the Controller VM:

Depending on the Nutanix features you use, you can choose to modify the memory allocated to the Controller VM. Run the following command on the Controller VM to modify the memory allocation:

```
1 xe vm-memory-limits-set uuid=<CVM UUID>
2 static-min=10GiB dynamic-min=10GiB dynamic-max=10GiB
3 static-max=10GiB
```

### Note:

Restart the host for the changes to take effect.

## Measured Boot Supplemental Pack

November 13, 2018

The XenServer Measured Boot Supplemental Pack enables customers to measure key components of their XenServer hosts at boot time. It also provides APIs that enable remote attestation solutions



to collect these measurements securely. This supplemental pack is compatible with Intel computer systems that support *Trusted Execution Technology* (TXT).

This supplemental pack is available to download from the [XenServer 7.6 Enterprise Edition](#) page.

**Note:**

Measured Boot Supplemental Pack is available for XenServer Enterprise Edition customers, or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement.

## Background

After installation of this Supplemental Pack, when a XenServer host next boots, Intel's TXT takes measurements of low level system components (such as firmware, BIOS, Xen hypervisor, dom0 kernel, and the dom0 initrd) and stores them in a secure location on the host known as the *Trusted Platform Module* (TPM). A new interface is provided for clients, such as a remote attestation solution, to collect these measurements securely.

## Remote attestation

Remote Attestation solutions work by connecting to a XenServer host that is in a 'known good' clean state. It can remotely and securely query the XenServer host's TPM for a list of low level key system measurements. It stores these measurements in a 'white-list' or 'known good' measurements list.

At this point, the remote attestation software periodically collects key system measurements and compares them to its 'known good' list.

A host is considered 'untrusted' in the following cases:

- If the remote attestation software is unable to collect the measurements
- If the measurements change
- If the cryptographic keys are not valid

In this event, the customer is notified. Higher-level orchestration software, such as CloudStack, OpenStack, or workload balancing software can perform intelligent security operations on the affected hosts.

## Prepare the XenServer host

For this Supplemental Pack to function correctly, before attempting to gather data, edit the following settings in their host's BIOS:

1. Set up the XenServer host to boot in legacy mode.

**Note:**

UEFI boot mode is not supported with measured boot.

2. Enable **Intel AES-NI**.
3. Switch on **TPM Security** or **On with pre-boot measurements**.
4. Clear the TPM.

This action erases any previous settings and passwords associated with the TPM to allow the XenServer Measured Boot Supplemental Pack to take control of the TPM.

**Note:**

A reboot is required after this step.

5. Enable **TPM**.
6. Enable **Intel TXT**.

**Note:**

- A reboot is required after step 5 and step 6.
- BIOS settings vary according to hardware manufacturer. Consult your hardware documentation to see how to enable the TPM and TXT for their specific environment.

## Install the Supplemental Pack

Use the XenServer CLI to install this Supplemental Pack. As with any software update, Citrix advises customers to back up their data before applying this supplemental pack.

Supplemental Packs can be transmitted within a *zip* file. If the Supplemental Pack ISO is contained within a zip file, unzip this zip file (to produce the disk ISO image), before carrying out the steps below.

### Install onto a running XenServer system

1. Download the Supplemental Pack directly to the XenServer host to be updated.

Citrix recommends storing it in the `/tmp/` directory.

Alternatively, you can download the file to an internet-connected computer, and burn the ISO image to a CD.

2. Use XenCenter to access the XenServer host's console, or use secure shell (SSH) to log on directly.
3. The simplest method is to install directly from the ISO file. Enter the following:

```
1 xe-install-supplemental-pack /tmp/XenServer-7.6-measured-boot.iso
```

Alternatively, if you chose to burn the ISO to a CD, you must mount the disk. For example, for a CD-ROM, enter the following:

```
1 mkdir -p /mnt/tmp
2 mount /dev/<path to cd-rom> /mnt/tmp
3 cd /mnt/tmp/
4 ./install.sh
5 cd /
6 umount /mnt/tmp
```

4. In order for the changes to take effect, reboot your host.

## Reinstallation

If you are installing this Supplemental Pack on top of a previous version, confirm overwriting the previous installation. Enter **Y** when prompted during `xe-install-supplemental-pack` installation.

## Update default password

In previous versions of the supplemental pack, the default password was set to `xenroot` with a trailing newline. This trailing newline has been removed for the default password in this version of the supplemental pack with the new default password being `xenroot`.

A custom password can be set in `/opt/xensource/tpm/config` and must be a sha1 hash of a plain text password, which can be generated with `echo -n <password> | sha1sum`. If `-n` is omitted from this command line, a trailing newline is included in the password.

## Set asset tags

Asset tags can be set using the `/opt/xensource/tpm/xentpm` binary with the `--tpm_set_asset_tag` and `--tpm_clear_asset_tag` methods, or can also be set using the management API `tpm` plug-in with the `tpm_set_asset_tag` (taking a 'tag' argument) and `tpm_clear_asset_tag` functions:

```
1 /opt/xensource/tpm/xentpm --tpm_set_asset_tag <tag_sha1>
2 /opt/xensource/tpm/xentpm --tpm_clear_asset_tag
3 xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=tpm_set_asset_tag
 args:tag=<tag_sha1>
4 xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=tpm_clear_asset_tag
```

**Note:**

A reboot is required after this step.

## More information

To download the Measured Boot Supplemental Pack, see the [XenServer 7.6 Enterprise Edition](#) page.

If you experience any difficulties with installing this Supplemental Pack, contact [Citrix Technical Support](#).

For XenServer 7.6 documentation, visit the [Citrix Product Documentation](#) website.

## Workload Balancing

March 28, 2019

Workload Balancing is a XenServer component, packaged as a virtual appliance, that:

- Creates reports about VM performance in your XenServer environment
- Evaluates resource utilization and locates virtual machines on the best possible hosts in the pool for their workload's needs

**Notes:**

- Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement.
- Workload Balancing 7.6 is compatible with all supported versions of XenServer.

Even if you don't want to use Workload Balancing to balance your VMs, you might want to run it anyway for the workload reporting feature. When deployed to manage virtual machine workloads, Workload Balancing can:

- Balance VM workloads across hosts in a XenServer resource pool
- Determine the best host on which to start a virtual machine
- Determine the best host on which to resume a virtual machine that you powered off
- Determine the best host to move a virtual machine to when a host fails
- Determine the optimal server for each of the host's virtual machines when you put a host into or take a host out of Maintenance Mode

Depending on your preference, Workload Balancing can accomplish these tasks automatically or prompt you to accept its rebalancing and placement recommendations. You can also configure

Workload Balancing to power off hosts automatically at specific times of day (for example, to save power at night).

Workload Balancing functions by evaluating the use of VMs across a pool. When a host exceeds a performance threshold, Workload Balancing relocates the VM to a less-taxed host in the pool. To rebalance workloads, Workload Balancing moves VMs to balance the resource use on hosts.

To ensure that the rebalancing and placement recommendations align with your environment's needs, you can configure Workload Balancing to optimize workloads for either resource performance or to maximize the number of virtual machines that fit on hosts. These optimization modes can be configured to change automatically at predefined times or stay the same always. For extra granularity, fine-tune the weighting of individual resource metrics (CPU, network, disk, and memory).

To help you perform capacity planning, Workload Balancing provides historical reports about host and pool health, optimization and VM performance, and VM motion history.

## Reports on workloads

Because Workload Balancing captures performance data, you can also use this component to generate reports, known as Workload Reports, about your virtualized environment.

Workload Reports provide data for a pool or host's health, for auditing, optimizations, and placement (or motion) history. Also, you can run a chargeback report that shows virtual machine usage and can help you measure and assign costs.

To run reports, you do not need to configure for Workload Balancing to make placement recommendations or move virtual machines. However, you must configure the Workload Balancing component. Ideally, you must set critical thresholds to values that reflect the point at which the performance of the hosts in your pool degrades.

For more information, see [Generate workload reports](#).

## Workload Balancing basic concepts

When virtual machines are running, they consume computing *resources* on the physical host, such as CPU, Memory, Network Reads, Network Writes, Disk Reads, and Disk Writes. For example, some virtual machines, depending on their *workload*, might consume more CPU resources than other virtual machines on the same host. Workload is defined by the applications running on a virtual machine and their user transactions. Naturally, the combined resource consumption of all virtual machines on a host reduces the available resources on the host.

Workload Balancing captures data for resource performance on virtual machines and physical hosts and stores it in a database. Workload Balancing uses this data, combined with the preferences you set, to provide optimization and placement recommendations.

Optimizations are a way in which hosts are “improved” to align with your goals: Workload Balancing makes recommendations to redistribute the virtual machines across hosts in the pool to increase either performance or density. When Workload Balancing is making recommendations, it makes them in light of its goal: to create balance or harmony across the hosts in the pool. If Workload Balancing acts on these recommendations, the action is known as an optimization.

Within a Workload Balancing context:

- **Performance** is the usage of physical resources on a host (for example, the CPU, memory, network, and disk utilization on a host). When you set Workload Balancing to maximize performance, it recommends placing virtual machines to ensure that the maximum amount of resources are available for each virtual machine.
- **Density** is the number of VMs on a host. When you set Workload Balancing to maximize density, it recommends placing VMs so you can reduce the number of hosts powered on in a pool. It ensures that the VMs have adequate computing power.

Workload Balancing does not conflict with settings you already specified for High Availability: Citrix designed these features to work together.

## Pool requirements

To balance a pool with Workload Balancing, the hosts in the pool must meet the requirements for XenMotion (live migration), including:

- Shared remote storage
- Similar processor configurations
- Gigabit Ethernet

If the hosts do not meet these requirements, Workload Balancing cannot migrate the virtual machines in the pool.

### Note

Workload Balancing is not supported for a pool that contains vGPU-enabled VMs. Workload Balancing cannot capacity plan for VMs that have a vGPU attached.

## Get started with Workload Balancing

January 2, 2019

You can configure the Workload Balancing virtual appliance in just a few easy steps:

1. Download the Workload Balancing virtual appliance from <http://www.citrix.com/downloads>, and import it into XenCenter.
2. Configure Workload Balancing Appliance from the virtual appliance console.
3. Connect your pool to the Workload Balancing virtual appliance.

The sections that follow explain these steps. For an overview of Workload Balancing and additional information, see the XenServer Workload Balancing 7.5 Administrator's Guide and the XenCenter Help.

To balance a pool with Workload Balancing, the pool's hosts must meet the requirements for XenMotion (live migration) as described in [Administer](#).

## Import the Workload Balancing virtual appliance

The Workload Balancing virtual appliance is a single pre-installed virtual machine designed to run on a XenServer host. Before importing it, review the prerequisite information and considerations.

### Prerequisites

This appliance is designed to run on XenServer 7.1 and higher. It can monitor pools running XenServer 5.5 hosts and higher. Citrix recommends using the XenCenter management console to import the virtual appliance. The Workload Balancing virtual appliance requires a minimum of 2 GB of RAM and 20 GB of disk space to run.

### Information to consider before importing the virtual appliance

Before importing the virtual appliance, note the following information and make the appropriate changes to your environment, as applicable. Also, check the Workload Balancing release notes for late-breaking, release-specific requirements.

- **Communications Port.** Before you launch the Workload Balancing Configuration wizard, determine the port over which you want the Workload Balancing virtual appliance to communicate. You are prompted for this port during Workload Balancing Configuration. By default, Workload Balancing server uses 8012.

#### Note:

Do not set the Workload Balancing port to port 443. The Workload Balancing virtual appliance cannot accept connections over port 443 (the standard SSL/HTTPS port).

- **Account for Workload Balancing.** The Workload Balancing Configuration wizard requires that you select and enter a user name and password for the Workload Balancing account and the

database account. You do not need to create these accounts before running the Configuration wizard. The Configuration wizard creates these accounts for you.

- **Monitoring Across Pools.** You can put the Workload Balancing virtual appliance in one pool and monitor a different pool with it. (For example, the Workload Balancing virtual appliance is in Pool A but you are using it to monitor Pool B.)

**Note:**

The Workload Balancing virtual appliance requires that the time on the physical computer hosting the virtual appliance matches that in use by the monitored pool. There is no way to change the time on the Workload Balancing virtual appliance. Citrix recommends pointing both the physical computer hosting Workload Balancing and the hosts in the pool it is monitoring to the same Network Time (NTP) server.

- **XenServer and Workload Balancing communicate over HTTPS.** Therefore, during Workload Balancing Configuration, Workload Balancing automatically creates a self-signed certificate on your behalf. You can change this certificate to one from a certificate authority or configure XenServer to verify the certificate or both. For information, see the Workload Balancing Administrator's Guide.
- **Storing Historical Data and Disk Space Size.** The amount of historical data you can store is based on the following:
  - The size of the virtual disk allocated to Workload Balancing (by default 20 GB)
  - The minimum disk required space, which is 2,048 MB by default and controlled by the `GroomingRequiredMinimumDiskSizeInMB` parameter in the `wlb.conf` file.

If you want to store much historical data, you can do one of the following:

- Archive the data as described in [Administer](#)
- Make the virtual disk size assigned to the Workload Balancing virtual appliance larger.

For example, when you want to use the WLB Pool Audit trail feature and configure the report granularity to medium or above.

To increase the disk size, import the virtual appliance and then increase the virtual disk size by following the procedures in the Workload Balancing Administrator's Guide.

- **Load balancing Workload Balancing.** If you want to use your Workload Balancing virtual appliance to manage itself, specify shared remote storage when importing the virtual appliance.

**Note:**

Workload Balancing cannot perform Start On placement recommendation for the Workload Balancing virtual appliance when you are using Workload Balancing to manage itself. The reason that Workload Balancing cannot make placement recommendations when it



is managing itself is because the virtual appliance must be running to perform that function. However, it can balance the Workload Balancing virtual appliance just like it would balance any other VM it is managing.

## Plan for resource pool sizing

Workload Balancing requires specific configurations to run successfully in large pools.

## Download the virtual appliance

The Workload Balancing virtual appliance is packaged in an `.xva` format. You can download the virtual appliance from the Citrix download page <http://www.citrix.com/downloads>. When downloading the file, save it to a folder on your local hard drive (typically on the computer where XenCenter is installed). When the `.xva` download is complete, you can import it into XenCenter.

## Import the virtual appliance into XenCenter

Use XenCenter to import the Workload Balancing virtual appliance into a pool.

To import the virtual appliance into XenServer:

1. Open XenCenter.
2. Right-click on the pool (or host) into which you want to import the virtual appliance package, and select **Import**.
3. Browse to the `vpx-wlb.xva` package.
4. Select the pool or Home Server where you want to run the Workload Balancing virtual appliance.

When you select the pool, the VM automatically starts on the most suitable host in that pool.

Alternatively, if you don't manage the Workload Balancing virtual appliance using Workload Balancing, you can set a Home Server for the Workload Balancing virtual appliance. This setting ensures that the virtual appliance always starts on the same host.

5. Choose a storage repository on which to store the virtual disk for the Workload Balancing virtual appliance. This repository must have a minimum of 20 GB of free space.

You can choose either local or remote storage. However, if you choose local storage, you cannot manage the virtual appliance with Workload Balancing.

6. Define the virtual interfaces for the Workload Balancing virtual appliance. In this release, Workload Balancing is designed to communicate on a single virtual interface.

7. Choose a network that can access the pool you want Workload Balancing to manage.
8. Leave the **Start VMs after import** check box enabled, and click **Finish** to import the virtual appliance.
9. After you finish importing the Workload Balancing `.xva` file, the Workload Balancing virtual machine appears in the **Resource** pane in XenCenter.

## Configure the Workload Balancing virtual appliance

After you finish importing the Workload Balancing virtual appliance, you must configure it before you can use it to manage your pool. To guide you through the configuration, the Workload Balancing virtual appliance provides you with a configuration wizard in XenCenter. To display it, select the virtual appliance in the Resource pane and click the Console tab. For all options, press Enter to accept the default choice.

1. After importing the Workload Balancing virtual appliance, click the **Console** tab.
2. Enter `yes` to accept the terms of the license agreement. To decline the EULA, enter `no`.

### Note:

The Workload Balancing virtual appliance is also subject to the licenses contained in the `/opt/vpx/wlb` directory in the Workload Balancing virtual appliance.

3. Enter and confirm a new root password for the Workload Balancing virtual machine. Citrix recommends selecting a strong password.

### Note:

When you enter the password, the console does not display placeholders, such as asterisks, for the characters.

4. Enter the computer name you want to assign to the Workload Balancing virtual appliance.
5. Enter the domain suffix for the virtual appliance.

For example, if the fully qualified domain name (FQDN) for the virtual appliance is `wlb-vpx-pos-pool.domain4.bedford4.ctx`, enter `domain4.bedford4.ctx`.

### Note:

The Workload Balancing virtual appliance does not automatically add its FQDN to your Domain Name System (DNS) server. Therefore, if you want the pool to use an FQDN to connect to Workload Balancing, you must add the FQDN to your DNS server.

6. Enter `y` to use DHCP to obtain the IP address automatically for the Workload Balancing virtual machine. Otherwise, enter `n` and then enter a static IP address, subnet mask, and gateway for the virtual machine.

**Note:**

Using DHCP is acceptable provided the lease of the IP address does not expire. It is important that the IP address does not change: When it changes, it breaks the connection between XenServer and Workload Balancing.

7. Enter a user name for the Workload Balancing database, or press **Enter** to use the default user name (postgres) of the database account.

You are creating an account for the Workload Balancing database. The Workload Balancing services use this account to read/write to the Workload Balancing database. Note the user name and password. You might need them if you ever want to administer to the Workload Balancing PostgreSQL database directly (for example, if you wanted to export data).

8. Enter a password for the Workload Balancing database. After pressing **Enter**, messages appear stating that the Configuration wizard is loading database objects.
9. Enter a user name and password for the Workload Balancing Server.

This action creates the account XenServer uses to connect to Workload Balancing. The default user name is **wlbuser**.

10. Enter the port for the Workload Balancing Server. The Workload Balancing server communicates by using this port.

By default, the Workload Balancing server uses 8012. The port number cannot be set to 443, which is the default SSL port number.

**Note:**

If you change the port here, specify that new port number when you connect the pool to Workload Balancing. For example, by specifying the port in the **Connect to WLB Server** dialog.

Ensure that the port you specify for Workload Balancing is open in any firewalls.

After you press **Enter**, Workload Balancing continues with the virtual appliance configuration, including creating self-signed certificates.

11. Now, you can also log in to the virtual appliance by entering the VM user name (typically **root**) and the root password you created earlier. However, logging in is only required when you want to run Workload Balancing commands or edit the Workload Balancing configuration file.

After configuring Workload Balancing, connect your pool to the Workload Balancing virtual appliance as described in *Connect to the Workload Balancing virtual appliance*.

If necessary, you can find the Workload Balancing configuration file in the following location: `/opt/vpx/wlb/wlb.conf`. The Workload Balancing log file is in this location: `/var/log/wlb/LogFile.log`. More information about these files and their purpose is in the *Workload Balancing Administrator's Guide*.

## Connect to the Workload Balancing virtual appliance

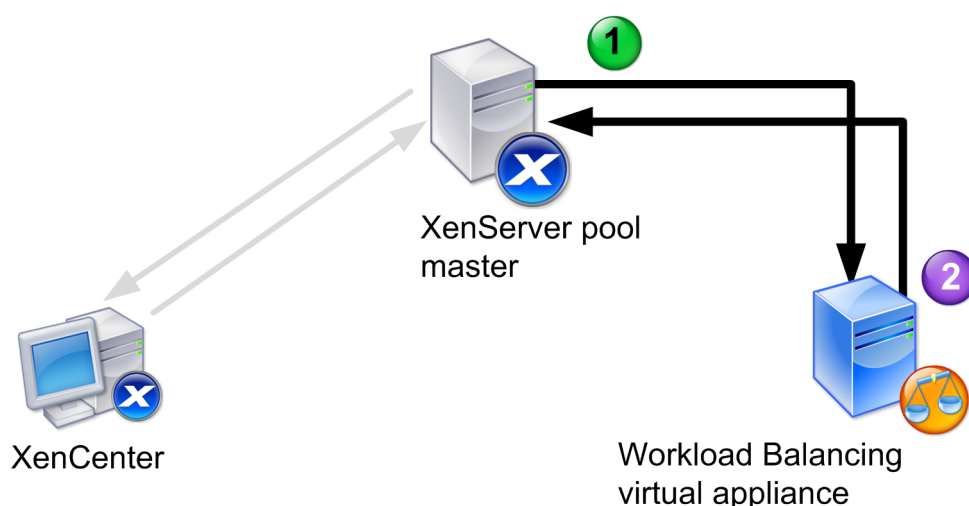
### Note:

Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

After configuring Workload Balancing, connect the pool you want managed to the WLB virtual appliance by using either the CLI or XenCenter.

To complete the XenCenter procedure that follows, you need the:

- IP address or FQDN of the Workload Balancing virtual appliance and its port number
- Credentials for the resource pool (that is, the pool master) you want Workload Balancing to monitor.
- Credentials for the Workload Balancing account you created during Workload Balancing configuration. XenServer uses this account to communicate with Workload Balancing.



To specify the Workload Balancing FQDN when connecting to the Workload Balancing server, first add its host name and IP address to your DNS server.

When you first connect to Workload Balancing, it uses the default thresholds and settings for balancing workloads. Automatic features, such as Automated Optimization Mode, Power Management, and Automation, are disabled by default.

## Connect to Workload Balancing and certificates

If you want to upload a different (trusted) certificate or configure certificate verification, note the following before connecting your pool to Workload Balancing:

- If you want XenServer to verify the self-signed Workload Balancing certificate, you must use the Workload Balancing IP address to connect to Workload Balancing. The self-signed certificate is issued to Workload Balancing based on its IP address.
- If you want to use a certificate from a certificate authority, it is easier to specify the FQDN when connecting to Workload Balancing. However, you can specify a static IP address in the **Connect to WLB Server** dialog. Use this IP address as the Subject Alternative Name (SAN) in the certificate.

More information about configuring certificates is provided in the Workload Balancing Administrator's Guide.

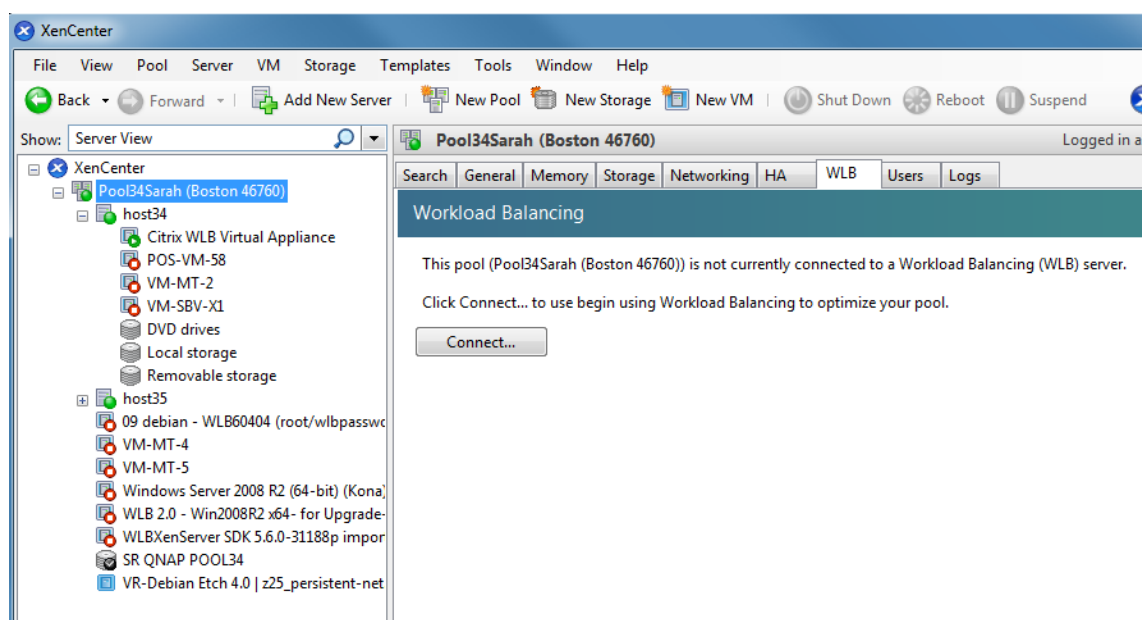
## To connect your pool to the Workload Balancing virtual appliance

### Note:

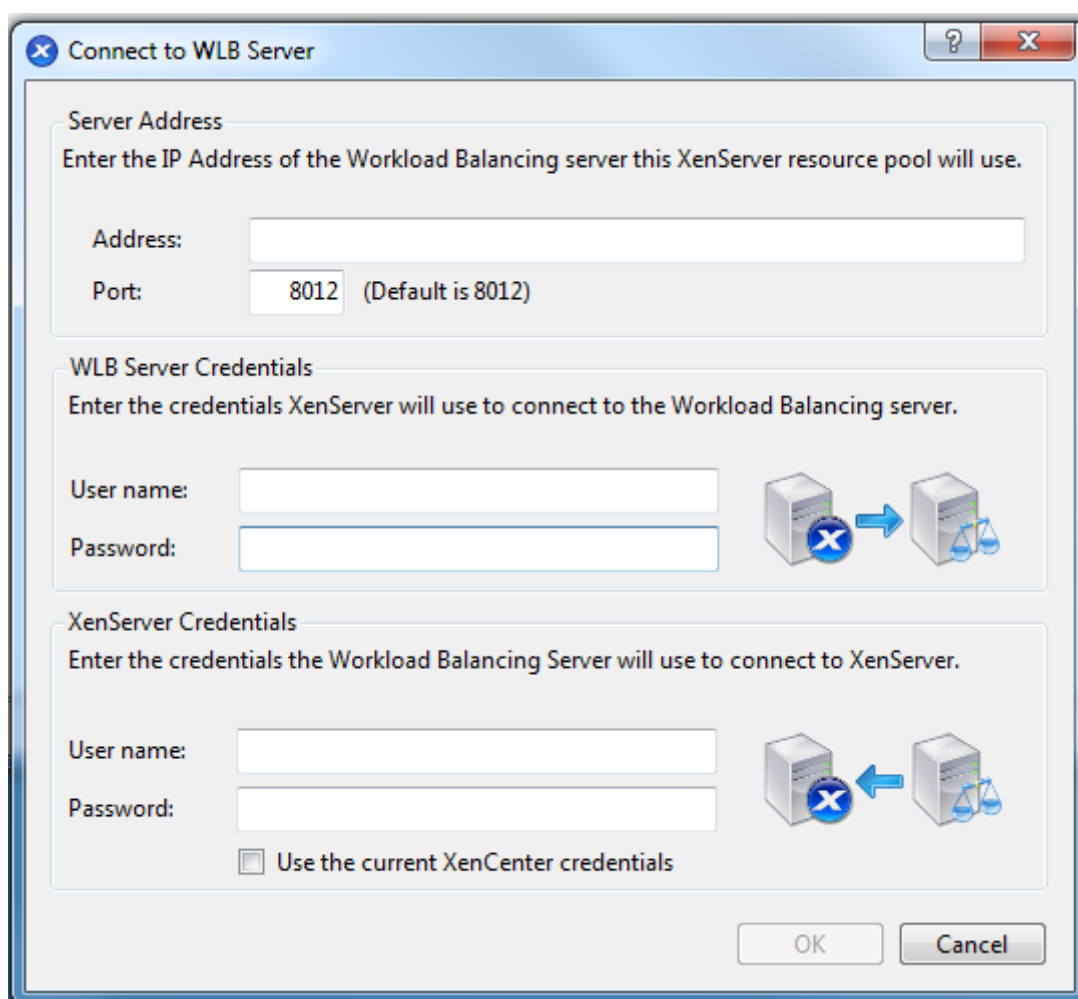
Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see the [XenServer 7.5 Licensing FAQ](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

1. In the Infrastructure pane of XenCenter, select XenCenter > *your-resource-pool*.
2. In the Properties pane, click the WLB tab.

The WLB tab displays the Connect button.



3. In the WLB tab, click Connect. The Connect to WLB Server dialog box appears.



The image shows a Windows-style dialog box titled "Connect to WLB Server". It has three main sections: "Server Address", "WLB Server Credentials", and "XenServer Credentials". Each section contains input fields for "Address" and "Password", and a "User name" field. The "Server Address" section also includes a "Port" field with the value "8012" and a note "(Default is 8012)". The "WLB Server Credentials" and "XenServer Credentials" sections each have a small icon of a server with a blue 'X' and a blue arrow pointing to a server with a blue scale. At the bottom of the dialog, there is a checkbox labeled "Use the current XenCenter credentials" and two buttons: "OK" and "Cancel".

**Connect to WLB Server**

**Server Address**  
Enter the IP Address of the Workload Balancing server this XenServer resource pool will use.

Address:

Port:  (Default is 8012)

**WLB Server Credentials**  
Enter the credentials XenServer will use to connect to the Workload Balancing server.

User name:

Password:

**XenServer Credentials**  
Enter the credentials the Workload Balancing Server will use to connect to XenServer.

User name:

Password:

☐ Use the current XenCenter credentials

OK Cancel

4. In the Server Address section, enter the following:

- a) In the Address box, type the IP address or FQDN of the Workload Balancing virtual appliance. For example, your `WLB-appliance-computername.yourdomain.net`.

**Tip:**

For more information, see To obtain the IP address for the WLB virtual appliance.

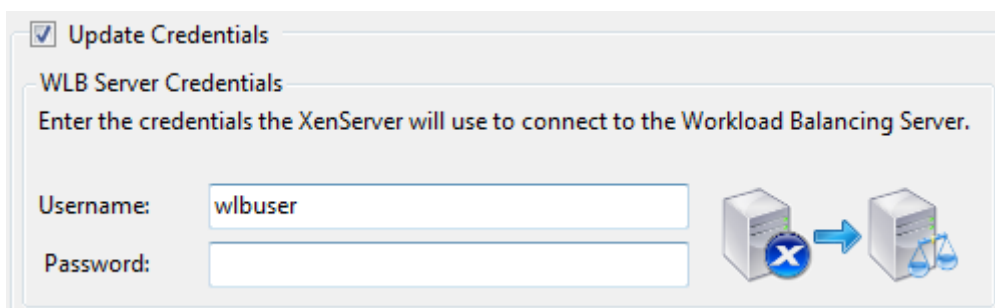
- b) (Optional) If you changed the Workload Balancing port during Workload Balancing Configuration, enter the port number in the Port box. XenServer uses this port to communicate with Workload Balancing.

By default, XenServer connects to Workload Balancing on port 8012.

**Note:**

Only edit the port number when you have changed it during Workload Balancing Configuration. The port number specified during Workload Balancing Configuration, in any firewall rules, and in the Connect to WLB Server dialog must match.

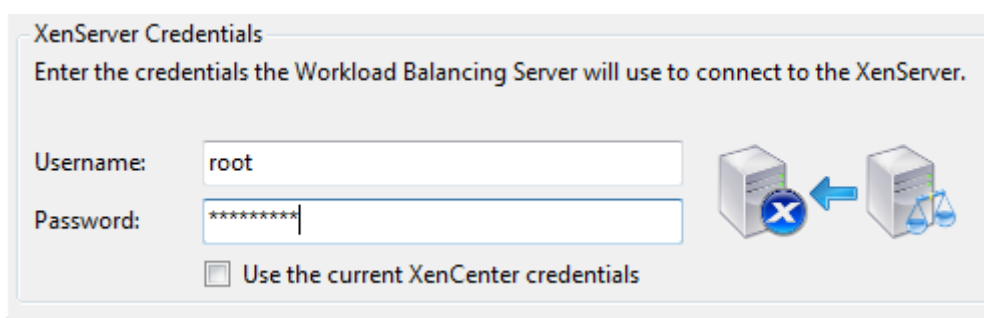
5. In the WLB Server Credentials section, enter the user name and password the XenServer pool (master) uses to connect to the Workload Balancing virtual appliance.



The screenshot shows a configuration window titled "Update Credentials" with a checked checkbox. Below it is the "WLB Server Credentials" section, which contains the instruction: "Enter the credentials the XenServer will use to connect to the Workload Balancing Server." There are two input fields: "Username:" with the text "wlbuser" and "Password:" which is empty. To the right of the fields is an icon showing a server rack with a blue 'X' and an arrow pointing to a server rack with a balance scale.

These credentials must be the account you created during Workload Balancing Configuration. By default, the user name for this account is **wlbuser**.

6. In the XenServer Credentials section, enter the user name and password for the pool you are configuring (typically the password for the pool master). Workload Balancing uses these credentials to connect to the hosts in the pool.



The screenshot shows a configuration window titled "XenServer Credentials" with the instruction: "Enter the credentials the Workload Balancing Server will use to connect to the XenServer." There are two input fields: "Username:" with the text "root" and "Password:" with masked text "\*\*\*\*\*". Below the password field is a checkbox labeled "Use the current XenCenter credentials" which is currently unchecked. To the right of the fields is an icon showing a server rack with a balance scale and an arrow pointing to a server rack with a blue 'X'.

To use the credentials with which you are currently logged into XenServer, select the Use the current XenCenter credentials check box. If you have assigned a role to this account by using the RBAC feature, ensure that the role has sufficient permissions to configure Workload Balancing. For more information, see the RBAC section of the Workload Balancing Administrator's Guide.

7. After connecting the pool to the Workload Balancing virtual appliance, Workload Balancing automatically begins monitoring the pool with the default optimization settings. To modify these settings or change the priority given to specific resources, wait at least 60 seconds before proceeding. Or wait until the XenCenter Log shows that discovery is finished.

#### Important:

After Workload Balancing is running for a time, if you do not receive optimal recommendations, evaluate your performance thresholds as described in [Administer](#). It is critical to set Workload Balancing to the correct thresholds for your environment or its recommendations might not be appropriate.

#### To obtain the IP address for the WLB virtual appliance

1. Select the Workload Balancing virtual appliance in the Resource pane in XenCenter, and select the Console tab.
2. Log in to the appliance. Enter the VM user name (typically “root”) and the root password you created when you imported the appliance.
3. Enter the following command at the prompt:

```
1 ifconfig
```

## Administer the Workload Balancing virtual appliance

March 28, 2019

This article provides information about the following subjects:

- Using Workload Balancing to start VMs on the best possible host
- Accepting the recommendations Workload Balancing issues to move VMs to different hosts

### Note:

Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

## Introduction to basic tasks

Workload Balancing is a powerful XenServer component that includes many features designed to optimize the workloads in your environment. These features include:

- Host power management
- Scheduling optimization-mode changes
- Running reports.

In addition, you can fine-tune the criteria Workload Balancing uses to make optimization recommendations.

However, when you first begin using Workload Balancing, there are two main tasks you use Workload Balancing for on a daily (or regular) basis:

- Determining the best host on which to run a VM
- Accepting Workload Balancing optimization recommendations



Running reports about the workloads in your environment, which is described in [Generate workload reports](#), is another frequently used task.

### **Determine the best host on which to run a VM**

VM placement enables you to determine the host on which to start and run a VM. This feature is useful when you want to restart a powered off VM and when you want to migrate a VM to a different host. Placement recommendations may also be useful in Citrix Virtual Desktops environments.

### **Accept Workload Balancing recommendations**

After Workload Balancing is running for a while, it begins to make recommendations about ways in which you can improve your environment. For example, if your goal is to improve VM density on hosts, at some point, Workload Balancing might recommend that you consolidate VMs on a host. If you aren't running in automated mode, you can choose either to accept this recommendation and apply it or to ignore it.

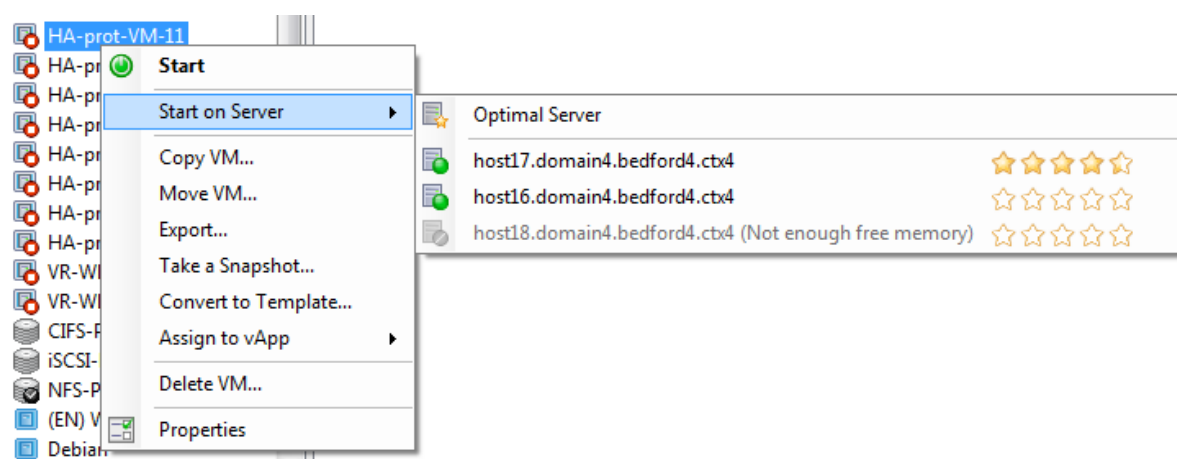
Both of these tasks, and how you perform them in XenCenter, are explained in more depth in the sections that follow.

#### **Important:**

After Workload Balancing runs for a time, if you don't receive optimal placement recommendations, evaluate your performance thresholds. This evaluation is described in [Understand when Workload Balancing makes recommendations](#). It is critical to set Workload Balancing to the correct thresholds for your environment or its recommendations might not be appropriate.

### **Choose the best host for a VM**

When you have enabled Workload Balancing and you restart an offline VM, XenCenter recommends the optimal pool members to start the VM on. The recommendations are also known as star ratings since stars are used to indicate the best host.



The term *optimal* indicates the physical server best suited to hosting your workload. There are several factors Workload Balancing uses when determining which host is optimal for a workload:

- **The amount of resources available on each host in the pool.** When a pool runs in Maximum Performance mode, Workload Balancing tries to balance the VMs across the hosts so that all VMs have good performance. When a pool runs in Maximum Density mode, Workload Balancing places VMs onto hosts as densely as possible while ensuring the VMs have sufficient resources.
- **The optimization mode in which the pool is running (Maximum Performance or Maximum Density).** When a pool runs in Maximum Performance mode, Workload Balancing places VMs on hosts with the most resources available of the type the VM requires. When a pool runs in Maximum Density mode, Workload Balancing places VMs on hosts that already have VMs running. This approach ensures that VMs run on as few hosts as possible.
- **The amount and type of resources the VM requires.** After WLB monitors a VM for a while, it uses the VM metrics to make placement recommendations according to the type of resources the VM requires. For example, Workload Balancing might select a host with less available CPU but more available memory if it is what the VM requires.

When Workload Balancing is enabled, XenCenter provides ratings to indicate the optimal hosts for starting a VM. These ratings are also provided:

- When you want to start the VM when it is powered off
- When you want to start the VM when it is suspended
- When you want to migrate the VM to a different host (Migrate and Maintenance Mode)

When you use these features with Workload Balancing enabled, host recommendations appear as star ratings beside the name of the physical host. Five empty stars indicate the lowest-rated (least optimal) server. If you can't start or migrate a VM to a host, the host name is grayed out in the menu command for a placement feature. The reason it cannot accept the VM appears beside it.

In general, Workload Balancing functions more effectively and makes better, less frequent optimization recommendations if you start VMs on the hosts it recommends. To follow the host recommenda-

tions, use one of the placement features to select the host with the most stars beside it.

### To start a virtual machine on the optimal server

1. In the Resources pane of XenCenter, select the VM you want to start.
2. From the VM menu, select Start on Server and then select one of the following:
  - **Optimal Server.** The optimal server is the physical host that is best suited to the resource demands of the VM you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
  - **One of the servers with star ratings** listed under the Optimal Server command. Five stars indicate the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

#### Tip:

You can also select Start on Server by right-clicking the VM you want to start in the Resources pane.

### To resume a virtual machine on the optimal server

1. In the Resources pane of XenCenter, select the suspended VM you want to resume.
2. From the VM menu, select Resume on Server and then select one of the following:
  - **Optimal Server.** The optimal server is the physical host that is best suited to the resource demands of the VM you are starting. Workload Balancing determines the optimal server based on its historical records of performance metrics and your placement strategy. The optimal server is the server with the most stars.
  - **One of the servers with star ratings** listed under the Optimal Server command. Five stars indicate the most-recommended (optimal) server and five empty stars indicates the least-recommended server.

#### Tip:

You can also select Resume on Server by right-clicking the suspended VM in the Resources pane.

### Accept optimization recommendations

Workload Balancing provides recommendations about ways you can migrate VMs to optimize your environment. Optimization recommendations appear in the WLB optimization tab in XenCenter.

Optimization Recommendations [View History...](#)

| VM/Host                      | Operation                                                             | Reason           |
|------------------------------|-----------------------------------------------------------------------|------------------|
| HA-prot-VM-7                 | Relocate from 'host17.domain4.bedford4.ctx4' to 'host16.domain4.be... | Consolidation    |
| host17.domain4.bedford4.ctx4 | Power off                                                             | Release Resource |

[Apply Recommendations](#)

Optimization recommendations are based on the:

- Placement strategy you select (that is, the optimization mode).
- Performance metrics for resources such as a physical host's CPU, memory, network, and disk utilization.
- The role of the host in the resource pool. When making placement recommendations, Workload Balancing considers the pool master for VM placement only if no other host can accept the workload. Likewise, when a pool operates in Maximum Density mode, Workload Balancing considers the pool master last when determining the order to fill hosts with VMs.

Optimization recommendations display the following information:

- The name of the VM that Workload Balancing recommends relocating
- The host that the VM currently resides on
- The host Workload Balancing recommends as the new location.

The optimization recommendations also display the reason Workload Balancing recommends moving the VM. For example, the recommendation displays "CPU" to improve CPU utilization. When Workload Balancing power management is enabled, Workload Balancing also displays optimization recommendations for hosts it recommends powering on or off. Specifically, these recommendations are for consolidations.

After you click Apply Recommendations, XenServer performs all operations listed in the Optimization Recommendations list.

**Tip:**

Find out the optimization mode for a pool by using XenCenter to select the pool. Look in the Configuration section of the WLB tab for the information.

### To accept an optimization recommendation

1. In the Resources pane of XenCenter, select the resource pool for which you want to display recommendations.

2. Click the WLB tab. If there are any recommended optimizations for any VMs on the selected resource pool, they display in the Optimization Recommendations section of the WLB tab.
3. To accept the recommendations, click Apply Recommendations. XenServer begins performing all the operations listed in the Operations column of the Optimization Recommendations section.

After you click Apply Recommendations, XenCenter automatically displays the Logs tab so you can see the progress of the VM migration.

### **Understand WLB recommendations under high availability**

If you have Workload Balancing and XenServer High Availability enabled in the same pool, it is helpful to understand how the two features interact. Workload Balancing is designed not to interfere with High Availability. When there is a conflict between a Workload Balancing recommendation and a High Availability setting, the High Availability setting always takes precedence. In practice, this precedence means that:

- If attempting to start a VM on a host violates the High Availability plan, Workload Balancing doesn't give you star ratings.
- Workload Balancing does not automatically power off any hosts beyond the number specified in the Failures allowed box in the **Configure HA** dialog.
  - However, Workload Balancing might still make recommendations to power off more hosts than the number of host failures to tolerate. (For example, Workload Balancing still recommends that you power off two hosts when High Availability is only configured to tolerate one host failure.) However, when you attempt to apply the recommendation, XenCenter might display an error message stating that High Availability is no longer guaranteed.
  - When Workload Balancing runs in automated mode and has power management enabled, recommendations that exceed the number of tolerated host failures are ignored. In this situation, the Workload Balancing log shows a message that power-management recommendation wasn't applied because High Availability is enabled.

### **Generate workload reports**

This section provides information about using the Workload Balancing component to generate reports about your environment, including reports about hosts and VMs. Specifically, this section provides information about the following:

- How to generate reports
- What workload reports are available

**Note:**

Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see the [Licensing](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

**Overview of workload reports**

The Workload Balancing reports can help you perform capacity planning, determine virtual server health, and evaluate how effective your configured threshold levels are.

Workload Balancing lets you generate reports on three types of objects: physical hosts, resource pools, and VMs. At a high level, Workload Balancing provides two types of reports:

- Historical reports that display information by date
- “Roll up” style reports, which provide a summarizing overview of an area

Workload Balancing provides some reports for auditing purposes, so you can determine, for example, the number of times a VM moved.

You can use the Pool Health report to evaluate how effective your optimization thresholds are. While Workload Balancing provides default threshold settings, you might need to adjust these defaults for them to provide value in your environment. If you do not have the optimization thresholds adjusted to the correct level for your environment, Workload Balancing recommendations might not be appropriate for your environment.

To generate a Workload Balancing report, the pool must be running Workload Balancing. Ideally, the pool has been running Workload Balancing for a couple of hours or long enough to generate the data to display in the reports.

**Generate a Workload Balancing report**

1. In XenCenter, from the Pool menu, select View Workload Reports.

**Tip:**

You can also display the Workload Reports screen from the WLB tab by clicking the Reports button.

2. From the Workload Reports screen, select a report from the Reports pane.
3. Select the Start Date and the End Date for the reporting period. Depending on the report you select, you might need to specify a host in the Host list box.

4. Click Run Report. The report displays in the report window. For information about the meaning of the reports, see Workload Balancing report glossary.

### Navigate in a Workload Balancing report

After generating a report, you can use the toolbar buttons in the report to navigate and perform certain tasks. To display the name of a toolbar button, pause your mouse over toolbar icon.

| Toolbar buttons                                                                     | Description                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Document Map</b> enables you to display a document map that helps you navigate through long reports.                                                                                                               |
|    | <b>Page Forward/Back</b> enables you to move one page ahead or back in the report.                                                                                                                                    |
|    | <b>Back to Parent Report</b> enables you to return to the parent report when working with drill-through reports. <b>Note:</b> This button is only available in drill-through reports, such as the Pool Health report. |
|  | <b>Stop Rendering</b> cancels the report generation.                                                                                                                                                                  |
|  | <b>Print</b> enables you to print a report and specify general printing options. These options include: the printer, the number of pages, and the number of copies.                                                   |
|  | <b>Print Layout</b> enables you to display a preview of the report before you print it. To exit Print Layout, click the Print Layout button again.                                                                    |
|  | <b>Page Setup</b> enables you to specify printing options such as the paper size, page orientation, and margins.                                                                                                      |
|  | <b>Export</b> enables you to export the report as an Acrobat (.PDF) file or as an Excel file with a .XLS extension.                                                                                                   |
|  | <b>Find</b> enables you to search for a word in a report, such as the name of a VM.                                                                                                                                   |

## Print a Workload Balancing report

Before you can print a report, you must first generate it.

1. (Optional) Preview the printed document by clicking the following Print Layout button:
2. (Optional) Change the paper size and source, page orientation, or margins by clicking the following Page Setup button:
3. Click the following Print button:

## Export a Workload Balancing report

You can export a report in either Microsoft Excel or Adobe Acrobat (PDF) formats.

1. After generating the report, click the following Export button:
2. Select one of the following items from the Export button menu:
  - Excel
  - Acrobat (PDF) file

### Note:

The data that appears between report export formats may be inconsistent, depending on the export format you select. Reports exported to Excel include all the data available for reports, including “drilldown” data. Reports exported to PDF and displayed in XenCenter only contain the data that you selected when you generated the report.

## Workload Balancing report glossary

This section provides information about the following Workload Balancing reports:

### Chargeback Utilization Analysis

You can use the Chargeback Utilization Analysis report (“chargeback report”) to determine how much of a resource a specific department in your organization used. Specifically, the report shows information about all the VMs in your pool, including their availability and resource utilization. Since this report shows VM up time, it can help you demonstrate Service Level Agreements compliance and availability.

The chargeback report can help you implement a simple chargeback solution and facilitate billing. To bill customers for a specific resource, generate the report, save it as Excel, and edit the spreadsheet to include your price per unit. Alternatively, you can import the Excel data into your billing system.

If you want to bill internal or external customers for VM usage, consider incorporating department or customer names in your VM naming conventions. This practice makes reading chargeback reports easier.



The resource reporting in the chargeback report is, sometimes, based on the allocation of physical resources to individual VMs.

The average memory data in this report is based on the amount of memory currently allocated to the VM. XenServer enables you to have a fixed memory allocation or an automatically adjusting memory allocation (Dynamic Memory Control).

The chargeback report contains the following columns of data:

- **VM Name.** The name of the VM to which the data in the columns in that row applies.
- **VM Uptime.** The number of minutes the VM was powered on (or, more specifically, appears with a green icon beside it in XenCenter).
- **vCPU Allocation.** The number of virtual CPUs configured on the VM. Each virtual CPU receives an equal share of the physical CPUs on the host. For example, consider the case where you configured eight virtual CPUs on a host that contains two physical CPUs. If the **vCPU Allocation** column has “1” in it, this value is equal to 2/16 of the total processing power on the host.
- **Minimum CPU Usage (%).** The lowest recorded value for virtual CPU utilization in the reporting period. This value is expressed as a percentage of the VM’s vCPU capacity. The capacity is based on the number of vCPUs allocated to the VM. For example, if you allocated one vCPU to a VM, **Minimum CPU Usage** represents the lowest percentage of vCPU usage that is recorded. If you allocated two vCPUs to the VM, the value is the lowest usage of the combined capacity of both vCPUs as a percentage.

Ultimately, the percentage of CPU usage represents the lowest recorded workload that virtual CPU handled. For example, if you allocate one vCPU to a VM and the pCPU on the host is 2.4 GHz, 0.3 GHz is allocated to the VM. If the **Minimum CPU Usage** for the VM was 20%, the VM’s lowest usage of the physical host’s CPU during the reporting period was 60 MHz.

- **Maximum CPU Usage (%).** The highest percentage of the VM’s virtual CPU capacity that the VM consumed during the reporting period. The CPU capacity consumed is a percentage of the virtual CPU capacity you allocated to the VM. For example, if you allocated one vCPU to the VM, the Maximum CPU Usage represents the highest recorded percentage of vCPU usage during the time reported. If you allocated two virtual CPUs to the VM, the value in this column represents the highest utilization from the combined capacity of both virtual CPUs.
- **Average CPU Usage (%).** The average amount, expressed as a percentage, of the VM’s virtual CPU capacity that was in use during the reporting period. The CPU capacity is the virtual CPU capacity you allocated to the VM. If you allocated two virtual CPUs to the VM, the value in this column represents the average utilization from the combined capacity of both virtual CPUs.
- **Total Storage Allocation (GB).** The amount of disk space that is currently allocated to the VM at the time the report was run. Frequently, unless you modified it, this disk space is the amount of disk space you allocated to the VM when you created it.

- **Virtual NIC Allocation.** The number of virtual interfaces (VIFs) allocated to the VM.
- **Current Minimum Dynamic Memory (MB).**
  - **Fixed memory allocation.** If you assigned a VM a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).
  - **Dynamic memory allocation.** If you configured XenServer to use Dynamic Memory Control, the minimum amount of memory specified in the range appears in this column. If the range has 1,024 MB as minimum memory and 2,048 MB as maximum memory, the **Current Minimum Dynamic Memory (MB)** column displays 1,024 MB.
- **Current Maximum Dynamic Memory (MB).**
  - **Dynamic memory allocation.** If XenServer adjusts a VM's memory automatically based on a range, the maximum amount of memory specified in the range appears in this column. For example, if the memory range values are 1,024 MB minimum and 2,048 MB maximum, 2,048 MB appears in the **Current Maximum Dynamic Memory (MB)** column.
  - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).
- **Current Assigned Memory (MB).**
  - **Dynamic memory allocation.** When Dynamic Memory Control is configured, this value indicates the amount of memory XenServer allocates to the VM when the report runs.
  - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Minimum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

**Note:**

If you change the VM's memory allocation immediately before running this report, the value reflected in this column reflects the new memory allocation you configured.

- **Average Assigned Memory (MB).**
  - **Dynamic memory allocation.** When Dynamic Memory Control is configured, this value indicates the average amount of memory XenServer allocated to the VM over the reporting period.
  - **Fixed memory allocation.** If you assign a VM a fixed amount of memory (for example, 1,024 MB), the same amount of memory appears in the following columns: Current Mini-

mum Dynamic Memory (MB), Current Maximum Dynamic Memory (MB), Current Assigned Memory (MB), and Average Assigned Memory (MB).

**Note:**

If you change the VM's memory allocation immediately before running this report, the value in this column might not change from what was previously displayed. The value in this column reflects the average over the time period.

- **Average Network Reads (BPS).** The average amount of data (in bits per second) the VM received during the reporting period.
- **Average Network Writes (BPS).** The average amount of data (in bits per second) the VM sent during the reporting period.
- **Average Network Usage (BPS).** The combined total (in bits per second) of the Average Network Reads and Average Network Writes. If a VM sends, on average, 1,027 bps and receives, on average, 23,831 bps during the reporting period, the Average Network Usage is the combined total of these values: 24,858 bps.
- **Total Network Usage (BPS).** The total of all network read and write transactions in bits per second over the reporting period.

## Host Health History

This report displays the performance of resources (CPU, memory, network reads, and network writes) on specific host in relation to threshold values.

The colored lines (red, green, yellow) represent your threshold values. You can use this report with the Pool Health report for a host to determine how the host's performance might affect overall pool health. When you are editing the performance thresholds, you can use this report for insight into host performance.

You can display resource utilization as a daily or hourly average. The hourly average lets you see the busiest hours of the day, averaged, for the time period.

To view report data which is grouped by hour, under **Host Health History** expand **Click to view report data grouped by house for the time period.**

Workload Balancing displays the average for each hour for the time period you set. The data point is based on a utilization average for that hour for all days in the time period. For example, in a report for May 1, 2009, to May 15, 2009, the Average CPU Usage data point represents the resource utilization of all 15 days at 12:00 hours. This information is combined as an average. If CPU utilization was 82% at 12PM on May 1, 88% at 12PM on May 2, and 75% on all other days, the average displayed for 12PM is 76.3%.

**Note:**

Workload Balancing smooths spikes and peaks so data does not appear artificially high.

**Pool Optimization Performance History**

The optimization performance report displays optimization events against that pool's average resource usage. These events are instances when you optimized a resource pool. Specifically, it displays resource usage for CPU, memory, network reads, and network writes.

The dotted line represents the average usage across the pool over the period of days you select. A blue bar indicates the day on which you optimized the pool.

This report can help you determine if Workload Balancing is working successfully in your environment. You can use this report to see what led up to optimization events (that is, the resource usage before Workload Balancing recommended optimizing).

This report displays average resource usage for the day. It does not display the peak utilization, such as when the system is stressed. You can also use this report to see how a resource pool is performing when Workload Balancing is not making optimization recommendations.

In general, resource usage declines or stays steady after an optimization event. If you do not see improved resource usage after optimization, consider readjusting threshold values. Also, consider whether the resource pool has too many VMs and whether or not you added or removed new VMs during the period that you specified.

**Pool Audit Trail**

This report displays the contents of the XenServer Audit Log. The Audit Log is a XenServer feature designed to log attempts to perform unauthorized actions and select authorized actions. These actions include:

- Import and export
- Host and pool backups
- Guest and host console access.

The report gives more meaningful information when you give XenServer administrators their own user accounts with distinct roles assigned to them by using the RBAC feature.

**Important:**

To run the audit log report, you must enable the Audit Logging feature. By default, Audit Log is always enabled in the Workload Balancing virtual appliance.

The enhanced Pool Audit Trail feature allows you to specify the granularity of the audit log report. You can also search and filter the audit trail logs by specific users, objects, and by time. The Pool

Audit Trail Granularity is set to Minimum by default. This option captures limited amount of data for specific users and object types. You can modify the setting at any time based on the level of detail you require in your report. For example, set the granularity to Medium for a user-friendly report of the audit log. If you require a detailed report, set the option to Maximum.

## Report contents

The Pool Audit Trail report contains the following:

- Time. The time XenServer recorded the user's action.
- User Name. The name of the person who created the session in which the action was performed. Sometimes, this value can be the User ID
- Event Object. The object that was the subject of the action (for example, a VM).
- Event Action. The action that occurred. For definitions of these actions, see Audit Log Event Names.
- Access. Whether or not the user had permission to perform the action.
- Object Name. The name of the object (for example, the name of the VM).
- Object UUID. The UUID of the object (for example, the UUID of the VM).
- Succeeded. This information provides the status of the action (that is, whether or not it was successful).

## Audit Log event names

The Audit Log report logs XenServer events, event objects and actions, including import/export, host and pool backups, and guest and host console access. The following table defines some of the typical events that appear frequently in the XenServer Audit Log and Pool Audit Trail report. The table also specifies the granularity of these events.

In the Pool Audit Trail report, the events listed in the [Event Action](#) column apply to a pool, VM, or host. To determine what the events apply to, see the [Event Object](#) and [Object Name](#) columns in the report. For more event definitions, see the events section of the XenServer Management API.

| Pool Audit Trail Granularity | Event Action                 | User Action                                 |
|------------------------------|------------------------------|---------------------------------------------|
| Minimum                      | <code>pool.join</code>       | Instructed the host to join a new pool      |
| Minimum                      | <code>pool.join_force</code> | Instructed (forced) the host to join a pool |

| Pool Audit Trail Granularity | Event Action                             | User Action                                                                                                              |
|------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Medium                       | <code>SR.destroy</code>                  | Destroyed the storage repository                                                                                         |
| Medium                       | <code>SR.create</code>                   | Created a storage repository                                                                                             |
| Medium                       | <code>VDI.snapshot</code>                | Took a read-only snapshot of the VDI, returning a reference to the snapshot                                              |
| Medium                       | <code>VDI.clone</code>                   | Took an exact copy of the VDI, returning a reference to the new disk                                                     |
| Medium                       | <code>VIF.plugin</code>                  | Hot-plugged the specified VIF, dynamically attaching it to the running VM                                                |
| Medium                       | <code>VIF.unplug</code>                  | Hot-unplugged the specified VIF, dynamically detaching it from the running VM                                            |
| Maximum                      | <code>auth.get_subject_identifier</code> | Queried the external directory service to obtain the subject identifier as a string from the human-readable subject name |
| Maximum                      | <code>task.cancel</code>                 | Requested that a task is canceled                                                                                        |
| Maximum                      | <code>VBD.insert</code>                  | Inserted new media into the device                                                                                       |
| Maximum                      | <code>VIF.get_by_uuid</code>             | Obtained a reference to the VIF instance with the specified UUID                                                         |
| Maximum                      | <code>VIF.get_shareable</code>           | Obtained the shareable field of the given VDI                                                                            |
| Maximum                      | <code>SR.get_all</code>                  | Returns a list of all of the SRs known to the system                                                                     |
| Maximum                      | <code>pool.create_new_blob</code>        | Created a placeholder for a named binary piece of data that is associated with this pool                                 |

| Pool Audit Trail Granularity | Event Action                      | User Action                                                                                                                                                       |
|------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum                      | <code>host.send_debug_keys</code> | Injected the given string as debugging keys into Xen                                                                                                              |
| Maximum                      | <code>VM.get_boot_record</code>   | Returned a record describing the VMs dynamic state, initialized when the VM boots, and updated to reflect runtime configuration changes, for example, CPU hotplug |

## Pool Health

The Pool Health report displays the percentage of time a resource pool and its hosts spent in four different threshold ranges: Critical, High, Medium, and Low. You can use the Pool Health report to evaluate the effectiveness of your performance thresholds.

A few points about interpreting this report:

- Resource utilization in the Average Medium Threshold (blue) is the optimum resource utilization regardless of the placement strategy you selected. Likewise, the blue section on the pie chart indicates the amount of time that host used resources optimally.
- Resource utilization in the Average Low Threshold Percent (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. If your placement strategy is Maximum Density and your resource usage is green, WLB might not be fitting the maximum number of VMs possible on that host or pool. If so, adjust your performance threshold values until most of your resource utilization falls into the Average Medium (blue) threshold range.
- Resource utilization in the Average Critical Threshold Percent (red) indicates the amount of time average resource utilization met or exceeded the Critical threshold value.

If you double-click on a pie chart for a host's resource usage, XenCenter displays the Host Health History report for that resource on that host. Clicking **Back to Parent Report** on the toolbar returns you to the Pool Health history report.

If you find that most of your report results are not in the Average Medium Threshold range, adjust the Critical threshold for this pool. While Workload Balancing provides default threshold settings, these defaults are not effective in all environments. If you do not have the thresholds adjusted to the correct level for your environment, the Workload Balancing optimization and placement recommendations might not be appropriate. For more information, see *Change the critical thresholds*.

## Pool Health History

This report provides a line graph of resource utilization on all physical hosts in a pool over time. It lets you see the trend of resource utilization—if it tends to be increasing in relation to your thresholds (Critical, High, Medium, and Low). You can evaluate the effectiveness of your performance thresholds by monitoring trends of the data points in this report.

Workload Balancing extrapolates the threshold ranges from the values you set for the Critical thresholds when you connected the pool to Workload Balancing. Although similar to the Pool Health report, the Pool Health History report displays the average utilization for a resource on a specific date. Instead of the amount of time overall the resource spent in a threshold.

Except for the Average Free Memory graph, the data points never average above the Critical threshold line (red). For the Average Free Memory graph, the data points never average *below* the Critical threshold line (which is at the bottom of the graph). Because this graph displays *free* memory, the Critical threshold is a low value, unlike the other resources.

A few points about interpreting this report:

- When the Average Usage line in the chart approaches the Average Medium Threshold (blue) line, it indicates the pool's resource utilization is optimum. This indication is regardless of the placement strategy configured.
- Resource utilization approaching the Average Low Threshold (green) is not necessarily positive. Whether Low resource utilization is positive depends on your placement strategy. In the case where:
  - Your placement strategy is Maximum Density
  - Most days the Average Usage line is at or below the green lineWorkload Balancing might not be placing VMs as densely as possible on that pool. If so, adjust the pool's Critical threshold values until most of its resource utilization falls into the Average Medium (blue) threshold range.
- When the Average Usage line intersects with the Average Critical Threshold Percent (red), this indicates the days when the average resource utilization met or exceeded the Critical threshold value for that resource.

If data points in your graphs aren't in the Average Medium Threshold range, but you are satisfied with performance, you can adjust the Critical threshold for this pool. For more information, see [Change the critical thresholds](#).

## Pool Optimization History

The Pool Optimization History report provides chronological visibility into Workload Balancing optimization activity.



Optimization activity is summarized graphically and in a table. Drilling into a date field within the table displays detailed information for each pool optimization performed for that day.

This report lets you see the following information:

- VM Name. The name of the VM that Workload Balancing optimized.
- Reason. The reason for the optimization.
- Method. Whether the optimization was successful.
- From Host. The physical server where the VM was originally hosted.
- To Host. The physical server where the VM was migrated.
- Time. The time when the optimization occurred.

**Tip:**

You can also generate a Pool Optimization History report from the WLB tab by clicking the View History link.

**Virtual Machine Motion History**

This line graph displays the number of times VMs migrated on a resource pool over a period. It indicates if a migration resulted from an optimization recommendation and to which host the VM moved. This report also indicates the reason for the optimization. You can use this report to audit the number of migrations on a pool.

Some points about interpreting this report:

- The numbers on the left side of the chart correspond with the number of migrations possible. This value is based on how many VMs are in a resource pool.
- You can look at details of the migrations on a specific date by expanding the + sign in the Date section of the report.

**Virtual Machine Performance History**

This report displays performance data for each VM on a specific host for a time period you specify. Workload Balancing bases the performance data on the amount of virtual resources allocated for the VM. For example, if Average CPU Usage for your VM is 67%, your VM uses, on average, 67% of its vCPU for the specified period.

The initial view of the report displays an average value for resource utilization over the period you specified.

Expanding the + sign displays line graphs for individual resources. You can use these graphs to see trends in resource utilization over time.

This report displays data for CPU Usage, Free Memory, Network Reads/Writes, and Disk Reads/Writes.

## **Manage Workload Balancing features and settings**

This section provides information about how to perform optional changes to Workload Balancing settings, including how to:

- Adjust the optimization mode
- Optimize and manage power automatically
- Change the critical thresholds
- Tune metric weightings
- Exclude hosts from recommendations
- Configure advanced automation settings and data storage
- Adjust the Pool Audit Trail granularity settings

This section assumes that you already connected your pool to a Workload Balancing virtual appliance. For information about downloading, importing, and configuring a Workload Balancing virtual appliance, see [Get started](#). To connect to the virtual appliance, see [Connect to the Workload Balancing Virtual Appliance](#).

## **Change Workload Balancing settings**

After connecting to the Workload Balancing virtual appliance, you can, if desired, edit the settings Workload Balancing uses to calculate placement and recommendations.

Placement and optimization settings that you can modify include the following:

- Changing the placement strategy
- Configuring automatic optimizations and power management
- Editing performance thresholds and metric weightings
- Excluding hosts.

Workload Balancing settings apply collectively to all VMs and hosts in the pool.

Provided the network and disk thresholds align with the hardware in your environment, consider using most of the defaults in Workload Balancing initially.

After Workload Balancing is enabled for a while, Citrix recommends evaluating your performance thresholds and determining whether to edit them. For example, consider if you are:

- Getting recommendations when they are not yet required. If so, try adjusting the thresholds until Workload Balancing begins providing suitable recommendations.

- Not getting recommendations when you expect to receive them. For example, if your network has insufficient bandwidth and you do not receive recommendations, you might need to tweak your settings. If so, try lowering the network critical thresholds until Workload Balancing begins providing recommendations.

Before you edit your thresholds, you can generate a Pool Health report and the Pool Health History report for each physical host in the pool.

You can use the Workload Balancing Configuration properties in XenCenter to modify the configuration settings.

To update the credentials XenServer and the Workload Balancing server use to communicate, see Edit the Workload Balancing configuration file.

In the Infrastructure pane of XenCenter, select XenCenter > [your-pool](#).

In the Properties pane, click the WLB tab.

In the WLB tab, click Settings.

### **Adjust the optimization mode**

Workload Balancing makes recommendations to rebalance, or optimize, the VM workload in your environment based on a strategy for placement you select. The placement strategy is known as the optimization mode.

Workload Balancing lets you choose from two optimization modes:

- **Maximize Performance.** (Default.) Workload Balancing attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts. When Maximize Performance is your placement strategy, Workload Balancing recommends optimization when a host reaches the High threshold.
- **Maximize Density.** Workload Balancing attempts to minimize the number of physical hosts that must be online by consolidating the active VMs.

When you select Maximize Density as your placement strategy, you can specify parameters similar to the ones in Maximize Performance. However, Workload Balancing uses these parameters to determine how it can pack VMs onto a host. If Maximize Density is your placement strategy, Workload Balancing recommends consolidation optimizations when a VM reaches the Low threshold.

Workload Balancing also lets you apply these optimization modes all of the time, Fixed, or switch between modes for specified time periods, Scheduled:

- **Fixed optimization modes** set Workload Balancing to have a specific optimization behavior always. This behavior can be either to try to create the best performance or to create the highest density.

- Scheduled optimization modes let you schedule for Workload Balancing to apply different optimization modes depending on the time of day. For example, you might want to configure Workload Balancing to optimize for performance during the day when you have users connected. To save energy, you can then specify for Workload Balancing to optimize for Maximum Density at night.

When you configure Scheduled optimization modes, Workload Balancing automatically changes to the optimization mode at the beginning of the time period you specified. You can configure Everyday, Weekdays, Weekends, or individual days. For the hour, you select a time of day.

In the Resources pane of XenCenter, select XenCenter > [your-pool](#).

In the Properties pane, click the WLB tab.

On the WLB tab, click Settings.

In the left pane, click Optimization Mode.

In the Fixed section of the Optimization Mode page, select one of these optimization modes:

- Maximize Performance. (Default.) Attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts.
- Maximize Density. Attempts to fit as many VMs as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online. (Workload Balancing considers the performance of consolidated VMs and issues a recommendation to improve performance if a resource on a host reaches a Critical threshold.)

In the Infrastructure pane of XenCenter, select XenCenter > [your-pool](#).

In the Properties pane, click the WLB tab.

On the WLB tab, click Settings.

In the left pane, click Optimization Mode

In the Optimization Mode pane, select Scheduled. The Scheduled section becomes available.

Click Add New.

In the Change to box, select one of the following modes:

- Maximize Performance. Attempts to spread workload evenly across all physical hosts in a resource pool. The goal is to minimize CPU, memory, and network pressure for all hosts.
- Maximize Density. Attempts to fit as many VMs as possible onto a physical host. The goal is to minimize the number of physical hosts that must be online.

Select the day of the week and the time when you want Workload Balancing to begin operating in this mode.

Create more scheduled mode changes (that is, “tasks”) until you have the number you need. If you only schedule one task, Workload Balancing switches to that mode as scheduled, but then it never switches back.

Click OK.

Display the Optimization Mode dialog box by following steps 1–4 in the previous procedure.

Select the task you want to delete or disable from the Scheduled Mode Changes list.

Do one of the following:

- **Delete the task permanently.** Click the Delete button.
- **Stop the task from running temporarily.** Right-click the task and click Disable.

**Tips:**

- You can also disable or enable tasks by selecting the task, clicking Edit, and selecting the Enable Task check box in the Optimization Mode Scheduler dialog.
- To re-enable a task, right-click the task in the Scheduled Mode Changes list and click Enable.

Do one of the following:

- Double-click the task you want to edit.
- Select the task you want to edit, and click Edit.

In the Change to box, select a different mode or make other changes as desired.

**Note:**

Clicking Cancel, before clicking OK, undoes any changes you made in the Optimization tab, including deleting a task.

## **Optimize and manage power automatically**

You can configure Workload Balancing to apply recommendations automatically (Automation) and turn hosts on or off automatically. To power down hosts automatically (for example, during low-usage periods), you must configure Workload Balancing to apply recommendations automatically and enable power management. Both power management and automation are described in the sections that follow.

## **Apply recommendations automatically**

Workload Balancing lets you configure for it to apply recommendations on your behalf and perform the optimization actions it recommends automatically. You can use this feature, which is known as Automatic optimization acceptance, to apply any recommendations automatically, including ones to

improve performance or power down hosts. However, to power down hosts as VMs usage drops, you must configure automation, power management, and Maximum Density mode.

By default, Workload Balancing does not apply recommendations automatically. If you want Workload Balancing to apply recommendations automatically, enable Automation. If you do not, you must apply recommendations manually by clicking Apply Recommendations.

Workload Balancing does not automatically apply recommendations to hosts or VMs when the recommendations conflict with High Availability settings. If a pool becomes overcommitted by applying Workload Balancing optimization recommendations, XenCenter prompts you whether or not you want to continue applying the recommendation. When Automation is enabled, Workload Balancing does not apply any power-management recommendations that exceed the number of host failures to tolerate in the High Availability plan.

When Workload Balancing is running with the Automation feature enabled, this behavior is sometimes called running in automated mode.

It is possible to tune how Workload Balancing applies recommendations in automated mode. For information, see Set conservative or aggressive automated recommendations.

### **Enable Workload Balancing power management**

The term power management means the ability to turn the power on or off for physical hosts. In a Workload Balancing context, this term means powering hosts in a pool on or off based on the pool's total workload.

Configuring Workload Balancing power management on a host requires that:

- The hardware for the host has remote power on/off capabilities
- The Host Power On feature is configured for the host
- The host has been explicitly selected as a host to participate in (Workload Balancing) Power Management

In addition, if you want Workload Balancing to power off hosts automatically, configure Workload Balancing to do the following actions:

- Apply recommendations automatically
- Apply Power Management recommendations automatically

If WLB detects unused resources in a pool in Maximum Density mode, it recommends powering off hosts until it eliminates all excess capacity. If there isn't enough host capacity in the pool to shut down hosts, WLB recommends leaving the hosts on until the pool workload decreases enough. When you configure Workload Balancing to power off extra hosts automatically, it applies these recommendations automatically and, so, behaves in the same way.

When a host is set to participate in Power Management, Workload Balancing makes power-on and power-off recommendations as needed.

If you run in Maximum Performance mode:

- If you configure WLB to power on hosts automatically, WLB powers on hosts when resource utilization on a host exceeds the High threshold.
- Workload Balancing never powers off hosts after it has powered them on.

If you turn on the option to apply Power Management recommendations automatically, you do so at the pool level. However, you can specify which hosts from the pool you want to participate in Power Management.

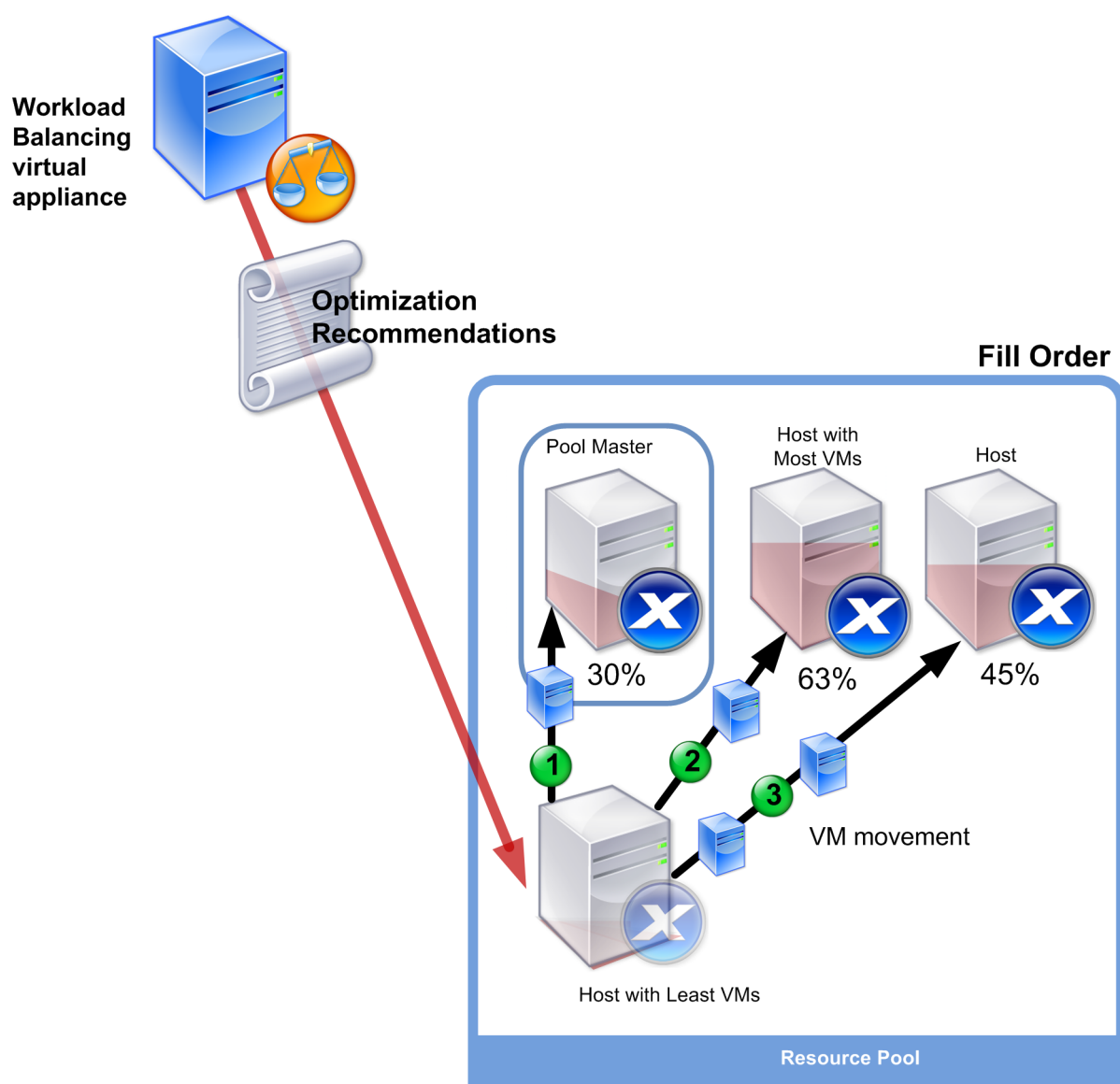
### **Understand power management behavior**

Before Workload Balancing recommends powering hosts on or off, it selects the hosts to transfer VMs to (that is, to “fill”). It does so in the following order:

1. Filling the pool master since it is the host that cannot be powered off.
2. Filling the host with the most VMs.
3. Filling subsequent hosts according to which hosts have the most VMs running.

When Workload Balancing fills the pool master, it does so assuming artificially low (internal) thresholds for the master. Workload Balancing uses these low thresholds as a buffer to prevent the pool master from being overloaded.

Workload Balancing fills hosts in this order to encourage density.



When WLB detects a performance issue while the pool is in Maximum Density mode, it recommends migrating workloads among the powered-on hosts. If Workload Balancing cannot resolve the issue using this method, it attempts to power on a host. (Workload Balancing determines which hosts to power on by applying the same criteria it would if the optimization mode was set to Maximum Performance.)

When WLB runs in Maximum Performance mode, WLB recommends powering on hosts until the resource utilization on all pool members falls below the High threshold.

If, while migrating VMs, Workload Balancing determines that increasing capacity benefits the pool's overall performance, it powers on hosts automatically or recommends doing so.



**Important:**

Workload Balancing only recommends powering on a host that Workload Balancing powered off.

**Design environments for power management and VM consolidation**

When you are planning a XenServer implementation and you intend to configure automatic VM consolidation and power management, consider your workload design. For example, you may want to:

- **Place Different Types of Workloads in Separate Pools.** If you have an environment with distinct types of workloads, consider whether to locate the VMs hosting these workloads in different pools. Also consider splitting VMs that host types of applications that perform better with certain types of hardware into different pool.

Because power management and VM consolidation are managed at the pool level, design pools so they contain workloads that you want consolidated at the same rate. Ensure that you factor in considerations such as those discussed in Control automated recommendations.

- **Exclude Hosts from Workload Balancing.** Some hosts might need to be always on. For more information, see Exclude hosts from recommendations.

**To apply optimization recommendations automatically**

1. In the Infrastructure pane of XenCenter, select XenCenter > [your-pool](#).
2. In the Properties pane, click the WLB tab.
3. In the WLB tab, click Settings.
4. In the left pane, click Automation.
5. Select one or more of the following check boxes:
  - Automatically apply Optimization recommendations. When you select this option, you do not need to accept optimization recommendations manually. Workload Balancing automatically accepts optimization and placement recommendations it makes.
  - Automatically apply Power Management recommendations. The behavior of this option varies according to the pool's optimization mode:
    - Maximum Performance Mode. When Automatically apply Power Management recommendations is enabled, Workload Balancing automatically powers on hosts when doing so improves host performance.
    - Maximum Density Mode. When Automatically apply Power Management recommendations is enabled, Workload Balancing automatically powers off hosts when resource utilization drops below the Low threshold. That is, Workload Balancing powers off hosts automatically during low usage periods.

6. (Optional.) Fine-tune optimization recommendations by clicking Advanced in the left pane of the Settings dialog and doing one or more of the following:

- Specifying the number of times Workload Balancing must make an optimization recommendation before the recommendation is applied automatically. The default is three times, which means the recommendation is applied on the third time it is made.
- Selecting the lowest level of optimization recommendation that you want Workload Balancing to apply automatically. The default is High.
- Changing the aggressiveness with which Workload Balancing applies its optimization recommendations.

You may also want to specify the number of minutes Workload Balancing has to wait before applying an optimization recommendation to a recently moved VM.

All of these settings are explained in more depth in Set conservative or aggressive automated recommendations.

7. Do one of the following:

- If you want to configure power management, click Automation/Power Management and proceed to the To select hosts for power management.
- If you do not want to configure power management and you are finished configuring automation, click OK.

### To select hosts for power management

1. In the Power Management section, select the hosts that you want Workload Balancing to recommend powering on and off.

#### Note:

Selecting hosts for power management recommendations without selecting **Automatically apply Power Management recommendations** causes WLB to suggest power-management recommendations but not apply them automatically for you.

2. Click OK. If none of the hosts in the resource pool support remote power management, Workload Balancing displays the message, “No hosts support Power Management.”

### Understand when Workload Balancing makes recommendations

Workload Balancing continuously evaluates the resource metrics of physical hosts and VMs across the pools it is managing against thresholds. Thresholds are preset values that function like boundaries that a host must exceed before Workload Balancing can make an optimization recommendation. At a very high level. The Workload Balancing process is as follows:

1. Workload Balancing detects that the threshold for a resource was violated.
2. Workload Balancing evaluates if it makes an optimization recommendation.
3. Workload Balancing determines which hosts it recommends function as the destination hosts. A destination host is the host where Workload Balancing recommends relocating one or more VMs.
4. Workload Balancing makes the recommendation.

After WLB determines that a host can benefit from optimization, before it makes the recommendation, it evaluates other hosts on the pool to decide the following:

1. The order to make the optimization (what hosts, what VMs)
2. Where to recommend placing a VM when it does make a recommendation

To accomplish these two tasks, Workload Balancing uses thresholds and weightings as follows:

- **Thresholds** are the boundary values that Workload Balancing compares your pool's resource metrics against. The thresholds are used to determine whether or not to make a recommendation and what hosts are a suitable candidate for hosting relocated VMs.
- **Weightings** are a way of ranking resources according to how much you want them to be considered, are used to determine the processing order. After Workload Balancing decides to make a recommendation, it uses your specifications of which resources are important to determine the following:
  - Which hosts' performance to address first
  - Which VMs to recommend migrating first

For each resource Workload Balancing monitors, it has four levels of thresholds (Critical, High, Medium, and Low), which are discussed in the sections that follow. Workload Balancing evaluates whether to make a recommendation when a resource metric on a host:

- Exceeds the High threshold when the pool is running in Maximum Performance mode (improve performance)
- Drops below the Low threshold when the pool is running in Maximum Density mode (consolidate VMs on hosts)
- Exceeds the Critical threshold when the pool is running in Maximum Density mode (improve performance)

If the High threshold for a pool running in Maximum Performance mode is 80%, when CPU utilization on a host reaches 80.1%, WLB evaluates whether to issue a recommendation.

When a resource violates its threshold, WLB evaluates the resource's metric against historical performance to prevent making an optimization recommendation based on a temporary spike. To do so, Workload Balancing creates a historically averaged utilization metric by evaluating the data for resource utilization captured at the following times:

| Data captured                                                             | Weight |
|---------------------------------------------------------------------------|--------|
| Immediately, at the time threshold was exceeded (that is, real-time data) | 70%    |
| 30 minutes before the threshold was exceeded                              | 25%    |
| 24 hours before the threshold was exceeded                                | 5%     |

If CPU utilization on the host exceeds the threshold at 12:02 PM, WLB checks the utilization at 11:32 AM that day, and at 12:02PM on the previous day. For example, if CPU utilization is at the following values, WLB doesn't make a recommendation:

- 80.1% at 12:02 PM that day
- 50% at 11:32 AM that day
- 78% at 12:32 PM the previous day

This behavior is because the historically averaged utilization is 72.47%, so Workload Balancing assumes that the utilization is a temporary spike. However, if the CPU utilization was 78% at 11:32AM, Workload Balancing makes a recommendation since the historically averaged utilization is 80.1%.

### Optimization and consolidation process

The Workload Balancing process for determining potential optimizations varies according to the optimization mode (Maximum Performance or Maximum Density). However, regardless of the optimization mode, optimization, and placement recommendations are made using a two-stage process:

1. Determine potential optimizations. (That is, what VMs to migrate off hosts.)
2. Determine placement recommendations. (That is, what hosts would be suitable candidates for new hosts.)

#### Note:

Workload Balancing only recommends migrating VMs that meet the XenServer criteria for live migration, including the destination host must have the storage the VM requires. The destination host must also have sufficient resources to accommodate adding the VM without exceeding the thresholds of the optimization mode configured on the pool. For example, the High threshold in Maximum Performance mode and the Critical threshold for Maximum Density mode.

When Workload Balancing is running in automated mode, you can tune the way it applies recommendations. For more information, see [Set conservative or aggressive automated recommendations](#).

### Optimization recommendation process in Maximum Performance mode

When running in Maximum Performance mode, Workload Balancing uses the following process to determine potential optimizations:

1. Every two minutes Workload Balancing evaluates the resource utilization for each host in the pool. It does so by monitoring on each host and determining if each resource's utilization exceeds its High threshold. See [Change the critical threshold](#) for more information about the High threshold.

If, in Maximum Performance mode, a resource's utilization exceeds its High threshold, WLB starts the process to determine whether to make an optimization recommendation. Workload Balancing determines whether to make an optimization recommendation based on whether doing so can ease performance constraints, such as ones revealed by the High threshold.

For example, consider the case where Workload Balancing sees that insufficient CPU resources negatively affect the performance of the VMs on Host A. If Workload Balancing can find another host with less CPU utilization, it recommends moving one or more VMs to another host.

2. If a resource's utilization on a host exceeds the relevant threshold, Workload Balancing combines the following data to form the historically averaged utilization:

- The resource's current utilization
- Historical data from 30 minutes ago
- Historical data from 24 hours ago

If the historically averaged utilization exceeds the resource's threshold, Workload Balancing determines it makes an optimization recommendation.

3. Workload Balancing uses metric weightings to determine what hosts to optimize first. The resource to which you have assigned the most weight is the one that Workload Balancing attempts to address first. See [Tune metric weightings](#) for information about metric weightings.
4. Workload Balancing determines which hosts can support the VMs it wants to migrate off hosts.

Workload Balancing makes this determination by calculating the projected effect on resource utilization of placing different combinations of VMs on hosts. (Workload Balancing uses a method of performing these calculations that in mathematics is known as permutation.)

To do so, Workload Balancing creates a single metric or score to forecast the impact of migrating a VM to the host. The score indicates the suitability of a host as a home for more VMs.

To score the host's performance, Workload Balancing combines the following metrics:

- The host's current metrics
- The host's metrics from the last 30 minutes
- The host's metrics from 24 hours ago
- The VM's metrics.

5. After scoring hosts and VMs, WLB attempts to build virtual models of what the hosts look like

with different combinations of VMs. WLB uses these models to determine the best host to place the VM.

In Maximum Performance mode, Workload Balancing uses metric weightings to determine what hosts to optimize first and what VMs on those hosts to migrate first. Workload Balancing bases its models on the metric weightings. For example, if CPU utilization is assigned the highest importance, Workload Balancing sorts hosts and VMs to optimize according to the following criteria:

- First, what hosts CPU utilization most affects (that is, are running closest to the High threshold for CPU utilization)
  - What VMs have the highest CPU utilization (or are running the closest to its High threshold).
6. Workload Balancing continues calculating optimizations. It views hosts as candidates for optimization and VMs as candidates for migration until predicted resource utilization on the VM's host drops below the High threshold. Predicted resource utilization is the resource utilization that Workload Balancing forecasts a host has after Workload Balancing has added or removed a VM from the host.

### **Consolidation process in Maximum Density mode**

WLB determines whether to make a recommendation based on whether it can migrate a VM onto a host and still run that host below the Critical threshold.

1. When a resource's utilization drops below its Low threshold, Workload Balancing begins calculating potential consolidation scenarios.
2. When WLB discovers a way that it can consolidate VMs on a host, it evaluates whether the destination host is a suitable home for the VM.
3. Like in Maximum Performance mode, Workload Balancing scores the host to determine the suitability of a host as a home for new VMs.

Before WLB makes recommendations to consolidate VMs on fewer hosts, it checks that resource utilization on those hosts after VMs are relocated to them is below Critical thresholds.

#### **Note:**

Workload Balancing does not consider metric weightings when it makes a consolidation recommendation. It only considers metric weightings to ensure performance on hosts.

4. After scoring hosts and VMs, WLB attempts to build virtual models of what the hosts look like with different combinations of VMs. It uses these models to determine the best host to place the VM.
5. WLB calculates the effect of adding VMs to a host until it forecasts that adding another VM causes a host resource to exceed the Critical threshold.

6. Workload Balancing recommendations always suggest filling the pool master first since it is the host that cannot be powered off. However, Workload Balancing applies a buffer to the pool master so that it cannot be over-allocated.
7. WLB continues to recommend migrating VMs on to hosts until no hosts remain that don't exceed a Critical threshold when a VM is migrated to them.

### Change the critical thresholds

You might want to change critical thresholds as a way of controlling when optimization recommendations are triggered. This section provides guidance about:

- How to modify the default Critical thresholds on hosts in the pool
- How values set for Critical threshold alter High, Medium, and Low thresholds.

Workload Balancing determines whether to produce recommendations based on whether the averaged historical utilization for a resource on a host violates its threshold. Workload Balancing recommendations are triggered when the High threshold in Maximum Performance mode or Low and Critical thresholds for Maximum Density mode are violated. For more information, see Optimization and consolidation process. After you specify a new Critical threshold for a resource, Workload Balancing resets the resource's other thresholds relative to the new Critical threshold. (To simplify the user interface, the Critical threshold is the only threshold you can change through XenCenter.)

The following table shows the default values for the Workload Balancing thresholds:

| Metric          | Critical  | High         | Medium      | Low         |
|-----------------|-----------|--------------|-------------|-------------|
| CPU Utilization | 90%       | 76.5%        | 45%         | 22.5%       |
| Free Memory     | 51 MB     | 63.75 MB     | 510 MB      | 1020 MB     |
| Network Reads   | 25 MB/sec | 21.25 MB/sec | 12.5 MB/sec | 6.25 MB/sec |
| Network Writes  | 25 MB/sec | 21.25 MB/sec | 12.5 MB/sec | 6.25 MB/sec |
| Disk Reads      | 25 MB/sec | 21.25 MB/sec | 12.5 MB/sec | 6.25 MB/sec |
| Disk Writes     | 25 MB/sec | 21.25 MB/sec | 12.5 MB/sec | 6.25 MB/sec |

To calculate the values for all metrics except memory, Workload Balancing multiplies the new value for the Critical threshold with the following factors:

- **High Threshold Factor:** 0.85
- **Medium Threshold Factor:** 0.50
- **Low Threshold Factor:** 0.25

For example, if you increase the Critical threshold for CPU Utilization to 95%, WLB resets the High, Medium, and Low thresholds to 80.75%, 47.5%, and 23.75%.

To calculate the threshold values for free memory, Workload Balancing multiplies the Critical threshold with these factors:

- **High Threshold Factor:** 1.25
- **Medium Threshold Factor:** 10.0
- **Low Threshold Factor:** 20.0

To perform this calculation for a specific threshold, multiply the factor for the threshold with the value you entered for the critical threshold for that resource:

### **High, Medium, or Low Threshold = Critical Threshold \* Threshold Factor**

For example, if you change the Critical threshold for Network Reads to 40 MB/sec, to get its Low threshold, multiply 40 by 0.25, which equals 10 MB/sec. To obtain the Medium threshold, you multiple 40 by 0.50, and so on.

While the Critical threshold triggers many optimization recommendations, other thresholds can also trigger optimization recommendations, as follows:

- **High threshold.**
  - **Maximum Performance.** Exceeding the High threshold triggers optimization recommendations to relocate a VM to a host with lower resource utilization.
  - **Maximum Density.** Workload Balancing doesn't recommend placing a VM on host when moving that VM to the host causes the host resource utilization to exceed a High threshold.
- **Low threshold.**
  - **Maximum Performance.** Workload Balancing does not trigger recommendations from the Low threshold.
  - **Maximum Density.** When a metric value drops below the Low threshold, WLB determines that hosts are underutilized and makes an optimization recommendation to consolidate VMs on fewer hosts. Workload Balancing continues to recommend moving VMs onto a host until the metric values for one of the host's resources reaches its High threshold.

However, after a VM is relocated, utilization of a resource on the VM's new host can exceeds a Critical threshold. In this case, WLB temporarily uses an algorithm similar to the Maximum Performance load-balancing algorithm to find a new host for the VMs. Workload Balancing continues to use this algorithm to recommend moving VMs until resource utilization on hosts across the pool falls below the High threshold.



**To change the critical thresholds**

1. In the Infrastructure pane of XenCenter, select XenCenter > [your-resource-pool](#).
2. In the Properties pane, click the WLB tab.
3. In the WLB tab, click Settings.
4. In the left pane, select Critical Thresholds. These critical thresholds are used to evaluate host resource utilization.
5. In Critical Thresholds page, type one or more new values in the Critical Thresholds boxes. The values represent resource utilization on the host.

Workload Balancing uses these thresholds when making VM placement and pool-optimization recommendations. Workload Balancing strives to keep resource utilization on a host below the critical values set.

**Tune metric weightings**

How Workload Balancing uses metric weightings when determining which hosts and VMs to process first varies according to the optimization mode: Maximum Density or Maximum Performance.

When Workload Balancing is processing optimization recommendations, it creates an optimization order. To determine this, Workload Balancing ranks the hosts to address first according to which hosts have the highest metric values for whatever resource is ranked as the most important in the metric weightings page.

In general, metric weightings are used when a pool is in Maximum Performance mode. However, when Workload Balancing is in Maximum Density mode, it does use metric weightings when a resource exceeds its Critical threshold.

**Maximum Performance mode**

In Maximum Performance mode, Workload Balancing uses metric weightings to determine (a) which hosts' performance to address first and (b) which VMs to recommend migrating first.

For example, if Network Writes is the most important resource for WLB, WLB first makes optimization recommendations for the host with the highest number of Network Writes per second. To make Network Writes the most important resource move the **Metric Weighting** slider to the right and all the other sliders to the middle.

If you configure all resources to be equally important, Workload Balancing addresses CPU utilization first and memory second, as these resources are typically the most constrained. To make all resources equally important, set the **Metric Weighting** slider is in the same place for all resources.

## Maximum Density mode

In Maximum Density mode, Workload Balancing only uses metric weightings when a host reaches the Critical threshold. At that point, Workload Balancing applies an algorithm similar to that for Maximum Performance until no hosts exceed the Critical thresholds. When using this algorithm, Workload Balancing uses metric weightings to determine the optimization order in the same way as it does for Maximum Performance mode.

If two or more hosts have resources exceeding their Critical thresholds, Workload Balancing verifies the importance you set for each resource. It uses this importance to determine which host to optimize first and which VMs on that host to relocate first.

For example, your pool contains Host A and Host B, which are in the following state:

- The CPU utilization on Host A exceeds its Critical threshold and the metric weighting for CPU utilization is set to the far right: **More Important**.
- The memory utilization on Host B exceeds its Critical threshold and the metric weighting for memory utilization is set to the far left: **Less Important**.

Workload Balancing recommends optimizing Host A first because the resource on it that reached the Critical threshold is the resource assigned the highest weight. After Workload Balancing determines that it must address the performance on Host A, Workload Balancing then begins recommending placements for VMs on that host. It begins with the VM that has the highest CPU utilization, since that CPU utilization is the resource with the highest weight.

After Workload Balancing has recommended optimizing Host A, it makes optimization recommendations for Host B. When it recommends placements for the VMs on Host B, it does so by addressing CPU utilization first, since CPU utilization was assigned the highest weight.

If there are more hosts that need optimization, Workload Balancing addresses the performance on those hosts according to what host has the third highest CPU utilization.

By default, all metric weightings are set to the farthest point on the slider (More Important).

### Note:

The weighting of metrics is relative. If all of the metrics are set to the same level, even if that level is Less Important, they are all be weighted the same. The relation of the metrics to each other is more important than the actual weight at which you set each metric.

## To edit metric weighting factors

1. Stopping
2. In the Infrastructure pane of XenCenter, select XenCenter > [your-resource-pool](#).
3. Click the WLB tab, and then click Settings.

4. In the left pane, select Metric Weighting.
5. In Metric Weighting page, as desired, adjust the sliders beside the individual resources.

Move the slider towards Less Important to indicate that ensuring VMs always have the highest available amount of this resource is not as vital for this pool.

### **Excluding hosts from recommendations**

When configuring Workload Balancing, you can specify that specific physical hosts are excluded from Workload Balancing optimization and placement recommendations, including Start On placement recommendations.

Situations when you might want to exclude hosts from recommendations include when:

- You want to run the pool in Maximum Density mode and consolidate and shut down hosts, but you want to exclude specific hosts from this behavior.
- You have two VM workloads that must always run on the same host. For example, if the VMs have complementary applications or workloads.
- You have workloads that you do not want moved (for example, a domain controller or database server).
- You want to perform maintenance on a host and you do not want VMs placed on the host.
- The performance of the workload is so critical that the cost of dedicated hardware is irrelevant.
- Specific hosts are running high-priority workloads (VMs), and you do not want to use the High Availability feature to prioritize these VMs.
- The hardware in the host is not the optimum for the other workloads in the pool.

Regardless of whether you specify a fixed or scheduled optimization mode, excluded hosts remain excluded even when the optimization mode changes. Therefore, if you only want to prevent Workload Balancing from shutting off a host automatically, consider not enabling (or deselecting) Power Management for that host instead. For more information, see [Optimize and manage power automatically](#).

When you exclude a host from recommendations, you are specifying for Workload Balancing not to manage that host at all. This configuration means that Workload Balancing doesn't make any optimization recommendations for an excluded host. In contrast, when you don't select a host to participate in Power Management, WLB still manages the host, but doesn't make power management recommendations for it.

### **To exclude hosts from Workload Balancing**

Use this procedure to exclude a host in a pool that Workload Balancing is managing from power management, host evacuation, placement, and optimization recommendations.

1. In the Resources pane of XenCenter, select XenCenter > [your-resource-pool](#).
2. In the Properties pane, click the WLB tab.
3. In the WLB tab, click Settings.
4. In the left pane, select Excluded Hosts.
5. In Excluded Hosts page, select the hosts for which you do not want WLB to recommend alternate placements and optimizations.

### **Control automated recommendations**

Workload Balancing supplies some advanced settings that let you control how Workload Balancing applies automated recommendations. These settings appear on the Advanced page of the Workload Balancing Configuration dialog.

In the Resources pane of XenCenter, select XenCenter > [your-resource-pool](#).

In the Properties pane, click the WLB tab.

In the WLB tab, click Settings.

In the left pane, select Advanced.

### **Set conservative or aggressive automated recommendations**

When running in automated mode, the frequency of optimization and consolidation recommendations and how soon they are automatically applied is a product of multiple factors, including:

- How long you specify Workload Balancing waits after moving a VM before making another recommendation
- The number of recommendations Workload Balancing must make before applying a recommendation automatically
- The severity level a recommendation must achieve before the optimization is applied automatically
- The level of consistency in recommendations (recommended VMs to move, destination hosts) Workload Balancing requires before applying recommendations automatically

#### **Important:**

In general, only adjust the settings for factors in the following cases:

- You have guidance from Citrix Technical Support
- You made significant observation and testing of your pool's behavior with Workload Balancing enabled

Incorrectly configuring these settings can result in Workload Balancing not making any recommendations.

### **VM migration interval**

You can specify the number of minutes WLB waits after the last time a VM was moved, before WLB can make another recommendation for that VM.

The recommendation interval is designed to prevent Workload Balancing from generating recommendations for artificial reasons (for example, if there was a temporary utilization spike).

When Automation is configured, it is especially important to be careful when modifying the recommendation interval. If an issue occurs that leads to continuous, recurring spikes, increasing the frequency (that is, setting a lower number) can generate many recommendations and, therefore, relocations.

#### **Note:**

Setting a recommendation interval does not affect how long Workload Balancing waits to factor recently rebalanced hosts into recommendations for Start-On Placement, Resume, and Maintenance Mode.

### **Recommendation count**

Every two minutes, Workload Balancing checks to see if it can generate recommendations for the pool it is monitoring. When you enable Automation, you can specify the number of times a consistent recommendation must be made before Workload Balancing automatically applies the recommendation. To do so, you configure a setting known as the Recommendation Count. The Recommendation Count and the Optimization Aggressiveness setting let you fine-tune the automated application of recommendations in your environment.

As described in the aggressiveness section, Workload Balancing uses the similarity of recommendations to make the following checks:

1. Whether the recommendation is truly needed
2. Whether the destination host has stable enough performance over a prolonged period to accept a relocated VM (without needing to move it off the host again shortly)

Workload Balancing uses the Recommendation Count value to determine a recommendation must be repeated before Workload Balancing automatically applies the recommendation.

Workload Balancing uses this setting as follows:

1. Every time Workload Balancing generates a recommendation that meets its consistency requirements, as indicated by the Optimization Aggressiveness setting, Workload Balancing increments the Recommendation Count. If the recommendation does not meet the consistency

requirements, Workload Balancing may reset the Recommendation Count to zero, depending on the factors described in Optimization aggressiveness.

2. When WLB generates enough consistent recommendations to meet the value for the Recommendation Count, as specified in the Recommendations text box, it automatically applies the recommendation.

If you choose to modify this setting, the value to set varies according to your environment. Consider these scenarios:

- If host loads and activity increase rapidly in your environment, you may want to increase value for the Recommendation Count. Workload Balancing generates recommendations every two minutes. For example, if you set this interval to **3**, then six minutes later Workload Balancing applies the recommendation automatically.
- If host loads and activity increase gradually in your environment, you may want to decrease the value for the Recommendation Count.

Accepting recommendations uses system resources and affects performance when Workload Balancing is relocating the VMs. Increasing the Recommendation Count increases the number of matching recommendations that must occur before Workload Balancing applies the recommendation. This setting encourages Workload Balancing to apply more conservative, stable recommendations and can decrease the potential for spurious VM moves. The Recommendation Count is set to a conservative value by default.

Because of the potential impact adjusting this setting can have on your environment, only change it with extreme caution. Preferably, make these adjustments by testing and iteratively changing the value or under the guidance of Citrix Technical Support.

### **Recommendation severity**

All optimization recommendations include a severity rating (Critical, High, Medium, Low) that indicates the importance of the recommendation. Workload Balancing bases this rating on a combination of factors including the following:

- Configuration options you set, such as thresholds and metric tunings
- Resources available for the workload
- Resource-usage history.

The severity rating for a recommendation appears in the Optimization Recommendations pane on the WLB tab.

When you configure WLB to apply recommendations automatically, you can set the minimum severity level to associate with a recommendation before Workload Balancing automatically applies it.

**Optimization aggressiveness**

To provide extra assurance when running in automated mode, Workload Balancing has consistency criteria for accepting optimizations automatically. This can help to prevent moving VMs due to spikes and anomalies. In automated mode, Workload Balancing does not accept the first recommendation it produces. Instead, Workload Balancing waits to apply a recommendation automatically until a host or VM exhibits consistent behavior over time. Consistent behavior over time includes factors like whether a host continues to trigger recommendations and whether the same VMs on that host continue to trigger recommendations.

Workload Balancing determines if behavior is consistent by using criteria for consistency and by having criteria for the number of times the same recommendation is made. You can configure how strictly you want Workload Balancing to apply the consistency criteria using the Optimization Aggressiveness setting.

Citrix primarily designed the Optimization Aggressiveness setting for demonstration purposes. However, you can use this setting to control the amount of stability you want in your environment before Workload Balancing applies an optimization recommendation. The most stable setting (Low aggressiveness) is configured by default. In this context, the term stable means the similarity of the recommended changes over time, as explained throughout this section. Aggressiveness is not desirable in most environments. Therefore, Low is the default setting.

Workload Balancing uses up to four criteria to ascertain consistency. The number of criteria that must be met varies according to the level you set in the Optimization Aggressiveness setting. The lower the level (for example, Low or Medium) the less aggressively Workload Balancing is in accepting a recommendation. In other words, Workload Balancing is stricter about requiring criteria to match (or less cavalier or aggressive) about consistency when aggressiveness is set to Low.

For example, if the aggressiveness level is set to Low, each criterion for Low must be met the number of times specified by the Recommendation Count value before automatically applying the recommendation.

If you set the Recommendation Count to **3**, Workload Balancing waits until all the criteria listed for Low are met and repeated in three consecutive recommendations. This setting helps ensure that the VM actually needs to be moved and that the recommended destination host has stable resource utilization over a longer period. It reduces the potential for a recently moved VM to be moved off a host due to host performance changes after the move. By default, this setting is set to a conservative setting (Low) to encourage stability.

Citrix does not recommend increasing the Optimization Aggressiveness setting to increase the frequency with which your hosts are being optimized. If you think that your hosts aren't being optimized quickly or frequently enough, try adjusting the Critical thresholds. Compare the thresholds against the Pool Health report.

The consistency criteria associated with the different levels of aggressiveness is the following:

**Low:**

- All VMs in subsequent recommendations must be the same (as demonstrated by matching UUIDs in each recommendation).
- All destination hosts must be the same in subsequent recommendations
- The recommendation that immediately follows the initial recommendation must match or else the Recommendation Count reverts to 1

**Medium:**

- All VMs in subsequent recommendations must be from the same host; however, they can be different VMs from the ones in the first recommendation.
- All destination hosts must be the same in subsequent recommendations
- One of the next two recommendations that immediately follows the first recommendation must match or else the Recommendation Count reverts to 1

**High:**

- All VMs in the recommendations must be from the same host. However, the recommendations do not have to follow each other immediately.
- The host from which Workload Balancing recommended that the VM move must be the same in each recommendation
- The Recommendation Count does not revert to 1 when the two recommendations that follow the first recommendation do not match

**Example**

The following example illustrates how Workload Balancing uses the Optimization Aggressiveness setting and the Recommendation Count to determine whether or not to accept a recommendation automatically.

The first column represents the recommendation number. The second column, “Placement Recommendations,” represents the placement recommendations made when Workload Balancing issued the optimization recommendation: each recommendation proposes three VM placements (moves). The third, fourth, and fifth columns represent the effect of the Optimization Aggressiveness setting on a group of placement recommendations. The row denotes the group, for example **Recommendation #1**. The number in the aggressiveness columns is the number of times there have been consecutive recommendation at that Optimization Aggressiveness setting. For example, 1 in the medium column for Recommendation #2 indicates that the recommendation was not consistent enough at that Optimization Aggressiveness setting. The counter was reset to 1.



In the following examples, when the Optimization Aggressiveness setting is set to High, the Recommendation Count continues to increase after Recommendation #1, #2, and #3. This increase happens even though the same VMs are not recommended for new placements in each recommendation. Workload Balancing applies the placement recommendation with Recommendation #3 because it has seen the same behavior from that host for three consecutive recommendations.

In contrast, when set to Low aggressiveness, the consecutive recommendations count does not increase for the first four recommendations. The Recommendation Count resets to 1 with each recommendation because the same VMs were not recommended for placements. The Recommendation Count does not start to increase until the same recommendation is made in Recommendation #5. Finally, Workload Balancing automatically applies the recommendation made in Recommendation #6 after the third time it issues the same placement recommendations.

**Recommendation #1:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host B
- Move VM5 from Host A to Host C

High Aggressiveness Recommendation Count: 1

Medium Aggressiveness Recommendation Count: 1

Low Aggressiveness Recommendation Count: 1

**Recommendation #2:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host C
- Move VM7 from Host A to Host C

High Aggressiveness Recommendation Count: 2

Medium Aggressiveness Recommendation Count: 1

Low Aggressiveness Recommendation Count: 1

**Recommendation #3:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host C
- Move VM5 from Host A to Host C

High Aggressiveness Recommendation Count: 3 (Apply)

Medium Aggressiveness Recommendation Count: 1

Low Aggressiveness Recommendation Count: 1

**Recommendation #4:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host B
- Move VM5 from Host A to Host C

Medium Aggressiveness Recommendation Count: 2

Low Aggressiveness Recommendation Count: 1

**Recommendation #5:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host B
- Move VM5 from Host A to Host C

Medium Aggressiveness Recommendation Count: 3 (Apply)

Low Aggressiveness Recommendation Count: 2

**Recommendation #6:**

- Move VM1 from Host A to Host B
- Move VM3 from Host A to Host B
- Move VM5 from Host A to Host C

Low Aggressiveness Recommendation Count: 3 (Apply)

**To configure VM recommendation intervals**

1. In the Resources pane of XenCenter, select XenCenter>[your-pool](#).
2. In the Properties pane, click the WLB tab.
3. In the WLB tab, click Settings.
4. In the left pane, click Advanced.
5. In the VM Recommendation Interval section, do one or more of the following:
  - In the Minutes box, type a value for the number of minutes Workload Balancing waits before making another optimization recommendation on a newly rebalanced host.
  - In the Recommendations box, type a value for the number of recommendations you want Workload Balancing to make before it applies a recommendation automatically.
  - Select a minimum severity level before optimizations are applied automatically.
  - Modify how aggressively Workload Balancing applies optimization recommendations when it is running in automated mode. Increasing the aggressiveness level reduces constraints on the consistency of recommendations before automatically applying them. The Optimization Aggressiveness setting directly complements the Recommendation Count setting (that is, the Recommendations box).

**Note:**

If you type “1” for the value in the Recommendations setting, the Optimization Aggressiveness setting is not relevant.

**To modify the Pool Audit Trail granularity settings**

Follow this procedure to modify the granularity settings:

1. Select the pool in the Infrastructure view, click the WLB tab, and then click Settings.
2. In the left pane, click Advanced.
3. On the Advance page, click the **Pool Audit Trail Report Granularity** list, and select an option from the list.

**Important:**

Select the granularity based on your audit log requirements. For example, if you set your audit log report granularity to Minimum, the report only captures limited amount of data for specific users and object types. If you set the granularity to Medium, the report provides a user-friendly report of the audit log. If you choose to set the granularity to Maximum, the report contains detailed information about the audit log report. Setting the audit log report to Maximum can cause the Workload Balancing server to use more disk space and memory.

4. To confirm your changes, click OK.

**To view Pool Audit Trail reports based on objects in XenCenter**

Follow this procedure to run and view reports of Pool Audit Trail based on the selected object:

1. After you have set the Pool Audit Trail Granularity setting, click Reports. The Workload Reports page appears.
2. Select Pool Audit Trail on the left pane.
3. You can run and view the reports based on a specific Object by choosing it from the **Object** list. For example, choose **Host** from the list to get the reports based on Host alone.

**Administer Workload Balancing**

This section provides information about the following subjects:

- How to reconfigure a pool to use a different Workload Balancing virtual appliance

- How to disconnect a pool from Workload Balancing or temporarily stop Workload Balancing
- Database grooming
- How to change configuration options

**Note:**

Workload Balancing is available for XenServer Enterprise edition customers or those who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

**Administer and Maintain Workload Balancing**

After Workload Balancing has been running for a while, there are routine tasks that you might need to perform to keep Workload Balancing running optimally. These tasks may arise either as the result of changes to your environment (such as different IP addresses or credentials), hardware upgrades, or routine maintenance.

Some administrative tasks you may want to perform on Workload Balancing include:

- Connecting or reconnecting a pool to a Workload Balancing virtual appliance
- Reconfiguring a pool to use another Workload Balancing virtual appliance
- Renaming the Workload Balancing user account
- Disconnecting the Workload Balancing virtual appliance from a pool
- Removing the Workload Balancing virtual appliance
- Understanding the Role Based Access Control permissions Workload Balancing requires

Workload Balancing lets you fine-tune some aspects of its behavior through a configuration file known as the `wlb.conf` file.

This section also discusses some database administration tasks for those users interested in extra ways to manage the Workload Balancing database.

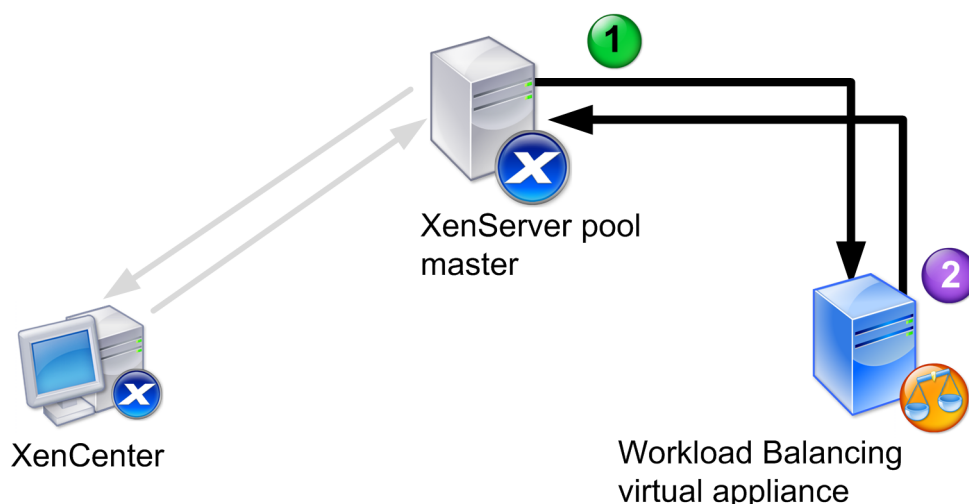
**Connect to the Workload Balancing Virtual Appliance**

After Workload Balancing configuration, connect the pool you want managed to the Workload Balancing virtual appliance using either the CLI or XenCenter. Likewise, you might need to reconnect to the same virtual appliance at some point.

To complete the XenCenter procedure that follows, you need the:

- Host name (or IP address) and port of the Workload Balancing virtual appliance.

- Credentials for the resource pool you want Workload Balancing to monitor.
- Credentials for the account you created on the Workload Balancing virtual appliance. This account is often known as the Workload Balancing user account. XenServer uses this account to communicate with Workload Balancing. You created this account on the Workload Balancing virtual appliance during Workload Balancing Configuration.



To specify the Workload Balancing virtual appliance's host name for use when connecting to the Workload Balancing virtual appliance, first add its host name and IP address to your DNS server.

If you want to configure certificates from a certificate authority, Citrix recommends specifying an FQDN or an IP address that does not expire.

When you first connect to Workload Balancing, it uses the default thresholds and settings for balancing workloads. Automatic features, such as Automated Optimization Mode, Power Management, and Automation, are disabled by default.

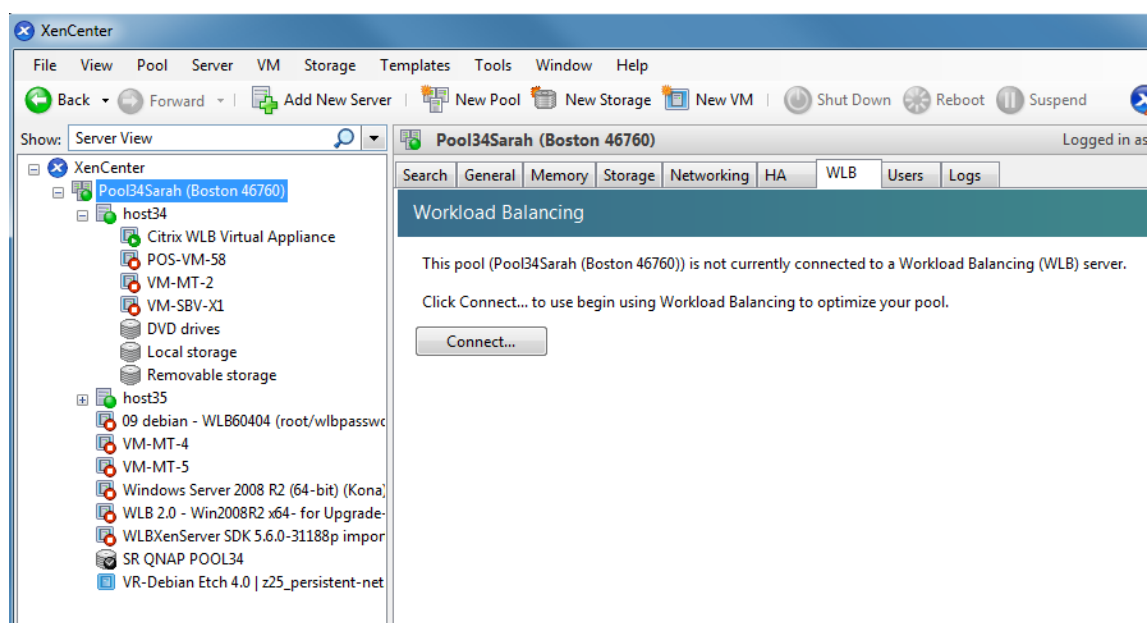
**Note:**

Workload Balancing is available for XenServer Enterprise edition customers or those customers who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer license, visit the [Citrix website](#).

### To connect your pool to the Workload Balancing virtual appliance

1. In the Resources pane of XenCenter, select XenCenter > *your-resource-pool*.
2. In the Properties pane, click the WLB tab.

The WLB tab displays the Connect button.



3. In the WLB tab, click Connect.

The Connect to WLB Server dialog box appears.

**Connect to WLB Server**

**Server Address**  
Enter the IP Address of the Workload Balancing server this XenServer resource pool will use.

Address:

Port:  (Default is 8012)

**WLB Server Credentials**  
Enter the credentials XenServer will use to connect to the Workload Balancing server.

User name:

Password:

**XenServer Credentials**  
Enter the credentials the Workload Balancing Server will use to connect to XenServer.

User name:

Password:

☐ Use the current XenCenter credentials

OK Cancel

4. In the Server Address section, enter the following:

- a) In the Address box, type the IP address or FQDN of the Workload Balancing virtual appliance (for example, `your-WLB-appliance-computername.yourdomain.net`).

**Tip:**

For more information, see To obtain the IP address for the WLB virtual appliance.

- b) Enter the port number in the Port box. XenServer uses this port to communicate with Workload Balancing.

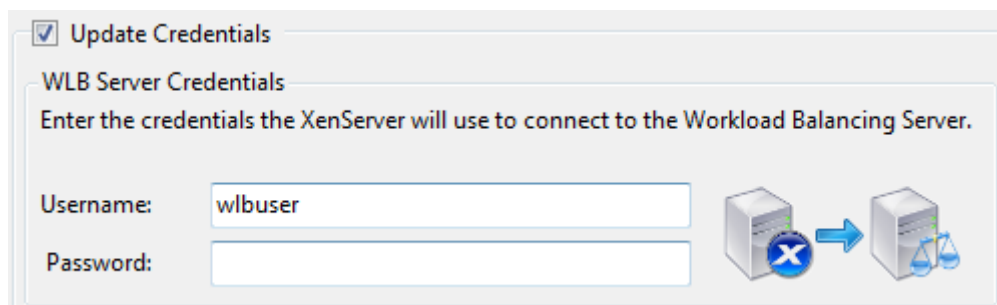
By default, XenServer connects to Workload Balancing (specifically the Web Service Host service) on port 8012. If you changed the port number during Workload Balancing Configuration, you must enter that port number here.

**Note:**

Use the default port number unless you changed it during Workload Balancing Configuration. The port number specified during Workload Balancing Configuration, in

any firewall rules, and in the Connect to WLB Server dialog must match.

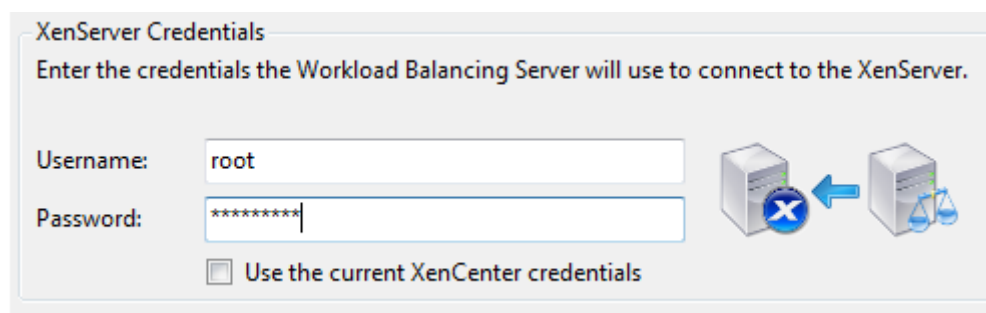
5. In the WLB Server Credentials section, enter the user name (for example, `wlbuser`) and password that the pool uses to connect to the Workload Balancing virtual appliance.



The screenshot shows a dialog box titled "Update Credentials" with a checked checkbox. Below it is the "WLB Server Credentials" section, which contains the instruction "Enter the credentials the XenServer will use to connect to the Workload Balancing Server." There are two input fields: "Username:" with the text "wlbuser" and "Password:" which is empty. To the right of the fields is an icon showing two server racks connected by a blue arrow, with a blue 'X' over the arrow.

These credentials must be for the account you created during Workload Balancing Configuration. By default, the user name for this account is `wlbuser`.

6. In the XenServer Credentials section, enter the user name and password for the pool you are configuring. Workload Balancing uses these credentials to connect to the XenServer hosts in that pool.



The screenshot shows a dialog box titled "XenServer Credentials" with the instruction "Enter the credentials the Workload Balancing Server will use to connect to the XenServer." There are two input fields: "Username:" with the text "root" and "Password:" with masked text "\*\*\*\*\*". Below the fields is a checkbox labeled "Use the current XenCenter credentials" which is currently unchecked. To the right of the fields is an icon showing two server racks connected by a blue arrow, with a blue 'X' over the arrow.

To use the credentials with which you are currently logged into XenServer, select the Use the current XenCenter credentials check box. If you have assigned a role to this account using the Access Control feature (RBAC), ensure that the role has sufficient permissions to configure Workload Balancing. For more information, see [Workload Balancing Access Control Permissions](#).

7. After connecting the pool to the Workload Balancing virtual appliance, Workload Balancing automatically begins monitoring the pool with the default optimization settings. If you want to modify these settings or change the priority given to resources, wait until the XenCenter Log shows that discovery is finished before proceeding. For more information, see [Change Workload Balancing Settings](#).

### To obtain the IP address for the WLB virtual appliance

1. Select the WLB virtual appliance in the Resource pane in XenCenter, and select the Console tab.
2. Log in to the appliance. Enter the VM user name (typically "root") and the root password you created when you imported the appliance.



3. Enter the following command at the prompt:

```
1 ifconfig
```

### Workload Balancing access control permissions

When Role Based Access Control (RBAC) is implemented in your environment, all user roles can display the WLB tab. However, not all roles can perform all operations. The following table lists the *minimum* role administrators require to use Workload Balancing features:

| Task                                                          | Minimum Required Role |
|---------------------------------------------------------------|-----------------------|
| Configure, Initialize, Enable, Disable WLB                    | Pool Operator         |
| Apply WLB Optimization Recommendations (in WLB tab)           | Pool Operator         |
| Modify WLB report subscriptions                               | Pool Operator         |
| Accept WLB Placement Recommendations ("star" recommendations) | VM Power Admin        |
| Generate WLB Reports, including the Pool Audit Trail report   | Read Only             |
| Display WLB Configuration                                     | Read Only             |

### Definition of permissions

The following table provides more details about permissions.

| Permission                                          | Allows Assignee To                                                                  |
|-----------------------------------------------------|-------------------------------------------------------------------------------------|
| Configure, Initialize, Enable, Disable WLB          | Configure WLB<br>Initialize WLB and change WLB servers<br>Enable WLB<br>Disable WLB |
| Apply WLB Optimization Recommendations (in WLB tab) | Apply any optimization recommendations that appear in the WLB tab                   |
| Modify WLB report subscriptions                     | Change the WLB report generated or its recipient                                    |

| Permission                                                    | Allows Assignee To                                                                             |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Accept WLB Placement Recommendations (“star” recommendations) | Select one of the servers Workload Balancing recommends for placement (“star” recommendations) |
| Generate WLB Reports, including the Pool Audit Trail report   | View and run WLB reports, including the Pool Audit Trail report                                |
| Display WLB Configuration                                     | View WLB settings for a pool as shown on the WLB tab                                           |

If a user tries to use Workload Balancing and that user doesn’t have sufficient permissions, a role elevation dialog appears. For more information about RBAC, see [Role-based access control](#).

### Determine the status of the Workload Balancing Virtual Appliance

Run the `service workloadbalancing status` command, as described in the Workload Balancing commands.

### Reconfigure a pool to use another WLB Appliance

You can reconfigure a resource pool to use a different Workload Balancing virtual appliance.

However, to prevent the old Workload Balancing virtual appliance from running against a pool, ensure that you first disconnect the pool from the old Workload Balancing virtual appliance.

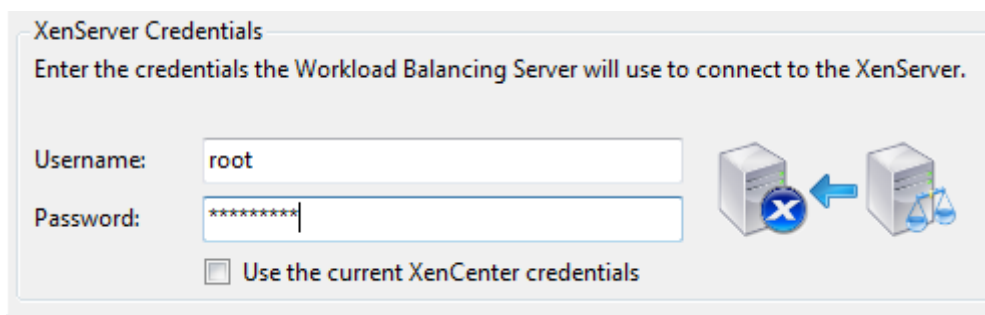
After disconnecting a pool from the old Workload Balancing virtual appliance, you can connect the pool by specifying the name of the new Workload Balancing virtual appliance. Perform the steps in the procedure that follows on the pool you want to connect to a different Workload Balancing virtual appliance.

To use a different Workload Balancing virtual appliance:

1. From the Pool menu, select Disconnect Workload Balancing Server and click Disconnect when prompted.
2. In the WLB tab, click Connect. The Connect to WLB Server dialog appears.
3. In the Address box, type the IP address or FQDN of the new Workload Balancing server.
4. In the WLB Server Credentials section, enter the user name and password that the XenServer pool uses to connect to the Workload Balancing virtual appliance.

These credentials must be for the account you created during Workload Balancing Configuration for the new virtual appliance. By default, the user name for this account is `wlbuser`.

5. In the XenServer Credentials section, enter the user name and password for the pool you are configuring (typically the password for the pool master). Workload Balancing uses these credentials to connect to the hosts in the pool.



**XenServer Credentials**  
Enter the credentials the Workload Balancing Server will use to connect to the XenServer.

Username:

Password:

☐ Use the current XenCenter credentials

The dialog box includes an icon showing two server racks connected by a blue arrow, with a blue 'X' over the left rack.

To use the credentials with which you are currently logged into XenServer, select the Use the current XenCenter credentials check box. If you have assigned a role to this account using the Access Control feature (RBAC), be sure that the role has sufficient permissions to configure Workload Balancing. For more information, see [Workload Balancing Access Control Permissions](#).

### Update Workload Balancing credentials

After initial configuration, if you want to update the credentials XenServer and the Workload Balancing appliance use to communicate, use the following process:

1. Pause Workload Balancing by clicking Pause in the WLB tab.
2. Change the WLB credentials by running the `wlbconfig` command. For more information, see [Workload Balancing Commands](#).
3. Re-enable Workload Balancing and specify the new credentials.
4. After the progress bar completes, click Connect.

The Connect to WLB Server dialog box appears.

5. Click Update Credentials.
6. In the Server Address section, modify the following as desired:
  - In the Address box, type the IP address or FQDN of the Workload Balancing appliance.
  - (Optional.) If you changed the port number during Workload Balancing Configuration, enter that port number. The port number you specify in this box and during Workload Balancing Configuration is the port number XenServer uses to connect to Workload Balancing.

By default, XenServer connects to Workload Balancing on port 8012.

#### Note:

Only edit this port number if you changed it when you ran the Workload Balancing Con-

figuration wizard. The port number value specified when you ran the Workload Balancing Configuration wizard and the Connect to WLB Server dialog must match.

7. In the WLB Server Credentials section, enter the user name (for example, `wlbuser`) and password the computers running XenServer uses to connect to the Workload Balancing server.
8. In the XenServer Credentials section, enter the user name and password for the pool you are configuring (typically the password for the pool master). Workload Balancing uses these credentials to connect to the computers running XenServer in that pool.
9. In the XenServer Credentials section, enter the user name and password for the pool you are configuring. Workload Balancing uses these credentials to connect to the computers running XenServer in that pool.

To use the credentials with which you are currently logged into XenServer, select the Use the current XenCenter credentials check box.

### Change the Workload Balancing IP address

Situations when you may want to update the

To change the Workload Balancing IP address, do the following:

1. Stop the Workload Balancing services by running the `service workloadbalancing stop` command on the virtual appliance.
2. Change the Workload Balancing IP address by running the `ifconfig` command on the virtual appliance.
3. Re-enable Workload Balancing and specify the new IP address.
4. Start the Workload Balancing services by running the `service workloadbalancing start` command on the virtual appliance.

### Stop Workload Balancing

Because Workload Balancing is configured at the pool level, when you want it to stop managing a pool, you must do one of the following:

- **Pause Workload Balancing.** Pausing Workload Balancing stops XenCenter from displaying recommendations for the specified resource pool and managing the pool. Pausing is designed for a short period and lets you resume monitoring without having to reconfigure. When you pause Workload Balancing, data collection stops for that resource pool until you enable Workload Balancing again.
- **Disconnect the pool from Workload Balancing.** Disconnecting from the Workload Balancing virtual appliance breaks the connection between the pool and if possible, deletes the pool data

from the Workload Balancing database. When you disconnect from Workload Balancing, Workload Balancing stops collecting data on the pool.

1. In the Resource pane of XenCenter, select the resource pool for which you want to disable Workload Balancing.
2. In the WLB tab, click Pause. A message appears on the WLB tab indicating that Workload Balancing is paused.

**Tip:**

To resume monitoring, click the Resume button in the WLB tab.

3. In the Infrastructure pane of XenCenter, select the resource pool on which you want to stop Workload Balancing.
4. From the Infrastructure menu, select *Disconnect Workload Balancing Server*. The *Disconnect Workload Balancing server* dialog box appears.
5. Click Disconnect to stop Workload Balancing from monitoring the pool permanently.

**Tip:**

If you disconnected the pool from the Workload Balancing virtual appliance, to re-enable Workload Balancing on that pool, you must reconnect to a Workload Balancing appliance. For information, see the [Connect to the Workload Balancing Virtual Appliance](#).

### Enter Maintenance Mode with Workload Balancing enabled

With Workload Balancing enabled, if you put a host in Maintenance Mode, XenServer migrates the VMs running on that host to their optimal hosts when available. XenServer migrates them based on Workload Balancing recommendations (performance data, your placement strategy, and performance thresholds).

If an optimal host is not available, the words Click here to suspend the VM appear in the Enter Maintenance Mode dialog box. In this case, because there is not a host with sufficient resources to run the VM, Workload Balancing does not recommend a placement. You can either suspend this VM or exit Maintenance Mode and suspend a VM on another host in the same pool. Then, if you reenter the Enter Maintenance Mode dialog box, Workload Balancing might be able to list a host that is a suitable candidate for migration.

**Note:**

When you take a host off-line for maintenance and Workload Balancing is enabled, the words “Workload Balancing” appear in the Enter Maintenance Mode wizard.

### To enter maintenance mode with Workload Balancing enabled:

1. In the Resources pane of XenCenter, select the physical host that you want to take off-line. From the Server menu, select Enter Maintenance Mode.
2. In the Enter Maintenance Mode dialog box, click Enter maintenance mode. The VMs running on the host are automatically migrated to the optimal host based on the Workload Balancing performance data, your placement strategy, and performance thresholds.

To take the host out of maintenance mode, right-click the host and select Exit Maintenance Mode. When you remove a host from maintenance mode, XenServer automatically restores that host's original VMs to that host.

### Increase the Workload Balancing disk size

This procedure explains how to resize the virtual disk of the Workload Balancing virtual appliance. Shut down the virtual appliance before performing these steps. Workload Balancing is unavailable for approximately five minutes.

#### Warning:

Citrix recommends taking a snapshot of your data before performing this procedure. Incorrectly performing these steps can result in corrupting the Workload Balancing virtual appliance.

1. Shut down the Workload Balancing virtual appliance.  
  
In the XenCenter resource pane, select the Workload Balancing virtual appliance (typically "Citrix WLB Virtual Appliance").
2. Click the Storage tab.
3. Select the "vdi\_xvda" disk, and click the Properties button.
4. In the "vdi\_xvda" Properties dialog, select Size and Location.
5. Increase the disk size as needed, and click OK.
6. Start the Workload Balancing virtual appliance and log in to it.
7. Run the following command on the Workload Balancing virtual appliance:

```
1 resize2fs /dev/xvda
```

#### Note::

If the `resize2fs` tool is not installed, ensure that you are connected to the internet and install it using the following command:

```
1 yum install -y --enablerepo=base,updates --disablerepo=citrix
 -* e2fsprogs
```

If there is no internet access:

1. Download the following from [http://mirror.centos.org/centos-7/7.2.1511/os/x86\\_64/Packages/](http://mirror.centos.org/centos-7/7.2.1511/os/x86_64/Packages/).
  - `libss-1.42.9-7.el7.i686.rpm`
  - `e2fsprogs-libs-1.42.9-7.el7.x86_64.rpm`
  - `e2fsprogs-1.42.9-7.el7.x86_64.rpm`
2. Upload them to WLB VM using SCP or any other suitable tool.
3. Run the following command from WLB VM:

```
1 rpm -ivh libss-*.rpm e2fsprogs-*.rpm
```

The tool `resize2fs` is now installed.

4. Run the `df -h` command to confirm the new disk size.

## Remove the Workload Balancing Virtual Appliance

Citrix recommends removing the Workload Balancing virtual appliance by using the standard procedure to delete VMs from XenCenter.

When you delete the Workload Balancing virtual appliance, the PostgreSQL database containing the Workload Balancing is deleted. To save this data, you must migrate it from the database before deleting the Workload Balancing virtual appliance.

## Manage the Workload Balancing database

The Workload Balancing database is a PostgreSQL database. PostgreSQL is an open-source relational database. You can find documentation for PostgreSQL by searching the web.

The following information is intended for database administrators and advanced users of PostgreSQL who are comfortable with database administration tasks. If you are not experienced with PostgreSQL, Citrix recommends that you become familiar with it before you attempt the database tasks in the sections that follow.

By default, the PostgreSQL user name is `postgres`. You set the password for this account during Workload Balancing Configuration.

The amount of historical data you can store is based on the size of the virtual disk allocated to WLB and the minimum required space. By default, the size of the virtual disk allocated to WLB is 20 GB. For more information, see Database grooming parameters.

To store a lot of historical data, for example if you want to enable the Pool Audit trail Report, you can do either of the following:

- Make the virtual disk size assigned to the Workload Balancing virtual appliance larger. To do so, import the virtual appliance, and increase the size of the virtual disk by following the steps in [Increase the Workload Balancing Disk Size](#).
- Create periodic duplicate backup copies of the data by enabling remote client access to the database and using a third-party database administration tool.

In terms of managing the database, you can control the space that database data consumes by configuring database grooming.

### Access the database

The Workload Balancing virtual appliance has firewall configured in it. Before you can access database, you must add the postgresql server port to the iptables.

From the Workload Balancing virtual appliance console, run the following command:

```
1 iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
2 state --state NEW,ESTABLISHED -j ACCEPT
```

(Optional.) To make this configuration persist after the virtual appliance is rebooted, run the following command:

```
1 iptables-save > /etc/sysconfig/potables
```

### Control database grooming

The Workload Balancing database automatically deletes the oldest data whenever the VPX reaches the minimum amount of disk space Workload Balancing requires to run. By default, the minimum amount of required disk space is set to 1,024 MB.

The Workload Balancing database grooming options are controlled through the `wlb.conf` file.

When there is not enough disk space left on the Workload Balancing virtual appliance, Workload Balancing automatically starts grooming historical data. The process is as follows:

1. At a predefined grooming interval, the Workload Balancing data collector checks if grooming is required. Grooming is required if the database data has grown to the point where the only space that remains unused is the minimum required disk space. Use [GroomingRequiredMinimumDiskSizeInMB](#) to set the minimum required disk space.  
  
You can change the grooming interval if desired using [GroomingIntervalInHour](#). However, by default Workload Balancing checks to see if grooming is required once per hour.
2. If grooming is required, Workload Balancing begins by grooming the data from the oldest day. Workload Balancing then checks to see if there is now enough disk space for it to meet the minimum disk-space requirement.



3. If the first grooming did not free enough disk space, then Workload Balancing repeats grooming up to `GroomingRetryCounter` times without waiting for `GroomingIntervalInHour` hour.
4. If the first or repeated grooming freed enough disk space, then Workload Balancing waits for `GroomingIntervalInHour` hour and returns to Step 1.
5. If the grooming initiated by the `GroomingRetryCounter` did not free enough disk space, then Workload Balancing waits for `GroomingIntervalInHour` hour and returns to Step 1.

### Database grooming parameters

There are five parameters in the `wlb.conf` file that control various aspects of database grooming. They are as follows:

- `GroomingIntervalInHour`. Controls how many hours elapse before the next grooming check is done. For example, if you enter **1**, Workload Balancing checks the disk space hourly. If you enter **2**, Workload Balancing checks disk space every two hours to determine if grooming must occur.
- `GroomingRetryCounter`. Controls the number of times Workload balancing tries rerunning the grooming database query.
- `GroomingDBDataTrimDays`. Controls the number of days worth of data Workload Balancing deletes from the database each time it tries to groom data. The default value is one day.
- `GroomingDBTimeoutInMinute`. Controls the number of minutes that the database grooming takes before it times out and is canceled. If the grooming query takes longer than is expected and does not finish running within the timeout period, the grooming task is canceled. The default value is 0 minutes, which means that database grooming never times out.
- `GroomingRequiredMinimumDiskSizeInMB`. Controls the minimum amount of free space left in the virtual disk assigned to the Workload Balancing virtual appliance. When the data in the virtual disk grows until there is only minimum disk size left on the virtual disk, Workload Balancing triggers database grooming. The default value is 2,048 MB.

To edit these values, see the Edit the Workload Balancing configuration file.

### Change the database password

While it is possible to change the database password by using the `wlb.conf` file, Citrix recommends running the `wlbconfig` command instead. For more information, see Modify the Workload Balancing configuration options.

### Archive database data

To avoid having older historical data deleted, you can, optionally, copy data from the database for archiving. To do so, you must perform the following tasks:

1. Enable client authentication on the database.
2. Set up archiving using the PostgreSQL database administration tool of your choice.

### **Enable client authentication to the database**

While you can connect directly to the database through the Workload Balancing console, you can also use a PostgreSQL database management tool. After downloading a database management tool, install it on the system from which you want to connect to the database. For example, you can install the tool on the same laptop where you run XenCenter.

Before you can enable remote client authentication to the database, you must:

1. Modify the database configuration files, including `pg_hba.conf` file and the `postgresql.conf`, to allow connections.
2. Stop the Workload Balancing services, restart the database, and then restart the Workload Balancing services.
3. In the database-management tool, configure the IP address of the database (that is, the IP address of the Workload Balancing VPX) and the database password.

### **Modify the database configuration files**

To enable client authentication on the database, you must modify two files on the Workload Balancing virtual appliance: the `pg_hba.conf` file and the `postgresql.conf` file.

#### **To edit the `pg_hba.conf` file:**

1. Modify the `pg_hba.conf` file. From the Workload Balancing virtual appliance console, open the `pg_hba.conf` file with an editor, such as VI. For example:

```
1 vi /var/lib/pgsql/9.0/data/pg_hba.conf
```

2. If your network uses IPv4, add the IP address from the connecting computer to this file. For example:

In the configuration section, enter the following under `##IPv4 local connections:`

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** 0.0.0.0/0
- **METHOD:** trust

3. Enter your IP address in the **CIDR-ADDRESS** field.

**Note:**

Instead of entering 0.0.0.0/0, you can enter your IP address and replace the last three digits with 0/24. The trailing “24” after the / defines the subnet mask and only allows connections from IP addresses within that subnet mask.

When you enter **trust** for the **Method** field, it enables the connection to authenticate without requiring a password. If you enter **password** for the **Method** field, you must supply a password when connecting to the database.

4. If your network uses IPv6, add the IP address from the connecting computer to this file. For example:

Enter the following under **##IPv6 local connections**:

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** ::0/0
- **METHOD:** trust

Enter the IPv6 addresses in the **CIDR-ADDRESS** field. In this example, the ::0/0 opens the database up to connections from any IPv6 addresses.

5. Save the file and quit the editor.
6. After changing any database configurations, you must restart the database to apply the changes. Run the following command:

```
1 service postgresql-9.0 restart
```

**To edit the postgresql.conf file:**

1. Modify the postgresql.conf file. From the Workload Balancing virtual appliance console, open the postgresql.conf file with an editor, such as VI. For example:

```
1 vi /var/lib/pgsql/9.0/data/postgresql.conf
```

2. Edit the file so that it listens on any port and not just the local host. For example:

- a) Find the following line:

```
1 # listen_addresses='localhost'
```

- b) Remove the comment symbol (##) and edit the line to read as follows:

```
1 listen_addresses='*'
```

3. Save the file and quit the editor.
4. After changing any database configurations, you must restart the database to apply the changes. Run the following command:

```
1 service postgresql-9.0 restart
```

### Change the database maintenance window

Workload Balancing automatically performs routine database maintenance daily at 12:05AM GMT (00:05), by default. During this maintenance window, data collection occurs but the recording of data may be delayed. However, the Workload Balancing user interface controls are available during this period and Workload Balancing still makes optimization recommendations.

#### Note:

To avoid a loss of Workload Balancing:

- During the maintenance window, the Workload Balancing server restarts. Ensure that you do not restart your VMs at the same time.
- At other times, when restarting all VMs in your pool, do not restart the Workload Balancing server.

Database maintenance includes releasing allocated unused disk space and reindexing the database. Maintenance lasts for approximately 6 to 8 minutes. In larger pools, maintenance may last longer, depending on how long Workload Balancing takes to perform discovery.

Depending on your time zone, you may want to change the time when maintenance occurs. For example, in the Japan Standard Time (JST) time zone, Workload Balancing maintenance occurs at 9:05 AM (09:05), which can conflict with peak usage in some organizations. If you want to specify a seasonal time change, such as Daylight Saving Time or summer time, you must build the change into value you enter.

### To change the maintenance time:

1. In the Workload Balancing console, run the following command from any directory:

```
1 crontab -e
```

Workload Balancing displays the following:

```
1 05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
```

The value 05 0 represents the default time for Workload Balancing to perform maintenance in minutes (05) and then hours (0). (The asterisks represent the day, month, and year the job runs: Do not edit these fields.) The entry 05 0 indicates that database maintenance occurs

at 12:05 AM, or 00:05, Greenwich Mean Time (GMT) every night. This setting means that if you live in New York, the maintenance runs at 7:05 PM (19:05) during winter months and 8:05 PM in summer months.

**Important:**

Do not edit the day, month, and year the job runs (as represented by asterisks). Database maintenance must run daily.

2. Enter the time at which you want maintenance to occur in GMT. For example, assuming that you want the maintenance to run at midnight:

| If your time zone is...                                                         | UTC Offset | Value for<br>Maintenance to Run<br>at 12:05 AM Local<br>Time | Value in Daylight<br>Saving Time |
|---------------------------------------------------------------------------------|------------|--------------------------------------------------------------|----------------------------------|
| Pacific Time Zone<br>(PST) in the United<br>States (for example,<br>California) | UTC-08     | 05 8                                                         | 05 7                             |
| Japan Standard Time<br>(JST)                                                    | UTC+09     | 05 15                                                        | N/A                              |
| Chinese Standard<br>Time                                                        | UTC +08    | 04 15                                                        | N/A                              |

1. Save the file and quit the editor.

## Customize Workload Balancing

Workload Balancing provides several methods of customization:

- **Command lines for scripting.** See the commands in Workload Balancing commands.
- **Host Power On scripting support.** You can also customize Workload Balancing (indirectly) through the Host Power On scripting.

## Upgrade Workload Balancing

Online upgrading of Workload Balancing has been deprecated for security reasons. Customers cannot to upgrade by using the yum repo anymore. Customers can upgrade WLB to the latest version by importing the latest WLB VPX downloadable at <https://www.citrix.com/downloads/xenserver/product-software/>.

## Troubleshoot Workload Balancing

While Workload Balancing usually runs smoothly, this series of sections provides guidance in case you encounter issues.

### General troubleshooting tips

- Start troubleshooting by reviewing the Workload Balancing log files (LogFile.log and wlb\_install\_log.log). You can find these logs in Workload Balancing virtual appliance in this location (by default):
  - /var/log/wlb
- Check the logs in the XenCenter Logs tab for more (different) information.
- To check the Workload Balancing virtual appliance build number, run the following command on a hosts in a pool that the VPX monitors:

```
1 xe pool-retrieve-wlb-diagnostics | more
```

The Workload Balancing version number appears at the top of the output.

### Error messages

Workload Balancing displays errors on screen as dialog boxes and as error messages in the Logs tab in XenCenter.

If an error message appears, review the XenCenter event log for additional information. For information about the location of this log, see the XenCenter Help.

### Issues entering Workload Balancing credentials

If you cannot successfully enter the virtual appliance user account and password while configuring the Connect to WLB Server dialog, try the following:

- Ensure that Workload Balancing virtual appliance imported and was configured correctly and all of its services are running. For more information, see [wlb-start](#).
- Check to ensure that you are entering the correct credentials. The default credentials appear in the Workload Balancing Quick Start.
- You can enter a host name in the Address box, but it must be the fully qualified domain name (FQDN) of the Workload Balancing virtual appliance. Do not enter the host name of the physical

server hosting the appliance. For example, `yourcomputername{#vrnmN320059}.yourdomain.net{#vrnmN32005F}`. If you are having trouble entering a computer name, try using the Workload Balancing appliance's IP address instead.

- Verify that the host is using the correct DNS server and the XenServer host can contact Workload Balancing server using its FQDN. To do this check, ping the Workload Balancing appliance using its FQDN from the XenServer host. For example, enter the following in the XenServer host console:

```
1 ping wlb-vpx-1.mydomain.net
```

## Issues with firewalls

The following error appears if the Workload Balancing virtual appliance is behind a (hardware) firewall, and you did not configure the appropriate firewall settings: “There was an error connecting to the Workload Balancing server: <pool name> Click Initialize WLB to reinitialize the connection settings.” This error may also appear if the Workload Balancing appliance is otherwise unreachable.

### Resolution:

If the Workload Balancing virtual appliance is behind a firewall, open port 8012.

Likewise, the port XenServer uses to contact Workload Balancing (8012 by default), must match the port number specified when you ran the Workload Balancing Configuration wizard.

## Lose the connection to Workload Balancing

If, after configuring and connecting to Workload Balancing, you receive a connection error, the credentials may no longer be valid. To isolate this issue, try:

- Verifying the credentials you entered in the Connect to WLB Server dialog box match the credentials:
  - You created during Workload Balancing Configuration
  - On XenServer (that is, the pool master credentials)
- Verifying the IP address or FQDN for the Workload Balancing virtual appliance that you entered in the Connect to WLB Server dialog box is correct.
- Verifying the user name you created during Workload Balancing Configuration matches the credentials you entered in the Connect to WLB Server dialog box.

### Workload Balancing connection errors

If you receive a connection error in the Workload Balancing Status line on the WLB tab, you might need to reconfigure Workload Balancing on that pool.

Click the Connect button on the WLB tab and reenter the server credentials.

### Workload Balancing stops working

If Workload Balancing doesn't work (for example, it doesn't let you save changes to settings), check the Workload Balancing log file for the following error message:

```
1 dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
```

#### Cause:

This error typically occurs in pools that have one or more problematic VMs. When VMs are problematic, you might see the following behavior:

- **Windows.** The Windows VM crashes due to a stop error ("blue screen").
- **Linux.** The Linux VM may be unresponsive in the console and typically does not shut down.

#### Workaround:

1. Force the VM to shut down. To do so, you can do one of the following on the host with the problematic VM:
  - In XenCenter, select the VM, and then from the VM menu, click Force Shutdown.
  - Run the `vm-shutdown` xe command with the force parameter set to true as described in the XenServer Administrator's Guide. For example:

```
1 xe vm-shutdown \
2 force=true \
3 uuid=vm_uuid \

```

You can find the host UUID on the General tab for that host (in XenCenter) or by running the `host-list` xe command. You can find the VM UUID on the General tab for the VM or by running the `vm-list` xe command. For more information, see [Command line interface](#).

2. In the xsconsole of the XenServer hosting the crashed VM or in XenCenter, migrate all of the VMs to another host, then run the `xe-toolstack-restart` command.

### Issues changing Workload Balancing servers

If you connect a pool to a different Workload Balancing server without disconnecting from Workload Balancing, both old and new Workload Balancing servers monitor the pool.

To solve this problem, you can take one of the following actions:



- Shut down and delete the old Workload Balancing virtual appliance.
- Manually stop the Workload Balancing services. These services are analysis, data collector, and Web service.

**Note:**

Do not use the `pool-deconfigure-wlb` xe command to disconnect a pool from the Workload Balancing virtual appliance or use the `pool-initialize-wlb` xe command to specify a different appliance.

## Workload Balancing commands

This section provides a reference for the Workload Balancing commands. You can perform these commands from the XenServer host or console to control Workload Balancing or configure Workload Balancing settings on the XenServer host. This appendix includes xe commands and service commands.

Run the following service commands on the Workload Balancing appliance. To do so, you must log in to the Workload Balancing virtual appliance.

### Log in to the Workload Balancing Virtual Appliance

Before you can run any service commands or edit the `wlb.conf` file, you must log in to the Workload Balancing virtual appliance. To do so, you must enter a user name and password. Unless you created extra user accounts on the virtual appliance, log in using the root user account. You specified this account when you ran Workload Balancing Configuration wizard (before you connected your pool to Workload Balancing). You can, optionally, use the Console tab in XenCenter to log in to the appliance.

#### To log in to the Workload Balancing virtual appliance:

1. At the *name-of-your-WLB-VPX* login prompt, enter the account user name. For example, where `wlb-vpx-pos-pool` is the name of your Workload Balancing appliance:

```
1 wlb-vpx-pos-pool login: root
```

2. At the Password prompt, enter the password for the account:

```
1 wlb-vpx-pos-pool login: root
```

**Note:**

To log off the Workload Balancing virtual appliance, simply type `logout` at the command prompt.

**wlb restart**

Run the `wlb restart` command from anywhere in the Workload Balancing appliance to stop and then restart the Workload Balancing Data Collection, Web Service, and Data Analysis services.

**wlb start**

Run the `wlb start` command from anywhere in the Workload Balancing appliance to start the Workload Balancing Data Collection, Web Service, and Data Analysis services.

**wlb stop**

Run the `wlb stop` command from anywhere in the Workload Balancing appliance to stop the Workload Balancing Data Collection, Web Service, and Data Analysis services.

**wlb status**

Run the `wlb status` command from anywhere in the Workload Balancing appliance to determine the status of the Workload Balancing server. After you execute this command, the status of the three Workload Balancing services (the Web Service, Data Collection Service, and Data Analysis Service) is displayed.

**Modify the Workload Balancing configuration options**

Many Workload Balancing configurations, such as the database and web-service configuration options, are stored in the `wlb.conf` file. The `wlb.conf` file is a configuration file on the Workload Balancing virtual appliance.

To make it easier to modify the most commonly used options, Citrix provides a command, `wlb config`. Running the `wlb config` command on the Workload Balancing virtual appliance lets you rename the Workload Balancing user account, change its password, or change the PostgreSQL password. After you execute this command, the Workload Balancing services are restarted.

**To run the wlb config command:**

1. Run the following from the command prompt:

```
1 wlb config
```

The screen displays a series of questions guiding you through changing your Workload Balancing user name and password and the PostgreSQL password. Follow the questions on the screen to change these items.

**Important:**

Double-check any values you enter in the `wlb.conf` file: Workload Balancing does not validate values in the `wlb.conf` file. Therefore, if the configuration parameters you specify are not within the required range, Workload Balancing does not generate an error log.

**Edit the Workload Balancing configuration file**

You can modify Workload Balancing configuration options by editing the `wlb.conf` file, which is stored in `/opt/vpx/wlb` directory on the Workload Balancing virtual appliance. In general, only change the settings in this file with guidance from Citrix. However, there are three categories of settings you can change if desired:

- **Workload Balancing account name and password.** It is easier to modify these credentials by running the `wlb config` command.
- **Database password.** This value can be modified using the `wlb.conf` file. However, Citrix recommends modifying it through the `wlb config` command since this command modifies the `wlb.conf` file and automatically updates the password in the database. If you choose to modify the `wlb.conf` file instead, you must run a query to update the database with the new password.
- **Database grooming parameters.** You can modify database grooming parameters, such as the database grooming interval, using this file by following the instructions in the database management section. However, if you do so, Citrix recommends using caution.

For all other settings in the `wlb.conf` file, Citrix currently recommends leaving them at their default, unless Citrix instructed you to modify them.

**To edit the `wlb.conf` file:**

1. Run the following from the command prompt on the Workload Balancing virtual appliance (using VI as an example):

```
1 vi /opt/vpx/wlb/wlb.conf
```

The screen displays several different sections of configuration options.

2. Modify the configuration options, and exit the editor.

You do not need to restart Workload Balancing services after editing the `wlb.conf` file. The changes go into effect immediately after exiting the editor.

**Important:**

Double-check any values you enter in the `wlb.conf` file: Workload Balancing does not validate values in the `wlb.conf` file. Therefore, if the configuration parameters you specify are not within the required range, Workload Balancing does not generate an error log.

## Increase the detail in the Workload Balancing log

The Workload Balancing log provides a list of events on the Workload Balancing virtual appliance, including actions for the analysis engine, database, and audit log. This log file is found in this location: `/var/log/wlb/LogFile.log`.

You can, if desired, increase the level of detail the Workload Balancing log provides. To do so, modify the Trace flags section of the Workload Balancing configuration file (`wlb.conf`), which is found in the following location: `/opt/vpx/wlb/wlb.conf`. Enter a 1 or true to enable logging for a specific trace and a 0 or false to disable logging. For example, to enable logging for the Analysis Engine trace, enter:

```
1 AnalEngTrace=1
```

You may want to increase logging detail before reporting an issue to Citrix Technical Support or when troubleshooting.

| Logging Option        | Trace Flag                       | Benefit or Purpose                                                                                                                                                                                                                     |
|-----------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Analysis Engine Trace | <code>AnalEngTrace</code>        | Logs details of the analysis engine calculations. Shows details of the decisions the analysis engine is making and potentially gain insight into the reasons Workload Balancing is not making recommendations.                         |
| Database Trace        | <code>DatabaseTrace</code>       | Logs details about database reads/writes. However, leaving this trace on increases the log file size quickly.                                                                                                                          |
| Data Collection Trace | <code>DataCollectionTrace</code> | Logs the actions of retrieving metrics. This value lets you see the metrics Workload Balancing is retrieving and inserting into the Workload Balancing data store. However, leaving this trace on increases the log file size quickly. |

| Logging Option         | Trace Flag                        | Benefit or Purpose                                                                                                                                                                                                                    |
|------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Compaction Trace  | <code>DataCompactionTrace</code>  | Logs details about how many milliseconds it took to compact the metric data.                                                                                                                                                          |
| Data Event Trace       | <code>DataEventTrace</code>       | This trace provides details about events Workload Balancing catches from XenServer.                                                                                                                                                   |
| Data Grooming Trace    | <code>DataGroomingTrace</code>    | This trace provides details about the database grooming.                                                                                                                                                                              |
| Data Metrics Trace     | <code>DataMetricsTrace</code>     | Logs details about the parsing of metric data. Leaving this trace on increases the log-file size quickly.                                                                                                                             |
| Queue Management Trace | <code>QueueManagementTrace</code> | Logs details about data collection queue management processing. (This option is for internal use.)                                                                                                                                    |
| Data Save Trace        | <code>DataSaveTrace</code>        | Logs details about the pool being saved to the database.                                                                                                                                                                              |
| Score Host Trace       | <code>ScoreHostTrace</code>       | Logs details about how Workload Balancing is arriving at a score for a host. This trace shows the detailed scores generated by Workload Balancing when it calculates the star ratings for selecting optimal servers for VM placement. |

| Logging Option       | Trace Flag                      | Benefit or Purpose                                                                                                                                                                                                                                |
|----------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit Log Trace      | <code>AuditLogTrace</code>      | Shows the action of the audit log data being captured and written. (This option is only for internal use and does not provide information that is captured in the audit log.) However, leaving this trace on increases the log file size quickly. |
| Scheduled Task Trace | <code>ScheduledTaskTrace</code> | Logs details about scheduled tasks. For example, if your scheduled mode changes are not working, you might want to enable this trace to investigate the cause.                                                                                    |
| Web Service Trace    | <code>WlbWebServiceTrace</code> | Logs details about the communication with the web-service interface.                                                                                                                                                                              |

## Configure Certificates for Workload Balancing

January 2, 2019

This section provides information about two optional tasks for securing certificates:

- Configuring XenServer to verify a certificate from a Trusted Authority
- Configuring XenServer to verify the default Citrix WLB self-signed certificate

### Overview

XenServer and Workload Balancing communicate over HTTPS. Consequently during Workload Balancing Configuration, the wizard automatically creates a self-signed test certificate. This self-signed test certificate lets Workload Balancing establish an SSL connection to XenServer.

#### Note:

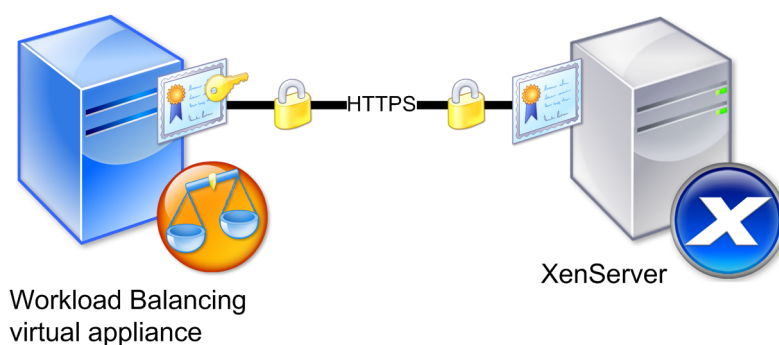
The self-signed certificate is a placeholder to facilitate HTTPS communication and is not from

a trusted certificate authority. For added security, Citrix recommends using a certificate signed from a trusted certificate authority.

By default, Workload Balancing creates this SSL connection with XenServer automatically. You do not need to perform any certificate configurations during or after configuration for Workload Balancing to create this SSL connection.

However, to use a certificate from another certificate authority, such as a signed one from a commercial authority, you must configure Workload Balancing and XenServer to use it.

Regardless of what certificate Workload Balancing uses, by default, XenServer does not validate the identity of the certificate before it establishes connection to Workload Balancing. To configure XenServer to check for a specific certificate, you must export the root certificate that was used to sign the certificate, copy it to XenServer, and configure XenServer to check for it when a connection to Workload Balancing is made. In this scenario, XenServer acts as the client and Workload Balancing acts as the server.



Depending on your security goals, you can either:

- Configure XenServer to verify the self-signed test certificate. See [Configure XenServer to Verify the Self-Signed Certificate](#).
- Configure XenServer to verify a certificate from a trusted certificate authority. See [Configure XenServer to Verify a Certificate-authority Certificate](#).

## Configure XenServer to verify the self-signed certificate

You can configure XenServer to verify that the Citrix WLB self-signed certificate is authentic before XenServer permits Workload Balancing to connect.

### Important:

To verify the Citrix WLB self-signed certificate, you must connect to Workload Balancing using its host name. To find the Workload Balancing host name, run `hostname` command on the virtual appliance.

If you want to configure Workload Balancing to verify the Citrix WLB self-signed certificate, perform the steps in the procedure that follows.

**To configure XenServer to verify the self-signed certificate:**

1. Copy the self-signed certificate from the Workload Balancing virtual appliance to the pool master. The Citrix WLB self-signed certificate is stored at `/etc/ssl/certs/server.pem`. Run the following on the pool master to copy the certificate:

```
1 scp root@wlb-ip:/etc/ssl/certs/server.pem .
```

2. If you receive a message stating that the authenticity of `wlb-ip` cannot be established, type `yes` to continue.
3. Enter Workload Balancing virtual appliance root password when prompted, the certificate will be copied to current directory.
4. Install the certificate. Run the `pool-certificate-install` command from the directory where you copied the certificate. For example:

```
1 xe pool-certificate-install filename=server.pem
```

5. Verify the certificate was installed correctly by running the `pool-certificate-list` command on the pool master:

```
1 xe pool-certificate-list
```

If you installed the certificate correctly, the output of this command includes the exported root certificate (for example, `server.pem`). Running this command lists all installed SSL certificates, including the certificate you just installed.

6. Synchronize the certificate from the master to all hosts in the pool by running the `pool-certificate-sync` command on the pool master:

```
1 xe pool-certificate-sync
```

Running the `pool-certificate-sync` command on the master synchronizes the certificate and certificate revocation lists on all the pool servers with the master. This ensures all hosts in the pool use the same certificates.

There is no output from this command. However, the next step does not work if this one did not work successfully.

7. Instruct XenServer to verify the certificate before connecting to the Workload Balancing virtual appliance. Run the following command on the pool master:

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```



**Tip:**

Pressing the Tab key automatically populates the UUID of the pool.

8. (Optional) To verify this procedure worked successfully, perform the following steps:
  - a) To test if the certificate synchronized to the other hosts in pool, run the `pool-certificate-list` command on those hosts.
  - b) To test if XenServer was set to verify the certificate, run the `pool-param-get` command with the `param-name=wlb-verify-cert` parameter. For example:

```
1 xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
```

## Configure XenServer to verify a certificate-authority certificate

You can configure XenServer to verify a certificate signed by a trusted certificate authority.

For trusted authority certificates, XenServer requires an exported certificate or certificate chain (the intermediate and root certificates) in .pem format that contains the public key.

If you want Workload Balancing to use a trusted authority certificate, do the following:

1. Obtain a signed certificate from the certificate authority. See Task 1: Obtaining a certificate-authority certificate.
2. Follow the instructions in Task 2: Specifying the New Certificate to specify and apply the new certificate.
3. Install the obtained certificates and enable certificate verification on the pool master. See Task 3: Importing the Certificate Chain into the Pool.

Before beginning these tasks, ensure:

- You know the IP address for the XenServer pool master.
- XenServer can resolve the Workload Balancing host name. (For example, you can try pinging the Workload Balancing FQDN from the XenServer console for the pool master.)

**Important:**

If you want to use an IP address to connect to Workload Balancing, you must specify that IP address as the Subject Alternative Name (SAN) when you create the certificate.

## Task 1: Obtaining a certificate-authority certificate

To obtain a certificate from a certificate authority, you must generate a Certificate Signing Request (CSR). Generating a CSR for the Workload Balancing virtual appliance is two-task process. You must

(1) create a private key and (2) use that private key to generate the CSR. You must perform both of these procedures on the Workload Balancing virtual appliance.

### Guidelines for specifying the Common Name

The Common Name (CN) you specify when creating a CSR must exactly match the FQDN of your Workload Balancing virtual appliance and the FQDN or IP address you specified in the Address box in the Connect to WLB Server dialog box.

To ensure the name matches, specify the Common Name using one of these guidelines:

- Specify the same information for the certificate's Common Name as you specified in the Connect to WLB Server dialog. For example, if your Workload Balancing virtual appliance is named `wlb-vpx.yourdomain`, specify `wlb-vpx.yourdomain` in the Connect to WLB Server and provide `wlb-vpx.yourdomain` as the Common Name when creating the CSR.
- If you connected your pool to Workload Balancing using an IP address, use the FQDN as the Common Name and specify the IP address as a Subject Alternative Name (SAN). However, this may not work in all situations.

#### Note:

Certificate verification is a security measure designed to prevent unwanted connections. As a result, Workload Balancing certificates must meet strict requirements or the certificate verification will not succeed and XenServer will not allow the connection. Likewise, for certificate verification to succeed, you must store the certificates in the specific locations in which XenServer expects to find the certificates.

### To create a private key file:

1. Create a private key file:

```
1 openssl genrsa -des3 -out privatekey.pem 2048
```

2. Remove the password:

```
1 openssl rsa -in privatekey.pem -out privatekey.nop.pem
```

#### Note:

If you enter the password incorrectly or inconsistently, you may receive some messages indicating that there is a user interface error. You can ignore the message and just rerun the command to create the private key file.

### To generate the CSR:

1. Generate the CSR:

- a) Create the CSR using the private key:

```
1 openssl req -new -key privatekey.nop.pem -out csr
```

- b) Follow the prompts to provide the information necessary to generate the CSR:

**Country Name.** Enter the SSL Certificate country codes for your country. For example, CA for Canada or JM for Jamaica. You can find a list of SSL 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 Workload Balancing server. This must match the name the pool uses to connect to Workload Balancing.

**Email Address.** This email address is included in the certificate when you generate it.

- c) Provide optional attributes or click Enter to skip providing this information.

The CSR request is saved in the current directory and is named `csr`.

2. Display the CSR in the console window by running the following commands in the Workload Balancing appliance console:

```
1 cat csr
```

3. Copy the entire Certificate Request and use the CSR to request the certificate from the certificate authority.

## Task 2: Specifying the new certificate

Use this procedure to specify Workload Balancing use a certificate from a certificate authority. This procedure installs the root and (if available) intermediate certificates.

### To specify a new certificate:

1. Download the signed certificate, root certificate and, if the certificate authority has one, the intermediate certificate from the certificate authority.
2. If you did not download the certificates to the Workload Balancing virtual appliance. Do one of the following:

- a) If you are copying the certificates from a Windows computer to the Workload Balancing appliance, use WinSCP or another copying utility, to copy the files.

For the host name, you can enter the IP address and leave the port at the default. The user name and password are typically root and whatever password you set during configuration.

- a) If you are copying the certificates from a Linux computer to the Workload Balancing appliance, use SCP or another copying utility, to copy the files to the directory of your choice on the Workload Balancing appliance. For example:

```
1 scp root_ca.pem root@wlb-ip:/path_on_your_WLB
```

3. On the Workload Balancing virtual appliance, merge contents of all the certificates (root certificate, intermediate certificate (if it exists), and signed certificate) into one file. For example:

```
1 cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
```

4. Rename the existing certificate and key using the move command:

```
1 mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
2 mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
```

5. Copy the merged certificate:

```
1 mv server.pem /etc/ssl/certs/server.pem
```

6. Copy the private key created previously:

```
1 mv privatekey.nop.pem /etc/ssl/certs/server.key
```

7. Make the private key readable only by root. Use `chmod` command to fix permissions.

```
1 chmod 600 /etc/ssl/certs/server.key
```

8. Restart `stunnel`:

```
1 killall stunnel
2 stunnel
```

### Task 3: Importing the certificate chain into the pool

After obtaining certificates, you must import (install) the certificates onto the XenServer pool master and synchronize the hosts in the pool to use those certificates. Then, you can configure XenServer to check the certificate's identity and validity each time Workload Balancing connects to a host.

1. Copy the signed certificate, root certificate and, if the certificate authority has one, the intermediate certificate from the certificate authority onto the XenServer pool master.
2. Install the root certificate on the pool master:

```
1 xe pool-certificate-install filename=root_ca.pem
```

3. If applicable, install the intermediate certificate on the pool master:

```
1 xe pool-certificate-install filename=intermediate_ca.pem
```

4. Verify both the certificates installed correctly by running this command on the pool master:

```
1 xe pool-certificate-list
```

Running this command lists all installed SSL certificates. If the certificates installed successfully, they appear in this list.

5. Synchronize the certificate on the pool master to all hosts in the pool:

```
1 xe pool-certificate-sync
```

Running the `pool-certificate-sync` command on the master synchronizes the certificates and certificate revocation lists on all the pool servers with the pool master. This ensures all hosts in the pool use the same certificates.

6. Instruct XenServer to verify a certificate before connecting to the Workload Balancing virtual appliance. Run the following command on the pool master:

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

**Tip:**

Pressing the Tab key automatically populates the UUID of the pool.

7. If, before you enabled certificate verification, you specified an IP address in the Connect to WLB dialog, you may be prompted to reconnect the pool to Workload Balancing.

In this case, specify the **FQDN** for the Workload Balancing appliance in the Address box in the Connect to WLB dialog *exactly as it appears in the certificate's Common Name (CN)*. (You must enter the FQDN since the Common Name and the name that XenServer uses to connect must match.)

## Troubleshooting tips

- If, after configuring certificate verification, the pool cannot connect to Workload Balancing, check to see if the pool can connect if you turn certificate verification off (by running `xe`

`pool-param-set wlb-verify-cert=false uuid=uuid_of_pool`). If it can connect with verification off, the issue is in your certificate configuration. If it cannot connect, the issue is in either your Workload Balancing credentials or your network connection.

- Some commercial certificate authorities provide tools to verify the certificate installed correctly. Consider running these tools if these procedures fail to help isolate the issue. If these tools require specifying an SSL port, specify port 8012 or whatever port you set during Workload Balancing Configuration.
- If, after following these procedures, an error message appears on the WLB tab stating, “There was an error connecting to the WLB server,” there may be a conflict between the Common Name in the certificate and the name of the Workload Balancing virtual appliance. The Workload Balancing virtual-appliance name and the Common Name of the certificate must match exactly.

## Conversion Manager

November 16, 2018

XenServer Conversion Manager helps you migrate workloads from VMware to XenServer by moving batches of VMware virtual machines to your XenServer environment.

XenServer Conversion Manager makes migration easier; it does more than just convert virtual machines. XenServer Conversion Manager helps you prepare the virtual machines for networking and storage connectivity. Following conversion the virtual machines are almost ready to run.

### Convert from VMware to XenServer

XenServer Conversion Manager allows you to:

- Convert multiple VMs using one simple wizard
- Map network settings between VMware and XenServer so your converted VMs can be up and running with the proper network settings
- Select a storage location where you would like your new XenServer VMs to run

#### Notes:

- XenServer Conversion Manager does not remove or change your existing VMware environment. VMs are duplicated onto your XenServer environment and not removed from VMware.
- XenServer Conversion Manager is available for XenServer Enterprise Edition customers or customers who have access to XenServer through their Citrix Virtual Apps and Desktops

entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer 7.6 license, visit the [Citrix website](#).

## Understand XenServer

Before you can convert your environment, it is suggested that you become familiar with XenServer concepts. For more information, see [Technical overview](#).

To use XenServer Conversion Manager successfully, perform the following tasks:

- Setting up a basic XenServer environment, including installing XenServer. For more information, see [Quick start](#)[(/en-us/xenserver/current-release/quick-start.html)] and [Install](#).
- Creating a network in XenServer, assigning an IP address to a NIC. For more information, see [Quick start](#).
- Connecting to storage. For more information, see [Quick start](#).

### Note:

XenServer documentation is available from [docs.citrix.com](#), Knowledge Center articles, and white papers are available from the [Citrix Knowledge Center](#).

## Compare VMware and XenServer terminology

The following table lists the approximate XenServer equivalent for common VMware features, concepts, and components:

| VMware Term                           | XenServer Equivalent                             |
|---------------------------------------|--------------------------------------------------|
| VMware vSphere Client                 | XenCenter (the management console for XenServer) |
| Cluster / Resource Pool               | Resource Pool                                    |
| Data Store                            | Storage Repository                               |
| vMotion                               | XenMotion                                        |
| Distributed Resource Scheduling (DRS) | Workload Balancing                               |
| High Availability (HA)                | High Availability (HA)                           |
| vCenter Converter                     | XenConvert, XenServer Conversion Manager         |
| Role Based Access Control (RBAC)      | Role Based Access Control (RBAC)                 |

## Conversion overview

XenServer Conversion Manager creates a copy of each targeted VM. After converting the targeted VM to a XenServer VM with comparable networking and storage connectivity, it imports the VM into your XenServer pool or host. You can use XenServer Conversion Manager to convert as few as one or two VMs or perform batch conversions of an entire environment.

### Note:

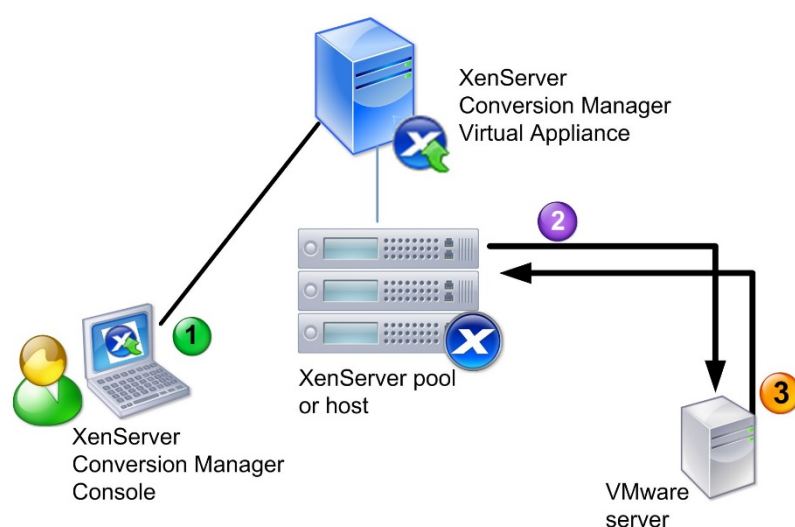
Before converting the VMs from vSphere, you must shut down the VMs (intended for conversion) on vSphere. The current version of XenServer Conversion Manager does not support converting a running VM using memory copied from vSphere to XenServer.

The XenServer Conversion Manager conversion process requires four items:

- **XenServer Conversion Manager Console** - the user interface where you set conversion options and control conversion. You can install the console on your Windows or a Linux local desktop. XenServer Conversion Manager requires a connection to XenServer and the XenServer Conversion Manager Virtual Appliance.
- **XenServer Conversion Manager Virtual Appliance** - a pre-packaged VM you import into the XenServer host or pool where you want to run the converted VMs. The virtual appliance converts the copies of the VMware VMs into the XenServer virtual-machine format. After conversion, it imports these copies into the XenServer pool or host.
- **XenServer standalone host or pool** - the XenServer environment where you want to run the converted VMs.
- **VMware server.** XenServer Conversion Manager requires a connection to a VMware server that manages the VMs you want to convert. This connection can be to a vCenter Server, ESXi Server, or ESX Server. The VMs are not removed from the VMware server. Instead, the XenServer Conversion Manager Virtual Appliance makes a copy of these VMs and converts them to XenServer virtual-machine format.

**The following illustration shows the relationships between these components:**





This illustration shows:

1. How XenServer Conversion Manager communicates with XenServer Conversion Manager Virtual Appliance.
2. How the XenServer Conversion Manager Virtual Appliance authenticates with the VMware server.
3. How the VMware server responds to the XenServer Conversion Manager Virtual Appliance during conversion.

The VMware server communicates with the XenServer Conversion Manager Virtual Appliance only when the appliance queries the VMware server for environment information and disk data throughout the conversion.

### Summary of how to convert VMs

You can configure the XenServer Conversion Manager and start to convert VMs in just a few easy steps:

1. Download the XenServer Conversion Manager Virtual Appliance and the XenServer Conversion Manager Console from the [XenServer 7.6 Enterprise Edition page].
2. Import the XenServer Conversion Manager Virtual Appliance into the XenServer using XenCenter.
3. Configure the XenServer Conversion Manager Virtual Appliance using XenCenter.
4. Install the XenServer Conversion Manager Console.
5. From the XenServer Conversion Manager Console, launch the conversion wizard and start to convert VMs.

The sections that follow explain these steps in detail. Information is also available in the XenServer Conversion Manager Help, which appears in the XenServer Conversion Manager Console.

## Prepare your environment

Before converting your VMware environment, you must create and prepare the target XenServer standalone host or environment to run the converted VMware VMs. Preparing your environment includes the following activities:

1. Defining a strategy of how you convert your VMware environment. Do you just want to convert 1 or 2 VMs? Do you want to convert your entire environment? Do you want to create a pilot first to ensure that your configuration is correct? Do you run both environments in parallel? Do you want to maintain your existing cluster design when you convert to XenServer?
2. Planning your networking configuration. Do you want to connect to the same physical networks? Do you want to simplify or change your networking configuration?
3. Installing XenServer on the hosts you want in the pool. Ideally, you should have the NICs on the hosts plugged in to their physical networks before you begin installation.
4. Creating a pool and performing any basic networking configuration. For example, do the following:
  - Configure a network to connect to the VMware cluster on the XenServer host (if the cluster is not on the same network as the XenServer host).
  - Configure a network to connect to the storage array. That is, if you use IP-based storage, create a XenServer network that connects to the physical network of the storage array.
  - Create a pool and add hosts to this pool.
5. (For shared storage and XenServer pools.) Preparing the shared storage where you store the virtual disks and creating a connection to the storage, known as a Storage Repository (SR) on the pool.
6. (Optional.) Although not a requirement for conversion, you may want to configure the administrator accounts on the XenServer pool to match those accounts on the VMware server. For information about configuring Role-based Access Control for Active Directory accounts, see the XenCenter Help or [Quick start](#).

## Install XenServer and create a pool

Before you can convert VMware VMs, ensure that you create a XenServer pool or host where you want to run the converted VMs. This pool must have networking configured so it can connect to the VMware server. You may also want to configure the same physical networks on the XenServer pool that you have in the VMware cluster, or simplify your networking configuration. If you want to run the converted VMs in a pool, create a storage repository before conversion and add the shared storage to the pool.

If you are new to XenServer, you can learn about XenServer basics, including basic installation and configuration, by reading [Quick start](#).

## **XenServer environment considerations**

Before installing XenServer and importing the virtual appliance, consider the following factors that may change your conversion strategy:

### **Selecting the host where you want to run the XenServer Conversion Manager Virtual Appliance.**

Import the virtual appliance into the stand-alone host or into a host in the pool where you run the converted VMs.

For pools, you can run the virtual appliance on any host in the pool, provided its storage meets the storage requirements.

**The storage configured for the pool or host where you want to run the converted VMs must meet specific requirements.** If you want to run your newly converted VMs in a pool, their virtual disks must be stored on shared storage. However, if the converted VMs run on a single standalone host (not a pool), their virtual disks can use local storage.

If you want to run the converted VMs in a pool, ensure that you add the shared storage to the pool by creating a storage repository.

**Guest operating systems supported for conversion.** XenServer Conversion Manager supports converting VMware VMs running any of the Windows guest operating systems that XenServer supports. For a list of Windows guest operating systems supported by XenServer, see [Guest operating system support](#). The following Linux operating systems are also supported.

- RHEL 5.4/5.6/6.4/7.0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 12.04/14.04/16.04

## **Meet networking requirements**

To convert VMware VMs, the XenServer Conversion Manager Virtual Appliance needs connectivity to a physical network or VLAN that can contact the VMware server. (In the following sections, this network is referred to as the “VMware network.”)

If the VMware server is on a different physical network than the hosts in the XenServer pool, add the network to XenServer before conversion.

## Map your existing network configuration

XenServer Conversion Manager includes features that can reduce the amount of manual networking configuration needed after you convert from your existing VMware VMs to XenServer. For example, XenServer Conversion Manager will:

- Preserve virtual MAC addresses on the VMware VMs and reuse them in the resulting XenServer VMs. Preserving the MAC addresses associated with virtual network adapters (virtual MAC addresses) may:
  - Help preserve IP addresses in environments using DHCP
  - Be useful for software programs whose licensing references the virtual MAC addresses
- Map (virtual) network adapters. XenServer Conversion Manager can map VMware networks onto XenServer networks so that after the VMs are converted, their virtual network interfaces are connected accordingly. XenServer networks you can choose include standard physical networks (known as External Networks), VLANs, single-server private networks, and cross-server private networks.

For example, if you map VMware 'Virtual Network 4' to XenServer 'Network 0', any VMware VM that had a virtual adapter connected to 'Virtual Network 4' is connected to 'Network 0' after conversion. XenServer Conversion Manager does not convert or migrate any hypervisor network settings. The wizard only alters a converted VM's virtual network interface connections based on the mappings provided.

### Note:

You do not need to map all of your VMware networks on to the corresponding XenServer networks. However, if you prefer, you can change the networks the VMs use, reduce, or consolidate the number of networks in your new XenServer configuration.

To gain the maximum benefit from these features, Citrix recommends the following:

- Before installing XenServer, plug the hosts into the networks on the switch (that is, the ports) that you would like to configure on the host.
- Ensure that the XenServer pool can see the networks that you would like to be detected. Specifically, plug the XenServer hosts into switch ports that can access the same networks as the VMware cluster.

Though it is easier to plug the XenServer NICs into the same networks as the NICs on the VMware hosts, it is not required. If you would like to change the NIC/network association, you can plug a XenServer NIC into a different physical network.

## Prepare for the XenServer Conversion Manager networking requirements

When you perform conversion, you must create a network connection to the network where the VMware server resides. XenServer Conversion Manager uses this connection for conversion traffic between the XenServer host and the VMware server.

To create this network connection, you must perform two tasks:

- When you import the XenServer Conversion Manager Virtual Appliance, specify the network you added for conversion traffic as a virtual network interface. You can do so by configuring **interface 1** so it connects to that network.
- Before you run the conversion wizard, add the network connecting VMware and XenServer to the XenServer host where you want to run the converted VMs.

By default, when you import the XenServer Conversion Manager Virtual Appliance, XenCenter creates one virtual network interface associated with Network 0 and NIC0 (eth0). However, by default, XenServer Setup configures NIC0 as the *management interface*, a NIC used for XenServer management traffic. As a result, when adding a network for conversion, you may want to select a NIC other than NIC0. Selecting another network may improve performance in busy pools. For more information about the management interface, see the XenCenter help.

#### **To add a network to XenServer:**

1. In the **Resource** pane in XenCenter, select the pool where you would like to run XenServer Conversion Manager.
2. Click the **Networking** tab.
3. Click **Add Network**.
4. On the **Select Type** page, select **External Network**, and click **Next**.
5. On the **Name** page, enter a meaningful name for the network (for example, "VMware network") and a description.
6. On the **Interface** page, specify the following:
  - **NIC.** The NIC that you want XenServer to use to create the network. Select the NIC that is plugged in to the physical or logical network of the VMware server.
  - **VLAN.** If the VMware network is a VLAN, enter the VLAN ID (or "tag").
  - **MTU.** If the VMware network uses jumbo frames, enter a value for the Maximum Transmission Unit (MTU) between 1500 and 9216. Otherwise, leave the MTU box at its default value of 1500.

#### **Note:**

Do not select the **Automatically add this network to new virtual machines** checkbox.

7. Click **Finish**.

### Meet storage requirements

Before you convert batches of VMware VMs, consider your storage requirements. Converted VM disks are stored on a XenServer storage repository.

This storage repository must be large enough to contain the virtual disks for all the converted VMs you want to run in that pool. For converted machines that only run on a standalone host, you can specify either local or shared storage as the location for the converted virtual disks. For converted machines running in pools, you can only specify shared storage.

#### To create a storage repository:

1. In the **Resource** pane in XenCenter, select the pool where you intend to run the XenServer Conversion Manager Virtual Appliance.
2. Click the **Storage** tab.
3. Click **New SR** and follow the instructions in the wizard. For more instructions, press **F1** to display the online help.

### XenServer requirements

You can run VMs converted with this release of XenServer Conversion Manager on the following versions of XenServer:

- XenServer 6.5 Service Pack 1
- XenServer 7.0
- XenServer 7.1
- XenServer 7.2
- XenServer 7.3
- XenServer 7.4
- XenServer 7.5

### VMware requirements

XenServer Conversion Manager can convert VMware VMs from the following versions of VMware:

- vCenter Server 5.5.0, 6.0.0, and 6.5.0
- vSphere 5.5.0, 6.0.0, and 6.5.0
- ESXi 5.5.0, 6.0.0, and 6.5.0

## Prepare to import the virtual appliance

Before importing the virtual appliance, note the following information and make the appropriate changes to your environment, as applicable.

## Download the virtual appliance

The XenServer Conversion Manager Virtual Appliance is packaged in an xva format. You can download the virtual appliance from the [XenServer 7.6 Enterprise Edition page]. When downloading the file, save it to a folder on your local hard drive (typically, but not necessarily, on the computer where XenCenter is installed). After the .xva file is on your hard drive, you can import it into XenCenter.

### Note:

XenServer Conversion Manager is available for XenServer Enterprise Edition customers or those who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, See [Licensing](#). To upgrade, or to buy a XenServer 7.6 license, visit the [Citrix website].

## Virtual appliance prerequisites

The XenServer Conversion Manager Virtual Appliance requires a minimum of:

- XenServer 6.5 Service Pack 1, XenServer 7.0, XenServer 7.1, XenServer 7.2, XenServer 7.3, XenServer 7.4, XenServer 7.5, XenServer 7.6
- Disk space: 30 GB of disk space
- Memory: 6.5 GB
- Virtual CPU allocation: 1 vCPU

## Import and configure the XenServer Conversion Manager virtual appliance

The XenServer Conversion Manager Virtual Appliance is a single pre-installed VM designed to run on a XenServer host. Before importing it, review the prerequisite information and considerations in the section called *Preparing to Import the Virtual Appliance*.

## Import the virtual appliance into XenServer

Import the XenServer Conversion Manager Virtual Appliance into the pool or host where you want to run the converted VMs. To import the XenServer Conversion Manager Virtual Appliance, use the XenCenter's **Import** wizard.

To import the virtual appliance into XenCenter:

1. Open XenCenter. Right-click on the pool (or host) into which you want to import the virtual appliance package, and select **Import**.
2. Browse to locate the virtual appliance package.
3. Select the pool or a *home server* where you want to run the XenServer Conversion Manager Virtual Appliance.

**Note:**

A home server is the host that provides the resources for a VM in a pool. While it can, a XenServer attempts to start the VM on that host, before trying other hosts. If you select a host, the XenServer Conversion Manager Virtual Appliance uses this host as its home server. If you select the pool, the virtual appliance automatically starts on the most suitable host in that pool.

4. Choose a storage repository on which to store the virtual disk for the XenServer Conversion Manager Virtual Appliance and then click **Import**. To add a storage repository to the pool, see the section called “Meeting Storage Requirements.” You can choose either local or shared storage.
5. Ensure the network to be used for conversion (the one that connects the VMware server to the XenServer host) is selected as the network associated with **interface 1** (“virtual NIC 1”).
  - If the correct network does not appear beside interface 1, use the list in the **Network** column to select a different network.
  - If you have not added the VMware network that is on a different physical network than the pool, do the following:
    - a) Exit the wizard.
    - b) Add the network to the pool.
    - c) Rerun the wizard.

For more information, see **To add a network to XenServer**.

**Warning:**

Do NOT configure NIC0 to your customer network. Assign NIC0 only to “Host internal management network.”

6. Leave the **Start VM(s) after import** check box enabled, and click **Finish** to import the virtual appliance.
7. After importing the .xva file, the XenServer Conversion Manager Virtual Appliance appears in the **Resources** pane in XenCenter.



## Configure the XenServer Conversion Manager virtual appliance

After you finish importing the XenServer Conversion Manager Virtual Appliance, you must configure it before you can use it to convert VMware VMs. Following the prompts in the XenCenter **Console** tab.

1. After importing the XenServer Conversion Manager Virtual Appliance, click the **Console** tab.
2. Enter **yes** to accept the terms of the license agreement. To decline the EULA, enter **no**.
3. Enter and confirm a new root password for the XenServer Conversion Manager Virtual Appliance. Citrix recommends selecting a strong password.
4. Enter a hostname for the XenServer Conversion Manager Virtual Appliance.
5. Enter the domain suffix for the virtual appliance. For example, if the fully qualified domain name (FQDN) for the virtual appliance is `citrix-migrate-vm.domain4.bedford4.ctx4`, then enter `domain4.bedford4.ctx4`.
6. Enter **y** to use DHCP to obtain the IP address automatically for the XenServer Conversion Manager Virtual Appliance. Otherwise, enter **n** and then enter a static IP address, subnet mask, and gateway for the VM.
7. Review the hostname and network setting and enter **y** when prompted. This step completes the XenServer Conversion Manager Virtual Appliance configuration process.
8. When you have successfully configured the appliance, a login prompt appears. Enter the login credentials and press Enter to log in to the XenServer Conversion Manager Virtual Appliance.

After you finish configuring the XenServer Conversion Manager Virtual Appliance, install XenServer Conversion Manager Console. For more information, see [Install the Conversion Manager console](#).

## Install the Conversion Manager console

After configuring the XenServer Conversion Manager virtual appliance, continue to install the XenServer Conversion Manager Console on your local workstation. The XenServer Conversion Manager Console is the user interface where you perform most conversion tasks. From the XenServer Conversion Manager Console, you can launch a conversion wizard that lets you select VMware VMs for conversion.

### Note:

XenServer Conversion Manager is available for XenServer Enterprise Edition customers or those who have access to XenServer through their Citrix Virtual Apps and Desktops entitlement. For more information about XenServer licensing, see [Licensing](#). To upgrade, or to buy a XenServer license, visit the [\[Citrix website\]](#).

## System requirements

### Supported guest operating systems:

XenServer Conversion Manager supports converting VMware VMs running any of the Windows guest operating systems that XenServer supports. For a list of Windows guest operating systems supported by XenServer, see [Guest operating system support](#). The following Linux operating systems are also supported.

- RHEL 5.4/5.6/6.4/7.0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 12.04/14.04/16.04

### Software requirements:

Microsoft .NET Framework 4.6

### Hard drive space required for installation:

10 MB

## Installation

The XenServer Conversion Manager Console is installed on the same computer where you run XenCenter.

### Important:

- Before installing the XenServer Conversion Manager Console, remove any other versions of the console from your computer.
- The XenServer Conversion Manager Console depends on the browser for proxy settings. If XenServer, ESXi and vCenter can only be reached through a proxy server, the details of the proxy server must be entered in the browser's proxy settings. If XenServer, ESXi and vCenter can be reached without a proxy server, and the user has set the browser's proxy to access the internet, then the addresses of XenServer, ESXi, and vCenter must be added in the proxy exception of the browser's proxy settings.

### To install the XenServer Conversion Manager Console:

1. Right-click **convui\_setup.exe**, and select **Run as administrator**.
2. On the **Welcome to the XenServer Conversion Manager Setup Wizard** page, click **Next**.
3. Review the license agreement and click **I Agree** to accept the terms of the agreement.

4. On the **Choose Install Location** page, choose where you want to install the XenServer Conversion Manager Console and click **Install**.

**Note:**

By default, the XenServer Conversion Manager Console is installed in **C:\Program Files (x86)\Citrix\XCM**.

5. Click **Finish**.

**To remove the XenServer Conversion Manager Console:**

1. Open the Windows Control Panel.
2. Open **Programs and Features**.
3. Select **XenServer Conversion Manager**.
4. Click **Uninstall**.

**Convert VMware VMs**

When you convert VMware VMs, they are imported into the XenServer pool or standalone host where you are running the XenServer Conversion Manager Virtual Appliance. Converted VMs retain their original VMware settings for virtual processor and virtual memory.

Using XenServer Conversion Manager to convert VMs requires the following tasks:

1. Starting the XenServer Conversion Manager Console.
2. Connecting to a XenServer host.
3. Starting the wizard to start new conversion job, which requires specifying VMware server credentials and selecting VMs and the storage repository.

**Notes:**

- XenServer Conversion Manager supports converting VMware VMs with different storage such as thin provisioning, thick provisioning, IDE, and SCSI.
- XenServer Conversion Manager does not require the source VMs to have VMware Tools installed. You can perform conversion on VMware VMs regardless of whether or not they have VMware Tools installed.

**Task 1: Start the XenServer Conversion Manager console****To start the XenServer Conversion Manager Console:**

1. From the Start menu, select **All Programs > Citrix > XenServer Conversion Manager**.

**Note:**

You can run only one instance of XenServer Conversion Manager per computer.

2. Continue on to **Connect to XenServer**.

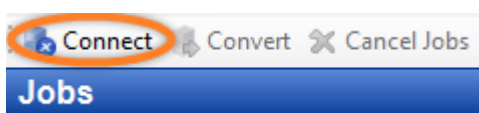
**Task 2: Connect to a XenServer host**

When you start the XenServer Conversion Manager Console, you must connect it to a XenServer host.

Before you begin, ensure that you have the credentials for the XenServer pool (or standalone host). Either the root account credentials or a Role-Based Access Control (RBAC) account with the Pool Admin role configured is acceptable.

**To connect to a XenServer host:**

1. If the **Connect to XenServer** dialog does not appear when you start the XenServer Conversion Manager console, click the **Connect** button in the toolbar.



2. In the **Connect to XenServer** dialog, enter the following details:
  - **Server.** Enter the IP address or Fully Qualified Domain Name (FQDN) for the XenServer host where you imported the XenServer Conversion Manager Virtual Appliance. To find the IP address, select the host in the XenCenter Resources pane, and click the **Search** tab.
  - **User name.** Enter the user name for a XenServer account for the pool (or standalone host). This account must be either the root account for the host or pool or have an RBAC role of Pool Admin. For detailed information about RBAC, see [RBAC overview](#).
  - **Password.** Enter the password for that account and click **Connect**.

After you successfully connect to the XenServer host, XenServer Conversion Manager displays the **Jobs** page.

**Task 3: Start a new conversion job**

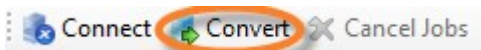
Before you start the conversion procedure, ensure that the following is true:

- You have the credentials for the VMware server containing the VMs you want to convert. The conversion procedure requires you connect the XenServer Conversion Manager Console to the VMware server.
- The VMware virtual machine to convert is powered off.

- The XenServer pool (or host) that run the converted VMs is connected to a storage repository. The storage repository must contain enough space for the converted virtual disks.
- XenServer pool (or host) has networks that the converted VMs use.

**To convert VMware VMs:**

1. Click the **Convert** button in the **Jobs** screen.

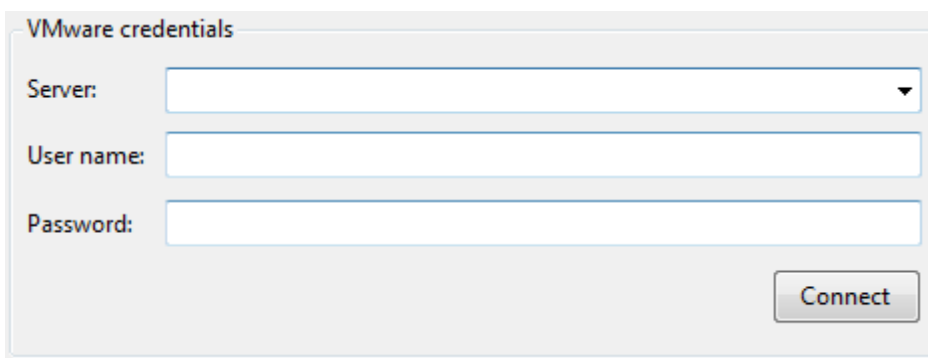


2. On the **Credentials** page, enter the following and then click **Connect**:

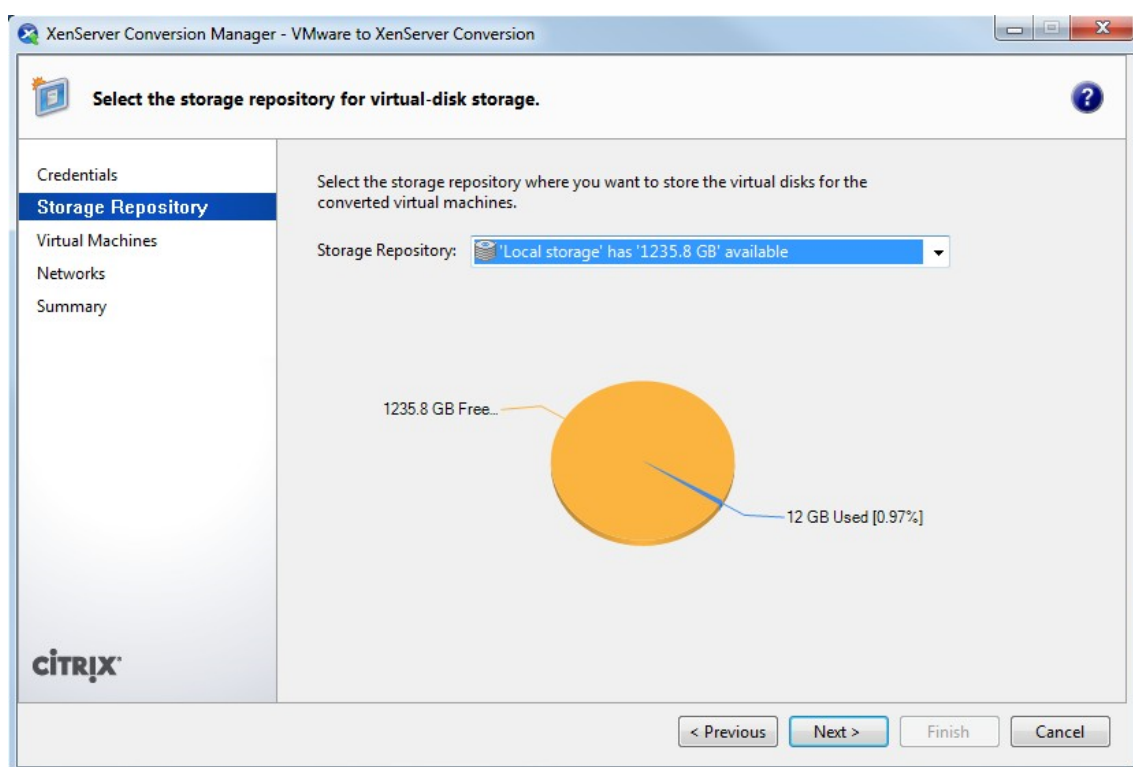
**Server.** Enter the IP address or FQDN for the VMware server that contains the VMs you want to convert to XenServer.

**User name.** Enter a valid user name for this VMware server. This account must either be a VMware admin account or have a Root role.

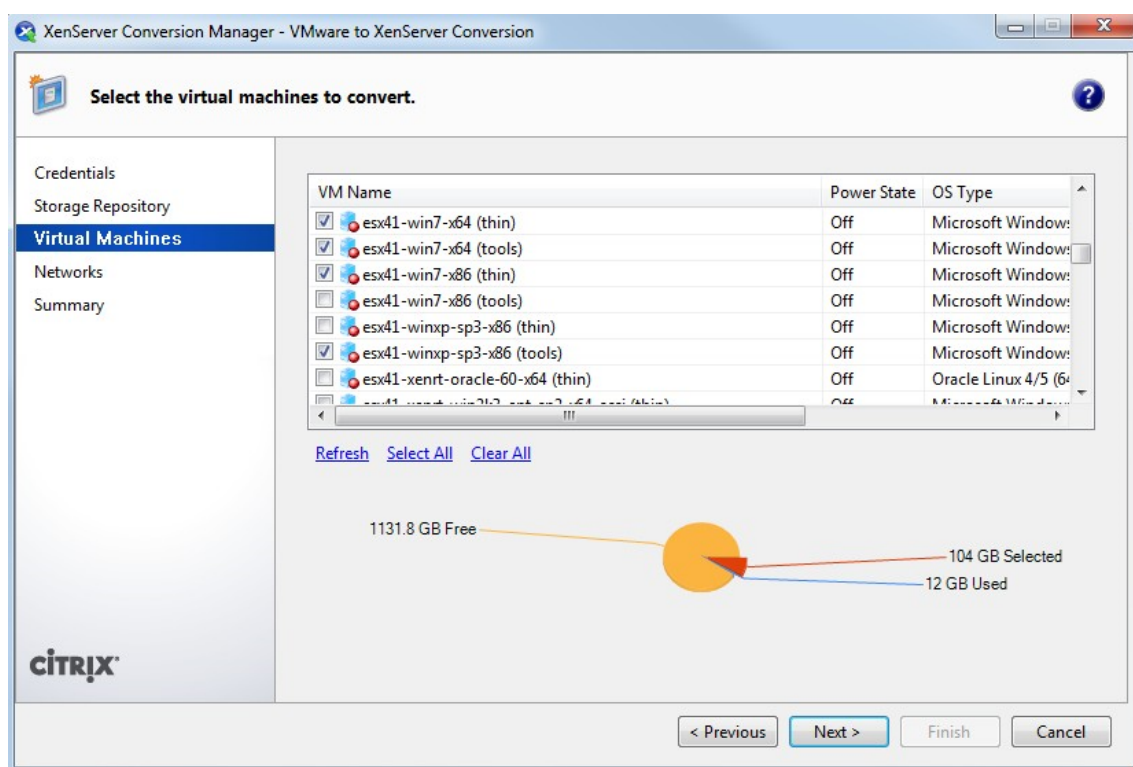
**Password.** Enter the password for the user account you specified in the **User name** box.

A screenshot of a 'VMware credentials' dialog box. It contains three input fields: 'Server:' (a dropdown menu), 'User name:' (a text box), and 'Password:' (a text box). A 'Connect' button is located at the bottom right of the dialog.

3. On the **Storage Repository** page, select the storage repository you want to use during conversion. This storage repository is where the VMs and the virtual disks that you are creating are stored permanently.



4. On the **Virtual Machines** page, select the VMware VMs you want to convert, and click **Next**.



As you select VMs to convert, the red-pie wedge increases to indicate what proportion of available storage for the converted VM's virtual disks to consume.

During conversion, XenServer Conversion Manager downloads and installs updated kernels for Linux VMs that are not updated. If there is no access to the Internet, XenServer Conversion Manager installs the kernel from the following location of the XenServer Conversion Manager appliance.

```
1 /opt/vpxxcm/conversion/linuxv2v/\${
2 distro }
3 /
```

The following table lists the kernel versions for the various Linux operating systems supported during conversion.

| Operating System | 32-bit/64-bit | Recommended Kernel Version Number                   |
|------------------|---------------|-----------------------------------------------------|
| CentOS 5.5       | 32-bit        | 2.6.18-412(kernel-Xen)                              |
| CentOS 6.3       | 32-bit        | 2.6.32-642                                          |
| CentOS 6.4       | 32-bit        | 2.6.32-642                                          |
| CentOS 6.5       | 32-bit        | 2.6.32-642                                          |
| RHEL 5.4         | 32-bit        | 2.6.18-164                                          |
| RHEL 5.6         | 32-bit        | 2.6.18-412                                          |
| RHEL 6.4         | 32-bit        | 2.6.32-642                                          |
| SLES 11 SP3      | 32-bit        | 3.0.76-0                                            |
| SLES 11 SP4      | 32-bit        | 3.0.101-63                                          |
| Ubuntu 12.04     | 32-bit        | Internet connection not needed to update Xen kernel |
| Ubuntu 14.04     | 32-bit        | Internet connection not needed to update Xen kernel |
| Ubuntu 16.04     | 32-bit        | Internet connection not needed to update Xen kernel |
| RHEL 5.4         | 64-bit        | 2.6.18-411                                          |
| RHEL 5.6         | 64-bit        | 2.6.18-411                                          |
| RHEL 6.4         | 64-bit        | 2.6.32-642                                          |
| RHEL 7.0         | 64-bit        | Internet connection not needed to update Xen kernel |
| CentOS 5.5       | 64-bit        | 2.6.18-412 (kernel-Xen)                             |
| CentOS 6.3       | 64-bit        | 2.6.32-642                                          |

| Operating System | 32-bit/64-bit | Recommended Kernel Version Number                   |
|------------------|---------------|-----------------------------------------------------|
| CentOS 6.4       | 64-bit        | 2.6.32-642                                          |
| CentOS 6.5       | 64-bit        | 2.6.32-642                                          |
| CentOS 7.0       | 64-bit        | Internet connection not needed to update Xen kernel |
| SLES 11 SP3      | 64-bit        | 3.0.76-0                                            |
| SLES 11 SP4      | 64-bit        | 3.0.101-59                                          |
| Ubuntu 12.04     | 64-bit        | Internet connection not needed to update Xen kernel |
| Ubuntu 14.04     | 64-bit        | Internet connection not needed to update Xen kernel |
| Ubuntu 16.04     | 64-bit        | Internet connection not needed to update Xen kernel |

5. *(Optional.)* On the **Networks** page, do one or more of the following tasks to specify how XenServer Conversion Manager converts the virtual network adapters in the VMs under conversion:

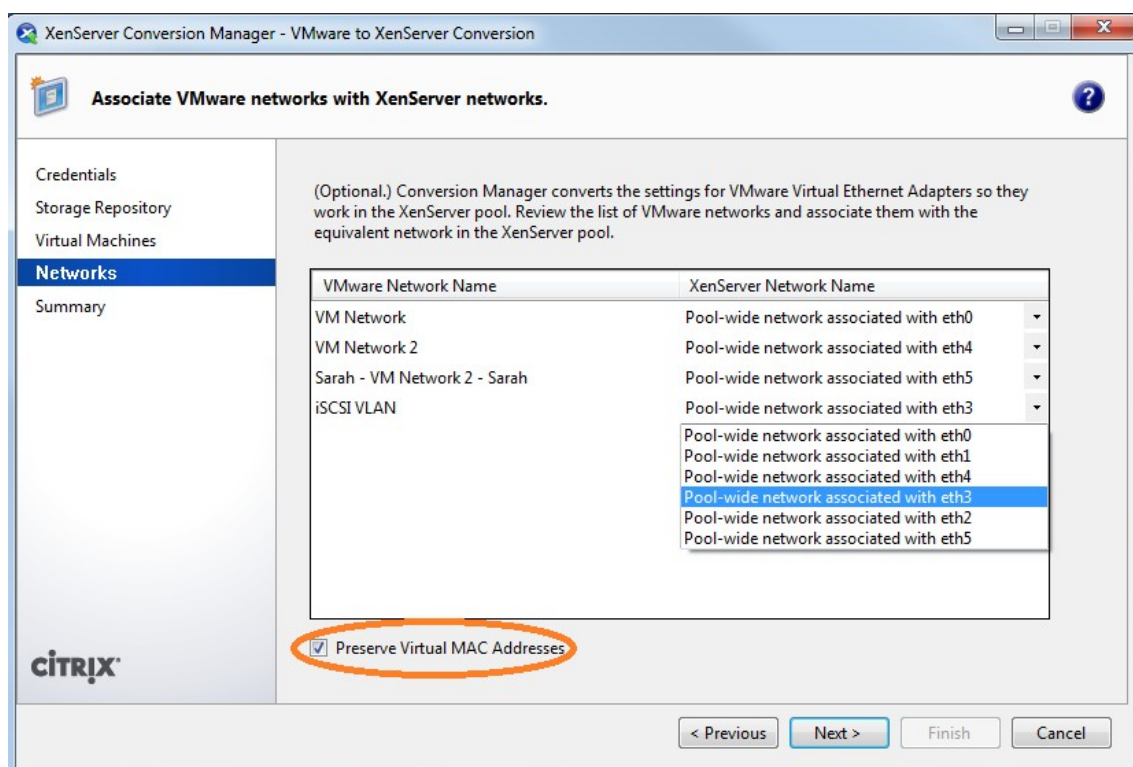
**Change any of the XenServer networks the VMware network adapters are mapped to.**

XenServer Conversion Manager detects the virtual network adapters on the VMs being converted and lets you associate those adapters with networks in XenServer. After conversion, the new VMs will have virtual network interfaces that connect to the XenServer networks you specified in this step.

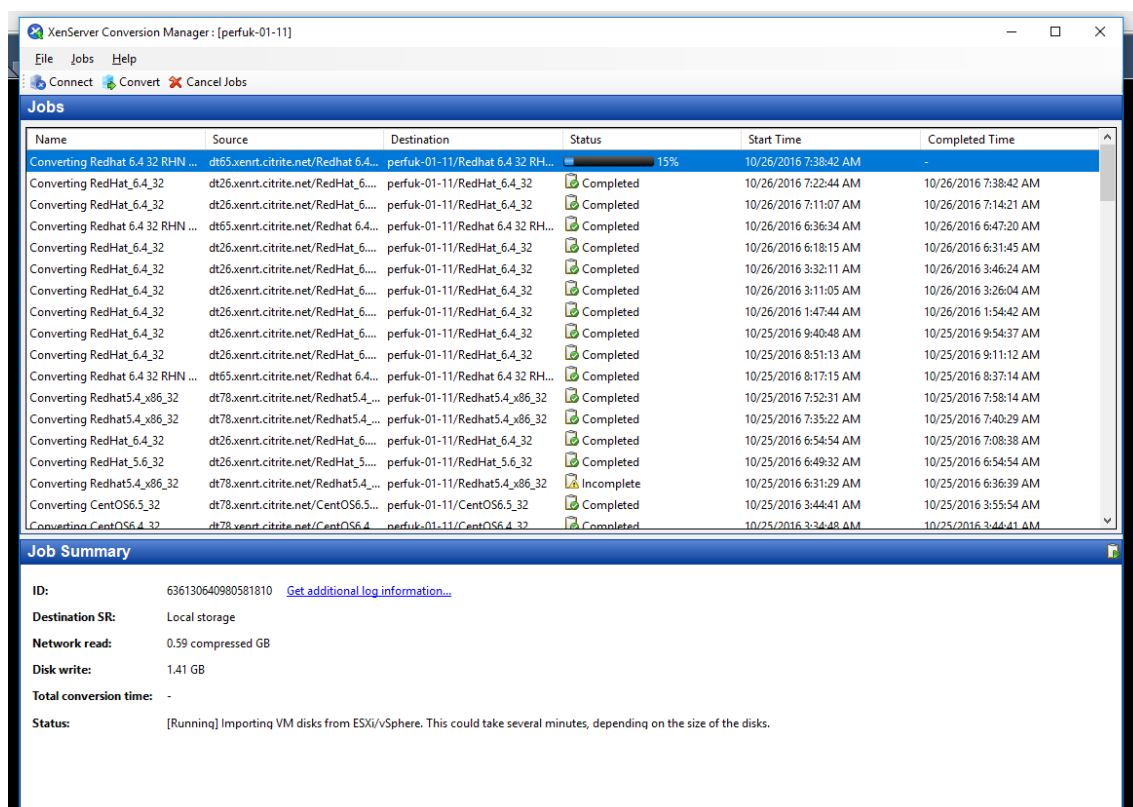
**Accept the default network mappings.** If you specified the VMware physical network or VLAN when you imported the XenServer Conversion Manager Virtual Appliance, you may want to leave the networks on this page at their default settings.

**Select the Preserve Virtual MAC Address check box.** XenServer can automatically generate virtual MAC addresses when you create or import VMs. However, you may want to preserve the virtual MAC addresses on your VMware VMs to preserve IP addresses in environments using DHCP. For more information, see the section **Preparing for the XenServer Conversion Manager Networking Requirements**.





6. On the Summary page, review the conversion details and click Finish. While the conversion is in progress, the status appears in the **Jobs** page.



**Note:**

Conversion from ESXi or vSphere can take several minutes depending on the size of the virtual disks.

**Task 4: Steps after conversion**

After conversion, open XenCenter and perform the following steps on your newly converted VMs:

**On Windows Machines:**

1. On Windows VMs, depending on your Microsoft licensing model, you may need to reactivate the VM's Windows license. This happens because the Windows operating system perceives the conversion as a hardware change.
2. On Windows VMs, install XenServer Tools to obtain high-speed I/O for enhanced disk and network performance. XenServer Tools also enable certain functions and features, including cleanly shutting down, rebooting, suspending, and live migrating VMs.

If you are working with a VM that does not have XenServer Tools installed, a Tools not installed message appears on the **General** tab in the Properties pane. For Windows VMs, you can double-click on this text to switch to the VM console, load the Tools ISO, and launch the Tools installation wizard.

**Note:**

XenServer Tools must be installed on each VM for the VM to have a fully supported configuration. Although VMs function without XenServer Tools, their performance can be impacted.

**Enable VNC On Linux machines**

On Linux VMs, perform the following steps to configure the VNC server.

**Note:**

VNC password must have at least six characters.

**For CentOS 5.5 and RHEL 5.4/5.6**

1. Customize RHEL-based VMs firewall to open the VNC port using the following command:

```
1 \> 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:

```
1 \>service iptables stop
```

3. For CentOS 5.5 and RHEL 5.4/5.6, if the VNC graphic console does not display properly, run:

```
1 init 5
```

Then check if the graphic console displays properly.

#### **For CentOS 6.3/6.4/6.5 and RHEL 6.4**

1. Set the VNC password

```
1 \>vncpasswd
```

2. Start the VNC server

```
1 \>service vncserver start
```

3. For firewall settings, open the file /etc/sysconfig/iptables and add the following line:

```
1 -A INPUT -m state \--state NEW -m tcp -p tcp \--dport 5900 -j
ACCEPT
```

#### **Note:**

Add the above line after:

```
1 -A INPUT -j REJECT \--reject-with icmp-host-prohibited:
```

4. Enter the following command to restart iptables:

```
1 \>service iptables restart
```

#### **For SLES Linux Enterprise Server 11 SP3 to SP4**

1. Set the VNC password in startup console.

```
1 \>vncpasswd
```

#### **Note:**

```
Would you like to enter a view-only password(y/n)? n
```

2. Configure the fire wall settings as follows:

- A. Open a text console on the VM and run the YaST utility:

```
1 \>yast
```

B. Use the arrow keys to select **Security and Users** in the left menu, then tab to the right menu and use the arrow keys to select **Firewall**. Press **Enter**.

C. In the **Firewall** screen, use the arrow keys to select **Custom Rules** in the left menu and then press **Enter**.

D. Tab to the **Add** button in the **Custom Allowed Rules** section and then press **Enter**.

E. In the **Source Network** field, enter **0/0**. Tab to the **Destination Port** field and enter **5900**.

F. Tab to the **Add** button and then press **Enter**.

g. Tab to the **Next** button and press **Enter**. In the **Summary** screen, Tab to the **Finish** button and press **Enter**. Finally, on the top-level YaST screen, Tab to the **Quit** button and press **Enter**.

3. Click **Switch to Graphical Console**.

4. If the Graphical Console does not display correctly, switch to **Text Console** and run command:

```
1 /etc/init.d/vncserver restart.
```

5. Click **Switch to Graphical Console**.

#### Notes:

- For other graphical console display issues, run: `/etc/init.d/vncserver restart.`
- Conversion of VMs with IDE disks are not supported for SLES 11 SP3 to SP4.

### For Ubuntu 12.04

1. Set the VNC password and log on.

### Other conversion tasks

This section lists other tasks you may want to perform when converting VMs. These tasks include clearing jobs, saving a summary of jobs, retrying jobs, canceling jobs, and displaying the log file.

#### To clear all jobs

From the **Jobs** menu, select **Clear Jobs**.

#### To save a summary of jobs

From the **File** menu, click **Save Job Summary**.

### To retry a job

Click **Retry jobs**.

**Note:**

The **Retry jobs** option is only enabled for failed or canceled jobs.

### To cancel a job

Click **Cancel jobs**.

**Note:**

Cancel jobs is only enabled for queued or running jobs.

### To save the XenServer Conversion Manager application log file

1. From the **Help** menu, select **Save Support Log Files**.
2. When prompted, specify where you want to store the log files for XenServer Conversion Manager Console ([XCMUI . log](#)) and XenServer Conversion Manager Virtual Appliance ([XCM . log](#)) logs.

### To display conversion details

1. Select the job in the XenServer Conversion Manager **Jobs** window.
2. In the **Job Summary** pane, click the **Get additional log information** link.

XenServer Conversion Manager Console retrieves the log from the XenServer Conversion Manager Virtual Appliance and displays the result in a text editor.

### To get log details

Logs for both Windows and Linux guests are present in the `/var/log/conversion/convsvc.log` file. If conversion fails, click the **Get additional log information** button for details. For Linux VMs, additional logs are present in `/var/log/conversion/linuxxenfix.log`.

## Troubleshoot conversion

This section provides information about troubleshooting the conversion process and converted VMs.

## Problems starting a converted VM

In general, conversion runs smoothly and XenServer Conversion Manager converts VMs without any issues. However, in some rare cases, you may receive errors when attempting to open converted VMs. The following sections provide some guidance on resolving errors and other issues.

### Blue screen with Windows STOP code 0x0000007B

This stop code indicates that XenServer Conversion Manager was unable to configure a Windows device that is critical to boot in XenServer for the first time. Save the logs and send them to Citrix Technical Support for further guidance.

### Windows product activation

Depending on your licensing model, an error message on system activation may appear when you attempt to start a Windows VM.

#### Note:

Conversion from ESXi or vSphere can take several minutes depending on the size of the virtual disks.

### Lost network settings in a Windows VM

If you import a Windows VM from an ESXi server to XenServer, the IPv4/IPv6 network settings can be lost. To retain the network settings, reconfigure the IPv4/IPv6 settings after completing the conversion.

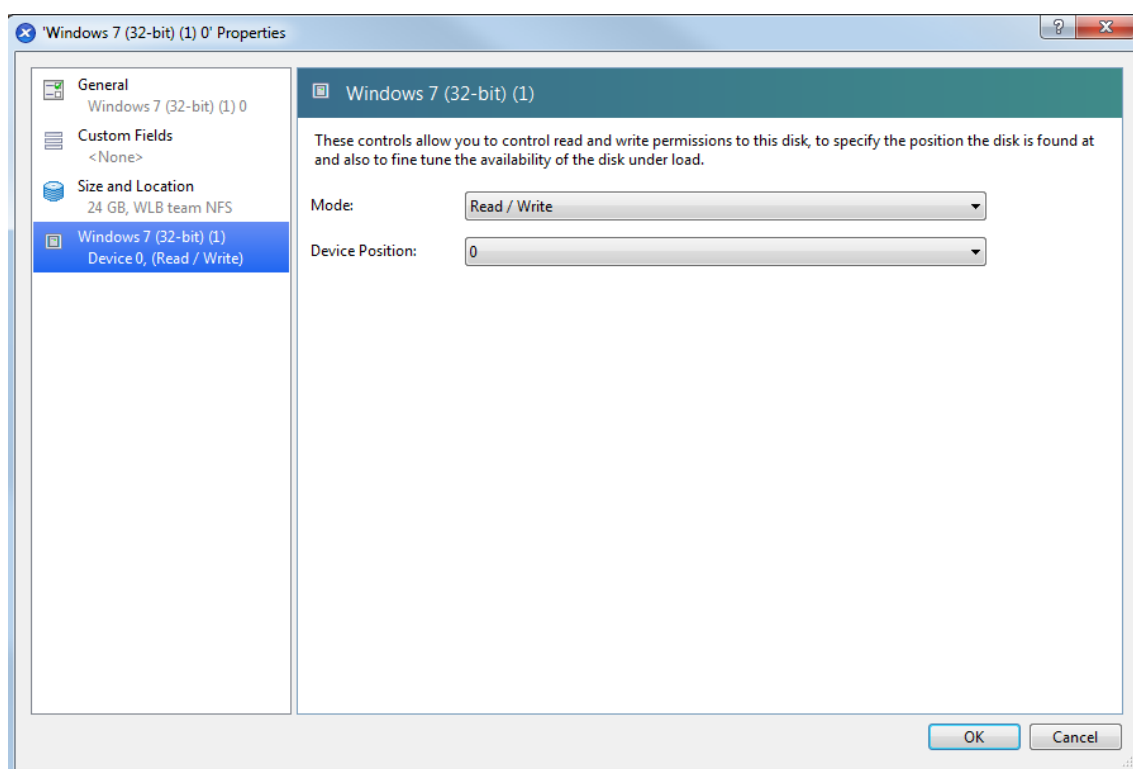
### Unable to start VMware SCSI disk

If a VMware VM boots from a SCSI disk but also has one or more IDE hard disks configured, the VM may not boot when you convert it to XenServer. This is because the migration process assigns the IDE hard disks lower device numbers than SCSI disks. However, XenServer boots from the hard disk assigned to device 0. To resolve this issue, rearrange the virtual disk position in XenCenter so that the VM reboots from the virtual disk that contains the operating system.

#### To change the position of the virtual disk containing the operating system:

1. In the XenCenter Resources pane, select the powered off guest VM.
2. Select the **Storage** tab.
3. On the **Virtual Disks** page, select the virtual disk containing the operating system and then click **Properties**.

4. In the **<operatingsystem> Properties** dialog, click the **<operatingsystem>** tab to display device options.



5. From the **Device Position** list, select **0** and Click **OK**.

## Problems during conversion

If you see any errors when converting Linux VMs, remove the converted VM, restart the XenServer Conversion Manager virtual appliance and retry. Logs of failed conversions are stored in **/var/log/x-ensource.log**. When you contact Citrix support to raise any issues, we recommend that you provide the log file for troubleshooting.

## vSwitch and Controller

September 5, 2018

The vSwitch brings visibility, security, and control to XenServer virtualized network environments. It consists of the following components:

- The *vSwitch*, a virtualization-aware switch running on each XenServer
- The *vSwitch Controller*, a centralized server that manages and coordinates the behavior of each individual vSwitch to provide the appearance of a single vSwitch

The vSwitch Controller supports fine-grained security policies to control the flow of traffic sent to and from a VM. It provides a detailed view of the behavior and performance for all traffic in the virtual network environment. A vSwitch greatly simplifies IT administration within your environment. When using vSwitch, VM configuration and statistics stay bound to a VM even when it migrates from one physical host to another.

## Get started

### Requirements

- At least one XenServer resource pool configured in XenCenter
- Sufficient capacity within that pool to deploy the vSwitch Controller virtual appliance

The requirements for the host that runs the controller are described in the next section.

### Process

Setting up the vSwitch Controller involves the following tasks:

1. Deploy the vSwitch Controller Virtual Appliance
2. Access the vSwitch Controller
3. Configure the vSwitch Controller IP address
4. Add resource pools
5. Configure high availability (optional)

#### Note:

This version of vSwitch Controller interoperates with all supported versions of XenServer.

## Deploy the vSwitch Controller virtual appliance

The XenServer host that runs the vSwitch Controller must meet the following minimum requirements:

- 2 CPUs
- 2 GB DRAM
- 16 GB Disk

The minimum allowed VM configuration for the vSwitch Controller appliance and the default configuration on import is:

- 2 vCPUs
- 2 GB DRAM
- 16 GB Disk



This configuration supports pools of up to 16 XenServer hosts and 256 Virtual Interfaces (VIFs) connected to the vSwitch Controller. For larger pools (up to the maximum supported limit of 64 XenServer hosts in total for all pools and 1024 VIFs), modify the VM configuration to:

- 4 vCPUs
- 4 GB DRAM
- 16 GB Disk

**Note:**

- If the appliance's disk is stored on a network storage, and is controlling the underlying XenServer host's network traffic, deadlock can happen in loaded situations, and the entire pool's network traffic can get stalled. To prevent this, Citrix strongly recommends customers to store the DVSC disk on a local storage or move the appliance into another pool which is not controlled by that DVSC.
- For each pool, you must restrict the pool size to 16 hosts or less.

The vSwitch Controller VM can run within a resource pool that it manages. Generally, this configuration runs as if the vSwitch Controller VM was running separately. However, it might take slightly longer (up to two minutes) to connect all the vSwitches when a Controller migration or restart occurs. This time is because of differences in how the individual vSwitches route control connections.

To install the vSwitch Controller, import the supplied virtual appliance VM image into a XenServer resource pool. During import, attach the VIF of the imported VM to a network through which you can reach the host or pool that you want to control.

After the VM has been imported, start it to begin the process of configuring the DVS.

## **Access the vSwitch Controller command-line interface**

You can access the vSwitch Controller command line interface (CLI) from within XenCenter or remotely using an SSH client. When the vSwitch Controller VM first boots, the console within XenCenter displays the IP address to use to access the controller remotely. If the VM did not receive an IP address, the text console indicates that an address must be assigned through the CLI. In either case, the text console displays a login prompt to log into the CLI locally in the XenCenter console. Full documentation of the available CLI commands is included in [command line interface](#).

## **Access the vSwitch Controller GUI**

Access the vSwitch Controller GUI remotely using a web browser or locally within the XenCenter console.

When the vSwitch Controller VM boots, the console within XenCenter displays the IP address to use to access the GUI remotely. If the VM did not receive an IP address, the GUI cannot be used locally or

remotely until one is assigned. The console provides instructions on setting the IP address locally in the command line interface. After the controller VM has the IP address, you can access the GUI locally within the XenCenter console.

**Note:**

If VNC is disabled, vSwitch Controller GUI can be accessed only from a web browser.

**Access the vSwitch Controller GUI remotely**

To access the vSwitch Controller interface remotely:

1. Open a browser and type the following URL, where *server* is the IP address or host name of the interface of the controller VM: <https://server-name:443/>
2. Type your user name and password, and click **Login**. The default administrator user name and password are **admin** and **admin**.

**Note:**

By default, the vSwitch Controller webserver uses a self-signed certificate. The certificate can cause browsers to show a security error when they connect to the GUI. You can safely ignore the error and install the certificate into your browser.

The following browsers are supported: Firefox 3.x, Safari 4.x, Internet Explorer 7 and 8. Other modern browsers with similar features (for example, Opera or Google Chrome) are not supported, but might work. Internet Explorer 9 addresses known memory and resource leak issues. However it has not received full testing.

When you log in for the first time, the system prompts you to change the default administrator password. It is important that you create a strong administrator password to protect the security of environment.

**Configure the vSwitch Controller IP address**

When the vSwitch Controller is started for the first time, it attempts to obtain an IP address using DHCP. However, we recommend that you assign a static IP address. If DHCP is configured, resource pools cannot be set to Fail-Safe mode

To assign a static IP address:

1. Access the vSwitch Controller interface locally.
2. Select the **Settings** tab and then **IP Configuration** in the side panel. The current settings are shown.
3. Select **Modify Configuration**, specify the new IP address information, and select **Make Changes**.

**Note:**

If DHCP is configured, resource pools cannot be set to Fail-Safe Mode.

## Add resource pools

Adding a resource pool allows the vSwitch Controller to begin managing all XenServer hosts in that pool automatically.

**To add a resource pool:**

1. Under **Visibility & Control**, open the **Status** tab and choose **All Resource Pools** in the resource tree to open the **Status** page for all resource pools.
2. Click **Add Resource Pool**. If you do not have the correct license to add another resource pool, an error message is displayed.
3. Type the IP address or DNS name of the master XenServer host in the **Pool Master Server (DNS/IP)** box.
4. Type the user name and password for administrative access to the server.

The user must have full management capabilities in the resource pool. The vSwitch Controller cannot properly manage the pool when the account has restricted capabilities.

Typically, this account is the user named `root`, but can be a different name when the RBAC features of the XenServer platform are in use.

5. Choose the **Steal** check box only when you want to override any existing vSwitch Controller configuration for this resource pool.
6. Click **Connect**.

The vSwitch Controller uses the provided user name and password to communicate with the pool master server using the XAPI protocol. When communications are established, the new resource pool is added to the resource tree, along with all of the associated resources. If the vSwitch Controller VM is unable to communicate with the pool master, it displays an error message describing the failure.

**Note:**

For the vSwitch Controller to communicate with the XenServer resource pool, the XenServer resource pool must use **Backwards compatibility mode**. This mode is the default. You can specify this setting on the **Pool Properties** page in XenCenter. For more information, see the *XenCenter Help*.

## Configure high availability

To ensure that XenServer hosts can always reach an active vSwitch Controller, use Citrix high availability for the vSwitch Controller VM. For more information about enabling high availability on XenServer, see [High Availability](#). Continuous operation of the vSwitch Controller is critical to the operation of networking for all VMs. To ensure high availability of the vSwitch Controller VM, set its `restart-priority` to 1 and `ha-always-run` to true.

## Manage vSwitch

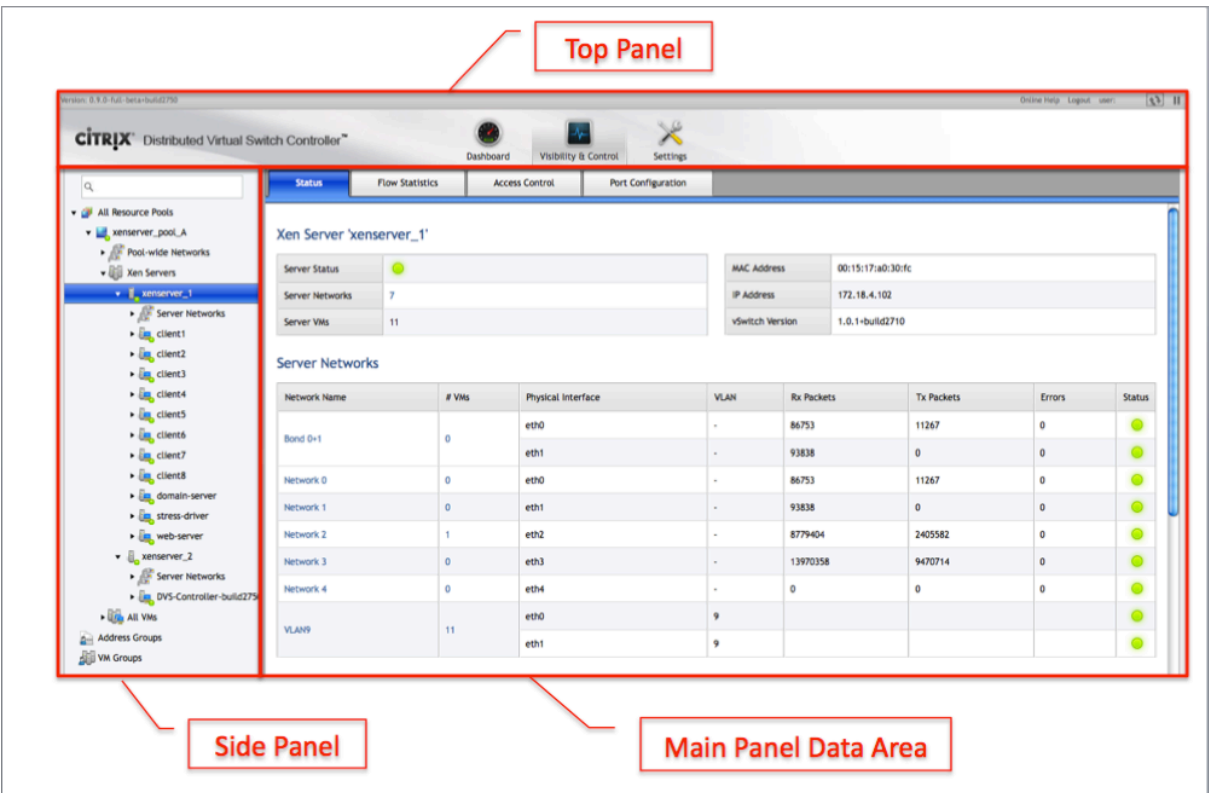
January 14, 2019

The vSwitch Controller GUI enables you to perform various management tasks, including:

- View status and flow statistics for elements within the virtual network
- Set up VM access control, Quality of Service, and traffic mirroring policies
- Modify configuration of the vSwitch Controller virtual appliance

## Interface overview

The vSwitch Controller GUI has three different panels. These panels are shown in the next figure.



## Top panel

The top panel is always visible when using the GUI and includes a status bar and a set of main navigation icons.

## Status bar

The gray status bar at the top of the vSwitch Controller window contains the following information and functions (left to right):

- Version: Current vSwitch Controller version.
- Online Help: Click to display or close an online help area near the top of the controller window.
- Logout: Click to log out of the vSwitch Controller GUI.
- User: Displays the user name of the user that is currently logged in.
- Refresh icon: Click to update the information on the page.
- Play/Pause: Click to toggle whether the GUI automatically refreshes data on the screen using background updates. In play mode, the data that is shown refreshes automatically every 15 seconds. In pause mode, most data is not updated. However, a few elements are updated, notably the resource tree. The status bar background behind the buttons turns orange and a “Data Updates Paused” indicator appears in the status bar when in pause mode.

## Top icons

Click the top icons to access the major functional areas within the GUI.

- Dashboard: View summary statistics and information about network and administrative events. See Monitor network status with the dashboard.
- Visibility and Control: View network status and statistics or configure access control, QoS, and traffic mirroring policies for virtual networks. See [Virtual network visibility and control](#).
- Settings: Perform vSwitch Controller maintenance and administrative functions. See [Administer and maintain the vSwitch Controller](#).

## Side panel

The side panel is available only in the Visibility and Control and Settings section.

For the Visibility and Control section, the side panel contains a resource tree that you can use to browse network elements within the virtual network environment. Similar to the resource tree in XenCenter, elements are organized hierarchically and provide an easy way to browse elements within the system. To expand a section of the resource tree, click the side-facing arrow next to the node text. An expanded node is marked with a down-facing arrow, which you can click to collapse.

When you select an element from the resource tree, the main panel displays status and configuration data for that node in the tree. For example, if you select a VM from the resource tree and choose **Status** in the **Visibility and Control** section, the main panel displays status information about the selected VM.

The resource tree includes a search function. To filter the contents based on a search string, enter text in the search field, and press **Enter**. Click the **X** symbol to clear the search. Searches support wildcards (\* for one or more characters and ? for a single character). If wildcards are not used, the system performs a substring search as if a \* wildcard is at the start and end of the search string. For example, the search “Lab” finds all items with “Lab” in the name, such as “Laboratory-1” and “New-Lab-5.”

For the Settings section, the side panel contains icons to select which area of vSwitch Controller configuration the user would like to view or modify

### Use the resource tree

At the highest level, the resource tree displays the following items:

- All Resource Pools: List of all the available resource pools. This list is the top-level resource for exploring all XenServer hosts, Networks, VMs, and VIFs that are part of each resource pool.
- Address Groups: Named sets of IP addresses and subnet ranges. These groups are used for the following purposes:
  - To limit the application of a rule in the access control section
  - To limit the scope of a query in the **Flow Statistics** section
- VM Groups: Named sets of VMs to be used to simplify viewing the status and flow statistics of a particular collection of VMs.

When you expand a resource pool in the resource tree, the following items are displayed:

- Pool-wide networks: This list includes all networks in the resource pool and is similar to the list in the Network tab of XenCenter. You can expand the list to show the individual networks, expand a network to show the VMs on that network, and expand a VM to show its VIFs on that network.
- XenServer hosts. This list is similar to the server hierarchy in XenCenter. You can expand the list to show all of the servers in the pool and expand a single server entry to show the networks, VMs, and VIFs associated with the server. The Server Networks listing is similar to what you see if you click a server in XenCenter and choose the Network tab.
- All VMs: This list shows all VMs in the resource pool, whether or not they are configured for a single server. You can expand the list to show the individual VMs, and expand a VM to show its VIFs.

Right-click context menus on nodes are available on most nodes to provide a simple way of adding, modifying, and deleting items in the resource tree.

### Color-coded icons

Color-coded icons in the resource tree show the state of tree nodes under the top-level “All Resource Pools” node. Similar to XenCenter, these color codes are based on data retrieved via XAPI from each pool master. When a node state changes, the icon is updated as follows:

- Green: A green icon indicates that the resource is active on the network and properly managed by the vSwitch Controller.
- Red: For a Resource Pool node, the red indicates that a XAPI connection can't be established to the pool master. If the Resource Pool node is green, a red icon for any node below it indicates that the element is not currently active on the network. For example, the element is powered off or disconnected.
- Orange: An orange icon indicates that the node, or one of its descendants, is not properly connected or managed. The status page for the associated resource displays an error message describing the problem.

The color codes on the tree menu items are also displayed on the Status page for the node. For detailed information on the color codes and status information, see [Troubleshoot vSwitch Controller issues](#).

### Main panel data area

The main panel data area contains status information, statistics, and configuration settings.

- Dashboard: There is no side menu and the main panel data area takes up the full area below the top panel. The dashboard main panel provides an overview of all virtual networks managed by the vSwitch Controller.
- Visibility and Control: The main panel takes up the right side of the window below the top panel. The panel includes tabs at the top that correspond to the following major visibility and control functions:
  - Status: View detailed status information for the selected resource tree node.
  - Flow Statistics: View a graph and data on network activity for the selected node.
  - Access Control: Set up access control policies for the selected node.
  - Port Configuration: Set up Quality of Service and traffic mirroring policies for the selected node.
- Settings: The main panel takes up the right side of the window below the top panel. The setting main panel displays details for viewing or configuring vSwitch Controller settings based on the subsection selected in the side panel.

Within the Visibility and Control section, the data displayed in the main panel changes to reflect the hierarchy level and the specific item that you selected in the side panel.

For example, if you select a resource pool in the side panel and click the Access Control tab, the main panel displays the following:

- The global access control security policy
- The policy for the selected resource pool

If you select a virtual interface (VIF) from the side panel and click the Access Control tab, the main panel displays:

- The global access control security policy
- The policy for the resource pool that contains the VIF
- The policy for the VM that contains the VIF
- The policy for the selected VIF

## **Monitor network status with the dashboard**

The dashboard presents summary statistics and information about events within the virtual network environment. To display the dashboard, click the **Dashboard** icon at the top of the vSwitch Controller interface.

The dashboard is divided into the areas described in this section. The information is automatically updated every few seconds.

### **Server statistics**

This section presents the following general information about the vSwitch Controller.

- Up Time: Length of time since the vSwitch Controller was last started.
- CPU Load: Current percent of CPU utilization for the vSwitch Controller virtual appliance.

### **Network statistics**

This section shows an inventory of network elements (resource pools, XenServer hosts, networks, and VMs) For each of the following categories:

- Managed: Number of elements of this type that are in a running state according to XAPI and currently managed by the vSwitch Controller.
- Active: Number of elements of this type that are in a running state according to XAPI. Includes managed and unmanaged elements.
- Total: Number of elements of this type (active or not) that are known to exist via XAPI.



When the system is configured and operating correctly, the managed and active counts are the same. The total count is always equal to or greater than the managed and active count. Components that are powered off are not shown as managed by the controller.

### **Recent network events**

This section lists the most recent events that have occurred within the managed virtual networks since the vSwitch Controller was last restarted. Use the scroll bar on the right to scroll through the list. The most recent event is listed first. Over time, older events are deleted from the list.

The following information is reported for each network event:

- **Priority:** Relative importance of the event.
- **Date/Time:** Date and time that the event occurred.
- **Event:** Description of the event. You can click hyperlinks in an event description to access the corresponding Visibility and Control Status pages of network elements mentioned in the event.

Network events can be exported to a syslog server for a more permanent record. For more information, see [Export syslog files](#).

### **Recent administrative events**

This section lists events that have occurred within the vSwitch Controller, often as a result of an administrator changing configuration within the GUI. Use the scroll bar on the right to scroll through the list. The most recent event is listed first. Over time, older events are deleted from the list.

The following information is reported for each administrative event:

- **Priority:** Relative importance of the event.
- **Date/Time:** Date and time that the event occurred.
- **Event:** Description of the event. You can click hyperlinks in an event description to access the Visibility and Control Status pages of network elements mentioned in the event.

Network events can be exported to a syslog server for a more permanent record. For more information, see [Export syslog files](#).

### **Throughput, flows, and bit-rate graphs**

These graphs display information about the behavior of the most active VMs and protocols.

The graphs display the following information:

- Aggregate Throughput (bits/sec) for the last hour
- Aggregate Packet Rate (packets/sec) for the last hour
- Aggregate Connection Rate (flows/sec) for the last hour

## Virtual network visibility and control

September 6, 2018

The Visibility and Control section allows you to monitor network behavior and configure network policy. To access the pages, select the **Visibility and Control** icon at the top of the vSwitch Controller interface.

### View status

The **Status** tab provides detailed information in table form about the node that is selected in the resource tree. The type of information that is presented varies according to the selected node. Most individual table entries are links. You can click these links to display the status page that applies to that table entry.

All byte counts and error counts continue to accumulate even when a XenServer host restarts or a VM restarts or migrates. The color codes follow the same rules as the color codes in the side panel. See [Color-coded icons](#).

### Global level

At the global level, the Status page presents a table listing all resources pools with the following information:

- Resource pool: Name of the resource pool.
- # Servers: Number of servers in the pool.
- # Networks: Number of networks in the pool.
- # VMs: Number of VMs in the pool.
- Status: Color-coded icon that shows the current pool status.

Clicking the gear icon on the right side of a row provides options for modifying the resource pool.

On this page, you can also specify available target VLANs for port configuration policies. See [Set up port configuration policies](#).

### Resource pool level

For a selected resource pool, the Status page presents the following information:

- Status: Color-coded icon that shows the current pool status.
- Pool Master: IP address or DNS name of the master server in the pool.
- Pool-Wide Networks: Number of networks in the pool.
- XenServer: Number of servers in the pool.

- All VMs: Number of VMs in the pool.
- Server list: List of servers in the pool, including server name, number of networks, number of VMs, and status.

In addition to displaying status information, you can configure how the XenServer hosts in the pool forward Netflow data. Select the following check boxes as appropriate, and click **Save Netflow Configuration**:

- vSwitch Controller (selected by default): Forwards Netflow information to the vSwitch Controller for use by the Flow Statistics section of the GUI. If you deselect this check box, the Netflow data is not sent to the vSwitch Controller and the Flow Statistics pages do not show data.
- External Netflow Controller: Allows you to forward Netflow data to an external third party Netflow collector. Enter the IP address of the external collector.

### **Fail-safe mode**

Use the **Fail Mode** section to configure how a vSwitch enforces the access control rules when it can't connect to its vSwitch Controller. It is important to maintain a high level of vSwitch Controller availability to avoid data loss. During times when the vSwitch Controller is not available, the following fail modes apply:

- Fail-open: all traffic is allowed, previously defined ACLs no longer apply until the vSwitch is able to reconnect with the vSwitch Controller.
- Fail-safe: existing ACLs continue to apply.

Under normal operation, the vSwitch maintains connections to its configured vSwitch Controller to exchange network management and status information. If the vSwitch Controller becomes unavailable, the vSwitch waits up to an inactivity timeout during which network traffic is dropped. After the inactivity timeout, the vSwitch enters into the configured fail mode.

In fail-safe mode, existing ACLs continue to apply after the vSwitch loses the connection to its configured vSwitch Controller. Traffic that does not match existing ACLs are denied. All ACLs, at any level of the policy hierarchy presented by the Controller, are enforced as sets of rules on VIFs in the vSwitch. As a result, new VIFs that appear in fail-safe mode while the Controller is unavailable cannot communicate until the Controller becomes available again. Existing VIFs that are unplugged then replugged have the same behavior as new VIFs. This situation occurs even if higher-level ACL policy rules (global, per-resource pool, per-network, or per-VM) that allow communication are present on existing VIFs. Furthermore, the vSwitch Controller can define ACLs based on IP addresses it has learned. In fail-safe mode, packets sent by a VM using an IP address the Controller has not associated with the VM before it became unavailable are denied. For example, an existing VM that uses a new IP address cannot communicate until the Controller is reachable again. Other examples where traffic is denied while in fail-safe mode include:

- Newly plugged VIFs

- A new VM
- A migrated VM (for example XenMotion or Workload Balancing)
- VMs on hosts added to a pool
- Applications that act like a router

If the vSwitch restarts in fail-safe mode and the controller is still unavailable after the vSwitch starts, all ACLs are lost and all traffic is denied. The vSwitch stays in fail-safe mode until a connection with the Controller is re-established and ACLs are pushed down to the vSwitch by the Controller.

**Warning:**

Removing a resource pool from vSwitch Controller management while in fail-safe mode can result in the vSwitch losing network connectivity and forcing an emergency reset situation. To prevent this situation, only remove a resource pool while its status is green.

You can also specify available target VLANs for port configuration policies on this page. For more information, see [Set up port configuration policies](#).

**Server level**

For a selected server, the Status page presents the following information:

- **Server Status:** Color-coded icon that shows the current server status.
- **Server Networks:** Number of networks in the resource pool.
- **MAC Address:** MAC address of the server management interface.
- **IP Address:** IP address of the server management interface.
- **vSwitch Version:** Build and version number of the vSwitch running on this XenServer.
- **Server Networks:** List of all networks associated with the server. This information includes:
  - The number of VMs on the server using that network
  - The associated physical interface,
  - The VLAN
  - The number of bytes transmitted and received
  - The number of errors
  - The status
- **Server VMs:** List of all VMs associated with the server. For each VIF on the VM, this information also includes:
  - The MAC address
  - The network
  - The IP address
  - The total bytes transmitted and received since the VM was booted
  - The status

On this page, you can also specify available target VLANs for port configuration policies. See [Set up port configuration policies](#).

## Network level

The Status tab for pool-wide networks lists summary information about each network in the resource pool. The Status tab for an individual network lists information about the network itself. The tab includes hyperlinked tables of information about the physical interfaces and VM interfaces currently connected to the network.

The status icon can be displayed in the following colors:

- Green if the network is active and properly managed by the vSwitch Controller
- Red if the network has no connected interfaces
- Orange if there is an error condition. The associated text describes the error.

For pool-wide networks, the following information is displayed:

- Network name: Specific network.
- VMs: Number of VMs associated with the network.
- XenServer: Server for the network.
- Physical Interface: Server interface for the network.
- Transmit (Tx) and receive (Rx) packets: Aggregated counters across all VIFs on the specified network.
- Errors: Aggregated counters across all VIFs on the specified network.
- Status: Color-coded icon that shows the current network.

For a selected network, the following information is presented:

- Network Status: Color-coded icon that shows the current network.
- VMs: Number of VMs associated with the network.
- Physical interfaces: List of physical interfaces, including VLAN, number of bytes transmitted and received, errors, and status.
- Switching XenServer (present on cross-server private networks only): Specifies the current active switching host for the network.

A cross-server private network enables communication between VMs in the same resource pool, without need for any additional configuration of the physical network. The VMs can be running on different hosts. This capability is accomplished by having a “switching host” establish GRE tunnels to each of the other hosts in the pool. The GRE tunnels are set up in a star topology. The other hosts have an active VM running on the private network.

If a switching host becomes unavailable or is deleted, a new switching host is automatically selected and new GRE tunnels are configured. See [Networking](#) for more information on cross-server private networks.

- VM interfaces: List of VMs, including MAC address, IP address, number of bytes transmitted and received, and status.

On this page, you can also specify available target VLANs for port configuration policies. For more information, see [Set up port configuration policies](#).

### **Virtual Machine (VM) level**

The following information is displayed for all VMs:

- VM name: Name of the specific VM.
- MAC address: MAC address assigned to the VM.
- Network name: Network to which the VM is assigned.
- Detected IP address: IP addresses assigned to the VM.
- Transmit (Tx) and receive (Rx) packets: Aggregated counters across all VIFs on the specified VM.
- Errors: Aggregated counters across all VIFs on the specified VM.

For a selected VM, the Status page displays the following information:

- Status: Color-coded icon that displays the current VM status.
- Resource Pool: Resource pool to which the VM belongs.
- Server Name: Name of the server to which the VM is assigned. This information is blank if the VM is not running and is not tied to a specific server.
- VM Group Membership: List of administrative groups to which the VM is assigned.
- VM interfaces: List of the VIFs on the VM. This information includes:
  - MAC address
  - Network name
  - Detected IP address
  - Transmit and receive bytes, packet, and error counts
  - Status
- Network Events: List of network events involving the VM, including priority, date/time, and description.

### **Virtual Interface (VIF) level**

For a selected VIF, the Status page presents the following information:

- Status: Color-coded icon that shows the current VIF status.
- Resource Pool: Resource pool to which the VIF belongs.
- Network: Network to which the VIF belongs.
- VM Name: VM to which the VIF belongs.
- MAC Address: MAC address of the VIF.

- IP Address: IP address of the VIF.
- Transmit and Receive bytes, packets, and errors: Traffic counts for the VIF.
- Switch Port ACL Statistics: Unlike transmit and receive counts, the ACL hit counts are instantaneous statistics read from the ACL rule statistics of the current vSwitch. Therefore, policy changes and VM actions, such as suspension, shut down, or migration causes these statistics to reset.

The vSwitch ACL statistics require an IP address to be identified on the network and able to collect statistics for IP-based protocols. If you find that there are no counts on IP-based rules, verify that an IP address is displayed in the IP address field.

### View flow statistics

By default, the vSwitch on each managed XenServer sends Netflow data to the vSwitch Controller, which uses this data to generate Flow Statistics tables and charts. The vSwitch generates Netflow records for all IPv4 flows after five seconds of no activity or 60 seconds of total activity.

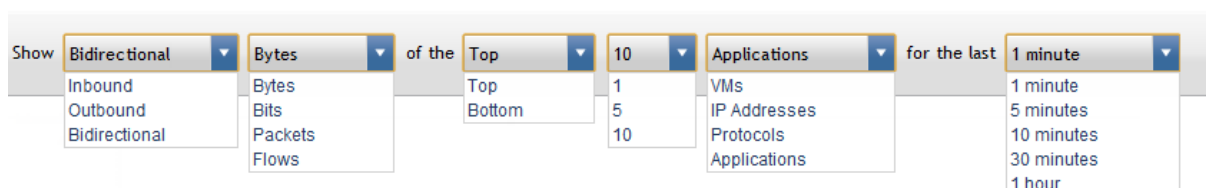
The data rate of a flow is represented as the total traffic of the flow averaged across the duration of the flow. For example, if a flow lasts 10 seconds with 900 KB sent in the first second and 10 KB sent in each of the nine remaining seconds, the resulting data is plotted as if the rate were 100 KB/second for the entire flow period.

Netflow uses UDP datagrams to transport NetFlow records between a switch and a collector (for example, the vSwitch Controller). Because NetFlow uses UDP datagrams, there is usually no way for the collector to know why a NetFlow record wasn't received. Dropped records can result in nondeterministic data with Flow Statistics tables or charts. For example, assume that a network generating 10 flows per second has a single 1 GB file transfer that lasts 10 seconds. The network generates a total of 202 flows (100 hping stimuli, 100 hping responses, 1 file transfer stimulus, and 1 file transfer response). If 50% of the UDP datagrams are dropped, there is a 50/50 probability that the collector reports either 1 GB of data, or 2 KB.

Because each vSwitch in a pool generates Netflow records, sources and destinations run on different XenServer hosts result in two records, doubling the statistics counts.

Disable flow visibility in deployments of more than 100 VMs to avoid overloading the vSwitch Controller virtual appliance and the network used to send NetFlow records.

The **Flow Statistics** tab displays a graph and associated table to show flows for the selected node.



Use the lists at the top of the page to specify the following:

- Direction: Bidirectional, Inward, Outbound
  - Units: Bytes, Bits, Packets, Flows
  - The top or bottom items (highest or lowest values) of one of the following groupings:
    - VMs: VMs residing within the resource pool as sources/destinations for traffic
    - IP Addresses: IP addresses as source or destination for traffic
    - Protocols: IP protocol traffic such as ICMP, TCP, and UDP
- Note:**  
Ethernet layer protocols (such as ARP) are not displayed due to the limitations in the Netflow protocol used to generate results.
- Application: “application”-level protocol traffic, identified by TCP/UDP port or ICMP type/code
  - Traffic (by type): VMs, IP Address, Protocols, Applications (shown by protocol type and port number, this information can allow you to infer the service)
  - Time interval.

The table below the graph displays some or all of the following information, depending upon the type of item selected in the list:

- VM
- IP
- Inbound bytes
- Inbound data rate (Kbit/s)
- Outbound bytes
- Outbound data rate (Kbit/s)
- Total bytes
- Total data rate (bps)

If NetFlow is not being forwarded to the vSwitch Controller, a warning blue status text is displayed under the Flow Statistics tab: `One or more selected pools are not configured to forward NetFlow records to vSwitch Controller`

To reconfigure forwarding, click the blue status text to see a list of resource pools. Select the resource pool desired from the list to navigate to the pool status page. From the status page, you can configure NetFlow data forwarding.

## Manage address groups

You can set up address groups to specify the IP addresses to use as the source or destination for ACLs and for reporting of flow statistics.

To add an address group:



1. Under **Visibility & Control**, select **Address Groups** in the resource tree (side panel) to open the Status page for all address groups.
2. Click **Create Group**.
3. Enter the name to identify the group, and an optional description.
4. Click **Create Group**. The new group is added to the list of address groups.
5. Select the new group in the resource tree to open its **Status** page.
6. Click the **Add Members** button.
7. In the pop-up window, specify one or more IP addresses or subnets (comma separated). Example: 192.168.12.5, 192.168.1.0/24
8. Click **Add**. Continue to add more networks as needed. Each set of addresses is added as a node under the network in the Address Groups list.

The new address group is now available for ACL policies and flow statistics.

You can remove an existing address group by clicking the Remove link in the row of the All Address Groups for that address group.

You can also update the name or description of an address group:

1. Select the new group in the resource tree to open its **Status** page.
2. Click the **Modify Group** button.
3. In the dialog that opens, change the name and description.
4. Click the **Modify Group** button to save the changes.

## Manage Virtual Machine groups

A VM group is a set of VMs that you identify as a group for viewing status and flow statistics. Each VM in a VM group must already be in a resource pool. The groups are otherwise independent of resource pools and servers.

To add a VM group:

1. Under **Visibility & Control**, select **VM Groups** in the resource tree (side panel) to open the Status page for all VM groups.
2. Click the Create Group button.
3. Enter the name to identify the group, and an optional description.
4. Click **Create Group**. The new group is added to the list of VM groups.
5. Select the new group in the resource tree to open its **Status** page.
6. Click **Add Member**.
7. In the pop-up window, select the VM from the list.
8. Click **Add**. Continue to add more VMs as needed. Each VM is added as a subnode under the group in the VM Groups list.

The following right-click options are available for each VM group:

- Add VM to group: Add a new group member.
- Modify Name/Description: Change the name or description.
- Remove Group: Delete the group.

## DVS policy configuration hierarchy

Use the Access Control and Port Configuration tabs within **Visibility & Control** to configure access control, QoS, and traffic mirroring policies within the virtual network environment. While all policies are applied at the VIF level, vSwitch Controller exposes a hierarchical policy model that supports declaring default policies across a collection of VIFs. The vSwitch Controller also provides a way to override this default policy by creating fine-grained exceptions when needed. For example, you can exempt a particular VM from the default resource pool policy.

Similar to the hierarchy used in the resource tree, the policy hierarchy has the following levels:

- Global (most general level): Includes all VIFs in all resource pools.
- Resource pools: All VIFs in a particular resource pool.
- Networks: All VIFs attached to a particular network.
- VMs: All VIFs attached to a particular VM
- VIFs (most specific level): A single VIF.

### Note:

XenServer hosts are not included in the policy hierarchy, since policies must apply regardless of what XenServer in a resource pool is running a VM.

## Set up Access Control policies

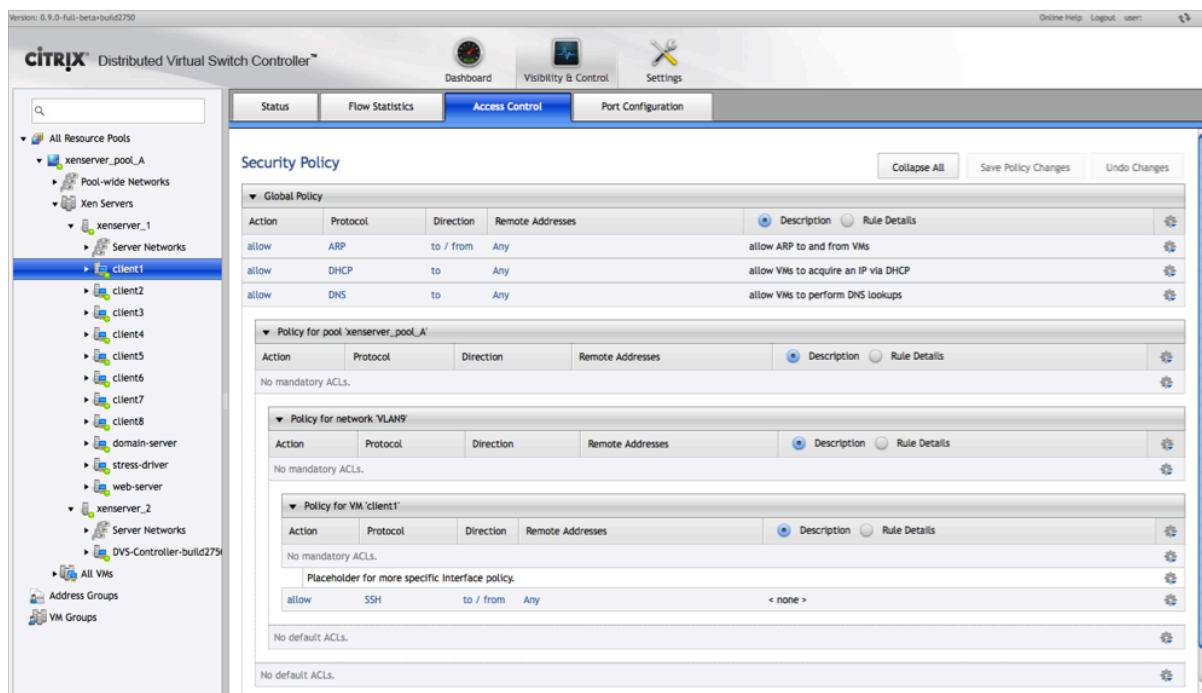
Choose the **Access Control** tab to set up policies that allow or deny VM traffic based on packet attributes.

An ACL policy consists of a set of rules, each of which includes the following:

- Action: Indication of whether traffic matching the rule is permitted (Allow) or dropped (Deny).
- Protocol: Network protocol to which the rule applies. You can apply the rule to all protocols (Any), choose from an existing protocol list, or specify a new protocol.
- Direction: Direction of traffic to which the rule applies. Read the text of the rules from left to right: “to” means traffic outbound from the VM, while “from” means traffic inbound to the VM.
- Remote Addresses: Indicates whether the rule is limited to traffic to/from a particular set of remote IP addresses.

Management of ACL policies closely follows the resource tree hierarchy. You can specify policies at any supported level of the hierarchy. At each level, rules are organized as follows:

- **Mandatory rules:** These rules are evaluated before any child policy rules. The only rules that take precedence over them are mandatory rules of parent (less specific) policies. Mandatory rules are used to specify rules that child (more specific) policies cannot override.
- **Child rules:** The child policy placeholder indicates the location in the rule order at which rules in child policies are evaluated. It divides the mandatory rules from the default rules.
- **Default rules:** These rules are evaluated last, after all mandatory rules and all child policy default rules. They only take precedence over default rules of parent policies. They are used to specify behavior that is only applied if a more specific child policy does not specify conflicting behavior.



## Global Access Control List (ACL) rules

To set up global ACL rules, click **All Resource Pools** in the resource tree. The page lists all of the ACL rules that are defined at the global level.

## Resource Pool Access Control List (ACL) rules

To set up ACL rules for a resource pool, select the resource pool in the resource tree.

The page shows an expandable bar for global policy, and an expanded area for resource pool rules. If you click the **Expand All** button, you can see how the resource pool rules are embedded in the global policy framework.

### Network Access Control List (ACL) rules

To set up ACL rules at the network level, click the network in the resource tree.

The page shows the following:

- An expandable bar for global rules
- An expandable bar for the resource pool to which the network belongs
- An expanded area for network rules

If you click **Expand All**, you can see how the network policies are embedded in the resource policy framework and in the global policy framework.

### VM Access Control List (ACL) rules

To set up policies at the VM level, click the VM in the resource tree.

The page shows the following:

- An expandable bar for global rules
- Expandable bars for the resource pool and network to which the VM belongs
- An expanded area for VM rules

If you click the **Expand All** button, you can see how the VM rules are embedded in the network, resource pool, and global framework.

If a VM contains VIFs on multiple networks, a “Change Network” link appears on the right side of the example bar for the network. This link allows you to view the rules for each network level policy that might apply to a VIF on that VM.

### VIF Access Control List (ACL) rules

To set up policies at the VIF level, click the VIF in the resource tree. Because policies are packaged and applied only at the VIF level, you must display the VIF pages to see the full policy context.

The page shows the following:

- Expandable bars for global rules
- Expandable bars for the resource pool, network, and VM to which the VIF belongs
- An expanded area for VIF rules

If you click the **Expand All** button, you can see how the VIF rules are embedded in the VM, network, resource pool, and global framework.

### Access Control List (ACL) rule enforcement order

While ACLs can be defined at different levels of the policy configuration hierarchy, ACLs are enforced on a per-VIF basis. For actual enforcement, the hierarchy is combined in the order described in this section and applied to each VIF. To see currently applied rules on a VIF and the associated statistics, select the VIF in the resource tree. View the ACL list in the Status tab.

The enforcement order is as follows:

1. Mandatory rules at the global level
2. Mandatory rules for the resource pool containing the VIF
3. Mandatory rules for the network containing the VIF
4. Mandatory rules for the VM containing the VIF
5. Rules for the VIF containing the VIF
6. Default rules for the VM containing the VIF
7. Default rules for the network containing the VIF
8. Default rules for the resource pool containing the VIF
9. Default rules for the global containing the VIF

The first rule that matches is executed, and no further rules are evaluated.

#### Note:

When a vSwitch Controller is unavailable, the resource pool enforces access control rules based on the configured fail mode. See the section called “Resource Pool Level” under “Viewing Status” for more details about a resource pool’s fail mode.

### Define Access Control List (ACL) rules

To define a new ACL rule, use the resource tree to choose the node at the appropriate level in the policy configuration hierarchy. You can add rules at each level for that level and for higher levels. For example, if you select a resource pool, you can add rules for that resource pool and global rules.

If you choose a resource tree node that doesn’t correspond to a level in the policy configuration hierarchy, a message is displayed. The message provides links to choose another levels.

New rules can be added in the following ways:

- To add a mandatory rule, click the gear icon in the header bar for the level, and choose **Add New Mandatory ACL**.
- To add a default rule, click the gear icon in the header bar for the level, and choose **Add New Default ACL**.
- To add a rule above an existing rule entry, click the gear icon for the entry, and choose **Add New ACL Above**.

- To add a rule below an existing rule entry, click the gear icon for the entry, and choose **Add New ACL Below**.

The new rule is added to the page with the following default settings:

- Action: Allow
- Protocol: Any
- Direction: To/From
- Remote Addresses: Any
- Description: None

To change a particular field within a rule, click the link representing the current field value and apply changes as described in the following list. When you apply a change, the rule is updated to show the values.

- **Action:** Click the link and choose **Change Action to Deny** or **Change Action to Allow**.
- **Protocol:** Click and choose one of these options:
  - Choose **Match Any Protocol** to apply the rule to all protocols.
  - Choose **Use an Existing Protocol** to specify a protocol. Select the protocol from the list, and click **Use Protocol**.
  - Choose **Use a New Protocol** to specify custom protocol characteristics. Specify the following information in the pop-up window, and click **Save & Use**:
    - \* Ethertype: Select IP or enter another Ethertype.
    - \* IP Protocol: Select one of the listed protocols, or enter another.
    - \* Destination Port (TCP/UDP only): Enter a port number or specify **Any**.
    - \* Source Port (TCP/UDP only): Enter a port number or specify **Any**. When defining an application that uses a well-known server port, define that well-known port as the destination port and leave the source port as **Any**. For example, you can use this approach for HTTP, which uses port 80.
    - \* ICMP Type (ICMP only): Choose **Any** or enter a specific ICMP type Protocol (ICMP) type.
    - \* ICMP Code (ICMP only): Choose **Any** or enter a specific ICMP code.
    - \* Match reply traffic: Indicate whether return traffic is automatically allowed as part of the rule. For example, if the rule allows UDP destination port 7777 traffic from the VM to a specified remote address and Match reply traffic is selected, UDP traffic is also allowed **from** source port 7777 of the remote address to the VM. Enable this option for any UDP protocol that requires bidirectional communication (the option is always enabled for TCP).
    - \* One-time Use vs. Multiple Uses: Select whether to use this protocol only for the current rule or to add it to the list of protocols in the protocol menu.
  - Choose **View/Modify Current Protocol** to modify characteristics for an already defined protocol.
- **Direction:** Choose whether the rule applies **from** or **to** the specified remote addresses, or both.

- **Remote Addresses:** To specify the remote addresses:
  1. Click the **Any** link to open a pop-up window that lists the available address groups.
  2. Select one or more address groups and use the arrows to move them to the **Selected** column.
  3. Use the **All** buttons to select or deselect all of the groups.
  4. To specify an IP address or subnet that is not part of an existing address group, enter the address or subnet (x.x.x.x or x.x.x.x/n). Click **Add**. Repeat to add more addresses.
  5. Click **Done**.
- **Description:** To add a text description of the rule:
  1. Click the **Description** button.
  2. Click the entry (<None> if there is no current description). A text entry area is displayed. Enter the text and press **Enter**.
- **Rule Details:** Click the **Rule Details** button to display a brief summary of the rule.

Click **Save Policy Changes** to apply the new rules. When you do so, the changes take effect immediately within the virtual network environment. If you have not already saved the rules, you can click **Undo Changes** to reverse the changes you have named.

When you change an ACL, all background updates for the vSwitch Controller GUI are paused. If another administrator modifies the policy simultaneously and commits changes before you, refresh the page to retrieve the new policy from the server. Reenter your changes.

You can change order of rules in a level by clicking the gear icon for the rule and choosing **Move Up** or **Move Down**. You cannot move a rule between levels in the hierarchy. To remove a rule, click the gear icon and choose **Delete**. Click the **Description** button to display the ACL description. Or the **Rule** button to display the ACL rule that you constructed.

ACL rules are always interpreted from the point of view of the virtual interface of the VM, even if configured higher in the policy hierarchy. This behavior is important when thinking about the meaning of the Remote Addresses field in the rules.

For example, if a VM in a pool has the IP address 10.1.1.1, you might expect a rule on the pool that specifies “deny all protocols to IP 10.1.1.1” to prevent any traffic reaching the VM. This behavior is the case for all other VMs in the resource pool because each VM enforces the rule when the VM transmits. However, machines that are external to the resource pool *can* communicate with the VM with IP address 10.1.1.1. This behavior is because no rules control the transmit behavior of the external machines. It is also because the VIF of the VM with IP address 10.1.1.1 has a rule that drops transmit traffic with that address. However, the rule does not drop *receive traffic* with that address.

If the policy behavior is unexpected, view the Status tab for the virtual interface where the entire set of rules from all policy levels is visualized.

## Set up port configuration policies

Use the **Port Configuration** tab to configure policies that apply to the VIF ports. The following policy types are supported:

- QoS: Quality of Service (QoS) policies control the maximum transmit rate for a VM connected to a DVS port.
- Traffic Mirroring: Remote Switched Port Analyzer (RSPAN) policies support mirroring traffic sent or received on a VIF to a VLAN to support traffic monitoring applications.
- Disable MAC address spoof check: MAC address spoof check policies control whether MAC address enforcement is performed on traffic outbound from a VIF. If the vSwitch Controller detects a packet with an unknown MAC address from a VIF, it drops the packet and all subsequent traffic from the VIF. MAC address spoof check policies are on by default. Disable these policies on VIFs running software like Network Load Balancing on Microsoft Windows servers.

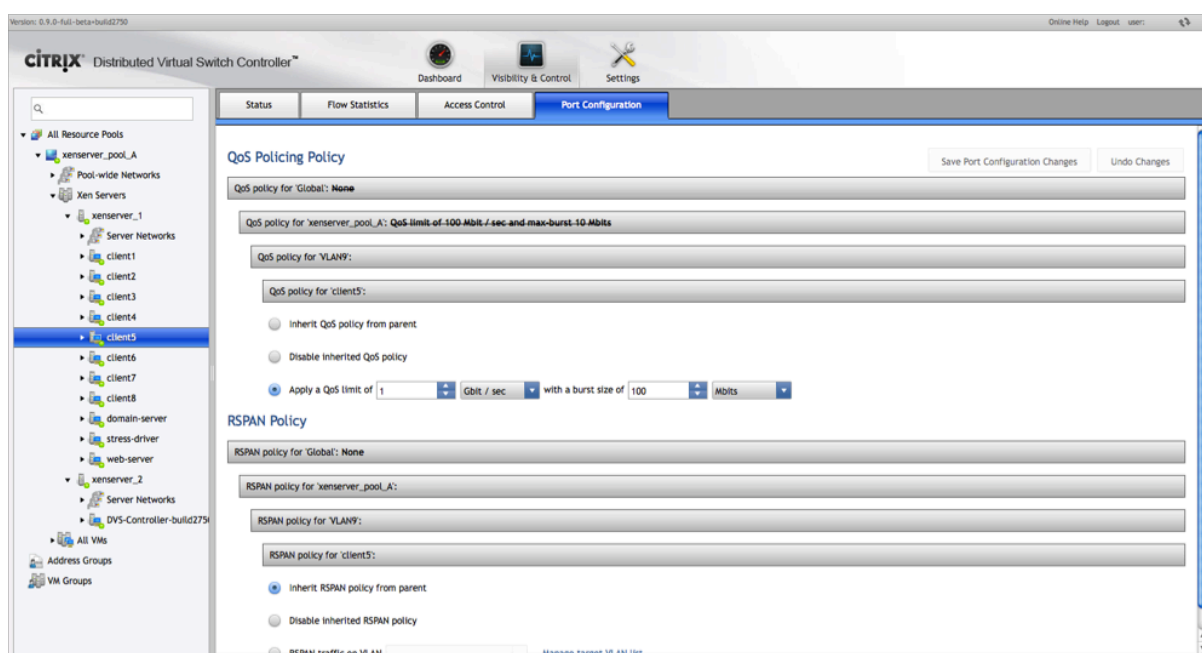
### Warning:

Enabling RSPAN without correct configuration of your physical and virtual network can cause a serious network outage. Read the instructions in Configure RSPAN carefully before enabling this feature.

You can configure QoS and Traffic Mirroring port policies at the global, resource pool, network, VM, and VIF levels. When you select a node in the resource tree and choose the **Port Configuration** tab, it shows the configuration for each parent level in the hierarchy. However, only the configuration at the selected policy level can be changed. For example, if you select a VM, the **Port Configuration** tab shows the values configured at the global, resource pool, and network levels. The tab lets you change the value at the VM level.

QoS and Traffic Mirroring configurations at a given level override the configurations at the higher levels. If a configuration is overridden, then the **Port Configuration** tab shows the higher level configuration crossed out. For example, the next figure shows a QoS configuration at the network level that overrides the configuration at the resource pool level.





To configure port policies, choose the node in the resource tree and choose the **Port Configuration** tab. If you choose a node that does not support port configuration policies, a message is displayed with links to nodes that do support port configuration.

## Configure QoS

For QoS policies, choose from the following options:

- Inherit QoS policy from parent (default): Applies the policy from the higher (that is, less specific) hierarchy level. This option does not exist at the global level.
- Disable inherited QoS policy: Ignores any policies that are set at higher (that is, less specific) levels such that all VIFs included in this policy level have no QoS configuration.
- Apply a QoS limit: Select a rate limit (with units), and a burst size (with units). Traffic to all VIFs included in this policy level is limited to the specified rate, with individual bursts limited to the specified number of packets.

### Warning:

Setting a too small burst size relative to the rate limit can prevent a VIF from sending enough traffic to reach the rate limit. This behavior is especially likely for protocols that perform congestion control such as TCP.

At minimum, the burst rate must be larger than the Maximum Transmission Unit (MTU) of the local network.

Setting QoS to an inappropriately low burst rate on any interface on which the vSwitch Controller

sits can result in losing all communication with the vSwitch Controller. This communication loss forces an emergency reset situation.

To prevent any inherited enforcement from taking place, disable the QoS policy at the VM level.

Click **Save Port Configuration Changes** to implement the changes, or click **Undo Changes** to remove any unsaved changes. The policy takes effect immediately after saving.

## Configure RSPAN

### Warning:

Configuring RSPAN when the server is connected to a switch that doesn't understand VLANs or isn't properly configured to support the RSPAN VLAN can cause traffic duplication and network outages. Review the documentation and configuration of your physical switches before enabling the RSPAN feature. This review is especially important at higher levels of the hierarchy where multiple physical switches might be involved.

Enabling RSPAN requires a series of steps, outlined below:

### Identify your RSPAN VLAN

When RSPAN is enabled on a VIF, the vSwitch for that VIF makes a copy of each packet sent to or from that VIF. The vSwitch transmits the copy of that packet tagged with VLAN value called the target VLAN. An administrator then places a host performing monitoring on the switch port that is configured to use the target VLAN. If the monitoring host interface uses promiscuous mode, it can see all traffic that is sent to and from the VIFs configured to use RSPAN.

### Configure the physical network with the target VLAN

It is critical to configure the physical network correctly to be aware of the RSPAN traffic to avoid network outages. Only enable RSPAN if the physical switching infrastructure connecting all RSPAN-enabled VIFs can be configured to disable learning on the target VLAN. For more information, see the documentation from your switch manufacturer.

Additionally, traffic sent on the target VLAN must be forwarded from each of the vSwitches to the monitoring hosts. If your physical infrastructure includes many switches in a hierarchy, this forwarding requires trunking the target VLAN between the different switches. For more information, see the documentation from your switch manufacturer.

### Configure vSwitch Controller with the target VLAN

Tell the vSwitch Controller about each target VLAN before using that VLAN ID for RSPAN port configuration. You can specify available target VLAN IDs at the resource pool, network, or server level. Target

VLANs added at a level of the hierarchy are available when configuring RSPAN port configuration at that level and all lower levels of the hierarchy. The correct level to specify a target VLAN depends on how widely you have configured your physical infrastructure to be aware of that target VLAN.

To specify available target VLANs:

1. Under **Visibility & Control**, open the **Status** tab for all resource pools, a specific resource pool, a specific server, or a specific network.
2. In the **RSPAN Target VLAN IDs** area, click **+** and enter the VLAN ID.
3. Repeat to add more VLAN IDs.
4. Click **Save Target VLAN Change**.

The VLANs are now available for selection on the Port Configuration tab, as described in this section.

### **Modify port configuration to enable RSPAN for a set of VIFs**

To configure RSPAN policies within the **Port Configuration** tab, select the appropriate node in the resource tree and choose from the following options:

- Inherit RSPAN policy from parent (default): Applies the policy from the next higher (that is, less specific) hierarchy level.
- Disable inherited RSPAN policy: Ignores any policies that are set at higher (that is, less specific) levels such that all VIFs included in this policy level have no RSPAN configuration.
- RSPAN traffic on VLAN: Choose a VLAN from the list of target VLANs. The only target VLANs that appear in the list are those VLANs configured for policy levels containing the currently selected node.

### **Configure MAC address spoof checking**

To disable MAC address enforcement, select **MAC address spoof checking**. Enforcement can only be configured on a per VIF basis and does not inherit or override parent configurations.

### **Save changes**

Click **Save Port Configuration Changes** to implement the changes, or click **Undo Changes** to remove any unsaved changes. The policy takes effect immediately after saving.

## **Administer and maintain the vSwitch Controller**

September 6, 2018

Use the **Settings** pages to perform administration and maintenance functions on the vSwitch Controller. To access the Settings pages, select the **Settings** icon in the top panel of the vSwitch Controller window.

## Configure IP address settings

Use the **IP Configuration** page to verify and configure the IP address of the vSwitch Controller. When the vSwitch Controller is started for the first time, it obtains an IP address through DHCP. However, we recommend that you assign a static IP address. If DHCP is configured, resource pools cannot be set to Fail-Safe mode.

To view and configure the controller IP address:

1. Under **Settings**, choose **IP Configuration** to display the current configuration.
2. To modify the configuration, click **Modify Configuration**.
3. Select **Manual Configuration** to assign a static IP address.
4. Enter the following information:
  - New IP address
  - Netmask
  - Gateway IP address
  - (Optional) One or two DNS server IP addresses

**Note:**

At least one DNS server IP address must be specified to enable name resolution on the Controller.

5. Click **Make Changes** to implement the changes.

**Warning:**

After changing the IP address of the vSwitch Controller, you might see an error message: Pool Managed By *old\_ip\_address*. This error message appears in the **Status** column of the pools that the vSwitch Controller manages. If you see this message, you must instruct the Controller to begin managing the pools again.

In the **All Resource Pools** tab, click the gear icon next to the **Status** column of the resource pools. Select **Steal Pool**.

By default, the vSwitch Controller virtual appliance uses a self-signed SSL certificate for connections with the vSwitch running on each XenServer. You can get a certificate authority to provide you with a signed certificate for your vSwitch connections. Follow the instructions of the certificate authority you plan to use when generating the public/private key pair to be signed. Submit the key to the authority. After you obtain the signed certificate from the authority, follow the steps in this section.

Under **Settings**, click **Server and Certificate Maintenance**.

Click **Update OVS Certificate**.

Browse to select the SSL/TLS certificate file.

After uploading the file, click **Update Certificate**.

To view information about the vSwitch SSL security certificate:

1. Under **Settings**, click **Server and Certificate Maintenance**.
2. Click **View OVS Certificate**.

This information also includes when the certificate expires.

After updating the vSwitch SSL certificate, as you add new pools for management, the vSwitch of each server in the pool automatically downloads the new certificate. However, for vSwitches running on existing pools under management you must manually update their SSL certificates.

On the XenServer host, copy the SSL certificate to `/etc/openvswitch/vswitchd.cacert`

Restart the XenServer host.

## Configure the controller hostname

To verify and configure the Controller hostname and DNS domain, use the IP Configuration page. By default, the controller hostname is `dvsc`, and the DNS domain name is unassigned.

Under **Settings**, choose **IP Configuration** to display the current configuration.

Click **Modify Host Settings**.

Enter the desired hostname and domain name into the appropriate fields.

The value of the domain name is used for both the domain name of the host and the domain to search for unqualified host names.

Click **Make Changes** to save changes, or choose **Cancel**.

## Collect information for trouble reports

To collect information to supply for trouble reports:

1. Click **Server and Certificate Maintenance** under **Settings**.
2. Click **Collect & Zip All Logs** to add all relevant vSwitch Controller logs to a zip file for download.
3. When the zip operation is complete, click the **here** link in the pop-up window to download the `dump.tar.gz` file.
4. After downloading, click **Close** to close the pop-up window.

## Restart the vSwitch Controller software

To restart the vSwitch Controller software, click **Server and Certificate Maintenance** under Settings, and then click **Restart Network Controller**. When the restart is complete, the login page opens.

## Manage administrative accounts

Multiple user accounts can be used to provide certain users with limited privileges when accessing the GUI. Entries in the Administrative Events log contain the name of the user who performed the action. Having multiple users can help determine who made a recent configuration change.

To add user accounts for access to the vSwitch Controller and to change user passwords:

1. Under **Settings**, choose **Administrative Accounts**.
2. Click **Create Account**.
3. Enter a user name and password, and reenter the password to confirm. Specify any of the following user privilege levels:
  - Superuser: All privileges.
  - Read-write: All privileges, except for the ability to modify other user accounts and restore snapshots.
  - Read-Only: Can see most information in the GUI but cannot modify anything in the vSwitch Controller except the user's own password.
4. Click **Add User**.

To change a user password, click the **Password** link for the user. Enter and confirm a new password, and click **Change Password**.

To remove a user, click the **Remove** link for the user. You cannot remove the admin user.

## Manage configuration snapshots

Snapshots provide a mechanism to save the current vSwitch Controller configuration so that you can restore to that exact configuration at a later point. It might be useful to snapshot the system before making major configuration changes. By default, the system automatically creates an automatic snapshot every 12 hours.

Click **Configuration Snapshots** under **Settings** to view the list of configuration backups and restore from backup. The page lists all recent backups, with the most recent listed first. Automatic backups are taken twice per day and each time the vSwitch Controller is restarted. When restoring from a backup, the current IP configuration of the vSwitch Controller is not updated. To change the vSwitch Controller IP address, see Configure IP address settings.

To restore the configuration from a backup, click the gear icon for the snapshot and choose **Restore to Snapshot**. When asked if you want to continue, click **Yes, Restore**.

To create a backup on demand, click **Create New Snapshot**. You can enter an optional description to identify the snapshot. Click **Create Snapshot**. The new backup is added to the top of the list.

To download a snapshot to store on another system, click the gear icon for the snapshot and choose **Download**. Follow the instructions in the popup windows to save the snapshot file.

To upload a previously saved snapshot to the controller, click **Upload Snapshot**. Browse to select the snapshot file, and click **Upload Snapshot**. The uploaded snapshot is added to the list on the Configuration Snapshots page.

To delete a snapshot, click the gear icon for the snapshot and choose **Delete Snapshot**. When asked if you want to continue, click **Delete Snapshot**.

The snapshot table also includes information on the software version and compatibility. Compatibility indicates whether the data in the snapshot is compatible with the current software version. It displays a green indicator if it is compatible and a red indicator if it is not. To revert to an incompatible snapshot, you must first change the software to a compatible version, as listed in the Software Version column.

By default, the system creates a configuration snapshot every 12 hours. These snapshots are listed with a description label of **Automatic periodic snapshot**. In addition, configuration snapshots are created each time the vSwitch Controller is restarted. These snapshots are listed with a description label of **Startup snapshot**. System initiated snapshots are automatically deleted when they are more than 30 days old. When manually creating a snapshot, enter a unique description label so it is not mistaken as a system initiated snapshot and deleted after 30 days. If a system initiated snapshot must be preserved beyond 30 days, download it and then reupload it by using a unique description label.

## Add Network Time Protocol (NTP) servers

The vSwitch Controller virtual appliance uses a connection to external Network Time Protocol (NTP) servers to manage its time settings. The controller comes with default servers already configured. Because these NTP servers might not be optimal for your environment, you can replace them with a local NTP server according to the following instructions.

To add an NTP server:

1. Under **Settings**, choose **Time & NTP**.
2. Click **Add Server**.
3. Enter the IP address of the server, and click **Add**.
4. Add more servers as needed.

To remove an NTP server, click the **Remove** link.

## Export Syslog files

Use the Syslog page to add servers to receive remote syslog messages, which consist of administrative and network event messages generated by the system. The most recent syslog entries are also displayed on the dashboard.

To add syslog servers:

1. Under **Settings**, choose **Syslog**.
2. Click **Add Server Address**.
3. Enter the IP address of the server, and click **Add**.
4. Add more servers as needed.

To remove a server, click the **Remove** link.

## Command-line interface

August 15, 2018

This section describes the vSwitch Controller CLI commands. You can access the CLI locally from the text console of the Controller VM in XenCenter. To access the CLI remotely, use an SSH client application and connect to the controller VM hostname or IP address on port 22.

During a CLI session you can get help with CLI commands in either of the following ways:

- Type **help** and then press **Enter**.
- Enter part of a command followed by a space and question mark (?), and then press **Enter**.

The interface supports completion of the command argument when you press the **Tab** key. Generally, you can abbreviate commands to the shortest, unique string at each level to reduce typing. You can access the command history within the current session is available by pressing the **Arrow** keys.

### To terminate the current CLI session

Run the command: `exit`

### To halt the vSwitch Controller

Run the command: `halt controller`

This command halts the vSwitch Controller appliance by gracefully shutting down the Controller.



## **To get information on commands**

Run the command: `help`

## **To upgrade or downgrade the existing version of the Controller**

Run the command: `install controller software-update scp-format-remote-filename`

This command securely copies a controller update file from the specified remote location and installs that version in place of the existing version.

This command can be used to install software versions that are both upgrades and downgrades. Upgrades automatically migrate the configuration to the new version. Downgrades revert to the most recent compatible configuration snapshot or an empty configuration when no compatible snapshot exists.

## **To ping a specified remote system**

Run the command: `ping name-or-IP-address [count]`

This command sends ICMP echo requests to the remote system identified by name-or-IP-address and waits for replies. If no count is specified, requests are sent once per second until interrupted with Ctrl-C. If a count is specified, that number of pings are sent.

## **To restart the Controller**

Run the command: `restart controller appliance`

This command shuts down and restarts the entire controller appliance.

This command is primarily for troubleshooting. Generally, the `halt` command is used to power off the controller appliance.

## **To restart the Controller daemon**

Run the command: `restart controller daemon`

This command shuts down and restarts the processes that implement the controller functions.

This command is primarily for troubleshooting.

## To set the hostname of the controller appliance

Run the command: `set controller hostname hostname`

This command sets the hostname of the controller appliance.

If the provided hostname contains one or more period characters (“.”), the hostname of the appliance is set to the string *before* the first period. The domain name of the appliance will be set to the string *after* the first period.

## To set the IP address of the Controller management interface via DHCP

Run the command: `set controller management-interface config dhcp`

This command sets the Controller management interface IP address using DHCP. If DHCP is configured, resource pools cannot be set to Fail-Safe mode.

This command takes effect when executed, so remote access to the CLI may be lost if the address changes.

## To set a static IP address for the Controller management interface

Run the command:

```
1 set controller management-interface config static
2 IP-address
3 netmask
4 gateway-IP
5 [dns-server-IP]
6 [dns-server-IP2
7 dns-search]] ‘
```

This command sets a static IP address for the Controller management interface. The DNS configuration information is optional. The ability to specify a DNS search path requires the specification of two DNS servers.

This command takes effect when executed so remote access to the CLI may be lost if the address changes.

## To display the current Controller hostname

Run the command: `show controller hostname`

### **To display a summary of the current configuration and status of the management interface**

Run the command: `show controller management-interface`

### **To display configuration values for the management interface**

Run the command: `show controller management-interface config`

### **To display the current default gateway for the Controller**

Run the command: `show controller management-interface default-gateway`

### **To display the current DNS configuration for the Controller**

Run the command: `show controller management-interface dns-server`

### **To display the current IP address of the Controller management interface**

Run the command: `show controller management-interface ip-address`

### **To display the current netmask of the Controller management interface**

Run the command: `show controller management-interface netmask`

### **To display the software version of the Controller**

Run the command: `show controller version`

## **Troubleshoot vSwitch Controller issues**

September 5, 2018

This section contains information to help with troubleshooting vSwitch Controller issues.

## **Resource tree node status**

The following table describes the status icons for each resource type. These icons appear in the resource tree and on the Status page for the item.

| Items/Status Icons     | Description                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VIFs</b>            |                                                                                                                                                                                   |
| Red                    | Associated virtual machine (VM) is shut down or unreachable.                                                                                                                      |
| Green                  | Virtual interface (VIF) is up and being managed.                                                                                                                                  |
| Orange                 | VM is running but the XenServer on which the VIF resides is not connected to the vSwitch Controller.                                                                              |
| <b>VMs</b>             |                                                                                                                                                                                   |
| Red                    | VM is shut down or unreachable.                                                                                                                                                   |
| Green                  | VM is in running state and VIFs are being managed.                                                                                                                                |
| Orange                 | VM is running but the XenServer on which the VM resides is not correctly connected to the vSwitch Controller. This status depends on the collective state of the respective VIFs. |
| <b>Server Networks</b> |                                                                                                                                                                                   |
| Red                    | XenServer is shut down or unreachable or no VMs have VIFs that are associated with the network.                                                                                   |
| Green                  | XenServer is correctly connected to the vSwitch Controller.                                                                                                                       |
| Orange                 | XenServer is not correctly configured to connect to the vSwitch Controller (depends on the collective state of the associated physical interfaces and VIFs).                      |
| <b>XenServer</b>       |                                                                                                                                                                                   |
| Red                    | XenServer is shut down or unreachable.                                                                                                                                            |
| Green                  | XenServer is correctly connected to the vSwitch Controller.                                                                                                                       |
| Orange                 | XenServer is not configured to connect to the vSwitch Controller (depends on the collective state of the associated physical interfaces and VIFs).                                |

| Items/Status Icons        | Description                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pool-Wide Networks</b> |                                                                                                                                                           |
| Red                       | Master XenServer is shut down or unreachable.                                                                                                             |
| Green                     | Master XenServer is configured to connect to the vSwitch Controller and the connection is up and working.                                                 |
| Orange                    | Master XenServer is not configured to connect to the vSwitch Controller (depends on the collective state of the associated physical interfaces and VIFs). |
| <b>Resource Pools</b>     |                                                                                                                                                           |
| Red                       | Master XenServer is shut down or unreachable.                                                                                                             |
| Green                     | Master XenServer is configured to connect to the vSwitch Controller and the connection is up and working.                                                 |
| Orange                    | Master XenServer is not configured to connect to the vSwitch Controller (depends on the collective state of the associated physical interfaces and VIFs). |

## Troubleshoot access policy issues

The following suggestions can help in troubleshooting when access control policies are not operating properly:

1. Select the **Status** page for the VIF of a VM that the policy is supposed to affect. View the hit counts for each rule while you generate traffic that the policy is not handling correctly. Identify the rule that the traffic is actually hitting instead of the rule you expected it to be hitting. For debugging purposes, you can, add a default rule that matches all traffic as the lowest priority default rule at the global level.

### Note:

This rule can have either an allow or deny action, depending on your desired network behavior while debugging. Delete this rule after debugging.

2. If the traffic hits a rule of lower priority than the one you expected, carefully check the rule matching criteria. Is the direction of the traffic correctly specified? Are the remote hosts prop-

erly identified? Is the protocol correctly defined? For example, is the protocol specifying a UDP port instead of a TCP port or the opposite way?

3. If the traffic hits a rule of higher priority than expected, resolve the conflict between this rule and the rule you expected the traffic to hit. You can resolve conflicts by redefining rules to be more or less granular or by changing the relative priorities of the two rules. For example, you can scope a rule to apply only to a particular set of remote IP addresses.
4. If the VM has multiple VIFs, check that it is transmitting and receiving the traffic on the VIF to which the policy applies. When appropriate, use RSPAN to mirror traffic from the VIF to a network analyzer. You can use this mirrored traffic to ensure that traffic is present that is supposed to match the rule.

**Note:**

When a vSwitch Controller is unavailable, the resource pool enforces access control rules based on the configured fail mode. See the section called “Resource Pool Level” under “Viewing Status” for more details about a resource pool’s fail mode.

## Create a trouble report

To address issues efficiently, collect information from the XenServer and vSwitch Controller that are involved in the issue. Collect this information as soon as possible after the issue occurs. Submit the information along with your trouble report.

- Include a Server Status report for each XenServer that is involved in the issue. For information about generating Server Status reports, see [Health check](#)
- Include a log bundle from the vSwitch Controller by clicking **Collect and Zip All Logs** in the **Server & Certificate Maintenance Settings** page. For more information, see [Collect information for trouble reports](#).

## Controller error messages

The following error messages can be seen:

- **Connecting to Pool** - Displayed when a new pool is added and vSwitch Controller has not yet successfully connected to the pool master. OR Displayed when the vSwitch Controller restarts and it has not yet successfully connected to the pool master. If a successful connection is not established in 30 seconds, this message is replaced with ‘Pool Connection Failed’.
- **Network control channels disconnected** - XenServer is not correctly connected to the vSwitch Controller.
- **Missing Pool Address** - No DNS name or IP address is available for the pool.
- **Pool Connection Failed** - This message is displayed in the following situations:

- There is a network problem between the controller and the pool master
  - There is a failure in DNS name resolution
  - There is an invalid DNS name or pool master IP address
  - The pool master is down or misconfigured
- **Unsupported Pool Version** - The DNS name or IP address configured to the pool does not resolve to a compatible version of XenServer.
- **Duplicate Pool: Pool Disabled** - The pool reports the same XAPI UUID as another pool already in the vSwitch Controller database.
- **Pool Authentication Failure** - vSwitch Controller was unable to authenticate to the pool master using the user name and password provided.
- **Pool Identity Changed** - The pool has been reinstalled and does not match the state of the matching pool.
- **Pool Synchronization Error** - An unsupported operation was seen when using XAPI to communicate with the pool master.
- **Unknown Error** - Cause of the error is not known.

## Command-line interface

March 29, 2019

The `xe` CLI enables you to script and automate system administration tasks. Use the CLI to integrate XenServer into an existing IT infrastructure.

The `xe` command line interface is installed by default on XenServer hosts and is included with XenCenter. A stand-alone remote CLI is also available for Linux.

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 RPM-based distributions (such as Red Hat), you can install the stand-alone `xe` command from the RPM named `xe-cli-6.00-BUILD.i386.rpm` on the main XenServer installation ISO. Use the following command:

```
1 rpm -ivh xe-cli-6.00-BUILD.i386.rpm
```

Basic help is available for CLI commands on-host by typing:

```
1 xe help command
```



A list of the most commonly used `xe` commands is displayed if you type:

```
1 xe help
```

Or a list of all `xe` commands is displayed if you type:

```
1 xe help --all
```

## Basic `xe` syntax

The basic syntax of all XenServer `xe` CLI commands is:

```
1 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 is executed 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 hostname 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 XenServer host (defaults to 443).

**Example:** On the local XenServer host:

```
1 xe vm-list
```

**Example:** On the remote XenServer host:

```
1 xe vm-list -user username -password password -server hostname
```

Shorthand syntax is also available for remote connection arguments:

- `-u` username
- `-pw` password
- `-pwf` password file

- `-p` port
- `-s` server

**Example:** On a remote XenServer host:

```
1 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 XenServer host, first run the following command:

```
1 export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=pass"
```

After running this command, you no longer have to specify the remote XenServer host 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 XenServer host, which is disabled by default.

## Special characters and syntax

To specify argument/value pairs on the `xe` command line, write:

```
1 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:

```
1 argument="value with spaces"
```

When you use the CLI on your XenServer host, 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 XenServer host. 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*
- *pbid*
- *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:

```
1 user-version (RW): 1
2 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:

```
1 platform (MRW): acpi: true; apic: true; pae: true; nx: false
2 allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
3 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

```
1 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.

- ***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.
- ***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.
- ***class-param-set*** *uuid=uuid param=value*  
Sets the value of one or more parameters.
- ***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.
- ***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.
- ***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:

```
1 xe vm-list params=name-label,other-config
```

Alternatively, to list all of the parameters, use the syntax:

```
1 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:

```
1 allowed-VBD-devices (SR0): <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:

```
1 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:

```
1 a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-
 af10baea96b7, \
2 42c044de-df69-4b30-89d9-2c199564581d
```

## Secrets

XenServer 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 XenServer host from a remote instance of the xe CLI.

To create a secret object, run the following command on your XenServer host.

```
1 xe secret-create value=my-password
```

A secret is created and stored on the XenServer 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 XenServer host where you created the secret, you can run the following command:

```
1 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"
```

## 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     |
|-------------------------------|---------------------------|----------|
| <code>uuid</code>             | The appliance uuid        | Required |
| <code>name-description</code> | The appliance description | Optional |
| <code>paused</code>           |                           | Optional |
| <code>force</code>            | Force shutdown            | Optional |

**appliance-assert-can-be-recovered**

```
1 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**

```
1 appliance-create name-label=name-label [name-description=name-
 description]
```

Creates an appliance/vApp. For example:

```
1 xe appliance-create name-label=my_appliance
```

Add VMs to the appliance:

```
1 xe vm-param-set uuid=VM-UUID appliance=appliance-uuid \
2 xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
```

**appliance-destroy**

```
1 appliance-destroy uuid=appliance-uuid
```

Destroys an appliance/vApp. For example:

```
1 xe appliance-destroy uuid=appliance-uuid
```

**appliance-recover**

```
1 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**

```
1 appliance-shutdown uuid=appliance-uuid [force=true|false]
```



Shuts down all VMs in an appliance/vApp. For example:

```
1 xe appliance-shutdown uuid=appliance-uuid
```

## **appliance-start**

```
1 appliance-start uuid=appliance-uuid [paused=true|false]
```

Starts an appliance/vApp. For example:

```
1 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     |
|-----------------------|----------------------------------------------------|----------|
| <code>filename</code> | Write the audit log of the pool to <i>filename</i> | Required |
| <code>since</code>    | Specific date/time point                           | Optional |

### **audit-log-get**

```
1 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:

```
1 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      |
|----------------------|-------------------------------------------------|-----------|
| <code>uuid</code>    | Unique identifier/object reference for the bond | Read only |
| <code>master</code>  | UUID for the master bond PIF                    | Read only |
| <code>members</code> | Set of UUIDs for the underlying bonded PIFs     | Read only |

## `bond-create`

```
1 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 XenServer host
- If fewer than 2 PIFs are supplied

## `bond-destroy`

```
1 bond-destroy uuid=bond_uuid
```

Deletes a bonded interface specified by its UUID from a host.

**bond-set-mode**

```
1 bond-set-mode uuid=bond_uuid mode=bond_mode
```

Change the bond mode.

**CD commands**

Commands for working with physical CD/DVD drives on XenServer hosts.

**CD parameters**

CDs have the following parameters:

| Parameter Name                  | Description                                                                  | Type                    |
|---------------------------------|------------------------------------------------------------------------------|-------------------------|
| <code>uuid</code>               | Unique identifier/object reference for the CD                                | Read only               |
| <code>name-label</code>         | Name for the CD                                                              | Read/write              |
| <code>name-description</code>   | Description text for the CD                                                  | Read/write              |
| <code>allowed-operations</code> | A list of the operations that can be performed on this CD                    | Read only set parameter |
| <code>current-operations</code> | A list of the operations that are currently in progress on this CD           | Read only set parameter |
| <code>sr-uuid</code>            | The unique identifier/object reference for the SR this CD is part of         | Read only               |
| <code>sr-name-label</code>      | The name for the SR this CD is part of                                       | Read only               |
| <code>vbd-uuids</code>          | A list of the unique identifiers for the VBDs on VMs that connect to this CD | Read only set parameter |
| <code>crashdump-uuids</code>    | Not used on CDs. Because crashdumps cannot be written to CDs                 | Read only set parameter |
| <code>virtual-size</code>       | Size of the CD as it appears to VMs (in bytes)                               | Read only               |

| Parameter Name                    | Description                                                                                 | Type                     |
|-----------------------------------|---------------------------------------------------------------------------------------------|--------------------------|
| <code>physical-utilisation</code> | Amount of physical space that the CD image takes up on the SR (in bytes)                    | Read only                |
| <code>type</code>                 | Set to User for CDs                                                                         | Read only                |
| <code>sharable</code>             | Whether or not the CD drive is sharable. Default is <b>false</b> .                          | Read only                |
| <code>read-only</code>            | Whether the CD is read-only, if <b>false</b> , the device is writable. Always true for CDs. | Read only                |
| <code>storage-lock</code>         | Value is <b>true</b> if this disk is locked at the storage level.                           | Read only                |
| <code>parent</code>               | Reference to the parent disk, if this CD is part of a chain.                                | Read only                |
| <code>missing</code>              | Value is <b>true</b> if SR scan operation reported this CD as not present on disk           | Read only                |
| <code>other-config</code>         | A list of key/value pairs that specify extra configuration parameters for the CD            | Read/write map parameter |
| <code>location</code>             | The path on which the device is mounted                                                     | Read only                |
| <code>managed</code>              | Value is <b>true</b> if the device is managed                                               | Read only                |
| <code>xenstore-data</code>        | Data to be inserted into the xenstore tree                                                  | Read only map parameter  |
| <code>sm-config</code>            | Names and descriptions of storage manager device config keys                                | Read only map parameter  |
| <code>is-a-snapshot</code>        | Value is <b>true</b> if this template is a CD snapshot                                      | Read only                |
| <code>snapshot_of</code>          | The UUID of the CD that this template is a snapshot of                                      | Read only                |

| Parameter Name             | Description                                                | Type      |
|----------------------------|------------------------------------------------------------|-----------|
| <code>snapshots</code>     | The UUIDs of any snapshots that have been taken of this CD | Read only |
| <code>snapshot_time</code> | The timestamp of the snapshot operation                    | Read only |

## cd-list

```
1 cd-list [params=param1,param2,...] [parameter=parameter_value]
```

List the CDs and ISOs (CD image files) on the XenServer host 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      |
|-------------------|--------------------------------------------------------|-----------|
| <code>uuid</code> | The unique identifier/object reference for the cluster | Read only |

| Parameter Name                         | Description                                                                                                                                          | Type                     |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>cluster-hosts</code>             | A list of unique identifiers/object references for the hosts in the cluster                                                                          | Read only set parameter  |
| <code>cluster-token</code>             | The secret key used by xapi-clusterd when it talks to itself on other hosts                                                                          | Read only                |
| <code>cluster-stack</code>             | The technology stack providing the clustering capabilities. Possible values are <code>corosync</code> .                                              | Read only                |
| <code>allowed-operations</code>        | 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  |
| <code>current-operations</code>        | 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  |
| <code>token-timeout</code>             | The corosync token timeout in seconds                                                                                                                | Read only                |
| <code>token-timeout-coefficient</code> | The corosync token timeout coefficient in seconds                                                                                                    | Read only                |
| <code>pool-auto-join</code>            | True if automatically joining new pool members to the cluster. This is set to <code>true</code> .                                                    | Read only                |
| <code>cluster-config</code>            | A list of key/value pairs that specify extra configuration parameters for the cluster.                                                               | Read only map parameter  |
| <code>other-config</code>              | A list of key/value pairs that specify extra configuration parameters for the cluster.                                                               | Read/write map parameter |

**cluster-host-create**

```
1 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**

```
1 cluster-host-destroy uuid=host_uuid
```

Destroy a cluster host, effectively leaving the cluster.

**cluster-host-disable**

```
1 cluster-host-disable uuid=cluster_uuid
```

Disable cluster membership for an enabled cluster host.

**cluster-host-enable**

```
1 cluster-host-enable uuid=cluster_uuid
```

Enable cluster membership for a disabled cluster host.

**cluster-host-force-destroy**

```
1 cluster-host-force-destroy uuid=cluster_host
```

Destroy a cluster host object forcefully, effectively leaving the cluster.

**cluster-pool-create**

```
1 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**

```
1 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**

```
1 cluster-pool-force-destroy cluster-uuid=cluster_uuid
```

Force destroy pool-wide cluster.

**cluster-pool-resync**

```
1 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      |
|-------------------------|--------------------------------------------------------------------------|-----------|
| <a href="#">uuid</a>    | The unique identifier/object reference for the console                   | Read only |
| <a href="#">vm-uuid</a> | The unique identifier/object reference of the VM this console is open on | Read only |



| Parameter Name             | Description                                                                                                                                                                                            | Type                     |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>vm-name-label</code> | The name of the VM this console is open on                                                                                                                                                             | Read only                |
| <code>protocol</code>      | Protocol this console uses.<br>Possible values are <code>vt100</code> : VT100 terminal, <code>rfb</code> : Remote Framebuffer Protocol (as used in VNC), or <code>rdp</code> : Remote Desktop Protocol | Read only                |
| <code>location</code>      | URI for the console service                                                                                                                                                                            | Read only                |
| <code>other-config</code>  | A list of key/value pairs that specify extra configuration parameters for the console.                                                                                                                 | Read/write map parameter |

## console

```
1 console
```

Attach to a particular console.

## Diagnostic commands

Commands for gathering diagnostic information from XenServer.

### diagnostic-compact

```
1 diagnostic-compact
```

Perform a major GC collection and heap compaction.

### diagnostic-db-log

```
1 diagnostic-db-log
```

Start logging the database operations. Warning: once started, this cannot be stopped.

### **diagnostic-db-stats**

```
1 diagnostic-db-stats
```

Print database statistics.

### **diagnostic-gc-stats**

```
1 diagnostic-gc-stats
```

Print GC statistics.

### **diagnostic-license-status**

```
1 diagnostic-license-status
```

Help diagnose pool-wide licensing problems.

### **diagnostic-net-stats**

```
1 diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2
...]
```

Print network statistics.

### **diagnostic-timing-stats**

```
1 diagnostic-timing-stats
```

Print timing statistics.

### **diagnostic-vdi-status**

```
1 diagnostic-vdi-status uuid=vdi_uuid
```

Query the locking and sharing status of a VDI.

**diagnostic-vm-status**

```
1 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**

```
1 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:

```
1 xe drtask-create type=lvmoiscsi device-config:target=target-ip-address
 \
2 device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
3 sr-whitelist=sr-uuid-list
```

**Note:**

The command `sr-whitelist` lists SR UUIDs. The `drtask-create` command only introduces and connects to an SR which has one of the whitelisted UUIDs

**drtask-destroy**

```
1 drtask-destroy uuid=dr-task-uuid
```

Destroys a disaster recovery task and forgets the introduced SR.

**vm-assert-can-be-recovered**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 sr-enable-database-replication uuid=sr_uuid
```

Enables XAPI database replication to the specified (shared) SR. For example:

```
1 xe sr-enable-database-replication uuid=sr-uuid
```

**sr-disable-database-replication**

```
1 sr-disable-database-replication uuid=sr_uuid
```

Disables XAPI database replication to the specified SR. For example:

```
1 xe sr-enable-database-replication uuid=sr-uuid
```

## Example usage

The example below shows the DR CLI commands in context:

On the primary site, enable database replication:

```
1 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`.

```
1 xe drtask-create type=lvmoiscsi \
2 device-config:target=target ip address \
3 device-config:targetIQN=target-iqn \
4 device-config:SCSIid=scsi-id \
5 sr-whitelist=sr-uuid
```

Look for database VDIs on the SR:

```
1 xe vdi-list sr-uuid=sr-uuid type=Metadata
```

Query a database VDI for VMs present:

```
1 xe vm-list database:vdi-uuid=vdi-uuid
```

Recover a VM:

```
1 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:

```
1 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                                                                   |
|----------------------|-------------------------------------------------------------------------------|
| <code>pool</code>    | A pool of physical hosts                                                      |
| <code>vm</code>      | A Virtual Machine                                                             |
| <code>host</code>    | A physical host                                                               |
| <code>network</code> | A virtual network                                                             |
| <code>vif</code>     | A virtual network interface                                                   |
| <code>pif</code>     | A physical network interface (separate VLANs are represented as several PIFs) |
| <code>sr</code>      | A storage repository                                                          |
| <code>vdi</code>     | A virtual disk image                                                          |
| <code>vbd</code>     | A virtual block device                                                        |
| <code>pbd</code>     | The physical block devices through which hosts access SRs                     |

## event-wait

```
1 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.

```
1 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:

```
1 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                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>uuid</code>                 | The unique identifier/object reference for the pGPU                                                                                                                         | Read only                |
| <code>vendor-name</code>          | The vendor name of the pGPU                                                                                                                                                 | Read only                |
| <code>device-name</code>          | The name assigned by the vendor to this pGPU model                                                                                                                          | Read only                |
| <code>gpu-group-uuid</code>       | The unique identifier/object reference for the GPU group that this pGPU has been automatically assigned to by XenServer. Identical pGPUs across hosts in a pool are grouped | Read only                |
| <code>gpu-group-name-label</code> | The name of the GPU group to which the pGPU is assigned                                                                                                                     | Read only                |
| <code>host-uuid</code>            | The unique identifier/object reference for the XenServer host to which the pGPU is connected                                                                                | Read only                |
| <code>host-name-label</code>      | The name of the XenServer host to which the pGPU is connected                                                                                                               | Read only                |
| <code>pci-id</code>               | PCI identifier                                                                                                                                                              | Read only                |
| <code>dependencies</code>         | Lists the dependent PCI devices passed-through to the same VM                                                                                                               | Read/write map parameter |

| Parameter Name                    | Description                                                                        | Type                     |
|-----------------------------------|------------------------------------------------------------------------------------|--------------------------|
| <code>other-config</code>         | A list of key/value pairs that specify extra configuration parameters for the pGPU | Read/write map parameter |
| <code>supported-VGPU-types</code> | List of virtual GPU types supported by the underlying hardware                     | Read only                |
| <code>enabled-VGPU-types</code>   | List of virtual GPU types which have been enabled for this pGPU                    | Read/Write               |
| <code>resident-VGPUs</code>       | List of vGPUs running on this pGPU                                                 | Read only                |

### **pgpu-disable-dom0-access**

```
1 pgpu-disable-dom0-access uuid=uuid
```

Disable PGPU access to dom0.

### **pgpu-enable-dom0-access**

```
1 pgpu-enable-dom0-access uuid=uuid
```

Enable PGPU access to dom0.

### **GPU group parameters**

GPU groups have the following parameters:

| Parameter Name                | Description                                              | Type       |
|-------------------------------|----------------------------------------------------------|------------|
| <code>uuid</code>             | The unique identifier/object reference for the GPU group | Read only  |
| <code>name-label</code>       | The name of the GPU group                                | Read/write |
| <code>name-description</code> | The descriptive text of the GPU group                    | Read/write |



| Parameter Name                    | Description                                                                             | Type                      |
|-----------------------------------|-----------------------------------------------------------------------------------------|---------------------------|
| <code>VGPU-uuids</code>           | Lists the unique identifier/object references for the virtual GPUs in the GPU group     | Read only set parameter   |
| <code>PGPU-uuids</code>           | Lists the unique identifier/object references for the pGPUs in the GPU group            | Read only set parameter   |
| <code>other-config</code>         | A list of key/value pairs that specify extra configuration parameters for the GPU group | Read/write map parameter  |
| <code>supported-VGPU-types</code> | Union of all virtual GPU types supported by the underlying hardware                     | Read only                 |
| <code>enabled-VGPU-types</code>   | Union of all virtual GPU types which have been enabled on the underlying pGPUs          | Read only                 |
| <code>allocation-algorithm</code> | 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**

```
1 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**

```
1 gpu-group-destroy uuid=uuid_of_group
```

Destroys the GPU Group; only permitted for empty groups.

### **gpu-group-get-remaining-capacity**

```
1 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**

```
1 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**

```
1 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      |
|-----------------------------|------------------------------------------------------------------------------------------------|-----------|
| <code>uuid</code>           | The unique identifier/object reference for the virtual GPU                                     | Read only |
| <code>vm-uuid</code>        | The unique identifier/object reference for the VM to which the virtual GPU is assigned         | Read only |
| <code>vm-name-label</code>  | The name of the VM to which the virtual GPU is assigned                                        | Read only |
| <code>gpu-group-uuid</code> | The unique identifier/object reference for the GPU group in which the virtual GPU is contained | Read only |

| Parameter Name                    | Description                                                                               | Type                     |
|-----------------------------------|-------------------------------------------------------------------------------------------|--------------------------|
| <code>gpu-group-name-label</code> | The name of the GPU group in which the virtual GPU is contained                           | Read only                |
| <code>currently-attached</code>   | True if a VM with GPU Pass-Through is running, false otherwise                            | Read only                |
| <code>other-config</code>         | A list of key/value pairs that specify extra configuration parameters for the virtual GPU | Read/write map parameter |
| <code>type-uuid</code>            | The unique identifier/object reference for the virtual GPU type of this virtual GPU       | Read/write map parameter |
| <code>type-model-name</code>      | Model name associated with the virtual GPU type                                           | Read only                |

### Virtual GPU type parameters

**Note:**

GPU Passthrough and virtual GPUs are not compatible with XenMotion, Storage XenMotion, 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 XenMotion, Storage XenMotion, and VM Suspend, see [Graphics](#).

Virtual GPU Types have the following parameters:

| Parameter Name            | Description                                                     | Type      |
|---------------------------|-----------------------------------------------------------------|-----------|
| <code>uuid</code>         | The unique identifier/object reference for the virtual GPU type | Read only |
| <code>vendor-name</code>  | Name of virtual GPU vendor                                      | Read only |
| <code>model-name</code>   | Model name associated with the virtual GPU type                 | Read only |
| <code>freeze-frame</code> | Framebuffer size of the virtual GPU type, in bytes              | Read only |

| Parameter Name                  | Description                                                  | Type      |
|---------------------------------|--------------------------------------------------------------|-----------|
| <code>max-heads</code>          | Maximum number of displays supported by the virtual GPU type | Read only |
| <code>supported-on-PGPUs</code> | List of pGPUs that support this virtual GPU type             | Read only |
| <code>enabled-on-PGPUs</code>   | List of pGPUs that have this virtual GPU type enabled        | Read only |
| <code>VGPU-uuids</code>         | List of virtual GPUs of this type                            | Read only |

## Virtual GPU operations

### **vgpu-create**

```
1 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**

```
1 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_vm param-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 XenServer host.

XenServer hosts are the physical servers running XenServer 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 XenServer host 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 XenServer hosts on which to perform the operation. The simplest is by supplying the argument `host=uuid_or_name_label`. You can also specify XenServer by filtering the full list of hosts on the values of fields. For example, specifying `enabled=true` selects all XenServer hosts whose `enabled` field is equal to `true`. Where multiple XenServer hosts match and the operation can be performed on multiple XenServer hosts, 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 XenServer hosts are given, the operation is performed on all XenServer hosts.

## Host parameters

XenServer hosts have the following parameters:

| Parameter Name                 | Description                                                                                                                                                                                         | Type       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>uuid</code>              | The unique identifier/object reference for the XenServer host                                                                                                                                       | Read only  |
| <code>name-label</code>        | The name of the XenServer host                                                                                                                                                                      | Read/write |
| <code>name-description</code>  | The description string of the XenServer host                                                                                                                                                        | Read only  |
| <code>enabled</code>           | Value is <code>false</code> if disabled. This prevents any new VMs from starting on the hosts and prepares the hosts to be shut down or rebooted. Value is <code>true</code> if the host is enabled | Read only  |
| <code>API-version-major</code> | Major version number                                                                                                                                                                                | Read only  |

| Parameter Name                                 | Description                                                                                                                                                                                                                                        | Type                     |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>API-version-minor</code>                 | Minor version number                                                                                                                                                                                                                               | Read only                |
| <code>API-version-vendor</code>                | Identification of API vendor                                                                                                                                                                                                                       | Read only                |
| <code>API-version-vendor-implementation</code> | Details of vendor implementation                                                                                                                                                                                                                   | Read only map parameter  |
| <code>logging</code>                           | Logging configuration                                                                                                                                                                                                                              | Read/write map parameter |
| <code>suspend-image-sr-uuid</code>             | The unique identifier/object reference for the SR where suspended images are put                                                                                                                                                                   | Read/write               |
| <code>crash-dump-sr-uuid</code>                | The unique identifier/object reference for the SR where crash dumps are put                                                                                                                                                                        | Read/write               |
| <code>software-version</code>                  | List of versioning parameters and their values                                                                                                                                                                                                     | Read only map parameter  |
| <code>capabilities</code>                      | List of Xen versions that the XenServer host can run                                                                                                                                                                                               | Read only set parameter  |
| <code>other-config</code>                      | A list of key/value pairs that specify extra configuration parameters for the XenServer host                                                                                                                                                       | Read/write map parameter |
| <code>chipset-info</code>                      | A list of key/value pairs that specify information about the chipset                                                                                                                                                                               | Read only map parameter  |
| <code>hostname</code>                          | XenServer host hostname                                                                                                                                                                                                                            | Read only                |
| <code>address</code>                           | XenServer host IP address                                                                                                                                                                                                                          | Read only                |
| <code>license-server</code>                    | 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 <a href="#">Change port numbers</a> | Read only map parameter  |

| Parameter Name                     | Description                                                                                                                                         | Type                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>supported-bootloaders</code> | List of bootloaders that the XenServer host supports, for example, pygrub, eliloader                                                                | Read only set parameter  |
| <code>memory-total</code>          | Total amount of physical RAM on the XenServer host, in bytes                                                                                        | Read only                |
| <code>memory-free</code>           | Total amount of physical RAM remaining that can be allocated to VMs, in bytes                                                                       | Read only                |
| <code>host-metrics-live</code>     | True if the host is operational                                                                                                                     | Read only                |
| <code>logging</code>               | The <code>syslog_destination</code> key can be set to the hostname of a remote listening syslog service.                                            | Read/write map parameter |
| <code>allowed-operations</code>    | 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  |
| <code>current-operations</code>    | 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  |
| <code>patches</code>               | Set of host patches                                                                                                                                 | Read only set parameter  |
| <code>blobs</code>                 | Binary data store                                                                                                                                   | Read only                |
| <code>memory-free-computed</code>  | A conservative estimate of the maximum amount of memory free on a host                                                                              | Read only                |
| <code>ha-statefiles</code>         | The UUIDs of all HA state files                                                                                                                     | Read only                |
| <code>ha-network-peers</code>      | The UUIDs of all hosts that could host the VMs on this host if there is a failure                                                                   | Read only                |

| Parameter Name                           | Description                                                        | Type                    |
|------------------------------------------|--------------------------------------------------------------------|-------------------------|
| <code>external-auth-type</code>          | Type of external authentication, for example, Active Directory.    | Read only               |
| <code>external-auth-service-name</code>  | The name of the external authentication service                    | Read only               |
| <code>external-auth-configuration</code> | Configuration information for the external authentication service. | Read only map parameter |

XenServer hosts contain some other objects that also have parameter lists.

CPUs on XenServer hosts have the following parameters:

| Parameter Name           | Description                                                                        | Type      |
|--------------------------|------------------------------------------------------------------------------------|-----------|
| <code>uuid</code>        | The unique identifier/object reference for the CPU                                 | Read only |
| <code>number</code>      | The number of the physical CPU core within the XenServer host                      | Read only |
| <code>vendor</code>      | The vendor string for the CPU name                                                 | Read only |
| <code>speed</code>       | The CPU clock speed, in Hz                                                         | Read only |
| <code>modelName</code>   | The vendor string for the CPU model, for example, "Intel(R) Xeon(TM) CPU 3.00 GHz" | Read only |
| <code>stepping</code>    | The CPU revision number                                                            | Read only |
| <code>flags</code>       | The flags of the physical CPU (a decoded version of the features field)            | Read only |
| <code>Utilisation</code> | The current CPU utilization                                                        | Read only |
| <code>host-uuid</code>   | The UUID of the host the CPU is in                                                 | Read only |
| <code>model</code>       | The model number of the physical CPU                                               | Read only |



| Parameter Name      | Description                    | Type      |
|---------------------|--------------------------------|-----------|
| <code>family</code> | The physical CPU family number | Read only |

Crash dumps on XenServer hosts have the following parameters:

| Parameter Name         | Description                                                                                                                                                             | Type      |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>uuid</code>      | The unique identifier/object reference for the crashdump                                                                                                                | Read only |
| <code>host</code>      | XenServer host the crashdump corresponds to                                                                                                                             | Read only |
| <code>timestamp</code> | Timestamp of the date and time that the crashdump occurred, in the form <code>yyyymmdd-hhmmss-ABC</code> , where <i>ABC</i> is the timezone indicator, for example, GMT | Read only |
| <code>size</code>      | Size of the crashdump, in bytes                                                                                                                                         | Read only |

## host-all-editions

```
1 host-all-editions
```

Get a list of all available editions

## host-apply-edition

```
1 host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition="
 free" "per-socket" "xendesktop"]
```

Assigns the XenServer license to a host server. When you assign a license, XenServer 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 XenServer for Citrix Virtual Desktops editions, use `"xendesktop"`.

For initial licensing configuration, see also `license-server-address` and `license-server-port`.

## host-backup

```
1 host-backup file-name=backup_filename host=host_name
```

Download a backup of the control domain of the specified XenServer host 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 hostname 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

```
1 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 Citrix 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 Citrix Support ftp site.

## host-call-plugin

```
1 host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args=
 args]
```

Calls the function within the plugin on the given host with optional arguments.

**host-compute-free-memory**

```
1 host-compute-free-memory
```

Computes the amount of free memory on the host.

**host-compute-memory-overhead**

```
1 host-compute-memory-overhead
```

Computes the virtualization memory overhead of a host.

**host-cpu-info**

```
1 host-cpu-info [uuid=uuid]
```

Lists information about the host's physical CPUs.

**host-crashdump-destroy**

```
1 host-crashdump-destroy uuid=crashdump_uuid
```

Delete a host crashdump specified by its UUID from the XenServer host.

**host-crashdump-upload**

```
1 host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [http-
 proxy=http_proxy_name]
```

Upload a crashdump to the Citrix Support ftp site or other location. If optional parameters are not used, no proxy server is identified and the destination is the default Citrix Support ftp site. Optional parameters are [http-proxy](#): use specified http proxy, and [url](#): upload to this destination URL.

**host-declare-dead**

```
1 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**

```
1 host-disable [host-selector=host_selector_value...]
```

Disables the specified XenServer hosts, which prevents any new VMs from starting on them. This action prepares the XenServer hosts 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**

```
1 host-disable-display uuid=host_uuid
```

Disable display for the host.

**host-disable-local-storage-caching**

```
1 host-disable-local-storage-caching
```

Disable local storage caching on the specified host.

**host-dmesg**

```
1 host-dmesg [host-selector=host_selector_value...]
```

Get a Xen `dmesg` (the output of the kernel ring buffer) from specified XenServer hosts.

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**

```
1 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**

```
1 host-emergency-management-reconfigure interface=
 uuid_of_management_interface_pif
```

Reconfigure the management interface of this XenServer host. Use this command only if the XenServer host 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-enable**

```
1 host-enable [host-selector=host_selector_value...]
```

Enables the specified XenServer hosts, 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**

```
1 host-enable-display uuid=host_uuid
```

Enable display for the host.

**host-enable-local-storage-caching**

```
1 host-enable-local-storage-caching sr-uuid=sr_uuid
```

Enable local storage caching on the specified host.

## host-evacuate

```
1 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

```
1 host-forget uuid=host_uuid
```

The XAPI agent forgets about the specified XenServer host 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.

### Tip:

This command is useful if the XenServer host to “forget” is dead. However, if the XenServer host is live and part of the pool, use `xe pool-eject` instead.

## host-get-cpu-features

```
1 host-get-cpu-features {
2 features=pool_master_cpu_features }
3 [uuid=host_uuid]
```

Prints a hexadecimal representation of the host's physical-CPU features.

## host-get-server-certificate

```
1 host-get-server-certificate
```

Get the installed server SSL certificate.

## host-get-sm-diagnostics

```
1 host-get-sm-diagnostics uuid=uuid
```

Display per-host SM diagnostic information.

## host-get-system-status

```
1 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

```
1 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:

```
1 <?xml version="1.0" ?>
2 <system-status-capabilities>
3 <capability content-type="text/plain" default-checked="yes" key="
 xenserver-logs" \
```

```

4 max-size="150425200" max-time="-1" min-size="150425200" min-
 time="-1" \
5 pii="maybe"/>
6 <capability content-type="text/plain" default-checked="yes" \
7 key="xenserver-install" max-size="51200" max-time="-1" min-size
 ="10240" \
8 min-time="-1" pii="maybe"/>
9 ...
10 </system-status-capabilities>
11
12 <?xml version="1.0" ?>
13 <system-status-capabilities>
14 <capability content-type="text/plain" default-checked="yes" key="
 incloudsphere-logs" \
15 max-size="150425200" max-time="-1" min-size="150425200" min-
 time="-1" \
16 pii="maybe"/>
17 <capability content-type="text/plain" default-checked="yes" \
18 key="incloudsphere-install" max-size="51200" max-time="-1" min-
 size="10240" \
19 min-time="-1" pii="maybe"/>
20 ...
21 </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**

```
1 host-get-thread-diagnostics uuid=uuid
```

Display per-host thread diagnostic information.

### **host-get-vms-which-prevent-evacuation**

```
1 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**

```
1 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 slave hosts even with no master host present.

### **host-license-add**

```
1 host-license-add [license-file=path/license_filename] [host-uuid=host_uuid]
```

For XenServer (free edition), use to parse a local license file and add it to the specified XenServer host.

### **host-license-remove**

```
1 host-license-remove [host-uuid=host_uuid]
```

Remove any licensing applied to a host.

## host-license-view

```
1 host-license-view [host-uuid=host_uuid]
```

Displays the contents of the XenServer host license.

## host-logs-download

```
1 host-logs-download [file-name=logfile_name] [host-selector=
 host_selector_value...]
```

Download a copy of the logs of the specified XenServer hosts. 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 filename 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 hostname 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

```
1 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 XenServer host the CLI is connected to. The command is not forwarded to the pool master when applied to a member XenServer host.

### 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

```
1 host-management-reconfigure [interface=device] [pif-uuid=uuid]
```

Reconfigures the XenServer host 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 XenServer host immediately rebinds. This command works both in normal and emergency mode.

If the UUID of a PIF object is specified, the XenServer host 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 reach the XenServer host.

## host-power-on

```
1 host-power-on [host=host_uuid]
```

Turns on power on XenServer hosts with the *Host Power On* function enabled. Before using this command, enable `host-set-power-on` on the host.

## host-reboot

```
1 host-reboot [host-selector=host_selector_value...]
```

Reboot the specified XenServer hosts. 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 XenServer hosts are members of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the XenServer hosts 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**

```
1 host-restore [file-name=backup_filename] [host-selector=
 host_selector_value...]
```

Restore a backup named `file-name` of the XenServer host 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**

```
1 host-send-debug-keys host-uuid=host_uuid keys=keys
```

Send specified hypervisor debug keys to specified host.

## **host-set-hostname-live**

```
1 host-set-hostname host-uuid=uuid_of_host hostname=new_hostname
```

Change the hostname of the XenServer host specified by `host-uuid`. This command persistently sets both the hostname in the control domain database and the actual Linux hostname of the XenServer host. The value of `hostname` is *not* the same as the value of the `name_label` field.

## **host-set-power-on-mode**

```
1 host-set-power-on-mode host=host_uuid power-on-mode={
2 """ | "wake-on-lan" | "iLO" | "DRAC" | "custom" }
3 \
```

```
4 [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 XenServer 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

```
1 host-shutdown [host-selector=host_selector_value...]
```

Shut down the specified XenServer hosts. The specified XenServer 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 XenServer hosts are members of a pool, the loss of connectivity on shutdown is handled and the pool recovers when the XenServer hosts 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

```
1 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 will delete all records of the datapath even if it could not be shutdown cleanly.

## host-sync-data

```
1 host-sync-data
```

Synchronise the non-database data stored on the pool master with the named host.

## host-syslog-reconfigure

```
1 host-syslog-reconfigure [host-selector=host_selector_value...]
```

Reconfigure the `syslog` daemon on the specified XenServer hosts. 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

```
1 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**

```
1 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**

```
1 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**

```
1 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.

## **Log commands**

Commands for working with logs.

**log-get**

```
1 log-get
```

Return the log currently stored in the string logger.

**log-get-keys**

```
1 log-get-keys
```

List the keys known by the logger.

**log-reopen**

```
1 log-reopen
```

Reopen all loggers (use this for rotating files).

**log-set-output**

```
1 log-set-output output=output [key=key] [level=level]
```

Set all loggers to the specified output (nil, stderr, string, file:*filename*, 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      |
|------------------------|----------------------------------------------------------------|-----------|
| <code>uuid</code>      | The unique identifier/object reference for the message         | Read only |
| <code>name</code>      | The unique name of the message                                 | Read only |
| <code>priority</code>  | The message priority. Higher numbers indicate greater priority | Read only |
| <code>class</code>     | The message class, for example VM.                             | Read only |
| <code>obj-uuid</code>  | The uuid of the affected object.                               | Read only |
| <code>timestamp</code> | The time that the message was generated.                       | Read only |
| <code>body</code>      | The message content.                                           | Read only |

### **message-create**

```
1 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**

```
1 message-destroy [uuid=message_uuid]
```

Destroys an existing message. You can build a script to destroy all messages. For example:

```
1 # Dismiss all alerts \
2 IFS=","; for m in $(xe message-list params=uuid --minimal); do \
3 xe message-destroy uuid=$m \
4 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                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <code>uuid</code>                 | The unique identifier/object reference for the network                                                                                                                                                       | Read only               |
| <code>name-label</code>           | The name of the network                                                                                                                                                                                      | Read/write              |
| <code>name-description</code>     | The description text of the network                                                                                                                                                                          | Read/write              |
| <code>VIF-uuids</code>            | A list of unique identifiers of the VIFs (virtual network interfaces) that are attached from VMs to this network                                                                                             | Read only set parameter |
| <code>PIF-uuids</code>            | A list of unique identifiers of the PIFs (physical network interfaces) that are attached from XenServer hosts to this network                                                                                | Read only set parameter |
| <code>bridge</code>               | Name of the bridge corresponding to this network on the local XenServer host                                                                                                                                 | Read only               |
| <code>default-locking-mode</code> | A network object used with VIF objects for ARP filtering. Set to <code>unlocked</code> to remove all the filtering rules associated with the VIF. Set to <code>disabled</code> so the VIF drops all traffic. | Read/write              |

| Parameter Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                       | Type       |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>purpose</code>                     | Set of purposes for which the XenServer host uses this network. Set to <code>nbd</code> to use the network to make NBD connections.                                                                                                                                                                                                                                                               | Read/write |
| <code>other-config:staticroutes</code>   | Comma-separated list of <i>subnet/netmask/gateway</i> formatted entries specifying the gateway address through which to route subnets. For example, setting <code>other-config:static-routes</code> to <code>172.16.0.0/15/192.168.0.3,172.18.0.0/16/192.168.0.4</code> 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 |
| <code>other-config:ethtoolautoneg</code> | Set to no to disable autonegotiation of the physical interface or bridge. Default is yes.                                                                                                                                                                                                                                                                                                         | Read/write |
| <code>other-config:ethtool-rx</code>     | Set to on to enable receive checksum, off to disable                                                                                                                                                                                                                                                                                                                                              | Read/write |
| <code>other-config:ethtool-tx</code>     | Set to on to enable transmit checksum, off to disable                                                                                                                                                                                                                                                                                                                                             | Read/write |
| <code>other-config:ethtool-sg</code>     | Set to on to enable scatter gather, off to disable                                                                                                                                                                                                                                                                                                                                                | Read/write |
| <code>other-config:ethtool-tso</code>    | Set to on to enable tcp segmentation offload, off to disable                                                                                                                                                                                                                                                                                                                                      | Read/write |
| <code>other-config:ethtool-ufo</code>    | Set to on to enable UDP fragment offload, off to disable                                                                                                                                                                                                                                                                                                                                          | Read/write |
| <code>other-config:ethtool-gso</code>    | Set to on to enable generic segmentation offload, off to disable                                                                                                                                                                                                                                                                                                                                  | Read/write |

| Parameter Name     | Description       | Type      |
|--------------------|-------------------|-----------|
| <code>blobs</code> | Binary data store | Read only |

## network-create

```
1 network-create name=label=name_for_network [name-description=
 descriptive_text]
```

Creates a network.

## network-destroy

```
1 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      |
|------------------------------|---------------------------------------------------------------------------------------|-----------|
| <code>physical-PIF</code>    | The PIF to enable SR-IOV.                                                             | Read only |
| <code>logical-PIF</code>     | An SR-IOV logical PIF. Users can use this parameter to create an SR-IOV VLAN network. | Read only |
| <code>requires-reboot</code> | If set to True, used to reboot host to bring SR-IOV enabling into effect.             | Read only |

| Parameter Name                  | Description                        | Type      |
|---------------------------------|------------------------------------|-----------|
| <code>remaining-capacity</code> | Number of available VFs remaining. | Read only |

### **network-sriov-create**

```
1 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**

```
1 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**

```
1 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**

```
1 sdn-controller-introduce [address=address] [protocol=protocol] [tcp-port=tcp_port]
```

Introduce an SDN controller.

## **sdn-controller-introduce**

```
1 sdn-controller-forget uuid=uuid
```

Remove an SDN controller.

## **Tunnel commands**

Commands for working with tunnels.

### **tunnel-create**

```
1 tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
```

Create a new tunnel on a host.

### **tunnel-destroy**

```
1 tunnel-destroy uuid=uuid
```

Destroy a tunnel.

## **Patch commands**

Commands for working with patches.

### **patch-apply**

```
1 patch-apply uuid=patch_uuid host-uuid=host_uuid
```

Apply the previously uploaded patch to the specified host.

### **patch-clean**

```
1 patch-clean uuid=uuid
```

Delete a previously uploaded patch file.

**patch-destroy**

```
1 patch-destroy uuid=uuid
```

Remove an unapplied patch record and files from the server.

**patch-pool-apply**

```
1 patch-pool-apply uuid=uuid
```

Apply the previously uploaded patch to all hosts in the pool.

**patch-pool-clean**

```
1 patch-pool-clean uuid=uuid
```

Delete a previously uploaded patch file on all hosts in the pool.

**patch-precheck**

```
1 patch-precheck uuid=uuid host-uuid=host_uuid
```

Run the prechecks contained within the patch previously uploaded to the specified host.

**patch-upload**

```
1 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 XenServer host 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                     |
|---------------------------------|-------------------------------------------------------------------------------------|--------------------------|
| <code>uuid</code>               | The unique identifier/object reference for the PBD.                                 | Read only                |
| <code>sr-uuid</code>            | The storage repository that the PBD points to                                       | Read only                |
| <code>device-config</code>      | Extra configuration information that is provided to the SR-backend-driver of a host | Read only map parameter  |
| <code>currently-attached</code> | True if the SR is attached on this host, False otherwise                            | Read only                |
| <code>host-uuid</code>          | UUID of the physical machine on which the PBD is available                          | Read only                |
| <code>host</code>               | The host field is deprecated. Use <code>host_uuid</code> instead.                   | Read only                |
| <code>other-config</code>       | Extra configuration information.                                                    | Read/write map parameter |

## pbd-create

```
1 pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:key
 =corresponding_value]
```

Create a PBD on your XenServer host. 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

```
1 pbd-destroy uuid=uuid_of_pbd
```



Destroy the specified PBD.

### **pbd-plug**

```
1 pbd-plug uuid=uuid_of_pbd
```

Attempts to plug in the PBD to the XenServer host. If this command succeeds, the referenced SR (and the VDIs contained within) should then become visible to the XenServer host.

### **pbd-unplug**

```
1 pbd-unplug uuid=uuid_of_pbd
```

Attempt to unplug the PBD from the XenServer host.

## **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                     |
|-----------------------------------------|-----------------------------------------------------------------|--------------------------|
| <a href="#">uuid</a>                    | The unique identifier/object reference for the PIF              | Read only                |
| <a href="#">device machine-readable</a> | Name of the interface (for example, eth0)                       | Read only                |
| <a href="#">MAC</a>                     | The MAC address of the PIF                                      | Read only                |
| <a href="#">other-config</a>            | Extra PIF configuration <a href="#">name:value</a> pairs.       | Read/write map parameter |
| <a href="#">physical</a>                | If true, the PIF points to an actual physical network interface | Read only                |

| Parameter Name                     | Description                                                                                        | Type      |
|------------------------------------|----------------------------------------------------------------------------------------------------|-----------|
| <code>currently-attached</code>    | Is the PIF currently attached on this host? <b>true</b> or <b>false</b>                            | Read only |
| <code>MTU</code>                   | Maximum Transmission Unit of the PIF in bytes.                                                     | Read only |
| <code>VLAN</code>                  | VLAN tag for all traffic passing through this interface. -1 indicates that no VLAN tag is assigned | Read only |
| <code>bond-master-of</code>        | The UUID of the bond this PIF is the master of (if any)                                            | Read only |
| <code>bond-slave-of</code>         | The UUID of the bond this PIF is the slave of (if any)                                             | Read only |
| <code>management</code>            | Is this PIF designated to be a management interface for the control domain                         | Read only |
| <code>network-uuid</code>          | The unique identifier/object reference of the virtual network to which this PIF is connected       | Read only |
| <code>network-name-label</code>    | The name of the virtual network to which this PIF is connected                                     | Read only |
| <code>host-uuid</code>             | The unique identifier/object reference of the XenServer host to which this PIF is connected        | Read only |
| <code>host-name-label</code>       | The name of the XenServer host to which this PIF is connected                                      | Read only |
| <code>IP-configuration-mode</code> | Type of network address configuration used; DHCP or static                                         | Read only |

| Parameter Name            | Description                                                                                                    | Type      |
|---------------------------|----------------------------------------------------------------------------------------------------------------|-----------|
| <code>IP</code>           | IP address of the PIF. Defined here when IP-configuration-mode is static; undefined when DHCP                  | Read only |
| <code>netmask</code>      | Netmask of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP         | Read only |
| <code>gateway</code>      | Gateway address of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP | Read only |
| <code>DNS</code>          | DNS address of the PIF. Defined here when IP-configuration-mode is static; undefined when supplied by DHCP     | Read only |
| <code>io_read_kbs</code>  | Average read rate in kB/s for the device                                                                       | Read only |
| <code>io_write_kbs</code> | Average write rate in kB/s for the device                                                                      | Read only |
| <code>carrier</code>      | Link state for this device                                                                                     | Read only |
| <code>vendor-id</code>    | The ID assigned to NIC's vendor                                                                                | Read only |
| <code>vendor-name</code>  | The NIC vendor's name                                                                                          | Read only |
| <code>device-id</code>    | The ID assigned by the vendor to this NIC model                                                                | Read only |
| <code>device-name</code>  | The name assigned by the vendor to this NIC model                                                              | Read only |
| <code>speed</code>        | Data transfer rate of the NIC                                                                                  | Read only |
| <code>duplex</code>       | Duplexing mode of the NIC; full or half                                                                        | Read only |

| Parameter Name                            | Description                                                                                                                                      | Type       |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>pci-bus-path</code>                 | PCI bus path address                                                                                                                             | Read only  |
| <code>other-config:ethtool-speed</code>   | Sets the speed of connection in Mbps                                                                                                             | Read/write |
| <code>other-config:ethtool-autoneg</code> | Set to no to disable autonegotiation of the physical interface or bridge. Default is yes.                                                        | Read/write |
| <code>other-config:ethtool-duplex</code>  | Sets duplexing capability of the PIF, either full or half.                                                                                       | Read/write |
| <code>other-config:ethtool-rx</code>      | Set to on to enable receive checksum, off to disable                                                                                             | Read/write |
| <code>other-config:ethtool-tx</code>      | Set to on to enable transmit checksum, off to disable                                                                                            | Read/write |
| <code>other-config:ethtool-sg</code>      | Set to on to enable scatter gather, off to disable                                                                                               | Read/write |
| <code>other-config:ethtool-tso</code>     | Set to on to enable tcp segmentation offload, off to disable                                                                                     | Read/write |
| <code>other-config:ethtool-ufo</code>     | Set to on to enable udp fragment offload, off to disable                                                                                         | Read/write |
| <code>other-config:ethtool-gso</code>     | Set to on to enable generic segmentation offload, off to disable                                                                                 | Read/write |
| <code>other-config:domain</code>          | Comma-separated list used to set the DNS search path                                                                                             | Read/write |
| <code>other-config:bondmiimon</code>      | Interval between link liveness checks, in milliseconds                                                                                           | Read/write |
| <code>other-config:bond-downdelay</code>  | 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 |

| Parameter Name                             | Description                                                                                                                                                                                      | Type       |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>other-config:<br/>bondupdelay</code> | 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 |
| <code>disallow-unplug</code>               | 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**

```
1 pif-forget uuid=uuid_of_pif
```

Destroy the specified PIF object on a particular host.

**pif-introduce**

```
1 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 XenServer host.

**pif-plug**

```
1 pif-plug uuid=uuid_of_pif
```

Attempt to bring up the specified physical interface.

## **pif-reconfigure-ip**

```
1 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**

```
1 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**

```
1 pif-scan host-uuid=host_uuid
```

Scan for new physical interfaces on your XenServer host.

## **pif-set-primary-address-type**

```
1 pif-set-primary-address-type uuid=uuid primary_address_type=
 address_type
```

Change the primary address type used by this PIF.

## **pif-unplug**

```
1 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 XenServer hosts. 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 XenServer host is really a pool consisting of a single member by default. When your XenServer host 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       |
|-------------------------------|---------------------------------------------------------------------------------------------------|------------|
| <code>uuid</code>             | The unique identifier/object reference for the pool                                               | Read only  |
| <code>name-label</code>       | The name of the pool                                                                              | Read/write |
| <code>name-description</code> | The description string of the pool                                                                | Read/write |
| <code>master</code>           | The unique identifier/object reference of XenServer host designated as the pool's master          | Read only  |
| <code>default-SR</code>       | The unique identifier/object reference of the default SR for the pool                             | Read/write |
| <code>crash-dump-SR</code>    | The unique identifier/object reference of the SR where any crash dumps for pool members are saved | Read/write |
| <code>metadata-vdis</code>    | All known metadata VDIs for the pool                                                              | Read only  |

| Parameter Name                            | Description                                                                                                  | Type                     |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>suspend-image-SR</code>             | The unique identifier/object reference of the SR where suspended VMs on pool members are saved               | Read/write               |
| <code>other-config</code>                 | A list of key/value pairs that specify extra configuration parameters for the pool                           | Read/write map parameter |
| <code>supported-sr-types</code>           | SR types that this pool can use                                                                              | Read only                |
| <code>ha-enabled</code>                   | True if HA is enabled for the pool, false otherwise                                                          | Read only                |
| <code>ha-configuration</code>             | Reserved for future use.                                                                                     | Read only                |
| <code>ha-statefiles</code>                | Lists the UUIDs of the VDIs being used by HA to determine storage health                                     | Read only                |
| <code>ha-host-failures-to-tolerate</code> | The number of host failures to tolerate before sending a system alert                                        | Read/write               |
| <code>ha-plan-exists-for</code>           | The number of hosts failures that can actually be handled, according to the calculations of the HA algorithm | Read only                |
| <code>ha-allow-overcommit</code>          | True if the pool is allowed to be overcommitted, False otherwise                                             | Read/write               |
| <code>ha-overcommitted</code>             | True if the pool is overcommitted                                                                            | Read only                |
| <code>blobs</code>                        | Binary data store                                                                                            | Read only                |
| <code>live-patching-disabled</code>       | Set to False to enable live patching. Set to True to disable live patching.                                  | Read/write               |
| <code>igmp-snooping-enabled</code>        | Set to True to enable IGMP snooping. Set to False to disable IGMP snooping.                                  | Read/write               |



### **pool-apply-edition**

```
1 pool-apply-edition edition=edition [uuid=uuid] [license-server-address=address] [license-server-port=port]
```

Apply an edition across the pool.

### **pool-certificate-install**

```
1 pool-certificate-install filename=file_name
```

Install an SSL certificate, pool-wide.

### **pool-certificate-list**

```
1 pool-certificate-list
```

List all installed SSL certificates.

### **pool-certificate-sync**

```
1 pool-certificate-sync
```

Sync SSL certificates and certificate revocation lists from master to slaves.

### **pool-certificate-uninstall**

```
1 pool-certificate-uninstall name=name
```

Uninstall an SSL certificate.

### **pool-crl-install**

```
1 pool-crl-install filename=file_name
```

Install an SSL certificate revocation list, pool-wide.

**pool-crl-list**

```
1 pool-crl-list
```

List all installed SSL certificate revocation lists.

**pool-crl-uninstall**

```
1 pool-crl-uninstall name=name
```

Uninstall an SSL certificate revocation list.

**pool-deconfigure-wlb**

```
1 pool-deconfigure-wlb
```

Permanently remove the configuration for workload balancing.

**pool-designate-new-master**

```
1 pool-designate-new-master host-uuid=uuid_of_new_master
```

Instruct the specified member XenServer host 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**

```
1 pool-disable-external-auth [uuid=uuid] [config=config]
```

Disables external authentication in all the hosts in a pool.

**pool-disable-local-storage-caching**

```
1 pool-disable-local-storage-caching uuid=uuid
```

Disable local storage caching across the pool.

**pool-disable-redo-log**

```
1 pool-disable-redo-log
```

Disable the redo log if in use, unless HA is enabled.

**pool-disable-ssl-legacy**

```
1 pool-disable-ssl-legacy [uuid=uuid]
```

Set ssl-legacy to False on each host.

**pool-dump-database**

```
1 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**

```
1 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**

```
1 pool-enable-local-storage-caching uuid=uuid
```

Enable local storage caching across the pool.

**pool-enable-redo-log**

```
1 pool-enable-redo-log sr-uuid=sr_uuid
```

Enable the redo log on the given SR if in use, unless HA is enabled.

**pool-enable-ssl-legacy**

```
1 pool-enable-ssl-legacy [uuid=uuid]
```

Set ssl-legacy to True on each host.”

**pool-eject**

```
1 pool-eject host-uuid=uuid_of_host_to_eject
```

Instruct the specified XenServer host to leave an existing pool.

**pool-emergency-reset-master**

```
1 pool-emergency-reset-master master-address=address_of_pool_master
```

Instruct a slave member XenServer host to reset its master address to the new value and attempt to connect to it. Do not run this command on master hosts.

**pool-emergency-transition-to-master**

```
1 pool-emergency-transition-to-master
```

Instruct a member XenServer host to become the pool master. The XenServer host 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**

```
1 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**

```
1 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**

```
1 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**

```
1 pool-initialize-wlb wlb_url=url wlb_username=wb_username wlb_password=
wlb_password xenserver_username=username xenserver_password=password
```

Initialize workload balancing for the current pool with the target WLB server.

**pool-join**

```
1 pool-join master-address=address master-username=username master-
password=password
```

Instruct your XenServer host to join an existing pool.

**pool-management-reconfigure**

```
1 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 XenServer 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 XenServer host, 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 do not reach the XenServer host.

**pool-recover-slaves**

```
1 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**

```
1 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**

```
1 pool-retrieve-wlb-configuration
```

Retrieves the pool optimization criteria from the Workload Balancing server.

**pool-retrieve-wlb-diagnostics**

```
1 pool-retrieve-wlb-diagnostics [filename=file_name]
```

Retrieves diagnostics from the Workload Balancing server.

### **pool-retrieve-wlb-recommendations**

```
1 pool-retrieve-wlb-recommendations
```

Retrieves VM migrate recommendations for the pool from the Workload Balancing server.

### **pool-retrieve-wlb-report**

```
1 pool-retrieve-wlb-report report=report [filename=file_name]
```

Retrieves reports from the Workload Balancing server.

### **pool-send-test-post**

```
1 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 SSL layer.

### **pool-send-wlb-configuration**

```
1 pool-send-wlb-configuration [config:=config]
```

Sets the pool optimization criteria for the Workload Balancing server.

### **pool-sync-database**

```
1 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**

```
1 pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|false]
```

Enables or disables IGMP snooping on a XenServer pool.

**PVS Accelerator commands**

Commands for working with the PVS Accelerator.

**pvs-cache-storage-create**

```
1 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**

```
1 pvs-cache-storage-destroy uuid=uuid
```

Remove a PVS cache.

**pvs-proxy-create**

```
1 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**

```
1 pvs-proxy-destroy uuid=uuid
```

Remove (or switch off) a PVS proxy for this VIF/VM.



**pvs-server-forget**

```
1 pvs-server-forget uuid=uuid
```

Forget a PVS server.

**pvs-server-introduce**

```
1 pvs-server-introduce addresses=addresses first-port=first_port last-port=
=last_port pvs-site-uuid=pvs_site_uuid
```

Introduce new PVS server.

**pvs-site-forget**

```
1 pvs-site-forget uuid=uuid
```

Forget a PVS site.

**pvs-site-introduce**

```
1 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 plugins.

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      |
|-----------------------------------|----------------------------------------------------------|-----------|
| <code>uuid</code>                 | The unique identifier/object reference for the SM plugin | Read only |
| <code>name-label</code>           | The name of the SM plugin                                | Read only |
| <code>name-description</code>     | The description string of the SM plugin                  | Read only |
| <code>type</code>                 | The SR type that this plugin connects to                 | Read only |
| <code>vendor</code>               | Name of the vendor who created this plugin               | Read only |
| <code>copyright</code>            | Copyright statement for this SM plugin                   | Read only |
| <code>required-api-version</code> | Minimum SM API version required on the XenServer host    | Read only |
| <code>configuration</code>        | Names and descriptions of device configuration keys      | Read only |
| <code>capabilities</code>         | Capabilities of the SM plugin                            | Read only |
| <code>driver-filename</code>      | The filename of the SR driver.                           | Read only |

## Snapshot commands

Commands for working with snapshots.

### snapshot-clone

```
1 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

```
1 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**

```
1 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**

```
1 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**

```
1 snapshot-export-to-template filename=file_name snapshot-uuid=
snapshot_uuid [preserve-power-state=true|false]
```

Export a snapshot to *filename*.

### **snapshot-reset-powerstate**

```
1 snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--
force]
```

Force the VM powerstate 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 (ie. you will not be able to resume your snapshot anymore).

## snapshot-revert

```
1 snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

Revert an existing VM to a previous checkpointed or snapshot state.

## snapshot-uninstall

```
1 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                    |
|---------------------------------|------------------------------------------------------------------|-------------------------|
| <code>uuid</code>               | The unique identifier/object reference for the SR                | Read only               |
| <code>name-label</code>         | The name of the SR                                               | Read/write              |
| <code>name-description</code>   | The description string of the SR                                 | Read/write              |
| <code>allowed-operations</code> | List of the operations allowed on the SR in this state           | Read only set parameter |
| <code>current-operations</code> | List of the operations that are currently in progress on this SR | Read only set parameter |

| Parameter Name                    | Description                                                                                                                                                                                                                                                             | Type                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>VDIs</code>                 | Unique identifier/object reference for the virtual disks in this SR                                                                                                                                                                                                     | Read only set parameter  |
| <code>PBDs</code>                 | Unique identifier/object reference for the PBDs attached to this SR                                                                                                                                                                                                     | Read only set parameter  |
| <code>physical-utilisation</code> | Physical space currently utilized on this SR, in bytes. For thin provisioned disk formats, physical utilization may be less than virtual allocation                                                                                                                     | Read only                |
| <code>physical-size</code>        | Total physical size of the SR, in bytes                                                                                                                                                                                                                                 | Read only                |
| <code>type</code>                 | Type of the SR, used to specify the SR back-end driver to use                                                                                                                                                                                                           | Read only                |
| <code>introduced-by</code>        | The drtask (if any) which introduced the SR                                                                                                                                                                                                                             | Read only                |
| <code>content-type</code>         | 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, recommends that you set this parameter either to empty, or the string user. | Read only                |
| <code>shared</code>               | True if this SR can be shared between multiple XenServer hosts; False otherwise                                                                                                                                                                                         | Read/write               |
| <code>other-config</code>         | List of key/value pairs that specify extra configuration parameters for the SR                                                                                                                                                                                          | Read/write map parameter |

| Parameter Name                  | Description                                                                  | Type                    |
|---------------------------------|------------------------------------------------------------------------------|-------------------------|
| <code>host</code>               | The storage repository host name                                             | Read only               |
| <code>virtual-allocation</code> | Sum of virtual-size values of all VDIs in this storage repository (in bytes) | Read only               |
| <code>sm-config</code>          | SM dependent data                                                            | Read only map parameter |
| <code>blobs</code>              | Binary data store                                                            | Read only               |

### **sr-create**

```
1 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 XenServer host. If `shared` is set to **true**, a PBD is created for each XenServer host in the pool. If `shared` is not specified or set to **false**, a PBD is created only for the XenServer host 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**

```
1 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**

```
1 sr-data-source-list"
```

List the data sources that can be recorded for a SR.

**sr-data-source-query**

```
1 sr-data-source-query data-source=data_source
```

Query the last value read from a SR data source.

**sr-data-source-record**

```
1 sr-data-source-record data-source=data_source
```

Record the specified data source for a SR.

**sr-destroy**

```
1 sr-destroy uuid=sr_uuid
```

Destroys the specified SR on the XenServer host.

**sr-enable-database-replication**

```
1 sr-enable-database-replication uuid=sr_uuid
```

Enables XAPI database replication to the specified (shared) SR. For example:

```
1 xe sr-enable-database-replication uuid=sr-uuid
```

**sr-disable-database-replication**

```
1 sr-disable-database-replication uuid=sr_uuid
```

Disables XAPI database replication to the specified SR. For example:

```
1 xe sr-enable-database-replication uuid=sr-uuid
```

**sr-forget**

```
1 sr-forget uuid=sr_uuid
```

The XAPI agent forgets about a specified SR on the XenServer host. 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**

```
1 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:

```
1 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**

```
1 sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=
value]
```

Performs a backend-specific scan, 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 backend-specific XML, 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**

```
1 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 e.g. `device-config:devs=/dev/sdb1`. Unlike `sr-probe`, this command returns results in the same human-readable format for every SR type.



**sr-scan**

```
1 sr-scan uuid=sr_uuid
```

Force an SR scan, syncing the XAPI database with VDIs present in the underlying storage substrate.

**sr-update**

```
1 sr-update uuid=uuid
```

Refresh the fields of the SR object in the database.

**lvhd-enable-thin-provisioning**

```
1 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**

```
1 session-subject-identifier-list
```

Return a list of all the user subject ids of all externally-authenticated existing sessions.

**session-subject-identifier-logout**

```
1 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**

```
1 session-subject-identifier-logout-all
```

Log out all externally-authenticated sessions.

**subject-add**

```
1 subject-add subject-name=subject_name
```

Add a subject to the list of subjects that can access the pool.

**subject-remove**

```
1 subject-remove subject-uuid=subject_uuid
```

Remove a subject from the list of subjects that can access the pool.

**subject-role-add**

```
1 subject-role-add uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

Add a role to a subject.

**subject-role-remove**

```
1 subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
 role_uuid]
```

Remove a role from a subject.

**secret-create**

```
1 secret-create value=value
```

Create a secret.

## **secret-destroy**

```
1 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      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <a href="#">uuid</a>             | The unique identifier/object reference for the Task                                                                                                                          | Read only |
| <a href="#">name-label</a>       | The name of the Task                                                                                                                                                         | Read only |
| <a href="#">name-description</a> | The description string of the Task                                                                                                                                           | Read only |
| <a href="#">resident-on</a>      | The unique identifier/object reference of the host on which the task is running                                                                                              | Read only |
| <a href="#">status</a>           | Status of the Task                                                                                                                                                           | Read only |
| <a href="#">progress</a>         | 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 |

| Parameter Name                  | Description                                                                                                                                                                                                              | Type      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>type</code>               | 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 |
| <code>result</code>             | 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 |
| <code>error_info</code>         | If the Task has failed, this parameter contains the set of associated error strings. Otherwise, this parameter's value is undefined                                                                                      | Read only |
| <code>allowed_operations</code> | List of the operations allowed in this state                                                                                                                                                                             | Read only |
| <code>created</code>            | Time the task has been created                                                                                                                                                                                           | Read only |
| <code>finished</code>           | Time task finished (that is, succeeded or failed). If task-status is pending, then the value of this field has no meaning                                                                                                | Read only |
| <code>subtask_of</code>         | Contains the UUID of the tasks this task is a subtask of                                                                                                                                                                 | Read only |
| <code>subtasks</code>           | Contains the UUIDs of all the subtasks of this task                                                                                                                                                                      | Read only |

## **task-cancel**

```
1 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. XenServer 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:

```
1 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:

```
1 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 XenServer host 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, etc. 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):

```
1 xe vm-param-set uuid=<vm_uuid> platform:parallel=none
```

To disable the emulation of a serial port for HVM guests:

```
1 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:

```
1 xe vm-param-set uuid=<vm_uuid> platform:usb=false
2 xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
```

To use qemu-upstream for USB Passthrough:

```
1 xe vm-param-set uuid=<vm_uuid> platform:device-model=qemu-
 upstream-compat
```

- `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 XenServer host on which a VM based on this template is resident. Appears as `not in database` for a template
- `affinity` (read/write) the XenServer host 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 could 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

```
1 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 filename.

## template-uninstall

```
1 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 XenServer host 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

XenServer host updates have the following parameters:

| Parameter Name                | Description                                               | Type      |
|-------------------------------|-----------------------------------------------------------|-----------|
| <code>uuid</code>             | The unique identifier/object reference for the update     | Read only |
| <code>host</code>             | The list of hosts that this update is applied to          | Read only |
| <code>host-uuid</code>        | The unique identifier for the XenServer host to query     | Read only |
| <code>name-label</code>       | The name of the update                                    | Read only |
| <code>name-description</code> | The description string of the update                      | Read only |
| <code>applied</code>          | Whether or not the update has been applied; true or false | Read only |

| Parameter Name                    | Description                                               | Type      |
|-----------------------------------|-----------------------------------------------------------|-----------|
| <code>installation-size</code>    | The size of the update in bytes                           | Read only |
| <code>after-apply-guidance</code> | Whether the XAPI toolstack or the host requires a restart | Read only |
| <code>version</code>              | The version of the update                                 | Read only |

## update-upload

```
1 update-upload file-name=update_filename
```

Upload a specified update file to the XenServer host. 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

```
1 update-precheck uuid=update_uuid host-uuid=host_uuid
```

Run the prechecks contained within the specified update on the specified XenServer host.

## update-destroy

```
1 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

```
1 update-apply host-uuid=host_uuid uuid=update_file_uuid
```

Apply the specified update file.

**update-pool-apply**

```
1 update-pool-apply uuid=update_uuid
```

Apply the specified update to all XenServer hosts in the pool.

**update-introduce**

```
1 update-introduce vdi-uuid=vdi_uuid
```

Introduce update VDI.

**update-pool-clean**

```
1 update-pool-clean uuid=uuid
```

Removes the update's files from all hosts in the pool.

**User commands****user-password-change**

```
1 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       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>uuid</code>               | The unique identifier/object reference for the VBD                                                                                                  | Read only  |
| <code>vm-uuid</code>            | The unique identifier/object reference for the VM this VBD is attached to                                                                           | Read only  |
| <code>vm-name-label</code>      | The name of the VM this VBD is attached to                                                                                                          | Read only  |
| <code>vdi-uuid</code>           | The unique identifier/object reference for the VDI this VBD is mapped to                                                                            | Read only  |
| <code>vdi-name-label</code>     | The name of the VDI this VBD is mapped to                                                                                                           | Read only  |
| <code>empty</code>              | If <b>true</b> , this VBD represents an empty drive                                                                                                 | Read only  |
| <code>device</code>             | The device seen by the guest, for example <code>hda</code>                                                                                          | Read only  |
| <code>userdevice</code>         | Device number specified by the device parameter during <code>vbd-create</code> , for example, 0 for <code>hda</code> , 1 for <code>hdb</code> , etc | Read/write |
| <code>bootable</code>           | True if this VBD is bootable                                                                                                                        | Read/write |
| <code>mode</code>               | The mode the VBD should be mounted with                                                                                                             | Read/write |
| <code>type</code>               | How the VBD appears to the VM, for example <code>disk</code> or <code>CD</code>                                                                     | Read/write |
| <code>currently-attached</code> | True if the VBD is attached on this host, false otherwise                                                                                           | Read only  |
| <code>storage-lock</code>       | True if a storage-level lock was acquired                                                                                                           | Read only  |
| <code>status-code</code>        | Error/success code associated with the last attach operation                                                                                        | Read only  |

| Parameter Name                        | Description                                                                                                                                                | Type                     |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>status-detail</code>            | Error/success information associated with the last attach operation status                                                                                 | Read only                |
| <code>qos_algorithm_type</code>       | The QoS algorithm to use                                                                                                                                   | Read/write               |
| <code>qos_algorithm_params</code>     | Parameters for the chosen QoS algorithm                                                                                                                    | Read/write map parameter |
| <code>qos_supported_algorithms</code> | Supported QoS algorithms for this VBD                                                                                                                      | Read only set parameter  |
| <code>io_read_kbs</code>              | Average read rate in kB per second for this VBD                                                                                                            | Read only                |
| <code>io_write_kbs</code>             | Average write rate in kB per second for this VBD                                                                                                           | Read only                |
| <code>allowed-operations</code>       | 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  |
| <code>current-operations</code>       | Links each of the running tasks using this object (by reference) to a <code>current_operation</code> enum which describes the nature of the task.          | Read only set parameter  |
| <code>unpluggable</code>              | True if this VBD supports hot unplug                                                                                                                       | Read/write               |
| <code>attachable</code>               | True if the device can be attached                                                                                                                         | Read only                |
| <code>other-config</code>             | Extra configuration                                                                                                                                        | Read/write map parameter |

## vbd-create

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 vbd-plug uuid=uuid_of_vbd
```

Attempt to attach the VBD while the VM is in the running state.

## vbd-unplug

```
1 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                    |
|------------------------------------|---------------------------------------------------------------------|-------------------------|
| <a href="#">uuid</a>               | The unique identifier/object reference for the VDI                  | Read only               |
| <a href="#">name-label</a>         | The name of the VDI                                                 | Read/write              |
| <a href="#">name-description</a>   | The description string of the VDI                                   | Read/write              |
| <a href="#">allowed-operations</a> | A list of the operations allowed in this state                      | Read only set parameter |
| <a href="#">current-operations</a> | A list of the operations that are currently in progress on this VDI | Read only set parameter |
| <a href="#">sr-uuid</a>            | SR in which the VDI resides                                         | Read only               |
| <a href="#">vbd-uuids</a>          | A list of VBDs that refer to this VDI                               | Read only set parameter |



| Parameter Name                    | Description                                                                                                                  | Type                     |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <code>crashdump-uuids</code>      | List of crash dumps that refer to this VDI                                                                                   | Read only set parameter  |
| <code>virtual-size</code>         | 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                |
| <code>physical-utilisation</code> | Amount of physical space that the VDI is taking up on the SR, in bytes                                                       | Read only                |
| <code>type</code>                 | Type of VDI, for example, System or User                                                                                     | Read only                |
| <code>sharable</code>             | True if this VDI may be shared                                                                                               | Read only                |
| <code>read-only</code>            | True if this VDI can only be mounted read-only                                                                               | Read only                |
| <code>storage-lock</code>         | True if this VDI is locked at the storage level                                                                              | Read only                |
| <code>parent</code>               | References the parent VDI when this VDI is part of a chain                                                                   | Read only                |
| <code>missing</code>              | True if SR scan operation reported this VDI as not present                                                                   | Read only                |
| <code>other-config</code>         | Extra configuration information for this VDI                                                                                 | Read/write map parameter |
| <code>sr-name-label</code>        | Name of the containing storage repository                                                                                    | Read only                |
| <code>location</code>             | Location information                                                                                                         | Read only                |
| <code>managed</code>              | True if the VDI is managed                                                                                                   | Read only                |

| Parameter Name                | Description                                                                                                                                                                                                        | Type                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <code>xenstore-data</code>    | Data to be inserted into the xenstore tree (/local/domain/0/backend/vbd/ <i>domid</i> / <i>device-id</i> /smdata) after the VDI is attached. The SM back-ends usually set this field on <code>vd_i_attach</code> . | Read only map parameter |
| <code>sm-config</code>        | SM dependent data                                                                                                                                                                                                  | Read only map parameter |
| <code>is-a-snapshot</code>    | True if this VDI is a VM storage snapshot                                                                                                                                                                          | Read only               |
| <code>snapshot_of</code>      | The UUID of the storage this VDI is a snapshot of                                                                                                                                                                  | Read only               |
| <code>snapshots</code>        | The UUIDs of all snapshots of this VDI                                                                                                                                                                             | Read only               |
| <code>snapshot_time</code>    | The timestamp of the snapshot operation that created this VDI                                                                                                                                                      | Read only               |
| <code>metadata-of-pool</code> | The uuid of the pool which created this metadata VDI                                                                                                                                                               | Read only               |
| <code>metadata-latest</code>  | Flag indicating whether the VDI contains the latest known metadata for this pool                                                                                                                                   | Read only               |
| <code>cbt-enabled</code>      | Flag indicating whether changed block tracking is enabled for the VDI                                                                                                                                              | Read/write              |

## vd\_i-clone

```
1 vd_i-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 `vd_i-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**

```
1 vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
```

Copy a VDI to a specified SR.

**vdi-create**

```
1 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.

**Note:**

Some SR types might round up the `virtual-size` value to make it divisible by a configured block size.

**vdi-data-destroy**

```
1 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**

```
1 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.

**Note:**

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**

```
1 vdi-disable-cbt uuid=uuid_of_vdi
```

Disable changed block tracking for the VDI.

**vdi-enable-cbt**

```
1 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 XenServer Enterprise Edition.

**vdi-export**

```
1 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 (EXT, 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`**

```
1 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`**

```
1 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`**

```
1 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**

```
1 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**

```
1 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 XenMotion)

For more information, see [Migrate VMs](#).

**vdi-resize**

```
1 vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
```

Change the size of the VDI specified by UUID.

**vdi-snapshot**

```
1 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**

```
1 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**

```
1 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:

```
1 xe vif-param-set \
2 uuid=<vif_uuid> \
3 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**, XenServer applies a filtering rule so that the VIF cannot send or receive traffic. If the default-lockingmode is set to **unlocked**, XenServer 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) XenServer applies a filtering rule is applied so that the VIF drops all traffic.

## **vif-create**

```
1 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**

```
1 vif-destroy uuid=uuid_of_vif
```

Destroy a VIF.

## **vif-move**

```
1 vif-move uuid=uuid network-uuid=network_uuid
```

Move the VIF to another network.

**vif-plug**

```
1 vif-plug uuid=uuid_of_vif
```

Attempt to attach the VIF while the VM is in the running state.

**vif-unplug**

```
1 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:

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
 gateway=gateway_address
```

For example:

```
1 VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
 192.168.1.1")
```

Clean IPv4 settings as below:

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=none
```

**vif-configure-ipv6**

Configure IPv6 settings for this virtual interface. Set IPv6 settings as below:

```
1 vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
 gateway=gateway_address
```

For example:

```
1 VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
 "fd06:7768:b9e5:8b00::1")
```

Clean IPv6 settings as below:

```
1 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**

```
1 vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
 uuid_of_network
```

Create a VLAN on your XenServer host.

### **pool-vlan-create**

```
1 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 on each host accordingly.

### **vlan-destroy**

```
1 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

```
1 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:

```
1 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 XenServer host. 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 XenServer host 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, etc. 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 Virtual Desktop Agent (VDA) to switch Windows 10 into Tablet mode:

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
```

To enable VDA to switch Windows 10 into Tablet mode:

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
```

To check current state:

```
1 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 XenServer host on which a VM is resident
- `affinity` (read/write) The XenServer host 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 time-zone 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 PV (paravirtual) or HVM (hardware virtual machine) 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 XenServer host.
- `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**

```
1 vm-assert-can-be-recovered uuid [database] vdi-uuid
```

Tests whether storage is available to recover this VM.

### **vm-call-plugin**

```
1 vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
 value]
```

Calls the function within the plugin on the given vm with optional arguments (`args:key=value`). To pass a "value" string with special characters in it (e.g. 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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:

```
1 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**

```
1 vm-compute-memory-overhead
```

Computes the virtualization memory overhead of a VM.

### **vm-copy**

```
1 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**

```
1 vm-copy-bios-strings host-uuid=host_uuid
```

Copy the BIOS strings of the given host to the VM.

### **vm-crashdump-list**

```
1 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**

```
1 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 see 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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**

```
1 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 filename to export the VM into using the `filename` parameter. By convention, the filename 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**

```
1 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.

The `filename` parameter can also point to an XVA-format VM, which is the legacy export format from XenServer 3.2. This format is used by some third-party vendors to provide virtual appliances. XVA format uses a directory to store the VM data, so set `filename` to the root directory of the XVA export and not an actual file. Subsequent exports of the imported legacy guest are upgraded automatically to the new filename-based format, which stores much more data about the configuration of the VM.

**Note:**

The older directory-based XVA format does not fully preserve all the VM attributes. In particular, imported VMs do not have any virtual network interfaces attached by default. If networking is required, create one using `vif-create` and `vif-plug`.

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 than in parallel.

**vm-install**

```
1 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**

```
1 vm-is-bios-customized
```

Indicates whether the BIOS strings of the VM have been customized.



**vm-memory-balloon**

```
1 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**

```
1 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**

```
1 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**

```
1 vm-memory-set memory=memory
```

Configure the memory allocation of a VM.

**vm-memory-shadow-multiplier-set**

```
1 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 XenServer host 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**

```
1 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**

```
1 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**

```
1 vm-memory-target-wait
```

Wait for a running VM to reach its current memory target.

### **vm-migrate**

```
1 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 XenServer host. For example, to migrate the VM to another host in the pool, where the VM disks are on storage shared by both hosts:

```
1 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 XenMotion):

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \
2 remote-username=username remote-password=password \
3 host-uuid=destination_host_uuid vdi=vdi_uuid
```

You can choose the SR where each VDI gets stored:

```
1 xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
2 vdi1:vdi_1_uuid=destination_sr_uuid \
3 vdi2:vdi_2_uuid=destination_sr2_uuid \
4 vdi3:vdi_3_uuid=destination_sr3_uuid
```

Additionally, you can choose which network to attach the VM after migration:

```
1 xe vm-migrate uuid=vm_uuid \
2 vdi1:vdi_1_uuid=destination_sr_uuid \
3 vdi2:vdi_2_uuid=destination_sr2_uuid \
4 vdi3:vdi_3_uuid=destination_sr3_uuid \
5 vif:vif_uuid=network_uuid
```

For cross-pool migration:

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \
2 remote-username=username remote-password=password \
3 host-uuid=destination_host_uuid vdi=vdi_uuid
```

For more information on Storage XenMotion, XenMotion and Live VDI Migration, see [Migrate VMs with XenMotion and Storage XenMotion](#).

By default, the VM is suspended, migrated, and resumed on the other host. The `live` parameter selects XenMotion. XenMotion 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, XenMotion 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**

```
1 vm-pause
```

Pause a running VM. Note this operation does not free the associated memory (see [vm-suspend](#)).

**vm-query-services**

```
1 vm-query-services
```

Query the system services offered by the given VMs.

**vm-reboot**

```
1 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**

```
1 vm-recover vm-uuid [database] [vdi-uuid] [force]
```

Recovers a VM from the database contained in the supplied VDI.

**vm-reset-powerstate**

```
1 vm-reset-powerstate [vm-selector=vm_selector_value...] {
2 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**

```
1 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**

```
1 vm-retrieve-wlb-recommendations
```

Retrieve the workload balancing recommendations for the selected VM.

### **vm-shutdown**

```
1 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**

```
1 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-snapshot-with-quiesce**

```
1 vm-snapshot-with-quiesce new-name-label=name_label [new-name-
 description+name_description]
```

Snapshot an existing VM with quiesce, using storage-level fast disk snapshot operation where available.

**vm-start**

```
1 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**

```
1 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

```
1 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) as well as 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

```
1 vm-unpause
```

Unpause a paused VM.

## vm-vcpu-hotplug

```
1 vm-vcpu-hotplug new-vcpus=new_vcpu_count [vm-selector=vm_selector_value ...]
```

Dynamically adjust the number of vCPUs available to a running PV or HVM 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 PV or HVM 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 XenServer 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

```
1 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

```
1 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:

```
1 xe vmss-create retained-snapshots=9 enabled=true frequency=daily \
2 name-description=sample name=label=samplepolicy type=snapshot \
3 schedule:hour=10 schedule:min=30
```

Snapshot schedules have the following parameters:

| Parameter Name     | Description                                       | Type       |
|--------------------|---------------------------------------------------|------------|
| name- <b>label</b> | Name of the snapshot schedule.                    | Read/write |
| name-description   | Description of the snapshot schedule.             | Read/write |
| type               | Disk snapshot; Memory snapshot; Quiesced snapshot | Read/write |
| frequency          | Hourly; Daily; Weekly                             | Read/write |
| retained-snapshots | Snapshots to be retained.<br>Range: 1-10.         | Read/write |



| Parameter Name        | Description                                                                                                                         | Type       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------|
| <code>schedule</code> | <code>schedule:days</code> (Monday to Sunday), <code>schedule:hours</code> (0 to 23), <code>schedule:minutes</code> (0, 15, 30, 45) | Read/write |

### **vmss-destroy**

```
1 vmss-destroy uuid=uuid
```

Destroys a snapshot schedule in the pool.

### **USB passthrough**

#### **USB passthrough enable/disable**

```
1 pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
```

Enable/disable USB Pass-through.

### **pusb-scan**

```
1 pusb-scan host-uuid=host_uuid
```

Scan PUSB and update.

### **vusb-create**

```
1 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**

```
1 vusb-unplug uuid=vusb_uuid
```

Unplugs USB from VM.

## **vusb-destroy**

```
1 vusb-destroy uuid=vusb_uuid
```

Removes the virtual USB list from VM.

## **SDKs and APIs**

August 13, 2018

The following developer documentation is available on <https://developer-docs.citrix.com/>.

- [Management API Guide](#)
- [Software Development Kit Guide](#)
- [Changed Block Tracking Guide](#)
- [Supplemental Packs and the DDK Guide](#)





#### **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

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).