Citrix XenServer 7.1 LTSR

Contents

XenServer 7.1 Long Term Service Release (LTSR)

February 22, 2021

The Long Term Service Release (LTSR) program for XenServer provides stability and long-term support for XenServer releases.

The XenServer product lifecycle strategy for Current Releases (CR) and Long Term Service Releases (LTSR) is described in https://www.citrix.com/support/product-lifecycle/milestones/xenserver.html.

A XenServer LTSR is currently available for version 7.1. Cumulative Update 2, released 12 December 2018, is the most recent update to the 7.1 LTSR. If you are new to the LTSR program and did not deploy the initial 7.1 LTSR release, there is no need for you to install it now. Instead, Citrix recommends that you begin with 7.1 Cumulative Update 2.

> **Important**
>
> In December 2019, version 9.x of the Windows I/O drivers (xenbus, xenvif, xenvbd, xeniface, xennet) were made available through Windows Update, for example, xeniface 9.0.0.11.
>
> The version 9.x drivers remove the quiesced snapshot capability. This capability is also removed from support in Citrix Hypervisor 8.1 and later. For more information, see Citrix Hypervisor 8.1 Deprecations and removals.
>
> To continue to use the quiesced snapshot feature with Windows VMs hosted on XenServer 7.1, do not update to the 9.x drivers and retain your current 8.x version of the Windows I/O drivers.

Documentation format

From XenServer 7.1 LTSR CU2, some of this product documentation is available in HTML instead of PDF. 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.

The PDF version of the guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

What's New

Cumulative Update 2 Release Notes (HTML)

Cumulative Update 1 Release Notes (PDF)

Release Notes (PDF)

Getting started

Quick Start Guide (PDF)

Installation Guide (HTML)

Core documentation

Administrator's Guide (PDF)

Virtual Machine User's Guide (HTML)

Configuring XenServer for Graphics (PDF)

Product reference information

Configuration limits (HTML)

Guest operating system support (HTML)

XenCenter documentation (HTML)

Licensing FAQ (PDF)

Technical FAQ (PDF)

Feature Matrix (PDF)

Common criteria

Citrix XenServer 7.1 Cumulative Update 2 is Common Criteria certified EAL2+. For more information, see Citrix Common Criteria Certification Information.

Common Criteria Evaluated Configuration Guide (PDF)

SDKs and APIs

Management API Guide (PDF)

Software Development Kit Guide (PDF)

Supplemental Packs and the DDK Guide (PDF)

Supplemental information

> **Note:**
>
> We recommend that you use the Workload Balancing 8.2 and Conversion Manager 8.2 virtual

> appliances with your XenServer 7.1 CU2 pool. These virtual appliances are available from the Citrix Hypervisor downloads page.
>
> To use the latest appliances with XenServer 7.1 CU2, ensure you have the following prerequisites:
>
> - Use the latest version of XenCenter provided with Citrix Hypervisor 8.2. This available from the Citrix Hypervisor downloads page.
> - Install Hotfix XS71ECU2040 on your XenServer 7.1 CU2 hosts.
> - Review the product documentation for the latest version of Workload Balancing and Conversion Manager.

Workload Balancing Quick Start Guide (PDF)

Workload Balancing Administrator's Guide (PDF)

Conversion Manager Guide (PDF)

Measured Boot Supplemental Pack Guide (PDF)

XenServer-Nutanix Integration Guide (PDF)

vSwitch Controller User Guide (PDF)

What's new

November 3, 2020

About this release

XenServer 7.1 LTSR CU2 is the second Cumulative Update for the XenServer 7.1 Long Term Service Release (LTSR). This article provides important information about the XenServer 7.1 CU2 release.

XenServer 7.1 CU2 is available in two commercial editions:

- Standard Edition
- Enterprise Edition

XenServer 7.1 Cumulative Update 2 and its subsequent hotfixes are available only to customers with Customer Success Services.

Support timeline

For XenServer 7.1 LTSR, mainstream support is available till 15 Aug 2022, with the option for customers to add up to five years of chargeable, extended support.

The XenServer 7.1 CU1 release is supported for three months following the release of XenServer 7.1 CU2. During this time, we will issue critical hotfixes for both XenServer 7.1 CU1 and XenServer 7.1 CU2. We will issue any functional hotfixes for XenServer 7.1 CU2 only.

To receive support and be eligible for any hotfixes issued after March 12, 2019, you must install this Cumulative Update to your Xenserver 7.1 servers by this date.

Included in XenServer 7.1 CU2

XenServer 7.1 CU2 rolls-up all previously issued XenServer 7.1 CU1 hotfixes and simultaneously introduces new fixes for issues reported on XenServer 7.1 CU1. For more information, see Fixed issues in XenServer 7.1 CU2.

Some performance or non-functional improvements are also included. For more information, see Improvements in XenServer 7.1 CU2.

To minimize changes within the LTSR product, no additional features are included in XenServer 7.1 CU2

Improvements in XenServer 7.1 CU2

In addition to the rolled-up hotfixes, XenServer 7.1 CU2 includes some performance or non-functional improvements that are available for all licensed LTSR customers.

Compatibility with Citrix Hypervisor 8.2 virtual appliances

You can use the Workload Balancing 8.2 and Conversion Manager 8.2 virtual appliances with your XenServer 7.1 CU2 pool. To use the latest appliances with XenServer 7.1 CU2, ensure you have the following prerequisites:

- Use the latest version of XenCenter provided with Citrix Hypervisor 8.2
- Install Hotfix XS71ECU2040 on your XenServer 7.1 CU2 hosts

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

Performance improvements

- Improved support for importing HyperV generated VHD images into XenServer.
- Updated Dom0 tools for supporting higher Ethernet speeds (50G/100G etc).

XenServer entitlement for Citrix Virtual Apps and Desktops service subscribers

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 for hosting these Desktops and Apps. XenServer 7.1 LTSR CU2 adds supports for this license type, enabling you to use all of the same premium features as with an on-premises XenApp and XenDesktop entitlement.

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.

Support for new guest operating systems

XenServer 7.1 CU2 now supports the following new guests:

- Debian Stretch 9.0
- RHEL/CentOS/OEL/Scientific Linux 6.9
- RHEL/CentOS/OEL/Scientific Linux 7.4
- RHEL/CentOS/OEL/Scientific Linux 7.5
- SUSE Linux Enterprise Desktop 12 SP3
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu 18.04
- Windows Server 2019 (drivers available on Windows Update or by installing hotfix XS71ECU2007)
- SUSE Linux Enterprise Desktop 12 SP4 (template available by installing hotfix XS71ECU2011)
- SUSE Linux Enterprise Server 12 SP4 (template available by installing hotfix XS71ECU2011)
- CentOS 8 (template available by installing hotfix XS71ECU2036)
- Red Hat Enterprise Linux 8 (template available by installing hotfix XS71ECU2036)
- SUSE Linux Enterprise Server 15 SP1 (template available by installing hotfix XS71ECU2036)

Support for new processors

The following processors are now supported in XenServer 7.1 CU2:

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

For more information, see the Hardware Compatibility List.

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 the XenCenter issued with the latest XenServer Cumulative Update to upgrade from any supported version of XenServer to XenServer 7.1 CU2.

> **Note:**
>
> Upgrading your XenServer hosts using the Rolling Pool Upgrade wizard is available only for licensed XenServer customers or those who have access to XenServer through their Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) 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 7.1 CU2 licensing, see Licensing.

Installation options

XenServer 7.1 CU2 is available to download from the XenServer Product Download page in the following packages:

- **XenServer 7.1.2 Cumulative Update 2 Installation** comprises only the fixes that make up the cumulative update. Use this ISO to apply the cumulative update to an existing installation of XenServer 7.1 CU1.
- **XenServer 7.1.2 Base Installation ISO including Cumulative Update 2** comprises both a base XenServer 7.1 installation and the fixes that make up the cumulative updates. Use this ISO to create a fresh installation of XenServer 7.1 including CU1 and CU2 or to upgrade from XenServer 6.2, 6.5, or 7.0.

The latest version of XenCenter is also available to download from XenServer 7.1 download page. This version of XenCenter can be more recent than the version of XenCenter released at the same time as Cumulative Update 2.

> **Important:**
>
> If you use XenCenter to update your hosts, update your XenCenter installation to the latest version supplied on the XenServer 7.1 download page before beginning.

The following table shows the available options when moving from an existing version of XenServer to XenServer 7.1 CU2.

Installed Version	Update using XenServer 7.1.2 Cumulative Update 2 Installation	Upgrade or fresh install using XenServer 7.1.2 Base Installation ISO including Cumulative Update 2
XenServer 7.1 CU1	YES	NO
XenServer 7.0	NO	YES

Installed Version	Update using XenServer 7.1.2 Cumulative Update 2 Installation	Upgrade or fresh install using XenServer 7.1.2 Base Installation ISO including Cumulative Update 2
XenServer 6.5.0	NO	YES
XenServer 6.2.0	NO	YES

> **Note:**
>
> Customers on XS 7.1 are required to first update to XenServer 7.1 CU1 before updating to XenServer 7.1 CU2.
>
> Always update the pool master before updating any other hosts in a pool.

Before beginning installation, review the System Requirements and Installation.

After installation of XenServer 7.1 CU2, the internal product version number is shown as 7.1.2.

If you use the vSwitch Controller Virtual Appliance or PVS Accelerator Supplemental Pack, ensure that you update these components to the latest version provided on the XenServer Product Download page for XenServer 7.1 Cumulative Update 2.

If you upgrade a host with legacy disk partition from XenServer 6.x to XenServer 7.1 CU1, and then attempt to apply XenServer 7.1 CU2 as an update, you may receive an insufficient space error.
To avoid this happening, apply XS71ECU1033 on XS 7.1 CU1 before attempting to update to CU2. If this does not solve the issue, refer to CTX202821 - File System on Control Domain Full for further actions to clear up space.

> **Note:**
>
> If you use XenCenter to update your hosts, the list of available updates will show both XenServer 7.1 CU2 and any currently released hotfixes for XenServer 7.1 that are not yet applied.
>
> As XenServer 7.1 CU2 includes all the hotfixes released to date, applying it avoids having to install earlier released hotfixes for XenServer 7.1 CU1. For more information, see Fixed issues in XenServer 7.1 CU2.
>
> For a period of 3 months after the release of XenServer 7.1 CU2, there might be further XenServer 7.1 critical hotfixes released that are not included in XenServer 7.1 CU2. These hotfixes will have equivalent hotfixes released for XenServer 7.1 CU2, if required. Customers on XenServer 7.1 CU1 can choose to apply the XenServer 7.1 CU1 hotfixes or to apply XenServer 7.1 CU2 and the equivalent hotfixes for XenServer 7.1 CU2.
>
> If you choose to use the Automated Updates feature to install updates on XenServer 7.1 CU1, it

> is recommended to update XenCenter to the version available for XenServer 7.1 CU2 first. When Automated Update is selected, the XenServer 7.1 CU2 update and hotfixes available for XenServer 7.1 CU2 are applied. For more details, See Update your hosts.

Optional components updated in XenServer 7.1 CU2

The following are new/updated optional components for the XenServer 7.1 CU2 release. All other optional components remain the same as the XenServer 7.1 CU1 release.

- vSwitch Controller Virtual Appliance
- PVS Accelerator Supplemental Pack
- Software Development Kit (SDK) 7.1.2
- Driver Development Kit (DDK) 7.1.2

Changing from XenServer 7.1 LTSR CU2 to the Current Release

If you're running XenServer 7.1 LTSR CU2, but want to take advantage of new features, you can instead 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.

The latest XenServer CR is available to download from the XenServer Product Download page.

Changing from the Current Release to XenServer 7.1 LTSR CU2

If you're running a XenServer CR, but want to move to a version of XenServer with a guaranteed and stable feature set, you can change to XenServer 7.1 LTSR CU2. Use the XenServer 7.1.2 Base Installation ISO including Cumulative Update 2 to create a fresh installation of XenServer. There is no upgrade path from the XenServer CR stream to XenServer 7.1 LTSR.

Licensing

Upgrade your Citrix License Server to version 11.14 or higher in order to use all XenServer 7.1 licensed features.

For more information about XenServer 7.1 licensing, see XenServer 7.1 Licensing FAQ.

Interoperability with Citrix products

XenServer 7.1 CU2 is interoperable with Citrix Virtual Apps and Desktops 1912 (LTSR), Citrix Virtual Apps and Desktops 7 1808.1 (CR), Citrix XenApp/XenDesktop 7.6 (LTSR), and 7.15 (LTSR). We recommend that you use this XenServer LTSR with a XenApp/XenDesktop LTSR.

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

Localization support

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

Product documentation

To access XenServer 7.1 LTSR product documentation, see XenServer LTSR Product Documentation.

Fixed issues in XenServer 7.1 CU2

March 15, 2022

Rollup Hotfixes in CU2

XenServer 7.1 CU2 includes the following XenServer 7.1 CU1 hotfixes:

- XS71ECU1001 - https://support.citrix.com/article/CTX227235
- XS71ECU1002 - https://support.citrix.com/article/CTX229904
- XS71ECU1003 - https://support.citrix.com/article/CTX228721
- XS71ECU1004 - https://support.citrix.com/article/CTX229066
- XS71ECU1005 - https://support.citrix.com/article/CTX231725
- XS71ECU1006 - https://support.citrix.com/article/CTX229540
- XS71ECU1007 - https://support.citrix.com/article/CTX230236
- XS71ECU1008 - https://support.citrix.com/article/CTX230160
- XS71ECU1009 - SUPERSEDED
- XS71ECU1010 - https://support.citrix.com/article/CTX231719
- XS71ECU1011 - https://support.citrix.com/article/CTX232564
- XS71ECU1012 - https://support.citrix.com/article/CTX233365
- XS71ECU1013 - https://support.citrix.com/article/CTX233363
- XS71ECU1014 - https://support.citrix.com/article/CTX233698
- XS71ECU1015 - https://support.citrix.com/article/CTX235209
- XS71ECU1016 - https://support.citrix.com/article/CTX234437
- XS71ECU1017 - https://support.citrix.com/article/CTX235131
- XS71ECU1018 - https://support.citrix.com/article/CTX236478
- XS71ECU1019 - https://support.citrix.com/article/CTX235723
- XS71ECU1022 - https://support.citrix.com/article/CTX235957
- XS71ECU1023 - https://support.citrix.com/article/CTX236150
- XS71ECU1024 - https://support.citrix.com/article/CTX236908

- XS71ECU1026 - https://support.citrix.com/article/CTX237088
- XS71ECU1027 - https://support.citrix.com/article/CTX237089
- XS71ECU1029 - https://support.citrix.com/article/CTX238647
- XS71ECU1031 - https://support.citrix.com/article/CTX239126
- XS71ECU1032 - https://support.citrix.com/article/CTX239435
- XS71ECU1033 - https://support.citrix.com/article/CTX239747

Additional issues fixed in CU2

The following issues are resolved in XenServer 7.1 CU2:

Dom0

- Updated for Brazil's change in Daylight Saving Date/Time (DST) to 4 Nov 2018. (CP-29838)

Performance

- HA-enabled VMs can take longer to restart after a failover. (CP-28117)
- The workarounds for Meltdown (CVE-2017-5754) patched in XS70E055, XS70E057, XS71ECU1009, XS71ECU1016, and XS71ECU1017 had reduced performance. Customers who had installed one or more of these hotfixes applied might have experienced degraded IOPS for both PV and HVM VMs. This fix includes a Xen PCID patch that recovers most of the regressed IOPS to the level before the workarounds were applied. The improvement is mostly visible in Xeon v3, Xeon v4, and later Intel CPUs. (CP-29203)

Installation

- If your XenServer 7.0 (or earlier) host has a fully qualified domain name specified as its host name, the domain part of the name can be lost when upgrading to XenServer 7.1 CU1. This issue is resovled for upgrades from XenServer 7.0 (or earlier) to XenServer 7.1 CU2. (CA-296524)

Networking

- In XenServer deployments with multiple VLANs containing different MTU values, restarting a VM can reset all the MTU values to the lowest value present on the network bridge. (CA-196520)

Guest Agent

- Users fail to install XenServer Tools on VMs using SUSE Linux Enterprise Server 12 SP1 template due to a lack of support for a system call (modify_ldt) in SUSE Linux Enterprise Server 12 SP1.

This fix solves the issue by rebuilding XenServer Tools with new version of GO, which removes the dependency for the unsupported option. (CA-297044)

Toolstack

- Automated guest agent update stops working after a host reboot, due to its dependency on entries in xenstore that were not properly recreated after the reboot. (CA-302194)
- In rare cases, after a sequence of pool joins, multiple Tools SRs might exist in a pool and prevent a host from being ejected from the pool. Pool join now ensures that only one Tools SR exists in a pool. (CA-300103) (CA-267661)
- Improved support for importing HyperV generated VHD images into XenServer. (CA-296067)
- On hosts with a legacy partition scheme, log rotation is not working as expected after an update of xapi-core which is part of the toolstack. (CA-293858)
- Importing a VHD type of VDI file larger than 1 TiB was unsupported and led to an VDI_IO_ERROR. (CA-292288)
- In rare cases, when a XenServer host in a pool is restarted, it might not be able to rejoin the pool. (CA-287865)

Windows PV/Guest Tools

- A Windows 10 VM with the I/O drivers installed can crash with bugcheck code 139. This is caused by a Windows issue which causes an inconsistent state during nonpaged memory allocation. (CP-29203)
- Windows VMs with the XenVBD driver installed can experience a high number of system interrupts when performing storage operations, especially if you are using fast storage and transferring large amounts of data. (CA-297860)

Xen

- The clock on dom0 drifts on Dell R740 hardware. (CA-285265)
- In some cases, PXE boot for VMs fail when using a proxy DHCP agent. This happens because of multiple issues in the iPXE version used by XenServer which prevented the VM from booting. (CA-247412) (CA-247413)

XenCenter and xsconsole

- Batch application of XenServer updates with mixed restart requirements may result in both host reboot and XAPI restart. (CA-297215)

- Emergency network reset fails with "Login Failed" reported when performed from xsconsole. (CA-248121) (CA-297085)

Known issues for CU2

December 14, 2020

Advisories and known issues in CU2

This article details advisories and minor issues with this release and any workarounds that you can apply.

General

- If you have more than 26 disks attached, when upgrading from XenServer 6.x to XenServer 7.1 CU2, the upgrade process can incorrectly delete the local storage SR. To work around this issue, ensure that your XenServer host retains the legacy partition layout by manually completing the upgrade (instead of by using XenCenter Rolling Pool Upgrade).
- After migrating Container Managed VMs between pools, the Container Management functionality stops working for the VMs. This is because Container Management is implemented using a pool-specific key. To work around this issue, the VM-specific preparation step for "Container Management" needs to be repeated on the new pool. This means:
  - For CoreOS, the Cloud Config Drive needs to be updated by changing the Config Drive configuration in the VM preferences.
  - For RHEL/CentOS/OL 7 and Ubuntu, the xscontainer-prepare-vm needs to be re-run. Note that even if the preparation-step is repeated, the old XenServer pool might keep access to the VMs.
- Renaming a container does not trigger the Container Managment view to update. Additionally on Ubuntu 14.04 the pause or unpause of a container from outside XenCenter does not trigger the view to update. This means 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 work around the refresh can be triggered manually by performing an action (i.e. start, stop) on an unrelated container that is running on the same VM. (EXT-118)
- XenServer's use of new hardware security features might reduce the overall performance of 32-bit PV VMs. Customers impacted by this issue can either:

    - Run a 64-bit version of the PV Linux VM, or
    - Boot Xen with the `no-smep no-smap` option. Note that we do not recommend this option as it can reduce the depth of security of the host. (CA-214564)

- On some systems, the XenServer host fails to boot when 4096 MB or more memory is assigned to dom0. To work around this issue, edit the boot parameters on the host to include `dma_bits=32` in the Xen command line

    1. Interrupt the Xen boot process to get to the boot options screen.
    2. Select to edit the configuration.
    3. Add `dma_bits=32` to the Xen boot options.
    4. Continue the boot process.
    5. After the XenServer host successfully boots, run the following command to ensure that the boot parameter is always used:

```
/opt/xensource/libexec/xen-cmdline --set-xen dma_bits=32
<!--NeedCopy-->
```

Conversion Manager

- When you import a Windows VM from an ESXi server to XenServer, the IPv4/IPv6 network settings can be lost. To retain the network settings, customers should reconfigure the IPv4/IPv6 settings after completing the conversion. (CA-90730)

Dom0

- In some cases, booting a XenServer host from FCoE SAN using software FCoE stack can cause the host to become unresponsive due to a temporary link disruption in the host initialization phase. If the host appears to be in an unresponsive state for a long time, reboot the host to work around this issue. (CA-233299)
- Customers should not assign more than 32GB of memory to Dom0, as otherwise intermittent VM freezes might occur during start of VMs. (CA-236674)
- Due to changes in the Dom0 file system, restore via XenCenter or "xe host-restore" might fail when users upgrade from XenServer 6.x to 7.x. This action is therefore not supported. (CA-302538)

Guests

- The console screen on HVM Linux guests can go blank after a period (typically ten minutes) of inactivity. You can work around this issue by adding `consoleblank=0` to the kernel boot parameters of the guest. Consult your guest OS documentation for information about updating the kernel boot parameters. (CA-148381)
- 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)
- On Windows VMs, when updating the xenbus driver to version 9.1.0.4, ensure that you complete both of the requested VM restarts. If both restarts are not completed, the VM might revert to emulated network adapters and use different settings, such as DHCP or different static IP addressing.

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

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

Installation

- If you have multiple high-speed NICs, you might experience out of memory issues in dom0 during XenServer installation. If you have more than four 10Gb NICs or more than two 40Gb NICs, consider increasing the amount of dom0 memory to 8 GiB. To change the amount of dom0 memory, go to the install options in the boot menu for the XenServer host and modify the Xen boot options to include `dom0_mem=max:8192M`. (XSI-602)

Networking

- XenServer does not prevent users from unplugging a NIC used by the FCoE SR. (CA-178651)

Storage Manager

- When starting VMs with at least one VBD, and either High Availability (HA) or redo log enabled, an extra number of login calls from SM to XAPI causes longer start time than expected. (CA-287884) (CA-287879)

Toolstack

- If a pool's CPU feature set changes 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), the VM will continue to use the feature set which was applied when it was started. To update the VM to use the pool's new feature set, the VM must be powered off and then started. Rebooting the VM, for example, by clicking 'Reboot' in XenCenter, does not cause the VM to update its feature set. (CA-188042)

- In scenarios with poor or interrupted network connectivity between the XenServer host and the Licensing virtual machine, too many licenses might be checked out from the License Server. (CA-293005)

XenCenter

- Modifying the font size or DPI on the computer on which XenCenter is running can result in the user interface displaying incorrectly. The default font size is 96 DPI; Windows 8 and Windows 10 refer to this 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)
- When applying automated updates on a XS 7.1 CU1, XenCenter will automatically install XS71ECU2 with all roll-up hotfixes applied. This will bring the hosts to the XenServer 7.1 CU2 but not XenCenter. To avoid this happening, users need to upgrade their XenCenter version to 7.1 CU2 before applying automated updates on a XenServer 7.1 CU1 host. (CA-304656)

Driver Disks

- Driver disks built for XenServer 7.1 with the `BASE_REQUIRES` value in the makefile set to the default of `product-version=7.1.0` do not install on XenServer 7.1 CU2. To ensure that your driver disks can be installed on XenServer 7.1 CU2 (CA-260318):
  - For updates that contain kernel device drivers, set `BASE_REQUIRES := kernel-uname -r=4.4.0+10`
  - For other updates, set `BASE_REQUIRES := platform-version=2.2.0`

Windows PV Tools

- After upgrading a XenServer host from a previous version to XenServer 7.1 CU2, Windows VMs with XenServer Tools installed might incorrectly report as not having the XenServer Tools installed, or display some of the functionalities as unavailable. To work around this issue, install XenServer Tools issued with XenServer 7.1 CU2. (CA-209186)

Linux guest tools

- If you attempt to install the Linux guest tools on a fully up to date CentOS 8 system, you see the error: `Fatal Error: Failed to determine Linux distribution and version`. This is caused by changes in that CentOS 8 updates release on Dec 08, 2020. To workaround this issue, specify the OS when installing the Linux guest tools: `./install.sh -d centos -m 8`. However, if you use this workaround, the operating system information is not reported back to the XenServer host and does not appear in XenCenter. (CA-349929)

vSwitch Controller

- The vSwitch controller can experience a possible memory leak in the stunnel service. You might see the following message in the vSwitch Controller syslog: "Possible memory leak at…" (XSI-592)

System Requirements

September 1, 2020

This article describes system requirements for both XenServer hosts and XenCenter.

XenServer requires at least two separate physical x86 computers: one to be the XenServer host and the other to run the XenCenter application. The XenServer host computer is dedicated entirely to the task of running XenServer — hosting VMs — and is not used for other applications.

> **Warning:**
>
> The installation of any third party software directly on the XenServer host (i.e. into the dom0 control domain) is not supported, except where it is supplied as an update package and is explicitly endorsed by Citrix.

The computer that runs XenCenter can be any general-purpose Windows computer that satisfies the hardware
requirements and can be used to run other applications.

XenServer Host System Requirements

While XenServer will generally be deployed on server-class hardware, XenServer is also compatible with many models of workstations and laptops. For a comprehensive XenServer hardware compatibility list, see http://www.citrix.com/xenserver/hcl. The following 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 which controls the interaction between the virtualized devices seen by VMs and the physical hardware.

XenServer can make use of:

- up to 5TB of RAM
- up to 16 NICs
- up to 288 logical processors per host

> **Note:**
>
> The maximum number of logical processors supported differs by CPU. Consult the XenServer Hardware Compatibility List (HCL) for more details.

The system requirements for the XenServer host are:

CPUs

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

To support VMs running Windows, an Intel VT or AMD-V 64-bit x86-based system with one or more CPU(s) is required.

> **Note:**
>
> To run Windows VMs, hardware support for virtualization must be enabled on the XenServer host. This is an option in the BIOS. It is possible your BIOS might have virtualization support disabled. Consult your BIOS documentation for more details.

To support VMs running supported paravirtualized Linux, a standard 64-bit x86-based system with one or more CPU(s) is required.

RAM

2GB minimum, 4GB or more recommended.

Disk Space

Locally attached storage (PATA, SATA, SCSI) with 46GB of disk space minimum, 70GB of disk space recommended, or SAN via HBA (not through software) if installing with multipath boot from SAN (see http://hcl.vmd.citrix.com for a detailed list of compatible storage solutions).

Network

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

For redundancy, multiple NICs are recommended. The configuration of NICs will differ depending on the storage type. See vendor documentation for details

> **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. Therefore, when setting up a 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, customers should investigate if an embedded management device, such as Dell DRAC or HP iLO can be configured. For more information on setting up serial console access, see CTX228930, How to Configure Serial Console Access on XenServer 7.0 and later.

XenCenter System Requirements

The system requirements for XenCenter are:

- *Operating System*: Windows 10, Windows 8.1, Windows 8, Windows 7 SP1, Windows Vista SP2, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1, Windows Server 2008 SP2
- *.NET Framework*: Version 4.6
- *CPU Speed*: 750MHz minimum, 1GHz or faster recommended
- *RAM*: 1GB minimum, 2GB or more recommended
- *Disk Space*: 100MB minimum
- *Network*: 100Mb or faster NIC
- *Screen Resolution*: 1024x768 pixels, minimum

XenCenter is compatible with all previous versions of XenServer from 6.0 onwards.

Supported Guest Operating Systems

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

Configuration limits

December 2, 2020

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 in the following tables. 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 might 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 Administrators Guide 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
Storage repositories per host (NFS)	400 (See note 5)
Networking	

Item	Limit
Physical NICs per host	16 (See note 6)
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 7)

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, network 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. To work with a large number of SRs, ensure that you install all of the latest hotfixes on XenServer 7.1 CU2.
6. If you have multiple high-speed NICs, you might experience out of memory issues in dom0 during XenServer installation. If you have more than four 10Gb NICs or more than two 40Gb NICs, consider increasing the amount of dom0 memory to 8 GiB. To change the amount of dom0 memory, go to the install options in the boot menu for the XenServer host and modify

> the Xen boot options to include `dom0_mem=max:8192M`.
>
> 7. 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	16
Networking	
VLANs per resource pool	800
Active hosts per cross-server private network	16
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
Disaster recovery	
Integrated site recovery storage repositories per resource pool	8
Storage	
Paths to a LUN	8
Multipathed LUNs per host	256 (See note 1)
Multipathed LUNs per host (used by storage repositories)	256 (See note 1)

Item	Limit
VDIs per SR (NFS, SMB, EXT, GFS2)	20000
VDIs per SR (LVM)	1000
Storage repositories per pool (NFS)	400 (See note 2)
Storage live migration	
(non-CDROM) VDIs per VM	6
Snapshots per VM	1
Concurrent transfers	3
XenCenter	
Concurrent operations per pool	25

> **Note:**
>
> 1. 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.
> 2. To work with a large number of SRs, ensure that you install all of the latest hotfixes on XenServer 7.1 CU2.

Guest operating system support

March 14, 2022

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 8.1 (32-bit)	HVM	1 GB	4 GB	24 GB (40 GB or more recommended)

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Windows 8.1 (64-bit)	HVM	2 GB	512 GB	24 GB (40 GB or more recommended)
Windows 10 (32-bit) [Latest tested version is 21H1]	HVM	1 GB	4 GB	24 GB (40 GB or more recommended)
Windows 10 (64-bit) [Latest tested version is 21H1]	HVM	2 GB	1.5 TB	32 GB (40 GB or more recommended)
Windows Server 2012, Windows Server 2012 R2 (64-bit)	HVM	512 MB	1.5 TB	24 GB (40 GB or more recommended)
Windows Server 2016, Windows Server Core 2016 (64-bit)	HVM	1 GB	1.5 TB	24 GB (40 GB or more recommended)
Windows Server 2019 (Desktop), Windows Server 2019 (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
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

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
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 (64-bit)	HVM	2 GB	1.5 TB	10 GB
CentOS 8 (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
Red Hat Enterprise Linux 6.2–6.9 (64-bit)	PV	1 GB	128 GB	8 GB
Red Hat Enterprise Linux 7 (64-bit)	HVM	2 GB	1.5 TB	10 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Red Hat Enterprise Linux 8 (64-bit)	HVM	2 GB	1.5 TB	10 GB
SUSE Linux Enterprise Server 10, 10 SP1, 10 SP, 10 SP3, 10 SP4 (32-bit)	PV	512 MB	16 GB	8 GB
SUSE Linux Enterprise Server 10, 10 SP1, 10 SP, 10 SP3, 10 SP4 (64-bit)	PV	512 MB	128 GB	8 GB
SUSE Linux Enterprise Server 11, 11 SP1, 11 SP2 (32-bit)	PV	1 GB	64 GB	8 GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (32-bit)	PV	1 GB	16 GB	8 GB
SUSE Linux Enterprise Server 11, 11 SP1, 11 SP2, 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, SP4 (64-bit)	HVM	1 GB	1.5 TB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
SUSE Linux Enterprise Server 15 SP1 (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, SP4 (64-bit)	HVM	1 GB	1.5 TB	8 GB
Oracle Linux 5.0–5.7, 5.10, 5.11 (32-bit)	PV	512 MB	64 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 5.11 (32-bit)	PV	512 MB	16 GB	8 GB

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
Scientific Linux 5.11 (64-bit)	PV	512 MB	128 GB	8 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
Ubuntu 10.04 (32-bit)	PV	128 MB	32 GB	8 GB
Ubuntu 10.04 (64-bit)	PV	128 MB	32 GB	8 GB
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

Operating System	Virtualization mode	Minimum RAM	Maximum RAM	Minimum Disk Space
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
NeoKylin Linux Advanced Server 6.5 (64-bit)	PV	1 GB	128 GB	8 GB
NeoKylin Linux Advanced Server 7.2 (64-bit)	HVM	1 GB	1.5 TB	10 GB

> **Important:**
>
> - RHEL, OL, and CentOS 5.x guest operating systems with the original kernel fail to start on XenServer. Before attempting to upgrade XenServer hosts to 7.1, 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 to exceed the maximum amount of physical memory that your operating system can address. Setting a memory maximum that is greater than the operating system supported limit might lead to stability problems within your guest.
>
> **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

Out-of-support operating systems

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

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

> **Note:**
>
> Windows versions that are supported by Microsoft as part of an LTSB branch are supported by Citrix Hypervisor.
> Windows versions that are out of support, but are part of an Extended Security Updates (ESU) agreement with Microsoft are not supported by Citrix Hypervisor.

Quick Start Guide

February 22, 2021

This guide is only available as a PDF.

Quick Start Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Technical FAQ

February 22, 2021

This guide is only available as a PDF.

Technical FAQ (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Licensing FAQ

February 22, 2021

This guide is only available as a PDF.

Licensing FAQ (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Install

October 13, 2021

This article guides you through the installation of Citrix XenServer 7.1 LTSR and its Cumulative Updates. It also contains information about troubleshooting problems that might occur during installation and points you to additional resources.

This article is primarily aimed at system administrators who wish to set up XenServer hosts on physical servers.

Installation overview

XenServer 7.1 Cumulative Updates are provided as both an update to the previous Cumulative Update of XenServer 7.1 and as a base installation that can be used to upgrade other versions of XenServer or to create a fresh installation.

> **Note:**
>
> There is no supported direct upgrade path from out-of-support versions of XenServer to

> XenServer 7.1 or its latest Cumulative Update. Instead, perform a fresh installation.

If you are updating an existing installation of XenServer 7.1 with the previous Cumulative Update installed:

- Use the XenServer 7.1 Cumulative Update *X* Installation file

  You can download this file from the download site

- Review the information in Update your hosts before updating your XenServer installation.

If you are creating a fresh installation of XenServer 7.1 Cumulative Update *X*:

- Use the XenServer 7.1 Base Installation ISO including Cumulative Update *X* file

  You can download this file from the download site

- Review the information in System Requirements, To license Citrix XenServer:, and Install XenServer and XenCenter before installing XenServer.

Install XenServer and XenCenter

This section steps through installing the XenServer host software on physical servers, installing XenCenter on Windows workstations and finally connecting them to form the infrastructure for creating and running Virtual Machines (VMs).

After guiding you through installation, this section describes a selection of common installation and deployment scenarios.

Installation Media and Methods

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; refer to the XenServer Hardware Compatibility List (HCL) for details.

The XenServer host consists of:

- The **Xen Hypervisor**: The hypervisor is the basic abstraction layer of software. The hypervisor is responsible for low-level tasks such as CPU scheduling and is responsible for memory isolation for resident VMs. The hypervisor abstracts from the hardware for the VMs. The hypervisor has no knowledge of networking, external storage devices, video, etc. The Linux Foundation Xen Project community develops and maintains the Xen hypervisor as free software licensed under the GNU General Public License. XenServer 7.1 uses v4.7 of the Xen hypervisor.

- The **Control Domain**: Also known as 'Domain0', or 'dom0', the Control Domain is a secure, privileged Linux VM (based on a CentOS 7.2 distribution) that runs the XenServer management toolstack. Besides providing XenServer management functions, the Control Domain also runs the driver stack that provides user created Virtual Machines (VMs) access to physical devices.
- The **management toolstack**: Also known as xapi, this software toolstack controls VM lifecycle operations, host and VM networking, VM storage, user authentication, and allows the management of XenServer resource pools. xapi provides the publicly documented XenAPI Management Interface which is used by all tools that manage VMs and resource pools.
- VM templates, for installing popular operating systems as VMs.
- A local Storage Repository (SR) reserved for VMs.

> **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 is an unsupported configuration.

Installation Media

Installers for both the XenServer host and XenCenter are located on the installation media. The installation media also includes the Readme First, which provides descriptions of and links to helpful resources, including product documentation for XenServer and XenCenter components.

While an installer for XenCenter is included in the installation media, more recent versions of XenCenter are provided as a separate download on the XenServer 7.1 Downloads page. We recommend that you get the latest version of XenCenter from this page. The latest version of XenCenter supersedes the previous versions.

Installation Methods

There are three methods by which to install the XenServer host:

- From a CD

  You can download the installer (ISO file format) and burn it to a CD. To download the installer, visit the XenServer Downloads page.

  The main XenServer installation file contains the basic packages required to set up XenServer on your host.

- 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 Installations.

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

  For details, see Boot from SAN Environments.

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 XenServer Supplemental Packs and the DDK Guide.

Upgrades

The installer presents the option to upgrade if 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 XenServer.

Install 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. For general help, press F1.
>
> **Warning**
>
> Installing XenServer overwrites data on any hard drives that you select to use for the installation. Back up data that you wish 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.

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 Upgrade 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 disk(s) you would like 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 utilization of available storage, select **Enable thin provisioning**. Citrix Virtual Desktop users are *strongly* recommended to select this option in order for local caching to work properly. For details, see IntelliCache.

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**:

   a) Set up networking so that the installer can connect to the XenServer installation media files.

      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) 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.

Download the latest version of XenCenter from the XenServer 7.1 Download page.

To install XenCenter:

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

May 16, 2019

This article 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:**
>
> Live migration of VMs between XenServer hosts is only available when they share storage.

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 (live migration) 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 the XenServer Administrator's Guide.

We recommend that you create a pool before you add shared storage. For pool requirements and setup procedures,see the XenCenter Help or the XenServer Administrator's Guide.

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:

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

   The `device-config-server` argument refers to the name of the NFS server and the `device-config-serverpath` argument refers to the path on the server. Since `shared` is set to true, the shared storage is automatically connected to every host in the pool. Any hosts that later join are also connected to the storage. The UUID of the created storage repository is printed to the console.

3. Find the UUID of the pool by using the `pool-list` command.
4. Set the new SR as the pool-wide default by entering the following:

```
xe pool-param-set uuid=pool_uuid \
       default-SR=storage_repository_uuid
<!--NeedCopy-->
```

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:

```
xe-set-iscsi-iqn iscsi_iqn
<!--NeedCopy-->
```

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

```
xe host-param-set uuid=host_uuid other-config-iscsi_iqn=iscsi_iqn
<!--NeedCopy-->
```

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:

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

```
xe sr-create name-label=name_for_sr \
    content-type=user device-config-target=iscsi_server_ip_address \
    device-config-targetIQN=iscsi_target_iqn \
    device-config-localIQN=iscsi_local_iqn \
    type=lvmoiscsi shared=true device-config-LUNid=lun_id
<!--NeedCopy-->
```

   The `device-config-target` argument refers to the name or IP address of the iSCSI server. The `device-config-LUNid` argument can be a list of LUN IDs (separated by commas). Since the `shared` argument is set to `true`, the shared storage is automatically connected to every host in the pool. Any hosts that subsequently join are also connected to the storage.

   The command returns the UUID of the created storage repository.

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

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

```
xe pool-param-set uuid=pool_uuid default-SR=iscsi_shared_sr_uuid
<!--NeedCopy-->
```

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

Upgrade from an existing version

October 13, 2021

This article documents how to upgrade your XenServer deployment from an existing version. It guides you through upgrading your XenServer hosts - both pooled and standalone - automatically and manually.

> **Notes:**
>
> - Use the latest version of XenCenter provided on the XenServer 7.1 Downloads page to update your hosts and pools.
> - We recommend that you upgrade directly to the latest Cumulative Update of XenServer 7.1. A Cumulative Update contains fixes that are not included in the initial XenServer 7.1 release.
> - You might prefer to perform a clean installation of the most recent version of XenServer rather than performing one or more upgrades.
> - VMs can be exported from all versions of XenServer from 6.0 and directly imported into 7.1. For more information, see the **Importing and Exporting VMs** section in the Virtual Machine User's Guide.
> - Ensure that after you upgrade from or import VMs from XenServer 6.x, you install the latest version of the XenServer PV Tools provided with this version of XenServer on your VMs. For more information, see the Virtual Machine User's Guide.
> - Upgrading a XenServer host - and particularly a pool of XenServer hosts - requires careful planning and attention. Be sure to map your upgrade path carefully. You can also use the XenCenter Rolling Pool Upgrade wizard. Ensure that you choose the option to *upgrade* when you step through the installer to avoid losing any existing data.
> - Boot from SAN setting is *not* inherited during the manual upgrade process. When upgrading using the ISO or PXE process, customers should 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.

XenServer hosts must be running at least version 6.2 to upgrade directly to version 7.1 or its latest Cumulative Update. Customers wishing to upgrade from earlier versions of XenServer must upgrade to version 6.2, before upgrading to version 7.1 or its latest Cumulative Update.

The following table lists the upgrade path from previous versions of XenServer:

Version	Direct upgrade to the latest XenServer 7.1 Cumulative Update?
XenServer 7.1 with all previous Cumulative Updates applied	No. Use the update mechanism instead. For more information, see Update your hosts.
Other XenServer 7.1	No. Use the update mechanism instead. You must apply all Cumulative Updates in order before applying the latest Cumulative Update. For more information, see Update your hosts.
XenServer 7.0	See note

Version	Direct upgrade to the latest XenServer 7.1 Cumulative Update?
XenServer 6.5.0	See note
XenServer 6.2.0	See note

> **Note:**
>
> XenServer 7.0, 6.5.0, and 6.2.0 were supported for direct upgrade to XenServer 7.1 Cumulatve Update 2 at the time of its release. However, these releases are now EoL and therefore not eligible for support.
> There is no supported direct upgrade path from out-of-support versions of XenServer to XenServer 7.1 Cumulatve Update 2. Instead, perform a fresh installation.

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.

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

You can perform a rolling pool upgrade by using XenCenter or the xe CLI. If you are 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, you need to perform the rolling upgrade manually by first planning your upgrade path and then live migrating running VMs between XenServer hosts accordingly.

The Rolling Pool Upgrade wizard is available only for licensed XenServer 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 7.1 Cumulative Update 2 to upgrade from any supported version of XenServer to XenServer 7.0 and later.

> **Note:**
>
> Rolling Pool Upgrade using XenCenter is only available only for licensed XenServer 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 the latest version of XenCenter from the XenServer Product Download page. Using XenCenter to upgrade to a newer version of XenServer is not supported.

  The latest version of XenCenter available on the download page is more recent than the version released at the same time as Cumulative Update 2. The latest version of XenCenter supersedes any earlier versions.

- 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 the XenServer Administrator's Guide. 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 XenCenter Rolling Pool Upgrade wizard:

1. Open the Rolling Pool Upgrade wizard: on the **Tools** menu, select **Rolling Pool Upgrade**.

2. Read the **Before You Start** information, and then click **Next** to continue.

3. Select the pools and any individual hosts that you want to upgrade, and then click **Next**.

4. Choose one of the following modes:

   - **Automatic Mode** for an automated upgrade from network installation files on an HTTP, NFS, or FTP server
   - **Manual Mode** for a manual upgrade from either a 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 would like XenCenter to automatically resolve all failed prechecks, click **Resolve All**.

   When all prechecks have been resolved, click **Next** to continue.
8. Prepare the XenServer installation media.

   If you choose **Automatic Mode**, enter the installation media details. Choose **HTTP**, **NFS** or **FTP** and then specify the path, username 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. You **cannot** migrate VMs from an upgraded host to one running an older version of XenServer. For example, from version 7.1 to version 7.0. 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 the XenServer Administrator's Guide. 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.

Before you begin your rolling pool upgrade

- If you are using XenCenter, upgrade XenCenter to the latest version available on the XenServer downloads page.

  The latest version of XenCenter available on the download page is more recent than the version released at the same time as Cumulative Update 2. The latest version of XenCenter supersedes any earlier versions.

  The latest 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 you upgrade 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 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 until the installer offers you the option to upgrade. For more information, see Install XenServer and XenCenter.

   > **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.

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 using the xe CLI:

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

   ```
   xe vbd-list type=CD empty=false
   <!--NeedCopy-->
   ```

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

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

   uuid ( RO) : ec174a21-452f-7fd8-c02b-86370fa0f654
   vm-uuid ( RO): db80f319-016d-0e5f-d8db-3a6565256c71
   ```

```
vm-name-label ( RO): VM01_DemoLinux
vdi-uuid ( RO): a14b0345-b20a-4027-a233-7cbd1e005ede
empty ( RO): false
device ( RO): xvdd
<!--NeedCopy-->
```

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

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

```
xe vbd-eject uuid=uuid
<!--NeedCopy-->
```

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:

```
xe host-disable host-selector=host_selector_value
<!--NeedCopy-->
```

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. For more information, see Install XenServer and XenCenter.

> **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 4, 2022

Updates can often be applied with minimal service interruption. Citrix recommends that customers use the latest version of XenCenter to apply all updates. If you are updating a pool of XenServer hosts, you can avoid downtime of VMs by using XenCenter's **Install Update** wizard to apply 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 periodically check for available XenServer and XenCenter updates and new versions. Any Alerts will be displayed in the **Notifications** pane. Use the latest version of XenCenter provided on the XenServer 7.1 Downloads page to update your hosts and pools.

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 (CUs)**, 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.

> **Note:**
>
> Both Hotfixes and Cumulative Updates can be applied by using the procedures in this article. For example, use the following procedures to apply a XenServer 7.1 Cumulative Update to XenServer 7.1.

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 a XenServer pool, customers should pay careful attention to the following:
>
> - Use the latest version of XenCenter provided on the XenServer 7.1 Downloads page to update your hosts and pools.
> - You must upgrade or update each host in a pool to the latest Cumulative Update of XenServer 7.1 before applying any hotfixes.
> - You must apply all Cumulative Updates in the order that they are released. You cannot apply the latest Cumulative Update of XenServer 7.1 before applying any previous Cumulative Updates.
> - Back up your data before applying an update. For backup procedures, see the XenServer Administrator's Guide.
> - Update all servers in a pool within a short period: running a mixed-mode pool (a pool that includes updated and non-updated servers) is not a supported configuration. Scheduled your updates to minimize the amount of time that a pool runs in a mixed state.
> - Update all servers within a pool sequentially, always starting with the pool master. XenCenter's **Install Update** wizard manages this process automatically.
> - After applying a Cumulative Update to all hosts in a pool, update any required driver disks before restarting XenServer hosts.

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 you upgrade 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 up-to-date. Where possible, XenCenter limits it to a single reboot at the end. For more information, see Apply Automated Updates.

Apply an update to a pool

To apply an update to a pool by using XenCenter:

1. From the XenCenter navigation pane, 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.
11. If you chose to perform post-update tasks manually, do so now.

    Ensure that you perform these post-update tasks before attempting to apply further updates.

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 wish to update by running the following:

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

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:

```
xe update-pool-apply uuid=UUID_of_file
<!--NeedCopy-->
```

   This applies the update or hotfix to all hosts in the pool.

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

```
xe upload-apply host-uuid=UUID_of_host uuid=UUID_of_file
<!--NeedCopy-->
```

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, as necessary such as, restarting the XAPI toolstack, or rebooting the hosts.

   Ensure that you perform these post-update tasks before attempting to apply further updates.

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 host(s) that you wish to update by using the `vm-shutdown` or `vm-suspend` commands.
3. Upload the update file to the host you wish to update by running the following:

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

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

   > **Tip:**
   >
   > When an update file has been uploaded to a 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 (for example, VMs are running on the host), it alerts you. Be sure to follow any guidance before continuing with the update.
5. Update the host, specifying the UUIDs of the host and the update file, by running the following:

   ```
   xe update-apply host-uuid=UUID_of_host uuid=UUID_of_file
   <!--NeedCopy-->
   ```

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).

   Ensure that you perform these post-update tasks before attempting to apply further updates.

Live patching

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 customers who have access to XenServer through their Citrix Virtual Apps and Desktops (formerly Citrix XenApp and XenDesktop) entitlement. To learn more about XenServer editions, and to find out how to upgrade, visit the Citrix website. For detailed information on Licensing, see XenServer 7.1 Licensing FAQ.

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.

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

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

Using XenCenter

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

Using the xe CLI

- To enable Live Patching, run the following command:

```
xe pool-param-set live-patching-disabled=false uuid=”pool_uuid”
<!--NeedCopy-->
```

- To disable Live Patching, run the following command:

```
xe pool-param-set live-patching-disabled=true uuid=”pool_uuid”
<!--NeedCopy-->
```

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.

As a prerequisite, 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. For more information on Licensing, refer to XenServer 7.1 Licensing FAQ.

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 of the pool master.
   > - 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.

Licensing

February 4, 2021

XenServer 7.1 is available in two commercial editions:

- Standard
- Enterprise

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. 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 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 (vGPU) with NVIDIA vGPU 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

Customers who have purchased Citrix Virtual Apps or Citrix Virtual XenDesktop (formerly Citrix XenApp and XenDesktop) have an entitlement to XenServer, which includes all the features listed previously. Note that in XenServer 7.1, all XenServer 7.1 customers are able to
use the In-memory Read Caching feature (previously available to Platinum customers only).

Apply a license

XenServer uses the same licensing mechanism, as used by many other Citrix products. XenServer 7.1 licensing requires Citrix License Server 11.13.1.2 or higher. You can download the License Server from Citrix Licensing. After purchasing a license, you will be provided with a .LIC license key. This license key should be installed on either:

- a Windows server running the Citrix License Server software.
- the Linux-based Citrix License Server virtual appliance.

Customers should allocate product licenses using a Citrix License Server, as with other Citrix components. From version 6.2.0 onwards, XenServer (other than through the XenDesktop 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 will display as Citrix XenServer Per-Socket Edition. All hosts in a pool must be licensed. Mixed pools of licensed and unlicensed hosts will behave as if all hosts were unlicensed.

> **Note:**
>
> Upgrades to the Enterprise edition are available from the Standard edition. Click here to purchase a XenServer 7.1 license.

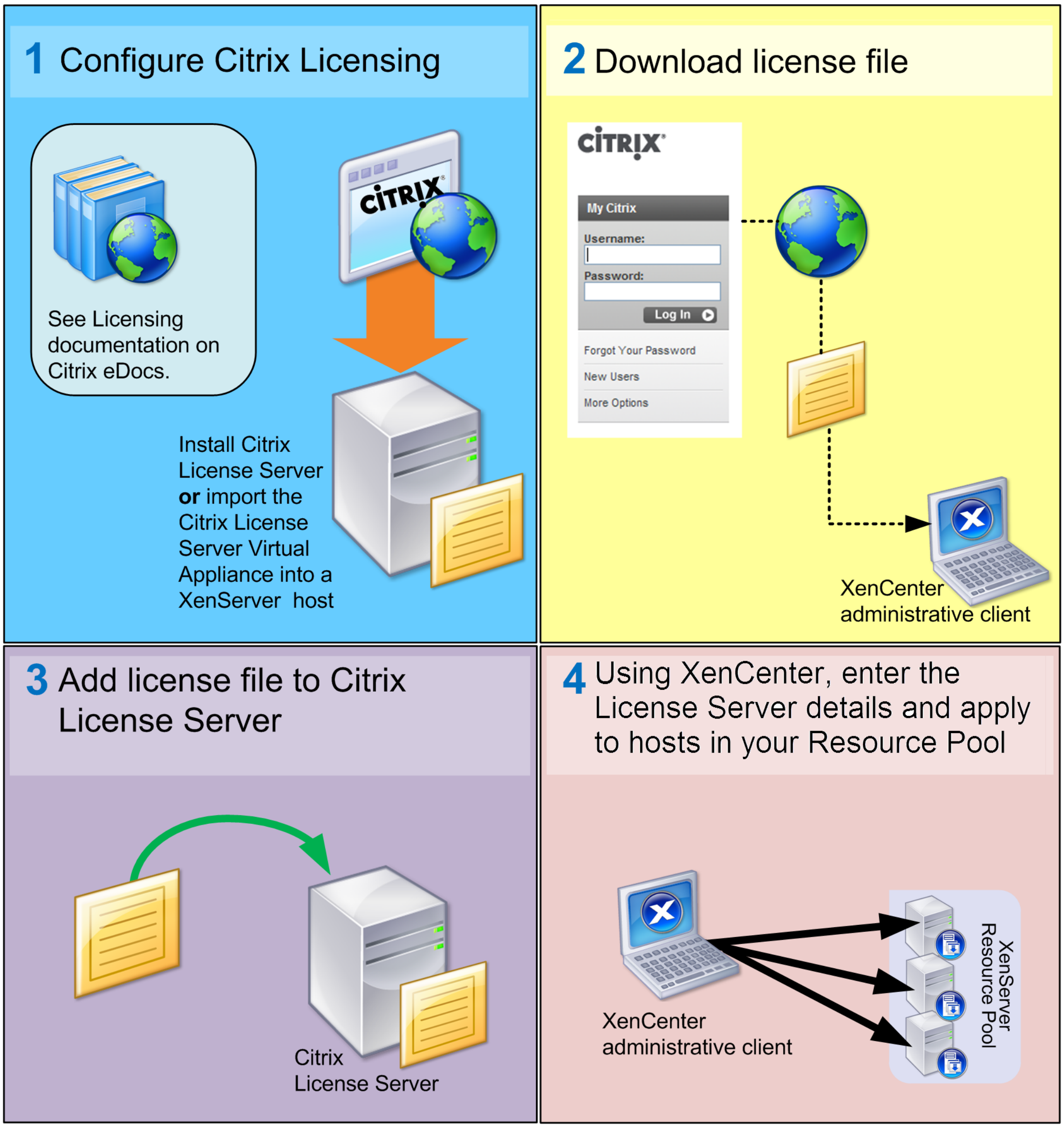
For instructions on applying a XenServer license to a Citrix License Server Virtual Appliance, see CTX200159.

To license Citrix XenServer

1. Install the Citrix License Server and console.

   For detailed installation procedures, see Licensing on the Citrix Product Documentation website.

2. Obtain your Citrix XenServer license files and load them on the Citrix License Server.
3. Configure licensing for each Citrix XenServer host using XenCenter or the xe CLI.

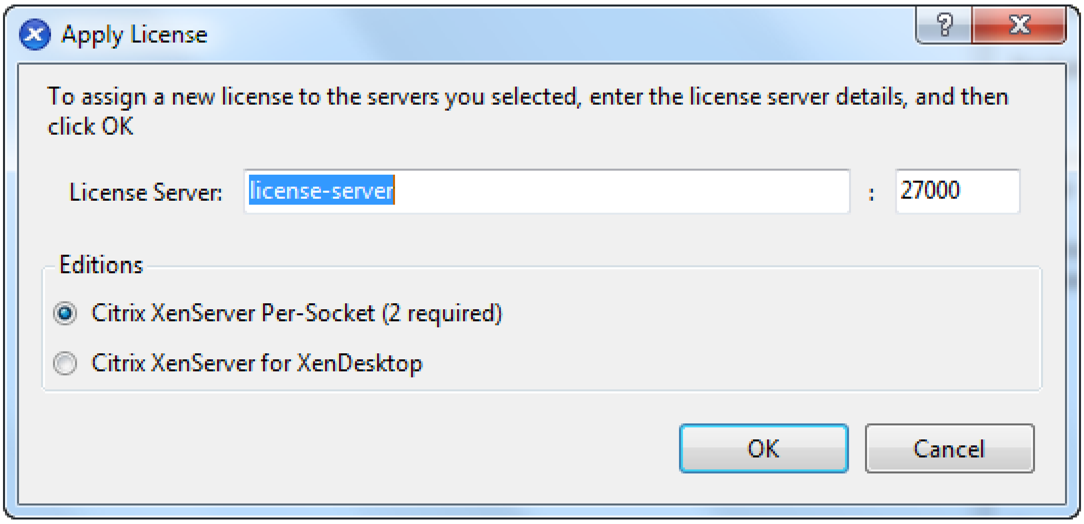

1 Configure Citrix Licensing
See Licensing documentation on Citrix eDocs.
CITRIX
Install Citrix License Server **or** import the Citrix License Server Virtual Appliance into a XenServer host
2 Download license file
CITRIX
My Citrix
Username:
Password:
Log In
Forgot Your Password
New Users
More Options
XenCenter administrative client
3 Add license file to Citrix License Server
Citrix License Server
4 Using XenCenter, enter the License Server details and apply to hosts in your Resource Pool
XenCenter administrative client
XenServer Resource Pool

To configure licensing by using XenCenter

For more information on using XenCenter press F1 to access the context sensitive Online Help.

1. On the Tools menu, select License Manager.
2. Select the host(s) or pool/s that you wish to assign a license. Click Assign License.

   This displays the Apply License window:



Apply License

To assign a new license to the servers you selected, enter the license server details, and then click OK

License Server: license-server : 27000

Editions

● Citrix XenServer Per-Socket (2 required)

○ Citrix XenServer for XenDesktop

3. In the Apply License window, choose the Citrix XenServer edition that you wish to license, and then enter the Citrix License Server details.

   > **Note**
   >
   > By default, the License Server uses port 27000 for communication with Citrix products. If you changed the default port on the License Server, enter the appropriate number in the Port number box. For more information about changing port numbers due to conflicts, refer to Licensing topics on the Citrix Product Documentation website.

4. Select OK to proceed.

   XenCenter contacts the specified License Server and checks out a license for the specified host(s) or pool/s. The information shown in the XenCenter License Manager will be updated.

To release a license (to revert a licensed XenServer host to unlicensed XenServer): from the License Manager, select a host, and then click Release License.

To configure licensing for Citrix XenServer hosts by using the xe CLI

Run the `host-apply-edition` command. For example, enter the following:

```
xe host-apply-edition edition= enterprise-per-socket|desktop-plus|
   desktop| \
        standard-per-socket\ license-server-address=
            license_server_address \
        host-uuid=uuid_of_host license-server-port=license_server_port
<!--NeedCopy-->
```

You will only need to supply the license server IP address and port number parameters for the first time you assign a license. The values are stored and used automatically if in future, you do not specify the license server parameters.

If no host UUID is specified, the license will be applied to the host that you are running the command on.

To configure a pool

Run the `pool-apply-edition` command. For example, enter the following:

```
xe pool-apply-edition edition= enterprise-per-socket|desktop-plus|desktop| \
        standard-per-socket\ license-server-address=license_server_address \
        pool-uuid=uuid_of_pool license-server-port=license_server_port
<!--NeedCopy-->
```

Discovering the license status of hosts and pools

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.

You can also go to the **General** tab of the server and find the license type in the **License Details** section.

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.

To find the license type of a server by using the command line, run the following command in the console of a server in your pool:

```
xe host-license-view host_uuid=<UUID> | grep sku_marketing_name
```

Additional Licensing Information

This section discusses miscellaneous licensing information, such as, license expiry and grace periods.

Refer to the XenServer 7.1 Licensing FAQ for more information.

License Expiry

XenCenter notifies you when your license is due to expire. You should purchase a license before it expires. When a XenServer license expires:

- XenCenter License Manager will display the status as Unlicensed.
- You will no longer be able to access licensed features or receive Citrix Technical Support for any host within the pool until you purchase another license.

License Grace Period

Citrix licensing has built-in timeout technology. After a startup license is checked out by a XenServer host, XenServer and the License Server exchange "heartbeat" messages every five minutes to indicate to each other that they are still up and running. If a XenServer host cannot contact the License Server, for example, due to problems with the License Server hardware or software or network failures, the server lapses into a 30-day licensing grace period. During the grace period, XenServer licenses itself through cached information and the hosts are allowed to continue operations as if they were still in communication with the License Server. The grace period is 30 days and when the grace period runs out, XenServer reverts to an unlicensed state. After communication is re-established between XenServer and the License Server, the grace period is reset.

Troubleshoot the installation

May 9, 2019

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.

For information on the different types of support and maintenance programmes offered by Citrix , see www.citrix.com/support/programs.html.

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.

In most cases, if you experience an unknown error during installation, The Citrix Technical Support will request that you capture the log file from your host and then send it along for the Support team to inspect. If requested, follow the procedure below.

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

To capture and save the log files:

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

```
/opt/xensource/installer/report.py
<!--NeedCopy-->
```

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`.

IntelliCache

May 16, 2019

> **Note:**
>
> This feature is only supported when using XenServer with XenDesktop.

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 XenDesktop 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.

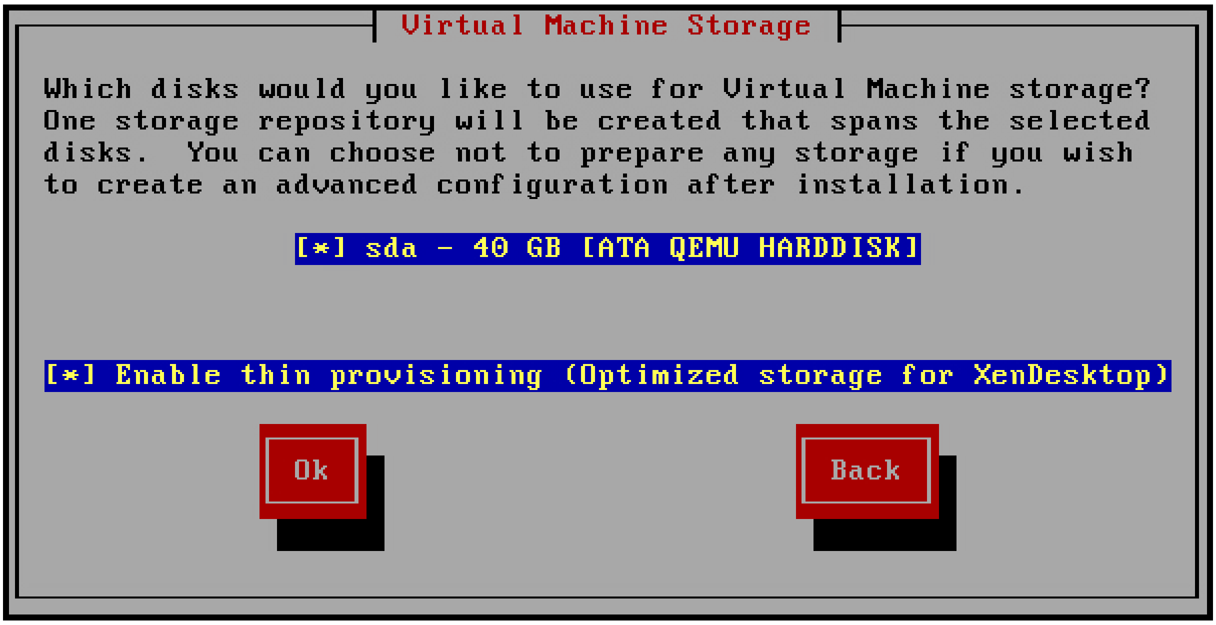
IntelliCache deployment

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.



Virtual Machine Storage

Which disks would you like to use for Virtual Machine storage? One storage repository will be created that spans the selected disks. You can choose not to prepare any storage if you wish to create an advanced configuration after installation.

[*] sda - 40 GB [ATA QEMU HARDDISK]

[*] Enable thin provisioning (Optimized storage for XenDesktop)

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.

```
    localsr=`xe sr-list type=lvm host=hostname params=uuid --minimal`
        echo localsr=$localsr
        pbd=`xe pbd-list sr-uuid=$localsr params=uuid --minimal`
        echo pbd=$pbd
        xe pbd-unplug uuid=$pbd
        xe pbd-destroy uuid=$pbd
        xe sr-forget uuid=$localsr
        sed -i ”s/'lvm'/'ext'/” /etc/firstboot.d/data/default-storage.conf
        rm -f /etc/firstboot.d/state/10-prepare-storage
        rm -f /etc/firstboot.d/state/15-set-default-storage
        service firstboot start
        xe sr-list type=ext
<!--NeedCopy-->
```

To enable local caching, enter the following commands:

```
    xe host-disable host=hostname
        localsr=`xe sr-list type=ext host=hostname params=uuid --minimal`
        xe host-enable-local-storage-caching host=hostname sr-uuid=$localsr
        xe host-enable host=hostname
<!--NeedCopy-->
```

VM 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 live migration and High Availability?

A: You can use live migration 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:

```
xe sr-list params=local-cache-sr,uuid,name-label
<!--NeedCopy-->
```

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.

Boot from SAN environments

May 16, 2019

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:

```
default xenserver
label xenserver
```

```
    kernel mboot.c32
    append /tftpboot/xenserver/xen.gz dom0_max_vcpus=1-2 \
    dom0_mem=1024M,max:1024M com1=115200,8n1 \
    console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
    xencons=hvc console=hvc0 console=tty0 \
    device_mapper_multipath=yes \
    install ---  /tftpboot/xenserver/install.img
<!--NeedCopy-->
```

For additional information on storage multipathing in your XenServer environment, see the XenServer Administrator's Guide.

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:

   ```
   ---  /install.img
   <!--NeedCopy-->
   ```

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

   ```
   use_ibft ---  /install.img
   <!--NeedCopy-->
   ```

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:

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

The following example shows PXE configuration for a multipathed LUN:

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

Network boot installations

December 16, 2020

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 article 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

To 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 `/tftboot` 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), `vmlinuz`, and `xen.gz` (from the `/boot` directory) to the new `/tftpboot/xenserver` directory on the TFTP server.
4. In the `/tftboot` 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.

```
    default xenserver
    label xenserver
    kernel mboot.c32
    append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
      dom0_mem=1024M,max:1024M com1=115200,8n1 \
    console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
    xencons=hvc console=hvc0 console=tty0 \
    ---  /tftpboot/xenserver/install.img
<!--NeedCopy-->
```

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.

```
    default xenserver-auto
    label xenserver-auto
       kernel mboot.c32
       append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
       dom0_mem=1024M,max:1024M com1=115200,8n1 \
       console=com1,vga ---  /tftpboot/xenserver/vmlinuz \
      xencons=hvc console=hvc0 console=tty0 \
      answerfile=http://pxehost.example.com/answerfile \
      install ---  /tftpboot/xenserver/install.img
<!--NeedCopy-->
```

For more information about PXE configuration file contents, see the SYSLINUX website.

Configuring 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:

```
menuentry ”XenServerInCloud Sphere Install (serial)” {

    multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M watchdog \
    dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
    module2 /EFI/xenserver/vmlinuz console=hvc0
    module2 /EFI/xenserver/install.img
 }

<!--NeedCopy-->
```

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.

> **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 leftmost.

```
default xenserver
label xenserver
    kernel mboot.c32
    append /tftpboot/EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M watchdog \
      dom0_max_vcpus=4 com1=115200,8n1 \
    console=com1,vga ---  /tftpboot/EFI/xenserver/vmlinuz \
    console=hvc0 console=tty0 \
    ---  /tftpboot/EFI/xenserver/install.img
<!--NeedCopy-->
```

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

> **Note**
>
> To specify which network adapter should be used for retrieving 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.

```
default xenserver-auto
label xenserver-auto
    kernel mboot.c32
    append /tftpboot/EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M watchdog \
        dom0_max_vcpus=4 com1=115200,8n1 \
        console=com1,vga ---  /tftpboot/EFI/xenserver/vmlinuz \
        console=hvc0 console=tty0 \
        answerfile=http://pxehost.example.com/answerfile \
        install ---  /tftpboot/EFI/xenserver/install.img
<!--NeedCopy-->
```

Refer to your server operating system manual for details of your specific operating system. 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:

```
<?xml version=”1.0”?>
<installation srtype=”ext”>
    <primary-disk>sda</primary-disk>
    <guest-disk>sdb</guest-disk>
    <guest-disk>sdc</guest-disk>
    <keymap>us</keymap>
    <root-password>mypassword</root-password>
    <source type=”url”>http://pxehost.example.com/xenserver/</source>
    <post-install-script type=”url”>
        http://pxehost.example.com/myscripts/post-install-script
    </post-install-script>
    <admin-interface name=”eth0” proto=”dhcp” />
    <timezone>Europe/London</timezone>
</installation>
<!--NeedCopy-->
```

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 XenDesktop to work properly. For more information, see the XenServer Administrator’s Guide.

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

- `<primary-disk>` (required)

  The name of the storage device where the control domain should be installed, equivalent to the choice made on the **Select Primary Disk** step of the interactive 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>
<!--NeedCopy-->
```

If this attribute is not specified, the default is yes. If you specify no, it is possible to automate an installation scenario where no storage repository is created, if, in addition, no guest-disk keys are specified

- `<guest-disk>`

  The name of a storage device to be used for storing guests. You should use one of these elements for each extra disk.

- `<keymap>` (required)

  The name of the keymap to use during installation

  ```
  <keymap>us</keymap>
  <!--NeedCopy-->
  ```

  The default value, us will be considered if you do not specify a value for this attribute.

- `<root-password>`

  The desired root password for the XenServer host. If a password is not provided, a prompt will be displayed when the host is first booted.

  Attributes:

  Type: hash or plaintext

  For example:

  ```
  <root-password type=”hash”>hashedpassword</root-password>
  <!--NeedCopy-->
  ```

- `<source>` (required)

  The location of the uploaded XenServer installation media or a Supplemental Pack. Element may occur multiple times.

  Attributes:

type: url, nfs, or local

If local, leave the element empty. For example,

```
<source type=”url”>http://server/packages</source>
<source type=”local” />
<source type=”nfs”>server:/packages</source>
<!--NeedCopy-->
```

- `<script>`

  Where the post-install-script is.

  Attributes:

  stage: filesystem-populated, installation-start, or installation-complete

  - When filesystem-populated is used, the script is invoked just before root file system is unmounted (for example, after installation/upgrade, initrds already built, etc.). The script receives an argument that is the mount point of the root file system.
  - When installation-complete is used, the script will be run once the installer has finished all operations (and hence the root file system will be unmounted). The script receives an argument that will have a value of zero if the installation completed successfully, and will be non-zero if the installation failed for any reason.

  type: url, nfs, or local

  If url or nfs, put the URL or NFS path in the PCDATA; if local, leave the PCDATA empty. For example,

```
<script stage=”filesystem-populated” type=”url”>
    http://prehost.example.com/post-install-script
</script>
<script stage=”installation-start” type=”local”>
    file:///scripts/run.sh
</script>
<script stage=”installation-complete” type=”nfs”>
    server:/scripts/installation-pass-fail-script
</script>
<!--NeedCopy-->
```

Note that if a local file is used, ensure that the path is absolute. This will generally mean that the `file://` prefix will be followed by a further forward slash, and the complete path to the script.

- `<admin-interface>`

  The single network interface to be used as the host administration interface.

  Attributes:

  Specify one of the following attributes:

  - `name` - The name of your network interface, for example `eth0`.
  - `hwaddr` - The MAC address of your network interface, for example `00:00:11:aa:bb:cc`.

  The attribute `proto` can have one of the following values: `dhcp` or `static`.

  If you specify `proto=”static”`, you must also specify all of these child elements:

  - `<ipaddr>`: The IP address
  - `<subnet>`: The subnet mask
  - `<gateway>`: The gateway

- `<timezone>` (required)

  In the format used by the TZ variable, for example Europe/London, or America/Los_Angeles.

- `<name-server>`

  The IP address of a nameserver. You should use one of these elements for each nameserver you want to use.

- `<hostname>`

  Specify if you want to manually set a hostname.

- `<ntp-server>`

  Specify one or more NTP servers.

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:

```
<?xml version=”1.0”?>
<installation mode=”upgrade”>
    <existing-installation>sda</existing-installation>
    <source type=”url”>http://pxehost.example.com/xenserver/</source>
    <post-install-script type=”url”>
        http://pxehost.example.com/myscripts/post-install-script
    </post-install-script>
</installation>
<!--NeedCopy-->
```

Host partition layout

May 9, 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 Install 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 7.1 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 7.1 to perform a Rolling Pool Upgrade (RPU) to XenServer 7.1

  > **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 7.1 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 7.1 on machines with a required initial partition that must be preserved continues to use the DOS partitioning scheme.
- Upgrades from Xenserver 5.x releases to 6.0 and then to 7.1 continue to use the existing DOS partitioning to retain any existing local storage.

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 `disable-gpt` 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

Operation	Number of partitions before upgrade	Number of partitions after installation/upgrade	Partition table type	
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

May 9, 2019

XenServer enables customers with smaller devices to install XenServer 7.1 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 7.1 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.

Administrator's Guide

February 22, 2021

This guide is only available as a PDF.

Administrator's Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Configuring XenServer for Graphics

February 22, 2021

This guide is only available as a PDF.

Configuring XenServer for Graphics (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

VM User's Guide

September 1, 2020

This article provides an overview of how to create Virtual Machines (VMs) using templates. It also explains other preparation methods, including cloning templates and importing previously exported VMs.

What is a Virtual Machine?

A Virtual Machine (VM) is a software computer that, like a physical computer, runs an operating system and applications. The VM is comprised of a set of specification and configuration files and is backed by the physical resources of a host. Every VM has virtual devices that provide the same functionality as physical hardware, and can have additional benefits in terms of portability, manageability, and security. In addition, you can tailor the boot behavior of each VM to your specific requirements - for more information refer to 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 which the virtual machine carries out, such that an unmodified operating system can be used. For network and storage access, emulated devices are presented to the virtual machine, or alternatively PV drivers can be used for performance and reliability reasons.

The following Linux distributions operate in HVM mode in XenServer 7.1:

- RHEL 7.x
- CentOS 7.x
- Oracle Linux 7.x
- Scientific Linux 7.x
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 18.04
- Debian Jessie 8.0
- Debian Jessie 9.0
- SUSE Linux Enterprise Server 12 SP3
- SUSE Linux Enterprise Desktop 12 SP3
- CoreOS Stable

This is because these VMs can take advantage of the x86 virtual container technologies in newer processors for improved performance. Network and storage access from these guests will still operate in PV mode, using drivers built-in to the kernels.

Creating VMs

Using VM Templates

VMs are prepared from templates. 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 "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.

Creating Windows VMs describes how to install Windows operating systems onto VMs.

Creating Linux VMs describes how to install Linux operating systems onto VMs.

Other Methods of VM Creation

In addition to creating VMs from the provided templates, you can create VMs by using the following methods:

1. Cloning an existing VM
2. Importing an exported VM

Cloning 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 instantiate VMs from. A VM can be customized and converted into a template; be sure to follow the appropriate preparation procedure for the VM (see Preparing for Cloning a Windows VM Using Sysprep for Windows and Preparing to Clone a Linux VM for Linux).

> **Note**
>
> Templates cannot be used as normal VMs.

XenServer has two mechanisms for cloning VMs:

1. A full copy

2. Copy-on-Write (CoW)

   The faster Copy-on-Write (CoW) mode only writes *modified* blocks to disk. CoW is designed to save disk space and allow fast clones, but will slightly slow down normal disk performance. A template can be fast-cloned multiple times without slowdown.

   > **Note**
   >
   > If a template is cloned into a VM and the clone converted back into a template, disk performance can linearly decrease depending on the number of times this 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 on a server where all VM virtual disks are on shared Storage Repositories (SR), the template cloning operation will be 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, then the template clone operation can only execute on the server that can access that SR.

Importing 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 additional VMs of a certain configuration so that you can increase the speed of your deployment. You might, for example, have a special-purpose server configuration that you use many times. Once you have set up a VM the way you want it, you can 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 a XenServer host that is in another resource pool.

For details and procedures on importing and exporting VMs, see Importing and Exporting VMs.

XenServer PV Tools

XenServer PV Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer PV Tools consist of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. XenServer PV Tools must be installed on each Windows Virtual Machine in order for the VM to have a fully supported configuration, and to be able to use the XenServer management tools (the xe CLI or XenCenter). The version of XenServer PV Tools installed on the VM must be the same as the version installed on the XenServer 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. During the installation 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 allows Windows to complete its installation using built-in drivers, but with reduced performance due to the overhead inherent in emulation of the controller drivers.

The Management Agent, also known as the Guest Agent, is responsible for high-level virtual machine management features and provides full functionality to XenCenter, including quiesced snapshots.

XenServer PV Tools must be installed on each Windows VM in order for the VM to have a fully-supported configuration. The version of XenServer PV Tools installed on the VM must be the same as the version installed on the XenServer host. A VM will function without the XenServer PV Tools, but performance will be significantly hampered when the I/O drivers (PV drivers) are not installed. You must install XenServer PV 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 to take effect)

Finding 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 PV Tools (I/O drivers and the Management Agent) are installed, and whether the VM has the capability to install and receive updates from Windows Update. The following section lists the messages displayed in XenCenter:

I/O optimized (not optimized): 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 PV Tools ISO.

> **Note**
>
> I/O drivers will be automatically installed on a Windows VM that has the ability to receive updates from Windows Update. For more information, see Updating the XenServer PV Tools.

Management Agent installed (not installed): displays whether or not the Management Agent is currently installed on the VM. Click the Install I/O drivers and Management Agent link to install the Management Agent from the XenServer PV Tools ISO.

Able to (Not able to) receive updates from Windows Update: specifies whether the VM has the capability to 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 located on the XenServer PV 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 PV Tools. For Linux VMs, clicking the status link switches to the VM's console and loads the XenServer PV Tools ISO. You can then mount the ISO and manually run the installation, as described in Install XenServer PV Tools

Supported Guests and Allocating Resources

For information about supported guest operating systems, virtual memory and virtual disk size limits, see Guest operating system support.

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, refer to the XenServer 7.1 Configuration Limits document. Factors such as hardware and environment can affect the limitations. For information about supported hardware, refer to 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 in the form of `xvd*` devices. It is also sometimes possible (depending on the OS) to get an `sd*` device using the same mechanism, where the PV driver inside the VM takes over the SCSI device namespace. This is not desirable so it is best to use `xvd*` where possible for PV guests (this is 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 PV Tools installs a special I/O driver that works in a similar way to Linux, except in a fully virtualized environment.

Windows VMs

June 1, 2021

> **Warning**
>
> Running a Windows VM without installing the XenServer PV Tools is not a supported configuration.

Installing Windows VMs on a 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 can be broken down into three steps:

- selecting the appropriate Windows template
- installing the Windows operating system
- installing the XenServer PV Tools (I/O drivers and the Management Agent)

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 subsequently 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 and Windows Server 2003 do not exist in XenServer 7.1. Customers who want to create a Windows XP or a Windows Server 2003 VM should use the 'other install media' template and then run `xenlegacy.exe` from the XenServer PV Tools ISO to install XenServer PV Tools on such VMs. Customers should note that this reflects Microsoft's decision to end extended support for these guests. If a support incident concerning Windows XP or Windows Server 2003 requires escalation, customers will be asked to upgrade to a supported guest operating system, as technical workarounds may 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 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 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 XenApp performance.
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).
Windows 8.1 (64-bit)	Used to install Windows 8.1 (64-bit).
Windows 10 (32-bit)	Used to install Windows 10.

Template Name	Description
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)
Windows Server 2019 (64-bit)	Used to install Windows Server 2019 or Windows Server Core 2019 (64-bit)

> **Warning**
>
> Experimental guest operating systems have received limited testing, may 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.

Attaching 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.

Using XenCenter to Create a VM

> **Note**
>
> The following procedure provides an example of creating Windows 10 (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 needed to create a new 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 intend to install on your new VM is compatible only with the original hardware (for example, an OS installation CD that was packaged with a specific computer), check the **Copy host BIOS strings** to VM box.
   >
   > To copy BIOS strings using the CLI, see Advanced
   >
   > After you first start a VM, you cannot change its BIOS strings. Ensure that the BIOS strings are correct before starting the VM for the first time.

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. To do so, 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. 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 menu.

5. Select a home server for the VM.

   A home server is the server which will provide 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 is not possible, an alternate server within the same pool will be selected automatically. To choose a home server, click Place the VM on this server and select a server from the list.

   > **Note**
   >
   > - In WLB-enabled pools, the nominated home server will not be 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 will not take effect. Instead, the server nomination will be 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 will be 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 2048 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 enables the VM to use the processing power of the GPU, providing 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 may 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.
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 may want to:

   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 NIC by selecting Add.
10. Review settings, and then click Create Now to create the new 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. Once the OS installation completes and the VM reboots, install the XenServer PV Tools.

Installing XenServer PV Tools

XenServer has a simpler mechanism to install and update XenServer PV Tools (I/O drivers and the Management Agent) on Windows VMs.

XenServer PV Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer PV Tools consist of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. XenServer PV Tools must be installed on each Windows VM in order for the VM to have a fully-supported configuration. A VM will function without them, but performance will be significantly hampered.

> **Note**
>
> To install XenServer PV Tools on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.
>
> Ensure that all requested VM restarts are completed as part of the installation process. Multiple restarts might be required.

To install XenServer Tools

1. Select the VM in the Resources pane, right-click, and then click Install XenServer PV Tools on the shortcut menu. Alternatively, on the VM menu, click Install XenServer PV Tools, or on the General tab of the VM, click Install I/O drivers and Management Agent.

   > **Note**
   >
   > When you install XenServer PV Tools on your VM, you will be 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 PV Tools to continue with the installation. This mounts the XenServer PV 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 PV Tools ISO:

   Click Run Setup.exe to begin XenServer PV Tools installation. This opens the Citrix 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.

   > **Note**
   >
   > When you install XenServer PV Tools using this method, the Management Agent will be configured to get updates automatically. However, the I/O drivers will not be updated by the management agent update mechanism. This is the default behavior. If you prefer to change the default behavior, install XenServer PV Tools using the following method.

Alternatively:

a) Click Open folders to view files and then run Setup.exe from the CD Drive. This option opens the Citrix XenServer Windows Management Agent Setup wizard and lets you customize the XenServer PV Tools installation and the Management Agent update settings.

b) Follow the instructions on the wizard to accept the license agreement and choose a destination folder.

c) Customize the settings on the Installation and Updates Settings page. The Citrix XenServer Windows Management Agent Setup wizard displays the following settings by default. The wizard:

   - Installs the I/O Drivers
   - Allows automatic updating of the Management Agent
   - Does not allow the Management Agent to update the I/O drivers automatically

   If you do not want to allow the automatic updating of the Management Agent, select Disallow automatic management agent updates. If you would like to allow the I/O drivers to be automatically updated by the Management Agent, 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, we recommend that you do not allow the Management Agent to update the I/O drivers automatically.

d) Click Install to begin the installation process. When prompted, perform any actions that are required to complete the XenServer PV Tools installation process and click Finish to exit the setup wizard.

Customers who install the XenServer PV 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 required) and to get your VM to an optimized state, we recommend that you specify the force restart option in RDP. Note that the force restart option will restart the VM only if it is required to get the VM to an optimized state.

If you prefer to install the I/O drivers and the Management Agent on a large number of Windows VMs, install `managementagentx86.msi` or `managementagentx64.msi` using your preferred MSI installation tool. These files can be found on the XenServer PV Tools ISO.

> **Note**
>
> I/O drivers will be automatically installed on a Windows VM that has the ability to receive updates from Windows Update. However, we recommend that you install the XenServer PV Tools package

> to install the Management Agent, and to maintain supported configuration.

Silent Installation

To silently install the XenServer PV Tools and to prevent the system from rebooting, run one of the following commands:

```
Msiexec.exe managementagentx86.msi /quiet /norestart
Msiexec.exe managementagentx64.msi /quiet /norestart
```

Or

```
Setup.exe /quiet /norestart
```

A non-interactive, but non-silent installation can be obtained by running:

```
Msiexec.exe managementagentx86.msi /passive
Msiexec.exe managementagentx64.msi /passive
```

Or

```
Setup.exe /passive
```

For interactive, silent, and passive installations, including those with the `/norestart` flag, following the next system restart (which may be manually initiated if the `/norestart` flag is provided) there may be several automated reboots before the XenServer PV Tools are fully installed.

The XenServer PV Tools are installed by default in the `C:\Program Files\Citrix\XenTools` directory on the VM.

> **Warning**
>
> Installing or upgrading the XenServer PV 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 PV Tools installation or upgrade.

Using the CLI to Create a Windows VM

This section describes the procedure to create a Windows VM from an ISO repository using the xe CLI.

Installing a Windows VM from an ISO Repository Using the CLI

1. Create a VM from a template:

   ```
   xe vm-install new-name-label=vm_name template=template_name
   ```

   This returns the UUID of the new VM.

2. Create an ISO Storage Repository:

   ```
   xe-mount-iso-sr path_to_iso_sr
   ```

3. List all of the available ISOs:

   ```
   xe cd-list
   ```

4. Insert the specified ISO into the virtual CD drive of the specified VM:

   ```
   xe vm-cd-add vm=vm_name cd-name=iso_name device=3
   ```

5. Start the VM and install the operating system:

   ```
   xe vm-start vm=vm_name
   ```

At this point, the VM console will now be visible in XenCenter.

For more information on using the CLI, see Appendix A, Command Line Interface, in the XenServer Administrator's Guide.

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. Once the VM and XenServer PV Tools have been installed you can add additional virtual disks. The boot device should always be one of the initial disks so that the VM can successfully boot without the XenServer PV 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 is because of interaction between the I/O drivers and the PnP 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.
- There is a bug in the VLC player DirectX back end that causes yellow to be replaced by blue when playing video if the Windows display properties are set to 24-bit color. VLC using OpenGL as a back end works correctly, and any other DirectX- 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 no longer supports the use of Windows 7 without Service Pack 1 installed. For a Windows 7 VM to be supported on XenServer, ensure that SP1 or later is installed.

Windows Vista

Microsoft Vista recommends a root disk of size 20GB or higher. The default size when installing this template is 24GB, which is 4GB greater than the minimum. Consider increasing this.

Windows Server 2008 R2

Microsoft no longer supports the use of Windows Server 2008 R2 without Service Pack 1 installed. For a Windows Server 2008 R2 VM to be supported on XenServer, ensure that SP1 or later is installed.

Creating Linux VMs

August 11, 2022

This article discusses how to create Linux VMs, either by installing them or cloning them. This article also contains vendor-specific installation instructions.

When you want to create a VM, you must 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 article focuses on using the CLI.

> **Note**
>
> Customers who want to create VM of a newer minor update of a Red Hat Enterprise Linux (RHEL release, than is supported for installation by XenServer, should install from the latest supported media and then use `yum update` to bring the VM up-to-date. This also applies to RHEL derivatives such as CentOS and Oracle Linux.
>
> For example, RHEL 5.10 is supported for release with XenServer 7.1; customers who want to use RHEL v5.11, should first install RHEL v5.10, and then use `yum update` to update to RHEL 5.11.

We recommend that you install the XenServer PV Tools immediately after installing the operating system. For some operating systems, the XenServer PV Tools include a XenServer specific kernel, 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 PV 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:

1. Installing from an internet repository
2. Installing from a physical CD
3. 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, and any VMs installed using the Other install media template are *not* supported.

> VMs created using the Other install media template is created as HVM guests, which may mean that some Linux VMs use slower emulated devices rather than the higher performance I/O drivers.

For information regarding specific Linux distributions, see *Release Notes*.

Supported Linux distributions

For a list of supported Linux distributions, see Guest operating system support.

Other Linux distributions are not supported. However, distributions that use the same installation mechanism as Red Hat Enterprise Linux (for example, Fedora Core) might be successfully installed using the same template.

Creating 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.

Example: Installing a Debian Squeeze VM from a network repository

1. Create a VM from the Debian Squeeze template. The UUID of the VM is returned:

   ```
   xe vm-install template=template-name new-name-label=squeeze-vm
   ```

2. Specify the installation repository - this should be a Debian mirror with at least the packages required to install the base system and the additional packages you plan to select during the Debian installer:

   ```
   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). 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*:

   ```
   xe network-list bridge=xenbr0 --minimal
   ```

4. Create a VIF to connect the new VM to this network:

   ```
   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:

   ```
   xe vm-start uuid=UUID
   ```

6. Follow the Debian Installer procedure to install the VM in the configuration you require.
7. See below for instructions on how to install the guest utilities and how to configure graphical display.

Creating a Linux VM by Installing from a Physical CD/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.

Example: Installing a Debian Squeeze VM from CD/DVD (using the CLI)

1. Create a VM from the Debian Squeeze template. The UUID of the VM is returned:

   ```
   xe vm-install template=template-name new-name-label=vm-name
   ```

2. Get the UUID of the root disk of the new VM:

   ```
   xe vbd-list vm-uuid=vm_uuid userdevice=0 params=uuid --minimal
   ```

3. Using the UUID returned, set the root disk to not be bootable:

```
xe vbd-param-set uuid=root_disk_uuid bootable=false
```

4. Get the name of the physical CD drive on the XenServer host:

   ```
   xe cd-list
   ```

   The result of this command should give 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:

   ```
   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:

   ```
   xe vbd-list vm-uuid=vm_uuid type=CD params=uuid --minimal
   ```

7. Make the VBD of the virtual CD boot-able:

   ```
   xe vbd-param-set uuid=cd_drive_uuid bootable=true
   ```

8. Set the install repository of the VM to be the CD drive:

   ```
   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:

    ```
    xe vm-start uuid=UUID
    ```

See the sections that follow for instructions on how to install the guest utilities and how to configure graphical display.

Creating 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.

Example: Installing a Linux VM from a Network-Accessible ISO Image

1. Run the command

   ```
   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*:

   ```
   xe network-list bridge=xenbr0 --minimal
   ```

3. Create a VIF to connect the new VM to this network:

   ```
   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:

   ```
   xe vm-param-set uuid=vm_uuid other-config:install-repository=http:
       //mirror.centos.org/centos/6/os/x86_64
   ```

5. Start the VM

   ```
   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) and 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://*&lt;server&gt;*/*&lt;path&gt;*
  ```

- **FTP.**

  ```
  ftp://*&lt;server&gt;*/*&lt;path&gt;*
  ```

- **NFS.**

  ```
  nfs://*&lt;server&gt;*/*&lt;path&gt;*
  ```

- **NFS.**

  ```
  nfs:*&lt;server&gt;*:/*&lt;path&gt;*
  ```

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, the `nfs://` style of path should always be used.

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 subsequently started, it begins the network installation process.

> **Warning**
>
> When installing a new Linux-based VM, it is important to fully finish the installation and reboot it before performing any other operations on it. This 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 may be helpful if 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 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. This can be done using the New VM wizard in XenCenter or by executing an xe CLI command like the following:

```
xe vm-param-set uuid=uuid PV-args=preseed_arguments
```

To install RHEL 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, exactly as it would be specified in the PXE config file, for example:

```
ks=http://server/path ksdevice=eth0
```

3. On the command line, use `vm-param-set` to set the `PV-args` parameter to make use of a Kickstart file

```
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:

```
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.

Installing the Linux Guest Agent

Although all the supported Linux distributions are natively paravirtualized (and therefore do not need special drivers for full performance), XenServer includes a guest agent which provides additional information about the VM to the host. You must 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 (see Updating VMs) as you upgrade your XenServer host.

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 PV Tools option in XenCenter.

2. Mount the image onto the guest by running the command:

```
mount -o ro,exec /dev/disk/by-label/XenServerincloudsphere\\x20Tools /mnt
```

> **Note**
>
> If mounting the image fails, you can locate the image by running the following:

> ```
> blkid -t LABEL=”XenServer PV Tools”
> ```

3. Execute the installation script as the root user:

   ```
   /mnt/Linux/install.sh
   ```

4. Unmount the image from the guest by running the command:

   ```
   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` in Ubuntu 10.10 and later) instead of as `/dev/cdrom` as you might expect. This is because they are not true CD-ROM devices, but normal devices. When the CD is ejected by either XenCenter or the CLI, it hot-unplugs the device from the VM and the device disappears. This is different from Windows Virtual Machines, where the CD remains in the VM in an empty state.

Additional Installation Notes for Linux Distributions

This following table lists additional, vendor-specific, configuration information that you should be aware of before creating the specified Linux VMs.

> **Important**
>
> For detailed release notes on all distributions, see *Release Notes*.

CentOS 5.x (32-/64-bit)

For a CentOS 5.x VM, you must ensure that the operating system is using the CentOS 5.4 kernel or later, which is available from the distribution vendor. Enterprise Linux kernel versions prior to 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 a RHEL 5.x VM, you must ensure that the operating system is using the RHEL 5.4 kernel (2.6.18-164.el5) or later, which is available from the distribution vendor. Enterprise Linux kernel versions prior to 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 Linux7.x (32-/64-bit)

This information applies to both Red Hat and Red Hat derivatives.

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.

Oracle Linux 5.x (32-/64-bit)

For an OEL 5.x VM, you must ensure that the operating system is using the OEL 5.4 kernel or later, which is available from the distribution vendor. Enterprise Linux kernel versions prior to 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 that 2 GB memory, set the boot parameter <`crashkernel=no`> to disable the crash kernel. The VM reboot 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 is only used to retrieve the installer kernel. Once the installer is running you will again need to enter 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 is only used to retrieve the installer kernel. Once the installer is running you will again need to enter the address of the mirror to be used for package retrieval.

Ubuntu 10.04 (32-/64-bit)

For Ubuntu 10.04 VMs with multiple vCPUs, Citrix strongly recommends that you update the guest kernel to "2.6.32-32 #64". For details on this issue, see the Knowledge Base article CTX129472 Ubuntu 10.04 Kernel Bug Affects SMP Operation.

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.

Linx Linux v6.0

Supports up to 6 vCPUs. To add disks to the Linx 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-UD 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/controlalt-delete.conf`. Thus, it cannot be rebooted by xe command or XenCenter. 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.

- Ensure that the following two lines are enabled in /etc/init/control-altdelete.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.

Debian Apt Repositories

For infrequent or one-off installations, it is reasonable to directly use a Debian mirror. However, if you intend to do several VM installations, we recommend that you use a caching proxy or local mirror. `Apt-cacher` is an implementation of proxy server that will keep a local cache of packages. `debmirror` is a tool that creates a partial or full mirror of a Debian repository. Either of these tools can be installed into a VM.

Preparing to Clone a Linux VM

Typically, when cloning a VM or a computer, unless you “generalize” the cloned image, attributes unique to that machine, such as the IP address, SID, or MAC address, will be duplicated in your environments.

As a result, XenServer automatically changes some virtual hardware parameters when you clone a Linux VM. If 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 make any modifications to 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.

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 it is part of.

IP address

A cloned VM must have a unique IP address within the network domain it is part of. Generally, this is not a problem if 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 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 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, if you configure two virtual NICs when you install a VM, and then shut it down and remove the first NIC, on reboot XenCenter shows just one NIC, but calls it `eth0`. Meanwhile the VM is deliberately forcing this to be `eth1`. The result is that networking does not work.

If the VM uses persistent names, Citrix recommends disabling these rules before cloning. If for some reason you do not want to turn persistent names off, you must reconfigure networking inside the VM (in the usual way). However, the information shown in XenCenter will not match the addresses actually in your network.

Linux VM Release Notes

Most modern Linux distributions support Xen paravirtualization directly, but have different installation mechanisms and some kernel limitations.

Red Hat Enterprise Linux 4.5–4.8

The following issues have been reported to Red Hat and are already fixed in the Xen kernel (which can be installed by using the `/mnt/Linux/install.sh` script in the built-in `guest-tools.iso` CD image):

- The Xen kernel in RHEL 4.8 can occasionally enter tickless mode when an RCU is pending. When this triggers, it is usually in `synchronize_kernel()` which means the guest essentially hangs until some external event (such as a `SysRQ`) releases it (Red Hat Bugzilla 427998)
- Live migration can occasionally crash the kernel under low memory conditions (Red Hat Bugzilla 249867)
- Guest kernel can occasionally hang due to other XenStore activity (Red Hat Bugzilla 250381)
- RHEL 4.7 contains a bug which normally prevents it from booting on a host with more than 64 GiB of RAM (Red Hat Bugzilla 311431). For this reason XenServer RHEL 4.7 guests are only allocated RAM addresses in the range below 64 GiB by default. This may cause RHEL 4.7 guests to fail to start even if RAM appears to be available, in which case rebooting or shutting down other guests can cause suitable RAM to become available. If all else fails, temporarily shut down other guests until your RHEL 4.7 VM can boot.

  Once you have succeeded in booting your RHEL 4.7 VM, install the XenServer PV Tools and run the command:

  ```
  xe vm-param-remove uuid=vm_uuid param-name=other-config \
  param-key=machine-address-size
  ```

  to remove the memory restriction.

- On some hardware (usually newer systems), the CPU generates occasional spurious page faults which the OS should ignore. Unfortunately versions of RHEL 4.5–4.7 fail to ignore the spurious fault and it causes them to crash (Red Hat Bugzilla 465914).

  This has been fixed in our kernel. The RHEL 4 VM templates have been set with the `suppress-spurious-page-faults` parameter. This assures that the installation continues safely to the point that the standard kernel is replaced with the Citrix-provided kernel.

  There is a performance impact with this parameter set, so, after the VM installation is complete, at the VM command prompt, run the command:

```
xe vm-param-remove uuid=vm_uuid other-config: \
param-key=suppress-spurious-page-faults
```

- In RHEL 4.5–4.7, if a xenbus transaction end command fails it is possible for the suspend_mutex to remain locked preventing any further xenbus traffic. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-5]
- In RHEL 4.5–4.8, use of the XFS filesystem can lead to kernel panic under exceptional circumstances. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-16]
- In RHEL 4.5–4.8, the kernel can enter no tick idle mode with RCU pending; this leads to a guest operating system lock up. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-21]
- In RHEL 4.7, 4.8, VMs may crash when a host has 64 GiB RAM or higher configured. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-30]
- In RHEL 4.5–4.8, the network driver contains an issue that can, in rare circumstances, lead to a kernel deadlock. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-45]

Additional Notes:

- RHEL 4.7, 4.8, sometimes when there are many devices attached to a VM, there is not enough time for all of these devices to connect and startup fails. [EXT-17]
- If you try to install RHEL 4.x on a VM that has more than two virtual CPUs (which RHEL 4.x does not support), an error message incorrectly reports the number of CPUs detected.

Preparing a RHEL 4.5–4.8 guest for cloning

To prepare a RHEL 4.5–4.8 guest for cloning (see Preparing to Clone a Linux VM), edit `/etc/sysconfig/network-scripts/ifcfg-eth0` before converting the VM into a template, and remove the `HWADDR` line.

> **Note**
>
> Red Hat recommends the use of Kickstart to perform automated installations, instead of directly cloning disk images (see Red Hat KB Article 1308).

RHEL Graphical Install Support

To perform a graphical installation, in XenCenter step through the New VM wizard. In the Installation Media page, in the **Advanced OS boot parameters** section, add `vnc` to the list parameters:

```
graphical utf8 vnc
```

You will then be 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 will initially start 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 7.1. Before attempting to upgrade a XenServer host to version 7.1, customers should update the kernel to version 5.4 (2.6.18-164.el5xen) or later.
- During the resume operation on a suspended VM, allocations can be made that can cause swap activity which cannot be performed because the swap disk is still being reattached. This is a rare occurrence. (Red Hat Bugzilla 429102).
- Customers running RHEL 5.3 or 5.4 (32/64-bit) should not use Dynamic Memory Control (DMC) as this may cause the guest to crash. If you want to use DMC, Citrix recommends that customers 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 and 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.

Preparing a RHEL 5.x guest for cloning

To prepare a RHEL 5.x guest for cloning (see Preparing to Clone a Linux VM), edit `/etc/sysconfig/network-scripts/ifcfg-eth0` before converting the VM into a template and remove the `HWADDR` line.

> **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 Bugzilla 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, may be unsuccessful and can result in a guest kernel crash with a `NULL pointer dereference at <xyz>`error message. Customers should update the kernel to version 6.3 (2.6.32-238.el6) or later to resolve this issue. For more information, see Red Hat Bugzilla 773219.

Red Hat Enterprise Linux 7

After migrating or suspending, RHEL 7.x guests may freeze during resume. For more information, see Red Hat Bugzilla 1141249.

CentOS 4

Refer to *RHEL 4 Limitations* for the list of CentOS 4 release notes.

CentOS 5

Refer to *RHEL 5 Limitations* for the list of CentOS 5.x release notes.

CentOS 6

Refer to *RHEL 6 Limitations* for the list of CentOS 6.x release notes.

CentOS 7

Refer to *RHEL 7 Limitations* for the list of CentOS 7.x release notes.

Oracle Linux 5

Refer to *RHEL 5 Limitations* for the list of Oracle Linux 5.x release notes.

Oracle Linux 6

Oracle Linux 6.x guests which were installed on the XenServer host running versions earlier than v6.5, will 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.

Refer to *RHEL 6 Limitations* for a list of OEL 6.x release notes.

Oracle Linux 7

Refer to *RHEL 7 Limitations* for the list of Oracle Linux 7.x release notes.

Scientific Linux 5

Refer to *RHEL 5 Limitations* for the list of Scientific Linux 5.x release notes.

Scientific Linux 6

Refer to *RHEL 6 Limitations* for the list of Scientific Linux 6.x release notes.

Scientific Linux 7

Refer to *RHEL 7 Limitations* for the list of Scientific Linux 7.x release notes.

SUSE Enterprise Linux 10 SP1

XenServer uses the standard Novell kernel supplied with SLES 10 SP2 as the guest kernel. Any bugs found in this kernel are reported upstream to Novell and listed below:

- A maximum of 3 virtual network interfaces is supported.
- Disks sometimes do not attach correctly on boot. (Novell Bugzilla 290346).

SUSE Enterprise Linux 10 SP3

Due to a defect in the packaging of Novell SUSE Linux Enterprise Server 10 SP3 (32-bit) edition, users will not be able to create a VM of this edition. As a workaround, you must install SLES 10 SP2 and then upgrade it to SLES SP3 using, for example, `yast` within the VM.

SUSE Enterprise Linux 11

XenServer uses the standard Novell kernel supplied with SLES 11 as the guest kernel. Any bugs found in this kernel are reported upstream to Novell and listed below:

- Live migration of a SLES 11 VM which is under high load may fail with the message `An error occurred during the migration process`. This is due to a known issue with the SLES 11 kernel which has been reported to Novell. It is expected that kernel update 2.6.27.23-0.1.1 and later from Novell will resolve this issue.

SUSE Enterprise Linux 11 SP2

Creating a SLES 11 SP2 (32-bit) VM can cause the SLES installer or the VM to crash due to a bug in the SLES 11 SP2 kernel. To work around this issue, customers should allocate at least 1 GB memory to the VM. The amount of assigned memory can be reduced after installing updates to the VM. For more information, see Novell Bugzilla 809166.

Preparing a SLES guest for cloning

> **Note**
>
> Before you prepare a SLES guest for cloning, ensure that you clear the udev configuration for network devices as follows:
>
> ```
> cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
> ```

To prepare a SLES guest for cloning (see Preparing to Clone a Linux VM):

1. Open the file `/etc/sysconfig/network/config`
2. Edit the line that reads:

   ```
   FORCE_PERSISTENT_NAMES=yes
   ```

   to

```
FORCE_PERSISTENT_NAMES=no
```

3. Save the changes and reboot the VM.

Ubuntu 10.04

On an Ubuntu 10.04 (64-bit) VM, attempts to set the value of maximum number of vCPUs available to a VM (`VCPUs-max`), higher than the vCPUs available during boot (`VCPUs-at-startup`), can cause the VM to crash during boot. For more information, see Ubuntu Launchpad 1007002.

Ubuntu 12.04

Ubuntu 12.04 VMs with original kernel can crash during boot. To work around this issue, customers should create Ubuntu 12.04 VMs using the latest install media supported by the vendor, or update an existing VM to the latest version using in-guest update mechanism.

Ubuntu 14.04

Attempts to boot a PV guest may 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 is caused by improperly calling a non-atomic function from interrupt context. Customers should update the linux-image package to version 3.13.0-35.62 to fix this issue. For more information, see Ubuntu Launchpad 1350373.

VM Migration with XenMotion and Storage XenMotion

March 31, 2020

This article discusses migrating running VMs using *XenMotion* and *Storage XenMotion* and how to move a VMs 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 and allows you to move a running VM from one host to another host, when the VMs disks are located on storage shared by both hosts. This allows for pool maintenance features such as High Availability (HA), and Rolling Pool Upgrade (RPU) to automatically move VMs. 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 GPU Pass-through 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

Storage XenMotion

> **Caution**
>
> Storage XenMotion must not be used in XenDesktop deployments.

Storage XenMotion additionally allows VMs to be moved from one host to another, where the VMs are not located 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 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 in addition to the historical performance metrics, such as CPU and network usage.

Compatibility Requirements

When migrating a VM with XenMotion or Storage XenMotion, the VMs to be migrated and the new VM host must meet the following compatibility requirements in order 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 PV Tools must be installed on each Windows VM that you want to migrate. The version of XenServer PV Tools installed on the VM must be the same as the version installed on the target XenServer host.
- For Storage XenMotion, if the CPUs on the source host and target host are different, the target host must provide at least the entire feature set as the source host's CPU. Consequently, it is unlikely to be possible to move a VM between, for example, AMD and Intel processors.
- For Storage XenMotion, 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 will fail to complete.
- For Storage XenMotion, 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 will be reduced during migration.
- For Storage XenMotion, pools protected by High Availability (HA) should have HA disabled before attempting VM migration.
- Time to completion of VM migration will depend on the memory footprint of the VM, and its activity, in addition, VMs being migrated with Storage XenMotion will be affected by the size of the VDI and its storage activity.
- IPv6 Linux VMs require a Linux Kernel greater than 3.0.

Migrating 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 opens the Migrate VM wizard.
    - To move a stopped VM: On the VM menu, select Move VM. This opens the Move VM wizard.
2. From the **Destination** menu, select a standalone server or a pool.

3. From the **Home Server** menu, 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** menu. This option allows you to select different SR for each virtual disk on the migrated VM.
5. From the **Storage network** menu, select a network on the destination pool that will be used for the live migration of the VM's virtual disks and 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 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

- Storage XenMotion must not be used in XenDesktop deployments.
- IPv6 Linux VMs require a Linux Kernel greater than 3.0.
- When you do a VDI live migration for a VM that remains on the same host, that VM temporarily requires twice the amount of RAM.

To Move Virtual Disks

1. In the **Resources** pane, select the SR where the Virtual Disk is currently 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**
   >
   > Make sure 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.

Updating VMs

April 26, 2021

This article discusses updating Windows VMs with updated operating systems, reinstalling XenServer PV Tools, and updating VMs with new Linux kernel revisions.

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 PV Tools on each VM.
- Suspend/Resume operation is not supported on Windows VMs until the XenServer PV Tools are upgraded.
- The use of certain anti-virus and firewall applications can crash Windows VMs, unless the XenServer PV Tools are upgraded.

Updating Windows Operating Systems

We recommend that you do not remove the XenServer PV Tools from your Windows VM before automatically updating the version of Windows on the VM.

Use Windows Update to upgrade the version of the Windows operating system on your Windows VMs.

> **Note:**
>
> Windows installation disks typically provide an upgrade option if you boot them on a server which has an earlier version of Windows already installed. However, if you use Windows Update to update your XenServer PV Tools, do not upgrade the Windows operating system from

> an installation disk. Instead, use Windows Update.

Updating XenServer PV Tools

XenServer has a simpler mechanism to automatically update I/O drivers (PV drivers) and the Management Agent for Windows VMs. This 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 or not the VM is able to 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, you should disable Windows Update on your VM, or specify a group policy.

> **Important:**
>
> Ensure that all requested VM restarts are completed as part of the update. Multiple restarts might be required. If all requested restarts are not completed, this might result in unexpected behavior.

The following sections contain information about automatically updating the I/O drivers and the Management Agent.

Updating the I/O drivers

If you are running newly created Windows VMs on XenServer 7.0 or higher, you will be able to get I/O driver updates automatically from Microsoft Windows Update, provided:

- You are running XenServer 7.1 with Enterprise Edition , or have access to XenServer through XenApp/XenDesktop entitlement
- You have created a Windows VM using XenCenter issued with XenServer 7.1

  > **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 located on the XenServer PV Tools ISO.
>
> Customers can also receive I/O driver updates automatically through the automatic Management Agent update mechanism. You can configure this setting during XenServer PV Tools installation.

Finding 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.

Updating the Management Agent

XenServer enables you to automatically update the Management Agent 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 PV Tools installation. See Install XenServer PV Tools for details. 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 will appear on the Console tab of the VM notifying users about the required action.

If you are running Windows VMs on XenServer 7.1, you can get the Management Agent updates automatically, provided:

- You are running XenServer 7.1 with Enterprise edition or have access to XenServer through XenApp/XenDesktop entitlement
- You have installed XenServer PV Tools issued with XenServer 7.0 or higher
- The Windows VM has access to the Internet

> **Important**
>
> - The ability to receive I/O drivers from Windows Update and the automatic updating of the Management Agent features are available for XenServer 7.1 Enterprise Edition, or those who have access to XenServer 7.1 through XenApp/XenDesktop entitlement.
> - Updates to XenServer PV 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 PV Tools issued as a hotfix.

Finding 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.

Managing Automatic Updates

XenServer enables customers to redirect Management Agent updates to an internal web server before they are installed. This allows customers to review the updates before they are automatically installed on the VM.

Redirecting the Management Agent Updates:

The Management Agent uses an updates file to get information about the available updates. The name of this updates file depends on the version of the Management Agent that you use:

- For Management Agent 7.1.0.1396 and later use https://pvupdates.vmd.citrix.com/updates.json.
- For Management Agent 7.1.0.1354 and earlier use https://pvupdates.vmd.citrix.com/updates.tsv.

Complete the following steps to redirect the Management Agent updates:

1. Download the updates file.
2. Download the Management Agent MSI files referenced in the updates file.
3. Upload the MSI files to an internal web server which can be accessed by your VMs.
4. Update the updates file to point to the MSI files on the internal web server.
5. Upload the updates file to the web server.

Automatic updates can also be redirected on a per-VM or a per-pool basis. To redirect updates on a per-VM basis:

1. On the VM, open a command prompt as an administrator.
2. Run the command

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url /d \
url of the update file on the web server
```

To redirect automatic updating of the Management Agent on a per-pool basis, run the following command:

`xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url of the update file on the web server`

Disabling the Management Agent Updates:

To disable automatic updating of the Management Agent on a per-VM basis:

1. On the VM, open a command prompt as an administrator.

2. Run the following command:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_DWORD /v DisableAutoUpdate /d 1
```

To disable automatic updating of the Management Agent on a per-pool basis, run the following command:

```
xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=false
```

Modifying the Automatic I/O Driver Update Settings:

During XenServer PV Tools installation, you can specify whether you would like to allow the Management Agent to automatically update the I/O drivers. If you prefer to update this setting after completing the XenServer PV Tools installation process, perform the following steps:

1. On the VM, open a command prompt as an administrator.
2. Run the following command:

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v \
InstallDrivers /d YES/NO
```

Updating Linux Kernels and Guest Utilities

The Linux guest utilities can be updated by re-running the `Linux/install.sh` script from the built-in `guest-tools.iso` CD image.

For `yum`-enabled distributions CentOS 4 and 5, RHEL 5.4 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 re-run `Linux/install.sh`. This script automatically determines if your VM needs any updates and installs if necessary.

Upgrading to Ubuntu 14.04, RHEL 7.x and CentOS 7.x Guests

Customers who wish to upgrade *existing* Linux guests to versions which now operate in HVM mode (that is, RHEL 7.x, CentOS 7.x, and Ubuntu 14.04) should perform an in-guest upgrade. At this point, the upgraded Guest will only run in PV mode - which is not supported and has known issues. Customers should run the following script to convert the newly upgraded guest to the supported HVM mode. To do this:

On the XenServer host, open a local shell, log on as root, and enter the following command:

```
/opt/xensource/bin/pv2hvm vm_name
```

or

```
/opt/xensource/bin/pv2hvm vm_uuid
```

Restart the VM to complete the process.

Importing and Exporting VMs

December 17, 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, it is necessary to 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. You need to configure networking settings for the Transfer VM in the XenCenter Import and Export wizards. For more information, see *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 `.xva`.
XenServer XVA Version 1 format	XVA Version 1 is the original 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 `ova.xml`.

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:

- 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:

- 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 more 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.

Selecting OVF or OVA Format

OVF packages contain a series of uncompressed files, which makes it easier if 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, you must be logged in as root or have the Pool Administrator Role Based Access Control (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. Situations in which this might occur include:

- 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, including 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 2 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 1 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 a XenServer host and then imported into another XenServer host with a different CPU type, it may not run properly. For example, a Windows VM created on a XenServer host with an Intel® VT Enabled CPU, and then exported, may not run when imported into a XenServer host with an AMD-VTM CPU.

XVA Version 1 Format

XVA Version 1 is the original 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 `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 1 file for each 1 GB chunk of the disk image. The base name of each file includes the chunk number in decimal. It contains 1 block of the disk image in raw binary format, compressed with gzip.

> **Important**
>
> If a VM is exported from a XenServer host and then imported into another XenServer host with a different CPU type, it may not run properly. For example, a Windows VM created on a XenServer host with an Intel® VT Enabled CPU, and then exported, may not run when imported into a XenServer 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, it may be necessary to configure or "fix up" the VM before it will boot properly on a 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. You need to 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, attempting to repair boot device-related problems with the imported VM that might prevent the operating system within from booting in a 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, you must enable the feature on the Advanced Options page of the XenCenter Import wizard and then specify a location where the Fixup ISO should be 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, extra configuration changes, driver installation, or other actions might be required following using the Fixup feature.

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, then the location of the GRUB configuration file is determined and 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 operating system and registered with the operating system. This 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 to transfer its contents between the disk image file location and a XenServer storage repository.

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`:

```
<sectionGroup name=”applicationSettings”
    type=”System.Configuration.ApplicationSettingsGroup, System, Version=2.0.0.0,
    Culture=neutral, PublicKeyToken=b77a5c561934e089” >
  <section name=”XenOvfTransport.Properties.Settings”
      type=”System.Configuration.ClientSettingsSection, System, Version=2.0.0.0,
      Culture=neutral, PublicKeyToken=b77a5c561934e089” requirePermission=”false”/>
</sectionGroup>
```

4. To the end of the file, add the following section:

```
<applicationSettings>
  <XenOvfTransport.Properties.Settings>
    <setting name=”TransferType” serializeAs=”String”> <value>UploadRawVDI</value>
    </setting>
  </XenOvfTransport.Properties.Settings>
</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.

Importing VMs

When you import a VM, you effectively create a VM, using many of the same steps required to provision a new VM, such as 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.

Importing 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 needed 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, it is necessary to 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 *Transfer VM*.

> **Tip**
>
> Ensure the target host has enough RAM to support the virtual machines being imported. A lack of available RAM will result in a failed import. See CTX125120 for details on how to resolve this issue.

Imported OVF packages appear as vApps when imported using XenCenter. When the import is complete, the new VMs will appear in the XenCenter Resources pane, and the new vApp will appear in the Manage vApps dialog box.

To Import VMs from OVF/OVA using XenCenter

1. Open the Import wizard by doing one of the following:

   - In the Resources pane, right-click, and then select Import on the shortcut menu.
   - On the File menu, select Import.

2. On the first page of the wizard, locate the file you want to import, and then click Next to continue.
3. Review and accept EULAs, if applicable.

   If the package you are importing includes any EULAs, accept them and then click Next to continue. If no EULAs are included in the package, the wizard will skip this step and advance straight to the next page.

4. Specify the pool or host to which you want to import the VM(s), and then (optionally) assign the VM(s) to a home XenServer host.

   To select a host or pool, choose from the Import VM(s) to menu.

   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 VM(s): 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, and then 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 if you choose to verify the manifest, as 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 VM(s) in the package you are importing were built on a virtualization platform other than XenServer, select the Use Operating System Fixup check box and then 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, and then choose to automatically or manually configure the network settings.

   - To use automated Dynamic Host Configuration Protocol (DHCP) to automatically 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. You must enter an IP address, but the subnet mask and gateway settings are optional.

   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 will appear 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. This will vary according to the version of Windows contained in the OVF package:
>
> - For Windows Vista, Server 2008, and later, set the platform parameter to device_id =0002. For example:
>
>   ```
>   xe vm-param-set uuid=VM uuid platform:device_id=0002
>   ```
>
> - For all versions of Windows, set the platform parameter to viridian=true. For example:
>
>   ```
>   xe vm-param-set uuid=VM uuid platform:viridian=true
>   ```

Importing 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 needed to create a new 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.
- DHCP has to be running on the management network XenServer is using.
- The Import wizard requires local storage on the server on which you are running it.

To Import VM(s) from a Disk Image 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 VM(s), and then (optionally) assign the VM(s) to a home XenServer host.

To select a host or pool, choose from the Import VM(s) to menu.

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 VM(s): 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, and then 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 image(s) you are importing were built on a virtualization platform other than XenServer, select the Use Operating System Fixup check box and then 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, and then choose to automatically or manually configure the network settings.

   - To use automated Dynamic Host Configuration Protocol (DHCP) to automatically 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. You must enter an IP address, but the subnet mask and gateway settings are optional.

   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. This will vary according to the version of Windows contained in the disk image:
>
> - For Windows Vista, Server 2008, and later, set the `platform` parameter to `device_id =0002`. For example:
>
>   ```
>   xe vm-param-set uuid=VM uuid platform:device_id=0002
>   ```
>
> - For all other versions of Windows, set the `platform` parameter to `viridian=true`. For example:
>
>   ```
>   xe vm-param-set uuid=VM uuid platform:viridian=true
>   ```

Importing VMs from XVA

You can import VMs, templates and snapshots that have previously been exported and stored locally in XVA format (with the `.xva` file name extension) or XVA Version 1 format (with the ova.xml file name extension). To do so, you follow the usual steps needed to create a new 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 created on a server with an Intel VT Enabled CPU, then exported, may not run when imported to a server with an AMD-VTM CPU.

To Import VM(s) from XVA Files VM 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, and then click Next, a Download Package dialog box opens and you must specify a folder on your XenCenter host where the file will be 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 using the xe CLI

To import the VM to the default SR on the target XenServer host, enter the following:

```
xe vm-import -h hostname -u root -pw password \
filename=pathname_of_export_file
```

To import the VM to a different SR on the target XenServer host, add the optional `sr-uuid` parameter:

```
xe vm-import -h hostname -u root -pw password \
filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
```

If you want to preserve the MAC address of the original VM, add the optional `preserve` parameter and set to **`true`**:

```
xe vm-import -h hostname -u root -pw password \
filename=pathname_of_export_file preserve=true
```

> **Note**
>
> Importing a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

Once the VM has been imported, the command prompt returns the UUID of the newly imported VM.

Exporting VMs

You can export OVF/OVA and XVA files using the XenCenter Export wizard; you can also export XVA files via the xe CLI.

Exporting VMs as OVF/OVA

Using the XenCenter Export wizard, you can export one or more VM(s) 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**
>
> In order 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 VM(s) as OVF/OVA using XenCenter

1. Shut down or suspend the VM(s) that you want to export.
2. Open the Export wizard: in the Resources pane, right-click the pool or host containing the VM(s) 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 file(s) to be saved, and select OVF/OVA Package (`*.ovf`, `*.ova`) from the Format menu. Click Next to continue.
4. From the list of available VMs, select the VM(s) that you want to include in the OVF/OVA package, and then click Next to continue.
5. If required, 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 or 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 one or more of its VMs, you may want to include the EULA text from that operating system. The text is displayed and must be accepted by the person who imports the appliance.

> **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 and is used to ensure 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, and then 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 which you have already created from a Trusted Authority and exported as either a .pem or .pfx file that contains 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 will have a hard disk image that consumes 26 GB of space, regardless of whether or not the VM actually requires it.

> **Note**
>
> Compressing the VHD files makes the export process take longer to complete, and importing a package containing compressed VHD files will also take longer, as the Import wizard must extract all of the VHD images as it imports them.

If both the Create OVA package (single OVA export file) and Compress OVF files options are checked, the result is a compressed OVA file with the file name extension .ova.gz.

7. Configure Transfer VM networking.

   Select a network from the list of network interfaces available in the destination pool or host, and then choose to automatically or manually configure the network settings.

   - To use automated Dynamic Host Configuration Protocol (DHCP) to automatically 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. You must enter an IP address, but the subnet mask and gateway settings are optional.

   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.

Exporting VMs as XVA

You can export an existing VM as an XVA file using the XenCenter Export wizard or the xe CLI. Citrix does recommend exporting a VM to a machine other than a XenServer host, on which you can maintain a library of export files (for example, 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 created on a server with an Intel VT Enabled

> CPU, then exported, may not run when imported to a server with an AMD-VTM CPU.

To Export VM(s) as XVA Files 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 file(s) to be saved, and select XVA File (`*.xva`) from the Format menu. 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 VM(s) as XVA Files using the xe CLI

1. Shut down the VM that you want to export.
2. Export the VM by running the following:

   ```
   xe vm-export -h hostname -u root -pw password vm=vm_name filename=
       pathname_of_file
   ```

   > **Note**
   >
   > Be sure to include the `.xva` extension when specifying the export file name. If the exported VM does not have this extension, and you later attempt to import it using XenCenter, it might fail to recognize the file as a valid XVA file.

Container Management

March 18, 2022

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 7.0
- 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, refer to the XenCenter online Help. Press F1 or click Help.

The Container Management Supplemental Park enables XenServer to query the VMs, interact with Cloud Config Drives, discover application containers, and display these within XenCenter's Infrastructure view. XenCenter also enables interaction with the containers to allow for start, stop and pause operations, and other monitoring capabilities. Refer to *Container Management Supplemental Pack* for more information.

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, refer to: https://www.docker.com/resources/what-container/.

> **Note**
>
> The XenServer Container Management feature complements, but not does replace the Docker ecosystem. Individual Docker Engine instances in the VMs can be managed by one of the many Docker management tools available.

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: easy access is provided to basic container information such as forwarded network ports, and originating Docker image name. This 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: 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 refer to the XenCenter Help. If you would prefer to install using the xe CLI, refer to the XenServer Supplemental Packs and the DDK guide.

Managing Docker Containers Using XenCenter

This section contains information on managing your CoreOS VMs using XenCenter. To manage CoreOS VMs, you should:

1. Install or upgrade your host to XenServer 7.1.
2. Install the XenCenter shipped with XenServer 7.1.
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. You should create a config drive if you are planning to use XenServer to manage containers running inside the VM.

   By default, XenCenter includes a predefined set of parameters on the Cloud-Config Parameters page. You can modify these parameters based on your requirements. Refer to CoreOS documentation for detailed information about supported configuration parameters.

   > **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 want to use Ubuntu 14.04, Debian 8, RHEL/CentOS/Oracle Linux 7, Windows Server 2016 TP VMs to manage Docker containers, you should first enable container management using the CLI. Once the container management is enabled on these VMs, you can use XenCenter to perform lifecycle operations such as start, stop, pause, and resume the containers.

Managing Containers on Other Linux Guests

CoreOS VMs that are created with the default Cloud Config Drive configuration are automatically prepared for Container Management and the capability only needs to be enabled. Other Linux guests can be prepared manually. This is supported for Debian 8, Ubuntu 14.04, and RHEL/CentOS/OEL 7.x VMs only.

To manually prepare a Linux guest:

1. Ensure the VM has XenServer PV 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`

1. Start docker.service

`systemctl start docker.service`

```
A non-root user should be used for container management; add the user to the 'docker' group to provide access to Docker.
```

1. 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 username on the VM that the Container Management will use for management access.
```

The preparation script guides you through the process and automatically enables container management for this VM.

Accessing 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 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.

Automating 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 example, for containers running on a CoreOS VM, the public key should be added to the Cloud-Config Parameters section on the VM's General tab in XenCenter. For Ubuntu 14.04, RHEL/CentOS/Oracle Linux 7.x, and Debian 8, the public key should be manually added 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`.

Managing 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**
>
> This functionality requires Windows Server 2016 VMs to be configured with one or more static IP addresses for TLS communication, as TLS server certificates will be bound to certain IP addresses.

To prepare Windows Server Containers for Container Management:

1. Ensure the VM has XenServer PV 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 HyperV Containers.

3. Create a file called ‘daemon.json’ in the folder ‘C:\ProgramData\docker\config’ with the contents:

```
{

  ”hosts”: [”tcp://0.0.0.0:2376”, ”npipe://”],
  ”tlsverify”: true,
  ”tlscacert”: ”C:\\ProgramData\\docker\\certs.d\\ca.pem”,
  ”tlscert”: ”C:\\ProgramData\\docker\\certs.d\\server-cert.pem”,
  ”tlskey”: ”C:\\ProgramData\\docker\\certs.d\\server-key.pem”
 }
```

4. 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 will be injected into the VM using a virtual CD, that might be copied by malicious users during the preparation.

```
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

```
xscontainer-prepare-vm -v vm-uuid -u root --mode tls --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**
>
> **In order 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, dom0) 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 only allow trusted sources to initiate a connection between the two networks.
>
> **If this recommended network configuration does not match your risk profile, or if you lack the necessary network or firewall expertise to secure this route sufficiently for your specific use-case, Citrix recommends that you do not use this feature in production.**

Network Partitioning and Firewalls

As with other VMs, container managed VMs should not be connected directly to XenServer's management network to provide necessary isolation.

In order 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 (Destination TCP port 22) connections from dom0 (the XenServer Management network) to Container Managed VMs (the VM network). To monitor Windows Server Containers - the networking topology and firewalls must allow outbound Docker TLS

(Destination TCP port 2376) connections from dom0 (the XenServer Management network) to Container Managed VMs (the VM network).

To mitigate the risk of allowing traffic between VM and the management network, all traffic should pass 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 or 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 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 PV 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. If the network topology cannot ensure that only the Container Managed VM can be contacted through its advertised IP (using IP Source Guard or similar means), 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 using the following command:

```
xe vm-parm-get-uuid=vm-uuid param-name=other-config  /
```

```
    param-key=xscontainer-sshhostkey
```

Where `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 using the `--generate-certs` option, a temporary `CA`, `server`, and `client` certificates are generated specifically for a certain pool and VM. Certificates use sha256 hash and are valid for up to 2*365 days, after which the preparation should be repeated. The TLS connection is always established using a AES128-SHA cipher.

vApps

October 28, 2019

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, to allow VMs which depend upon one another to be automatically sequenced. This means that an administrator no longer has to manually sequence the startup of dependent VMs should a whole service require restarting (for instance in the case of a software update). The VMs within the vApp do not have to reside on one host and will be distributed within a pool using the normal rules.

The vApp functionality is useful in the Disaster Recovery situation where an Administrator may choose to group all VMs which reside on the same Storage Repository, or which relate to the same Service Level Agreement (SLA).

> **Note**

> vApps can be created and modified using both XenCenter and the xe CLI. For information on working with vApps using the CLI, see the XenServer Administrator's Guide.

Managing vApps in XenCenter

XenCenter's Manage vApps dialog box allows you to create, delete and modify vApps, start and shutdown 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 on the right.

To change the name or description of a vApp, add or remove VMs from the vApp, and change the startup sequence of the VMs in the vApp, use the Manage vApps dialog box.

1. Select the pool and, on the **Pool** menu, click **Manage vApps**.

   Alternatively, right-click in the **Resources** pane and click **Manage vApps** on the shortcut menu.

2. Select the vApp and click **Properties** to open its Properties dialog box.
3. Click the **General** tab to change the vApp name or description.
4. Click the **Virtual Machines** tab to add or remove VMs from the vApp.
5. Click 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 the **Properties** dialog box.

See the XenCenter help for further details. Press F1 or click **Help** to display the Help.

Creating vApps

To group VMs together in a vApp follow the procedure:

1. Select the pool and, on the Pool menu, click Manage vApps. This displays the Manage vApps window.
2. Enter a name for the vApp, and optionally a description, and then click Next.

   You can choose any name you like, but a descriptive name is best. Although it is advisable to avoid having multiple vApps with the same name, it is not a requirement, and XenCenter does not enforce any uniqueness constraints on vApp names. It is not necessary to use quotation marks for names that include spaces.

3. Choose which VMs to include in the new vApp, and then click Next.

   You can use the search box to list only VMs with names that include the specified 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 will be started up within the vApp, allowing certain VMs to be restarted before others. VMs with a start order value of 0 (zero) will be started first, then VMs with a start order value of 1, then VMs with a start order value of 2, and so on.
- **Attempt to start next VM after**: This is 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, that is, VMs with a lower start order.

5. On the final page of the wizard, you can review the vApp configuration. Click Previous to go back and modify any settings, or Finish to create the vApp and close the wizard.

> **Note**
>
> A vApp can span across multiple servers in a single pool, but cannot span across several pools.

Deleting vApps

To delete a vApp follow the procedure:

1. Select the pool and, on the **Pool** menu, click **Manage vApps**.
2. Select the vApp you want to delete from the list, then click **Delete**.

> **Note**
>
> The VMs in the vApp will not be deleted.

Start and Shutdown vApps using XenCenter

To start or shut down a vApp, use the Manage vApps dialog box, 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 and changed at any time from the vApp Properties dialog box or from the individual VM Properties dialog box.

To start a vApp

1. Open the Manage vApps dialog box: select the pool where the VMs in the vApp are located and, on the **Pool** menu, click Manage vApps. Alternatively, right-click in the **Resources** pane and click Manage vApps on the shortcut menu.
2. Select the vApp and click **Start** to start all of the VMs it contains.

To shut down a vApp

1. Open the Manage vApps dialog box: select the pool where the VMs in the vApp are located and, on the **Pool** menu, click Manage vApps. Alternatively, right-click in the **Resources** pane and click Manage vApps on the shortcut menu.
2. Select the vApp and click **Shut Down** to shut down all of the VMs in the vApp.

   A soft shutdown will be attempted on all VMs. If this is not possible, then a forced shutdown will be 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 may not always shut down all running processes and you risk losing data if you shut down a VM in this way. A forced shutdown should only be used when a soft shutdown is not possible.

Importing and Exporting vApps

vApps can be imported and exported as OVF/OVA packages. For more information, see Importing and Exporting VMs.

To export a vApp

1. Open the Manage vApps dialog box: on the **Pool** menu, click Manage vApps.
2. Select the vApp you want to export in the list and click **Export**.
3. Follow the procedure described in Exporting OVAs.

Exporting a vApp may take some time.

To import a vApp

1. Open the Manage vApps dialog box: on the **Pool** menu, click Manage vApps.
2. Click **Import** to open the **Import** wizard.
3. Follow the procedure described in Importing OVAs.

When the import is complete, the new vApp appears in the list of vApps in the Manage vApps dialog box.

Importing the Demo Linux Virtual Appliance

July 18, 2019

Citrix provides a fully functional installation of a Demo Linux Virtual Appliance, based on a CentOS 5.5 distribution. This is available for download, in a single `xva` file from the Citrix 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 a quick and simple VM deployment and can be used to test XenServer product features such as XenMotion, Dynamic Memory Control and High Availability. XenServer PV Tools are preinstalled in the Demo Linux Virtual Appliance and it also includes preconfigured networking connectivity in addition to a Web Server for test purposes.

> **Warning**
>
> The Demo Linux Virtual Appliance should NOT be used for running production workloads.

To Import the Demo Linux Virtual Appliance Using XenCenter

1. Download the Demo Linux Virtual Appliance from the Citrix XenServer Download page.

   Customers will require access to **My Account** to access this page. If you do not have an account, you can register on the Citrix home page.

2. In the Resources pane, select a host or a Pool, then right-click and select Import. The Import Wizard is displayed.
3. Click Browse and navigate to the location of the downloaded Demo Linux Virtual Appliance `xva` file on your computer.
4. Click Next.
5. Select the target XenServer host or pool, then click Next.
6. Select a storage repository on which to create the virtual appliance's disk, then click Next.
7. Click Finish to import the virtual appliance.

> **Note**
>
> When you first start the VM, you will be prompted to enter a root password. The IP address of the VM will then be displayed. Ensure you record this, as it will be useful for test purposes.

Useful Tests

This section lists some useful tests to carry out to ensure that your Demo Linux Virtual Appliance is correctly configured.

1. Test that you have external networking connectivity.

   Log in to the VM from the XenCenter console. Run this comment to send ping packets to Google and back:

   ```
   ping -c 10 google.com
   ```

   Other installed networking tools include:

   - `ifconfig`
   - `netstat`
   - `tracepath`

2. Using the IP address displayed on VM boot, test that you can ping the VM from an external computer.

3. Test that the web server is configured.

   In a web browser, enter the VM IP address. The "Demonstration Linux Virtual Machine" page should display. This page shows simple information about the VM mounted disks, their size, location and usage.

You can also use the webpage to mount a disk.

Mounting a disk using the Demonstration Linux Virtual Machine Web Page

1. In XenCenter, add a virtual disk to your VM. Select the VM in the Resources pane, click 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.

   You should make sure that the storage repository (SR) on which the virtual disk will be stored has sufficient space for the new virtual disk.

4. Select the SR where the new virtual disk will be stored.
5. Click Create to add the new virtual disk and close the dialog box.
6. Click the Console tab, and user your normal tools to partition and format the disk as required.
7. Refresh the Demonstration Linux Virtual Machine webpage, the new disk is displayed.
8. Click Mount. This mounts the disk, and filesystem information is displayed.

For more information on adding virtual disks, see the XenCenter help.

Advanced Notes for Virtual Machines

December 14, 2021

This article 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 make any changes to its boot behavior setting.

Persist (XenDesktop - Private Desktop Mode)

This is the default behavior 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 do this, shut down the VM, and then enter the following command:

```
xe vdi-param-set uuid=vdi_uuid on-boot=persist
```

Reset (XenDesktop - 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 will be lost when the VM is next booted.

Select this option if you plan to deliver standardized desktops that users cannot permanently change. To do this, shut down the VM, and then enter the following command:

```
xe vdi-param-set uuid=vdi_uuid on-boot=reset
```

> **Warning**
>
> After making the change to `on-boot=reset`, any data saved to the VDI will be discarded after the next shutdown/start or reboot

Making 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, this is accomplished by setting the no_root_squash flag when you create the share entry in /etc/exports on the NFS server.

Then either use XenCenter to attach the ISO library, or connect to the host console and run the command:

```
xe-mount-iso-sr host:/volume
```

For advanced use, additional arguments to the mount command may be passed.

If making a Windows SMB/CIFS share available to the XenServer host, either use XenCenter to make it available, or connect to the host console and run the following command:

```
xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
```

The unc_path argument should have back-slashes replaced by forward-slashes. For example:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
```

If you are using NLTMv2 authentication for your CIFS ISO SR, ensure that you also specify the cache=none parameter. For example:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain,
    sec=ntlmv2,cache=none
```

After mounting the share, any available ISOs will be available from the **Install from ISO Library or DVD drive** menu in XenCenter, or as CD images from the CLI commands.

The ISO should be attached to an appropriate Windows template.

Windows Volume Shadow Copy Service (VSS) provider

The Windows tools also include a XenServer VSS provider 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.

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.

> **Note**
>
> The VSS provider is automatically uninstalled when the PV drivers are uninstalled, and need to be activated again upon reinstallation. They can be uninstalled separately from the PV drivers by using `uninstall-XenProvider.cmd` in the same directory.

Connecting to a Windows VM Using Remote Desktop

There are two ways of viewing a Windows VM console, both of which support full keyboard and mouse interactivity.

1. Using XenCenter. This provides a standard graphical console and uses XenServer's in-built VNC technology to provide remote access to your virtual machine console.
2. Connecting using Windows Remote Desktop. This 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 will be disabled. To enable it, you will need to install the XenServer PV Tools and follow the procedure below to enable it in each VM that you want to connect using Remote Desktop:

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. If you want 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 will now be able to 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, so make sure the settings for sleep and hibernation on the remote computer are set to Never.

Time Handling in Windows VMs

For Windows guests, time is initially driven from the control domain clock, and is updated during VM lifecycle operations such as suspend, reboot and so on. Citrix recommends running a reliable NTP service in the control domain and all Windows VMs.

If you manually set a VM to be 2 hours ahead of the control domain (for example, using a time-zone offset within the VM), then it will persist. If you subsequently change the control domain time (either manually or, if it is automatically corrected, by NTP), the VM will shift accordingly but maintain the 2 hour 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/resume operations or live relocation using XenMotion, it is important to have up-to-date XenServer PV Tools installed, as they notify the Windows kernel that a time synchronization is required after resuming (potentially on a different physical host).

> **Note**
>
> Customers who are running Windows VMs in XenDesktop environment MUST ensure that the host clock has the same source as their 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

Time handling, in Linux VMs time handling, in 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. For example, 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, make sure that you change the time-zone from the default UTC to your local value (see Linux VMs for specific distribution instructions).

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 is a convenient mode, as only the control domain needs to be running 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 wall clock behavior for PV Linux VMs:

Guest OS	Default wall clock behavior	`independent_wallclock` 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 5.x (32-/64-bit)	Dependent	Yes
Scientific Linux 6.x (32-/64-bit)	Independent	
SLES 11 SP3, 11 SP4 (32-/64-bit)	Dependent	Yes
SLES 12 SP1, 12 SP2 (64-bit)	Dependent	Yes
SLED 11 SP3, 11 SP4 (64-bit)	Dependent	Yes
SLED 12 SP1, 12 SP2 (64-bit)	Dependent	Yes
Debian 6 (32-/64-bit)	Independent	

Guest OS	Default wall clock behavior	`independent_wallclock` setting available?
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 wall clock 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 wallclock behavior

1. From a root prompt on the VM, run the command: `echo 1 > /proc/sys/xen/independent_wallclock`

2. This can be persisted across reboots by changing the `/etc/sysctl.conf` configuration file and adding:

```
# Set independent wall clock time
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 wallclock behavior

1. From a root prompt on the VM, run the command: `echo 0 > /proc/sys/xen/independent_wallclock`

2. This can be persisted across reboots by changing the `/etc/sysctl.conf` configuration file and adding:

```
# Set independent wall clock time
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, refer to the documentation for your VM operating system.

You cannot change the XenServer time handling behavior for HVM Linux VMs.

Installing HVM VMs from Reseller Option Kit (BIOS-locked) Media

HVM VMs can be:

- BIOS-generic: the VM has generic XenServer BIOS strings;
- BIOS-customized: the VM has a copy of the BIOS strings of a particular server in the pool;
- without BIOS strings: immediately after its creation. If a VM does not have BIOS strings set when it is started, the standard XenServer BIOS strings will be inserted into it, and the VM will become BIOS-generic.

To allow installation of Reseller Option Kit (BIOS-locked) OEM versions of Windows, onto a VM running on a XenServer host, the BIOS strings of the VM will need to be copied from the host with which the ROK media was supplied.

> **Note:**
>
> After you first start a VM, you cannot change its BIOS strings. Ensure that the BIOS strings are correct before starting the VM for the first time.

In order to install the BIOS-locked media that came with your host, you will need to follow the steps below:

Using XenCenter

1. Click the **Copy host BIOS strings** to VM check box in the New VM Wizard.

Using the xe CLI

1. Run the `vm-install copy-bios-strings-from` command and specify the `host-uuid` as the host from which the strings should be copied (that is, the host that the media was supplied with):

   ```
   xe vm-install copy-bios-strings-from=host uuid \
     template=template name sr-name-label=name of sr \
     new-name-label=name for new VM
   ```

   This returns the UUID of the newly created VM.

   For example:

   ```
   xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786ef4 \
     template=”win7sp1” sr-name-label=Local\ storage  \
     new-name-label=newcentos
   7cd98710-bf56-2045-48b7-e4ae219799db
   ```

2. If the relevant BIOS strings from the host have been successfully copied into the VM, the command `vm-is-bios-customized` will confirm this:

   ```
   xe vm-is-bios-customized uuid=VM uuid
   ```

   For example:

   ```
   xe vm-is-bios-customized \
      uuid=7cd98710-bf56-2045-48b7-e4ae219799db
   This VM is BIOS-customized.
   ```

When you start the VM, it will be 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.

Preparing for Cloning a Windows VM Using Sysprep

Sysprep, for preparing Windows VM for cloning sysprepThe only supported way to clone a windows VM is by using the Windows utility `sysprep` to prepare the VM.

The `sysprep` utility modifies 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.

The steps that you need to take to clone Windows VMs are:

1. Create, install, and configure the Windows VM as desired.
2. Apply all relevant Service Packs and updates.
3. Install the XenServer PV Tools.
4. Install any applications and perform any other configuration.
5. Run `sysprep`. This will shut 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 will get a new SID and name, run a mini-setup to prompt for configuration values as necessary, and finally restart, before being available for use.

    > **Note**
    >
    > The original, sys-prepped VM (the "source" VM) should *not* be restarted again after the `sysprep` stage, and should be converted to a template immediately afterwards to prevent this. If the source VM is restarted, `sysprep` must be run on it again before it can be safely used to make additional clones.

For more information on using `sysprep`, visit the following Microsoft website:

The Windows Automated Installation Kit (AIK)

Assigning a GPU to a Windows VM (for Use with XenDesktop)

XenServer allows you to assign a physical GPU in a XenServer host machine to a Windows VM running on the same host. This GPU pass-through feature is intended for graphics power users, such as CAD designers, who require high performance graphics capabilities. **It is supported only for use with XenDesktop**.

While XenServer supports only one GPU for each VM, it automatically detects and groups together 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. Once 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 HA enabled, those VMs are overlooked by both features and 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 http://hcl.vmd.citrix.com to check the hardware compatibility list.

Before Assigning a GPU to a VM

Before you assign a GPU to a VM, you need to put the appropriate physical GPU(s) in your XenServer host and then restart the machine. Upon restart, XenServer automatically detects any physical GPU(s). To view all physical GPU(s) across hosts in the pool, use the `xe pgpu-list` command.

Ensure that the IOMMU chipset feature is enabled on the host. To do so, enter the following:

```
xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=iommu
```

If the value printed is **`false`**, IOMMU is not enabled, and GPU pass-through is not available using the specified XenServer host.

To assign a GPU to a Windows VM 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 using the xe CLI

1. Shut down the VM that you want to assign a GPU group by using the `xe vm-shutdown` command.
2. Find the UUID of the GPU group by entering the following:

   ```
   xe gpu-group-list
   ```

   This command prints all GPU groups in the pool. Note the UUID of the appropriate GPU group.
3. Attach the VM to a GPU group by entering the following:

   ```
   xe vpgu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
   ```

   To ensure that the GPU group has been attached, run the `xe vgpu-list` command.
4. Start the VM by using the `xe vm-start` command.
5. Once the VM starts, install the graphics card drivers on the VM.

   Installing the drivers is essential, as the VM has direct access to the hardware on the host. Drivers are provided by your hardware vendor.

   > **Note**
   >
   > If you try to start a VM with GPU pass-through on a XenServer host without an available GPU in the appropriate GPU group, XenServer prints an error message.

To detach a Windows VM from a GPU 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 using the xe CLI

1. Shut down the VM by using the `xe vm-shutdown` command.
2. Find the UUID of the vGPU attached to the VM by entering the following:

   ```
   xe vgpu-list vm-uuid=uuid_of_vm
   ```

3. Detach the GPU from the VM by entering the following:

   ```
   xe vgpu-destroy uuid=uuid_of_vgpu
   ```

4. Start the VM by using the `xe vm-start` command.

Creating ISO Images

XenServer can use ISO images of CD-ROM or DVD-ROM disks as installation media and data sources for Windows or Linux VMs. This section describes how to make ISO images from CD/DVD media.Creating an ISO image

Creating an ISO on a Linux computer

1. Put the CD- or DVD-ROM disk into the drive. The disk should not be mounted. To check, run the command:

   ```
   mount
   ```

   If the disk is mounted, unmount the disk. Refer to your operating system documentation for assistance if required.

2. As root, run the command

   ```
   dd if=/dev/cdrom of=/path/cdimg_filename.iso
   ```

This will take some time. When the operation is completed successfully, you should see something like:

```
1187972+0 records in
1187972+0 records out
```

Your ISO file is ready.

Creating an ISO on a Windows computer

1. 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.

Enabling VNC for Linux VMs

July 18, 2019

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 the XenCenter graphical console, you need to ensure that the VNC server and an X display manager are installed on the VM and properly configured. This section describes the procedures for configuring VNC on each of the supported Linux operating system distributions to allow proper interactions with the XenCenter graphical console.

CentOS-based VMs should use the instructions for the Red Hat-based VMs below, as they use the same base code to provide graphical VNC access. CentOS 4 is based on Red Hat Enterprise Linux 4, and CentOS 5 is based on Red Hat Enterprise Linux 5.

Enabling 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. See Install the Linux Guest Agent for details.

The graphical console for Debian Squeeze virtual machines is provided by a VNC server running inside the VM. In the recommended configuration, this is controlled by a standard display manager so that a login dialog 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):

   ```
   apt-get install vnc4server
   ```

   > **Note**
   >
   > Significant CPU time can be taken by the Debian Squeeze Graphical Desktop Environment, which uses the Gnome Display Manager version 3 daemon. Citrix strongly advises that customers uninstall the Gnome Display Manager `gdm3` package and install the `gdm` package as follows:

   ```
   apt-get install gdm
   apt-get purge gdm3
   ```

3. Set up a VNC password (not having one is a serious security risk) using the `vncpasswd` command, passing in a file name to write the password information to. For example:

   ```
   vncpasswd /etc/vncpass
   ```

4. Modify your `gdm.conf` file (`/etc/gdm/gdm.conf`) to configure a VNC server to manage display `0` by extending the `[servers]` and `[daemon]` sections as follows:

   ```
   [servers]
   0=VNC
   [daemon]
   VTAllocation=false
   [server-VNC]
   name=VNC
   command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/vncpass BlacklistTimeout=0
   flexible=true
   ```

5. Restart GDM, and then wait for the graphical console to be detected by XenCenter:

   ```
   /etc/init.d/gdm restart
   ```

> **Note**
>
> You can check that the VNC server is running using a command like `ps ax | grep vnc`.

Enabling a Graphical Console on Red Hat, CentOS, or Oracle Linux VMs

> **Note**
>
> Before setting up your Red Hat VMs for VNC, be sure that you have installed the Linux guest agent. See Install the Linux Guest Agent for details.

To configure VNC on Red Hat VMs, you need to 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 will then be modified in several subsequent procedures in this section.

Determining the Location of your VNC Configuration File

If you are using Red Hat Linux version 4 the GDM configuration file is `/etc/X11/gdm/gdm.conf`. This is a unified configuration file that contains default values as specified by the provider of your version of GDM in addition to your own customized configuration. This type of file is used by default in older versions of GDM, as included in these versions of Red Hat Linux.

If you are using Red Hat Linux version 5.x the GDM configuration file is `/etc/gdm/custom.conf`. This 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, as included in these versions of Red Hat Linux.

Configuring 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` should appear, with their version numbers specified.

   If these package names are displayed, the appropriate packages are already installed. If you see a message saying that one of the packages is not installed, then you may not have selected the graphical desktop options during installation. You will need to install these packages before you can continue. See the appropriate Red Hat Linux x86 Installation Guide for details regarding installing additional software on your VM.

2. Open the GDM configuration file with your preferred text editor and add the following lines to the file:

```
[server-VNC]
name=VNC Server
command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
   depth 16 \
-BlacklistTimeout 0
flexible=true
```

- With configuration files on 4.x, this should be added above the `[server-Standard]` section.
- With configuration files on Red Hat Linux 5.x, this should be added into the empty `[servers]` section.

3. Modify the configuration so that the `Xvnc` server is used instead of the standard X server:

   - If you are using Red Hat Linux 3 or 4, there will be a line just above that reads:

     ```
     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.
5. 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 is configured to start up in runlevel 3, change this for the display manager to be started (and therefore to get access to a graphical console).

Firewall Settings

Configuring VNC firewall settings, RHELThe firewall configuration by default does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, you need to 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 just zero). So a VNC server setup for Display-0 will listen on TCP port `5900`, Display-1 is `TCP-5901`, and so on. Consult your firewall documentation to make sure these ports are open.

You might want to further customize your firewall configuration if you want to use IP connection tracking or limit the initiation of connections to be from one side only.

To customize Red Hat-based VMs firewall to open the VNC port

1. For Red Hat Linux 4.x and 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 can of course expose extra services to the outside world and reduce the overall security of your VM.

VNC Screen Resolution

If after connecting to a VM with the graphical console the screen resolution is mismatched (for example, the VM display is too large to comfortably fit in the **Graphical Console** pane), you can control it by setting the VNC server `geometry` parameter as follows:

1. Open the GDM configuration file with your preferred text editor.
2. Find the `[server-VNC]` section you added above.
3. Edit the command line to read, for example:

   ```
   command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
   ```

   where the value of the `geometry` parameter can be any valid screen width and height.
4. Save and close the file.

Enabling VNC for RHEL, CentOS, or OEL 6.x VMs

If you are using Red Hat Linux version 6.x, the GDM configuration file is `/etc/gdm/custom.conf`. This 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, as included in these versions of Red Hat Linux.

During the operating system installation, select **Desktop** mode.

1. On the RHEL installation screen, select **Desktop**, Customize now, and then click **Next**.

   This displays the **Base System** screen, ensure that Legacy UNIX compatibility is selected.

2. Select **Desktop**, Optional packages, then click **Next**.

   This 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:

```
[security]
DisallowTCP=false

[xdmcp]
Enable=true
```

2. Create the file, `/etc/xinetd.d/vnc-server-stream`:

```
service vnc-server
{

              id = vnc-server
         disable = no
            type = UNLISTED
            port = 5900
     socket_type = stream
            wait = no
            user = nobody
           group = tty
          server = /usr/bin/Xvnc
     server_args = -inetd -once -query localhost -SecurityTypes None -geometry 800x600 -depth 16
 }
```

3. Enter the following command to start the `xinetd` service:

```
# service xinetd start
```

4. Open the file `/etc/sysconfig/iptables` and add the following line. The line should be added above the line reading, `-A INPUT -j REJECT --reject-with icmp-host-prohibited`:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
   ```

5. Enter the following command to restart `iptables`:

   ```
   # service iptables restart
   ```

6. Enter the following command to restart `gdm`:

   ```
   # telinit 3
   # telinit 5
   ```

> **Note**
>
> Red Hat Linux uses runlevel 5 for graphical startup. If your installation is configured to start up in runlevel 3, change this for the display manager to be started (and therefore to get access to a graphical console).

Setting 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 allows you to connect an external VNC viewer to your guest to allow you to view the graphical console; the methodology for using the SLES remote administration feature is slightly different than that provided by XenCenter, but it is possible to modify the configuration files in your SUSE Linux VM such that it is integrated with the graphical console feature.

Checking for a VNC Server

Before making configuration changes, verify that you have a VNC server installed. SUSE ships the `tightvnc` server by default; this is a suitable VNC server, but you can also use the standard RealVNC distribution if you prefer.

You can check that you have the `tightvnc` software installed by running the command:

```
rpm -q tightvnc
```

Enabling Remote Administration

If Remote Administration was not enabled during installation of the SLES software, you can enable it as follows:

1. Open a text console on the VM and run the `YaST` utility:

   ```
   yast
   ```

2. Use the arrow keys to select Network Services in the left menu, then 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 that you will need 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.

Modifying the `xinetd` Configuration

After enabling Remote Administration, you need to modify a configuration file if you want to allow XenCenter to connect, or else use a third party VNC client.

1. Open the file `/etc/xinetd.d/vnc` in your preferred text editor.

   The file contains sections like the following:

   ```
   service vnc1
   {

   ```

```
socket_type = stream
protocol    = tcp
wait        = no
user        = nobody
server      = /usr/X11R6/bin/Xvnc
server_args = :42 -inetd -once -query localhost -geometry 1024x768 -depth 16
type        = UNLISTED
port        = 5901
 }
```

2. Edit the `port` line to read

```
port = 5900
```

3. Save and close the file.
4. Restart the display manager and `xinetd` service with the following commands:

```
/etc/init.d/xinetd restart
rcxdm restart
```

SUSE Linux uses runlevel 5 for graphical startup. If your remote desktop does not appear, verify that your VM is configured to start up in runlevel 5.

Firewall Settings

Configuring VNC firewall settings, SLESBy default the firewall configuration does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, you need to 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 just zero). So a VNC server setup for Display-0 will listen on TCP port `5900`, Display-1 is `TCP-5901`, and so on Consult your firewall documentation to make sure these ports are open.

You might want to further customize your firewall configuration if you want to use IP connection tracking or limit the initiation of connections to be from one side only.

To Open the VNC Port on SLES 10.x VMs' Firewall

1. Open a text console on the VM and run the `YaST` utility:

```
yast
```

2. Use the arrow keys to select Security and Users in the left menu, then 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 the Allowed Services in the left menu.
4. Tab to the Firewall Configuration: Allowed Services fields on the right. Use the arrow keys to select the Advanced button (near the bottom right, just above the Next button) and press Enter.
5. In the Additional Allowed Ports screen, enter *5900* in the TCP Ports field. Tab to the OK button and press Enter.
6. Tab to the Next button and press Enter, then in the Summary screen Tab to the Accept button and press Enter, and finally on the top-level `YaST` screen Tab to the Quit button and press Enter.
7. Restart the display manager and `xinetd` service with the following commands:

```
/etc/init.d/xinetd restart
rcxdm restart
```

Alternatively, you can disable the firewall until the next reboot by running the `rcSuSEfirewall2 stop` command, or permanently by using `YaST`. This can of course expose additional services to the outside world and reduce the overall security of your VM.

To Open the VNC Port on SLES 11.x VMs' Firewall

1. Open a text console on the VM and run the `YaST` utility:

```
yast
```

2. Use the arrow keys to select Security and Users in the left menu, then 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, then in the Summary screen Tab to the Finish button and press Enter, and finally on the top-level `YaST` screen Tab to the Quit button and press Enter.

8. Restart the display manager and `xinetd` service with the following commands:

   ```
   /etc/init.d/xinetd restart
   rcxdm restart
   ```

Alternatively, you can disable the firewall until the next reboot by running the `rcSuSEfirewall2 stop` command, or permanently by using `YaST`. This can of course expose additional services to the outside world and reduce the overall security of your VM.

VNC Screen Resolution

If after connecting to a Virtual Machine with the Graphical Console the screen resolution is mismatched (for example, the VM display is too big to comfortably fit in the Graphical Console pane), you can control it by setting the VNC server `geometry` parameter as follows:

1. Open the `/etc/xinetd.d/vnc` file with your preferred text editor and find the `service_vnc1` section (corresponding to `displayID` 1).
2. Edit the `geometry` argument in the `server-args` line to the desired display resolution. For example,

   ```
   server_args  = :42 -inetd -once -query localhost -geometry 800x600 -depth 16
   ```

   where the value of the `geometry` parameter can be any valid screen width and height.
3. Save and close the file.
4. Restart the VNC server:

   ```
   /etc/init.d/xinetd restart
   rcxdm restart
   ```

Checking Runlevels

Red Hat and SUSE Linux VMs use runlevel 5 for graphical startup. This section describes how to verify that your VM is configured to start up in runlevel 5 and how to change it if it is not.Linux runlevels

1. Check `/etc/inittab` to see what the default runlevel is set to. Look for the line that reads:

```
id:n:initdefault:
```

If *n* is not 5, edit the file to make it so.

2. You can run the command `telinit q ; telinit 5` after this change to avoid having to actually reboot to switch runlevels.

Troubleshooting VM Problems

July 18, 2019

Citrix provides two forms of support: free, self-help support on the Citrix Support[Citrix] 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 Support site hosts various resources that may 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 experience unusual VM behavior, this article aims to help you solve the problem describes where application logs are located and other information that can help your XenServer Solution Provider and Citrix track and resolve the issue.

Troubleshooting of installation issues is covered in the XenServer Installation Guide. Troubleshooting of XenServer host issues is covered in the XenServer Administrator's Guide.

> **Note**
>
> Citrix recommends that you follow the troubleshooting information in this article solely under the guidance of your XenServer Solution Provider or Citrix Support.
>
> Vendor Updates: Citrix recommends that VMs are kept up-to-date with operating system vendor-supplied updates. VM crashed and other failures, may have been fixed by the vendor.

VM Crashes

If you are experiencing VM crashes, it is possible that a kernel crash dump can help identify the problem. If the crash is reproducible, follow this procedure and consult your guest OS vendor for further investigation on this issue.

Controlling Linux VM Crashdump Behavior

Troubleshooting Linux VM general problemsFor Linux VMs, the crashdump behavior can be controlled through the `actions-after-crash` parameter. The following are the possible values:

Value	Description
preserve	leave the VM in a paused state (for analysis)
restart	no core dump, just reboot VM (this is the default)
destroy	no coredump, 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:

   ```
   xe vm-list name-label=name params=uuid --minimal
   ```

2. Change the `actions-after-crash` value using `xe vm-param-set`. For example, run the following command on dom0:

   ```
   xe vm-param-set uuid=vm_uuid actions-after-crash=preserve
   ```

3. Crash the VM.

   For PV guests, run the following command on the VM:

   ```
   echo c | sudo tee /proc/sysrq-trigger
   ```

4. Execute the dump core on dom0. For example, run:

   ```
   xl dump-core domid filename
   ```

Controlling Windows VM Crashdump Behavior

Troubleshooting Windows VM general problemsFor Windows VMs, the core dump behavior cannot be controlled by the `actions-after-crash` parameter. 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**.

Troubleshooting Boot Problems on Linux VMs

Troubleshooting Linux VM boot problemsThere is a utility script named `xe-edit-bootloader` in the XenServer host control domain which can be used to edit the bootloader configuration of a shutdown Linux VM. This can be used to fix problems which are preventing it from booting.

To use this script:

1. To ensure that the VM in question is shut down, run the command

   ```
   xe vm-list
   ```

   The value of *power-state* will be *halted*

2. You can use the UUID as follows:

   ```
   xe-edit-bootloader -u linux_vm_uuid -p partition_number
   ```

   or the name-label as follows:

   ```
   xe-edit-bootloader -n linux_vm_name_label -p partition_number
   ```

   The partition number represents the slice of the disk which has the filesystem. In the case of the default Debian template, this is *1* since it is the first partition.

3. You will be dropped into an editor with the `grub.conf` file for the specified VM loaded. Make the changes to fix it, and save the file, exit the editor, and start the VM.

Workload Balancing Guides

February 22, 2021

These guides are only available as PDF.

Workload Balancing Quick Start Guide (PDF)

Workload Balancing Administrator's Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

> **Note:**
>
> We recommend that you use the Workload Balancing 8.2 virtual appliance with your XenServer 7.1 CU2 pool. This virtual appliance is available from the Citrix Hypervisor downloads page.
>
> To use the latest appliance with XenServer 7.1 CU2, ensure you have the following prerequisites:
>
> - Use the latest version of XenCenter provided with Citrix Hypervisor 8.2. This available from the Citrix Hypervisor downloads page.
> - Install Hotfix XS71ECU2040 on your XenServer 7.1 CU2 hosts.
> - Review the product documentation for the latest version of Workload Balancing.

Supplemental Guides

February 22, 2021

These guides are only available as PDF.

Conversion Manager Guide (PDF)

Measured Boot Supplemental Pack Guide (PDF)

XenServer-Nutanix Integration Guide (PDF)

vSwitch Controller User Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

> **Note:**
>
> We recommend that you use the Conversion Manager 8.2 virtual appliance with your XenServer 7.1 CU2 pool. This virtual appliance is available from the Citrix Hypervisor downloads page.
>
> To use the latest appliances with XenServer 7.1 CU2, ensure you have the following prerequisites:
>
> - Use the latest version of XenCenter provided with Citrix Hypervisor 8.2. This available from the Citrix Hypervisor downloads page.
> - Install Hotfix XS71ECU2040 on your XenServer 7.1 CU2 hosts.

> - Review the product documentation for the latest version of Conversion Manager.

Common Criteria Evaluated Configuration Guide

February 22, 2021

This guide is only available as a PDF.

Common Criteria Evaluated Configuration Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Third party notices

July 19, 2021

This release of XenServer includes third-party software licensed under a number of different licenses.

To extract the licensing information from your installed XenServer product and components, see the instructions in Citrix Hypervisor Open Source Licensing and Attribution.

In addition, note the following information:

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

SDKs and APIs

February 22, 2021

These guides are only available as PDF.

Management API Guide (PDF)

Software Development Kit Guide (PDF)

Supplemental Packs and the DDK Guide (PDF)

The PDF guides are no longer being updated. Any changes or additions to the PDF documentation are listed in the Addenda.

Addenda to XenServer 7.1 LTSR PDF guides

April 25, 2022

The XenServer 7.1 PDF guides are no longer updated. This article includes addenda to the information in the guides.

> Note:
>
> Some of the addenda are already included in the English-language PDF guides, but not in the PDF guides for other languages. These addenda are marked with the note (Localized only).

Administrator's Guide

2.1. Authenticating Users With Active Directory (AD)

- Addition of the following note to this section:

  > **Note:**
  >
  > You can enable LDAP channel binding and LDAP signing on your AD domain controllers. For more information, see Microsoft Security Advisory.

- (Localized only) Addition of the following text before the first note in the **Understanding Active Directory Authentication in the XenServer Environment** section: To qualify a user name, you must enter the user name in Down-Level Logon Name format. For example, `mydomain\myuser`
  .
- (Localized only) Removal of the following example text from the first note in the **Understanding Active Directory Authentication in the XenServer Environment** section: (for example, enter either `mydomain\myuser` or `myser@mydomain.com`).

2.2.2. Definitions of RBAC Roles and Permissions

- (Localized only) In the **Definitions of Permissions** table, updates to the **Allows Assignee to** cell of the **VM create/destroy operations** row:
  - **Original text:**
    - Install or delete
    - Clone VMs
    - Add, remove, and configure virtual disk/CD devices
    - Add, remove, and configure virtual network devices
    - Import/export VMs
    - VM configuration change

- **Updated text:**
  - 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

3.9.3. Restart Priorities

- (Localized only) This section has been rewritten. The following content replaces the existing section:

3.9.3. Restart configuration settings

Virtual machines can be considered protected, best-effort or unprotected by HA. The value of ha-restartpriority 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** HA guarantees to restart a protected VM that goes offline or whose host goes offline, provided the pool is not overcommitted and the VM is agile.
  If a protected VM cannot be restarted at the time of a server failure (for example, if the pool was overcommitted when the failure occurred), further attempts to start this VM are made when extra capacity becomes available in a pool, which might now succeed.

  `ha-restart-priority`value: `restart`

- **Best-effort** If the host where a best-effort VM is running goes offline, HA attempts to restart the best-effort VM on another host only after all protected VMs have been successfully restarted. HA makes only one attempt to restart a best-effort VM and if this attempt fails no further restart is attempted.

  `ha-restart-priority`value: `besteffort`

- **Unprotected** If an unprotected VM or the host it runs on is stopped, HA does not attempt to restart the VM.

  `ha-restart-priority`value: An empty string

> **Note:**
>
> HA 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 enters a state where the number of tolerable failures drops to zero, the protected VMs are no longer guaranteed to be restarted. If this condition is reached, a system alert is generated.

In this case, if an additional failure occurs, all VMs that have a restart priority set behave according to the best-effort behavior.

3.9.3.1. Start order

The start order is the order in which XenServer HA attempts to restart protected VMs if a failure occurs. The start order is determined by the values of the `order` property for each of the protected VMs.

The `order` property of a VM is used by HA and also by other features that start and shutdown VMs. Any VM can have the `order` property set, not just those marked as protected for HA. However, HA 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 HA. 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:

```
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.

3.10.1. Enabling HA Using the CLI

- (Localized only) Updates to step 2:
  - **Original text:** For each VM you wish to protect, set a restart priority. You can do this as follows:

    ```
    xe vm-param-set uuid=<vm_uuid> ha-restart-priority=<1> ha-always-run=true
    ```

  - **Update text:** For each VM you wish to protect, set a restart priority and start order. You can do this as follows:

```
xe vm-param-set uuid=<vm_uuid> ha-restart-priority=restart
    order=<1>
```

- The default timeout value is 60 seconds, not 30 seconds.
  - **Original text:** If you do not specify a timeout when you enable HA, XenServer will use the default 30 seconds timeout.
  - **Update text:** If you do not specify a timeout when you enable HA, XenServer will use the default 60 seconds timeout.

3.10.2. Removing HA Protection from a VM using the CLI

- (Localized only) Updates to this section.
  - **Original text:** To disable HA features for a VM, use the `xe vm-param-set` command to set the `ha-always-run` parameter to **`false`**. This does not clear the VM restart priority settings. You can enable HA for a VM again by setting the `ha-always-run` parameter to **`true`**.
  - **Updated text:** To disable HA features for a VM, use the `xe vm-param-set` command to set the `ha-restart-priority` parameter to be an empty string. This does not clear the start order settings. You can enable HA for a VM again by setting the `ha-restart-priority` parameter to `restart` or `best-effort` as appropriate.

3.12 Communicating with XenServer hosts and Resource Pools

- Add the following information:

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

  Ciphers:

  - 3des-cbc
  - blowfish-cbc
  - cast128-cbc
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-gcm@openssh.com

- aes256-gcm@openssh.com
- chacha20-poly1305@openssh.com

MACs:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512
- umac-64@openssh.com
- umac-128@openssh.com
- hmac-sha1-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- umac-64-etm@openssh.com
- umac-128-etm@openssh.com

Key Exchange algorithms:

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- curve25519-sha256
- curve25519-sha256@libssh.org

Host Key algorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- rsa-sha2-256
- rsa-sha2-512
- ssh-dss
- ssh-dss-cert-v01@openssh.com
- ssh-ed25519

- ssh-ed25519-cert-v01@openssh.com
- ssh-rsa
- ssh-rsa-cert-v01@openssh.com

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

4.1. Networking Support

- (Localized only) Correction of the number of supported bonded network interfaces
  - **Original text:** XenServer supports up to 16 physical network interfaces (or up to 8 bonded network interfaces) per XenServer host and up to 7 virtual network interfaces per VM.
  - **Updated text:** XenServer supports up to 16 physical network interfaces (or up to 4 bonded network interfaces) per XenServer host and up to 7 virtual network interfaces per VM.

4.3.5. NIC Bonds

- (Localized only) Addition of the following note: NIC bonds are not supported on NICs that carry FCoE traffic.

4.4.6. Creating NIC Bonds in Resource Pools

- (Localized only) Removal of the following section:

  > **Note:**
  >
  > If you are not using XenCenter for NIC bonding, the quickest way to create pool-wide NIC bonds is to create the bond on the master, and then restart the other pool members. Alternatively, you can use the `service xapi restart` command. This causes the bond and VLAN settings on the master to be inherited by each host. The management interface of each host must, however, be manually reconfigured.

  Follow the procedure in previous sections to create a NIC Bond, see Adding NIC Bonds to a New Pool.

5.1.1. Storage Repositories (SRs)

- (Localized only) Updates to the following paragraph:
  - **Original text** 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 in common.

  - **Updated text** 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 in the pool. All hosts in a single resource pool must have at least one shared SR in common. Shared storage cannot be shared between multiple pools.

5.8.4.1. Limitations and Caveats

- (Localized only) Removal of the following limitation: VDIs with more than one snapshot cannot be migrated.

5.7 PVS-Accelerator

- Addition of the following text to the note:
  - The PVS-Accelerator feature is not supported in resource pools that are managed by the vSwitch Controller.
  - If you are using XenServer 7.1 with Cumulative Update 2 or later applied, ensure that you update your PVS Accelerator Supplemental Pack to the latest version provided on the XenServer Product Download page for XenServer 7.1 Cumulative Update 2. This version of the PVS Accelerator Supplemental Pack is the same as the version provided for XenServer 7.6 CR.

5.7.3. Caching Operation

- (Localized only) Addition of the following point to the list of considerations:
  - Do not use a large port range for PVS server communication. Setting a range of more than 20 ports is rarely necessary. A large port range can slow packet processing and increase the boot time of the XenServer control domain when using PVS-Accelerator.

6.1. What is Dynamic Memory Control (DMC)?

- (Localized only) Addition of the following note:

> **Note:**
>
> Dynamic Memory Control is not supported with VMs that have a virtual GPU.

6.2.3. Updating Memory Properties

- (Localized only) Updates to a note to remove an unsupported operation.

  Original note: To alter the static maximum of a VM – you will need to suspend or shut down the VM

  Updated note: To alter the static maximum of a VM – you must shut down the VM

9.2.2. Configuring Performance Alerts Using the xe CLI

- (Localized only) Addition of the following section after the note that says "Multiple `<variable>` nodes are allowed"

  After setting the new configuration, use the following command to refresh perfmon for each host:

  ```
  xe host-call-plugin host=<host_uuid> plugin=perfmon fn=refresh
  ```

  If this is not done,there will be a delay before the new configuration takes effect,since by default, `perfmon` checks for new configuration once every thirty minutes. This default can be changed in `/etc/sysconfig/perfmon`.

A.4. Secrets

- (Localized only) Addition of new section with the following content:

  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.

  ```
  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:

```
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=”io” shared=”true”
```

A.5.3.3. bond-destroy

- (Localized only) Update to the example command.
  - **Original text:** `host-bond-destroy uuid=<bond_uuid>`
  - **Updated text:** `bond-destroy uuid=<bond_uuid>`

A.5.6.1. drtask-create

- (Localized only) Update to the example command.
  - **Original text:** `xe dr-task-create type=lvmoiscsi device-config:target=<target-ip-address> device-config:targetIQN=<targetIQN> device-config:SCSIid=<SCSIid> sr-whitelist=<sr-uuid-list>`
  - **Updated text:** `xe drtask-create type=lvmoiscsi device-config:target=<target-ip-address> device-config:targetIQN=<targetIQN> device-config:SCSIid=<SCSIid> sr-whitelist=<sr-uuid-list>`

A.5.18. Template Commands

- (Localized only) Addition of the following note.

  > **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.

A.5.18.1. VM Template Parameters

- (Localized only) Addition of the following text to the **Description** field of the `is-a-template` row of the table.

After this value has been set to true it cannot be reset to false. Template VMs cannot be converted into VMs using this parameter.

- (Localized only) Change to the text in the **Description** field of the `ha-restart-priority` row of the table to the following:

  restart or best effort

A.5.22.6. vdi-export

- (Localized only) Addition of the following new section:

  `vdi-export uuid=<uuid_of_vdi> filename=<filename_to import_from> [base =<uuid_of_base_vdi>] [format=<format>] [--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 VHDbased 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.

A.5.22.8. vdi-import

- (Localized only) Update the content of this section to the following text:

  `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

A.5.24.2. pool-vlan-create

- (Localized only) Update to fix an error in a command.

  - **Original text:** `vlan-create pif-uuid=<uuid_of_pif> vlan=<vlan_number> network-uuid=<uuid_of_network>`
  - **Updated text:** `pool-vlan-create pif-uuid=<uuid_of_pif> vlan=<vlan_number > network-uuid=<uuid_of_network>`

A.5.25.1. VM Selectors

- (Localized only) Update to fix an error in a command.
  - **Original text:** The full list of fields that can be matched can be obtained by the command `xe vm-list params-all`.
  - **Updated text:** The full list of fields that can be matched can be obtained by the command `xe vm-list params=all`.

A.5.25.2. VM Parameters

- (Localized only) Addition of the following text to the **Description** field of the `is-a-template` row of the table.

  After this value has been set to true it cannot be reset to false. Template VMs cannot be converted into VMs using this parameter.

- (Localized only) Update to the text in the **Description** field of the `ha-restart-priority` row of the table to the following:

  restart or best effort

Workload Balancing Administrator Guide

6.1.10.5. Changing the Database Maintenance Window

- (Localized only) Addition of the following note after the first paragraph of the section:

  > **Note:**
  >
  > To avoid a loss of Workload Balancing:
  >
  > During the maintenance window, 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.

6.2 Upgrading Workload Balancing

- (Localized only) This section has been removed and replaced with the following note:

  Online upgrading of Workload Balancing has been deprecated for security reasons. Customers cannot upgrade via 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/.

vSwitch Controller User Guide

2.1 Deploying the vSwitch Controller Virtual Appliance

- Addition of a note to this section that includes the following restriction:

  > **Note:**
  >
  > vSwitch Controller is not supported in conjunction with the PVS-Accelerator feature. Do not use vSwitch controller to manage a resource pool that uses PVS-Accelerator.

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