Citrix XenServer ® 7.5 Virtual Machine User's Guide

Published May 2018
1.0 Edition

Citrix XenServer ® 7.5 Virtual Machine User's Guide

Version: 7.5

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

Disclaimers

Trademarks

Citrix®
XenServer ®
XenCenter ®

CITRIX

Contents

CITRIX

Chapter 1. About this Document

1.1. Overview

This is a guide to using Virtual Machines (VMs) with XenServer, the platform virtualization solution from Citrix. It describes how to create, configure, and manage VMs running on XenServer hosts.

This section summarizes the rest of the guide so that you can find the information you need. The following topics are covered:

- General information about preparing and creating VMs
- Creating Windows VMs
- Creating Linux VMs
- Updating VMs
- Migrating VMs
- Using Container Management
- Creating and using ISO images of vendor media for installing VMs
- Setting up a network repository of vendor media for installing VMs
- Troubleshooting VMs

1.2. XenServer Documentation

XenServer documentation shipped with this release includes:

- *XenServer Release Notes* cover new features in XenServer 7.5 and any advisories and known issues that affect this release.
- *XenServer Quick Start Guide* provides an introduction for new users to the XenServer environment and components. This guide steps through the installation and configuration essentials to get XenServer and the XenCenter management console up and running quickly. After installation, it demonstrates how to create a Windows VM, VM template and pool of XenServer hosts. It introduces basic administrative tasks and advanced features, such as shared storage, VM snapshots and XenMotion live migration.
- *XenServer Installation Guide* steps through the installation, configuration and initial operation of XenServer and the XenCenter management console.
- *XenServer Virtual Machine User's Guide* describes how to install Windows and Linux VMs within the XenServer environment. This guide explains how to create new VMs from installation media, from VM templates included in the XenServer package and from existing physical machines (P2V). It explains how to import disk images and how to import and export appliances.
- *XenServer Administrator's Guide* gives an in-depth description of the tasks involved in configuring a deployment of XenServer, including setting up storage, networking and pools. It describes how to administer XenServer using the xe Command Line Interface.
- *vSwitch Controller User's Guide* is a comprehensive user guide to the vSwitch Controller for XenServer.
- *Supplemental Packs and the DDK* introduces the XenServer Driver Development Kit, which can be used to modify and extend the functionality of XenServer.
- *XenServer Software Development Kit Guide* presents an overview of the XenServer SDK. It includes code samples that demonstrate how to write applications that interface with XenServer hosts.
- *XenAPI Specification* is a reference guide for programmers to the XenServer API.

For additional resources, visit the Citrix Product Documentation website.

Chapter 2. Virtual Machines

This chapter provides an overview of how to create Virtual Machines (VMs) using templates. It also explains other preparation methods, including physical to virtual conversion (P2V), cloning templates, and importing previously-exported VMs.

What is a Virtual Machine?
A Virtual Machine (VM) is a software computer that, like a physical computer, runs an operating system and applications. The VM 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 Section 11.1, “VM Boot Behavior”.

XenServer supports guests with any combination of IPv4 or IPv6 configured addresses.

2.1. 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.

2.2. Creating VMs

2.2.1. 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 in order 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.

Chapter 4, *Creating Windows VMs* describes how to install Windows operating systems onto VMs.

Chapter 5, *Creating Linux VMs* describes how to install Linux operating systems onto VMs.

> **Note:**
>
> Templates created by older versions of XenServer can be used in newer version of XenServer. However, templates created in newer versions of XenServer are not compatible with older versions of XenServer. If you have a VM template that you created with XenServer 7.5 and you want to use it with an earlier version of XenServer, export the VDIs separately and recreate the VM.

2.2.2. Other Methods of VM Creation

In addition to creating VMs from the provided templates, there are 3 other methods that you can use to create VMs.

1. Physical to Virtual Conversion (P2V)
2. Cloning an existing VM
3. Importing an exported VM

2.2.2.1. Physical to Virtual Conversion (P2V)

Physical to Virtual Conversion (P2V) is the process by which an existing Windows operating system on a physical server — its file system, configuration, and so on — is converted to a virtualized instance of the operating system. This is then transferred, instantiated, and started as a VM on the XenServer host.

2.2.2.2. 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 Section 11.8, "Preparing for Cloning a Windows VM Using Sysprep" for Windows and Section 5.7, "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.

2.2.2.3. 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 the XenServer host that is in another resource pool.

For details and procedures on importing and exporting VMs, see Chapter 13, *Importing and Exporting VMs*.

2.3. XenServer Tools

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

Agent. XenServer Tools must be installed on each 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 Tools installed on the VM must be the same as the latest available version installed on the XenServer host. For example, some hotfixes include an updated XenServer Tools ISO that updates the version installed on the host.

The I/O drivers contain storage and network drivers, and low-level management interfaces. These drivers replace the emulated devices and provide high-speed transport between Windows and the XenServer product family software. 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 Tools must be installed on each Windows VM in order for the VM to have a fully-supported configuration. The version of XenServer Tools installed on the VM must be the same as the version installed on the XenServer host. A VM will function without the XenServer Tools, but performance will be significantly hampered when the I/O drivers (PV drivers) are not installed. You must install XenServer Tools on Windows VMs to be able to perform the following operations:

- Cleanly shut down, reboot, or suspend a VM
- View VM performance data in XenCenter
- Migrate a running VM (using XenMotion or Storage XenMotion)
- Create quiesced snapshots or snapshots with memory (checkpoints), or revert to snapshots
- Adjust the number of vCPUs on a running Linux VM (Windows VMs require a reboot for this to take effect)

2.3.1. 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 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 on the **Install I/O drivers and Management Agent** link to install the I/O drivers from the XenServer 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 Section 7.3, “Updating XenServer Tools”.

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

Able to (Not able to) receive updates from Windows Update: specifies whether the VM 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 Tools ISO.

Install I/O drivers and Management Agent: this message is displayed when the VM does not have the I/O drivers or the Management Agent installed. Click the link to install XenServer Tools. For Linux VMs, clicking the status

link switches to the VM's console and loads the XenServer Tools ISO. You can then mount the ISO and manually run the installation, as described in Section 4.3.1, “Installing XenServer Tools”

Chapter 3. Supported Guests and Allocating Resources

This chapter describes how to allocate resources to your VMs, and the supported guest operating systems. It lists virtual memory and virtual disk size minimums, and describes the differences in virtual device support for the members of the XenServer product family.

3.1. Supported Guests, Virtual Memory, and Disk Size Limits

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

Important:

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

Warning:

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

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Windows 7 SP1, Windows 8.1, Windows 10 (32-bit)	1GB	4GB	24GB (40GB or more recommended)
Windows 7 SP1 (64-bit)	2GB	192GB	24GB (40GB or more recommended)
Windows 8.1 (64-bit)	2GB	512GB	24GB (40GB or more recommended)
Windows 10 (64-bit)	2GB	1.5TB	24GB (40GB or more recommended)
Windows Server 2008 SP2 (32-bit)	512MB	64GB	24GB (40GB or more recommended)
Windows Server 2008 SP2 (64-bit)	512MB	1TB	24GB (40GB or more recommended)
Windows Server 2008 R2 SP1	512MB	1.5TB	24GB (40GB or more recommended)
Windows Server 2012, Windows Server 2012 R2 (64-bit), Windows Server 2016, Windows Server Core 2016 (64-bit)	1GB	1.5TB	32GB (40GB or more recommended)
CentOS 5.x (32-bit)	512MB	16GB	8GB
CentOS 5.0 - 5.7 (64-bit)	512MB	16GB	8GB
CentOS 5.8 - 5.11 (64-bit)	512MB	128GB	8GB
CentOS 6.0, 6.1 (32-bit)	1GB	8GB	8GB

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
CentOS 6.0, 6.1 (64-bit)	512MB	32GB	8GB
CentOS 6.2 - 6.9 (32-bit)	512MB	16GB	8GB
CentOS 6.2 - 6.9 (64-bit)	1GB	128GB	8GB
CentOS 7.x (64-bit)	2GB	1.5TB	10GB
Red Hat Enterprise Linux 5.x (32-bit)	512MB	16GB	8GB
Red Hat Enterprise Linux 5.0 - 5.7 (64-bit)	512MB	16GB	8GB
Red Hat Enterprise Linux 5.8 - 5.11 (64-bit)	512MB	128GB	8GB
Red Hat Enterprise Linux 6.0, 6.1 (32-bit)	512MB	8GB	8GB
Red Hat Enterprise Linux 6.0, 6.1 (64-bit)	1GB	32GB	8GB
Red Hat Enterprise Linux 6.2 - 6.9 (32-bit)	512MB	16GB	8GB
Red Hat Enterprise Linux 6.2 - 6.9 (64-bit)	1GB	128GB	8GB
Red Hat Enterprise Linux 7.x (64-bit)	2GB	1.5TB	10GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (32-bit)	1GB	16GB	8GB
SUSE Linux Enterprise Server 11 SP3, 11 SP4 (64-bit)	1GB	128GB	8GB
SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64-bit)	1GB	128GB	8GB
SUSE Linux Enterprise Server 12 SP3 (64-bit)	512MB	1.5TB	8GB
SUSE Linux Enterprise Desktop 11 SP3 (64-bit)	1GB	128GB	8GB
SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64-bit)	1GB	128GB	8GB
SUSE Linux Enterprise Desktop 12 SP3 (64-bit)	512MB	1.5TB	8GB
Oracle Linux 5.0 - 5.7, 5.10, 5.11 (32-bit)	512MB	64GB	8GB
Oracle Linux 5.8, 5.9 (32-bit)	512MB	16GB	8GB
Oracle Linux 5.x (64-bit)	512MB	128GB	8GB
Oracle Linux 6.x (32-bit)	512MB	8GB	8GB

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Oracle Linux 6.0, 6.1 (64-bit)	1GB	32GB	8GB
Oracle Linux 6.2 - 6.9 (64-bit)	1GB	128GB	8GB
Oracle Linux 7.x (64-bit)	2GB	1.5TB	10GB
Scientific Linux 6.6 - 6.9 (32-bit)	512MB	16GB	8GB
Scientific Linux 6.6 - 6.9 (64-bit)	1GB	128GB	8GB
Scientific Linux 7.x (64-bit)	2GB	1.5TB	10GB
Debian Squeeze 6 (32/64-bit)	128MB	32GB	8GB
Debian Wheezy 7 (32-bit)	512MB	32GB	8GB
Debian Wheezy 7 (64-bit)	512MB	128GB	8GB
Debian Jessie 8 (32-bit)	128MB	64GB	8GB
Debian Jessie 8 (64-bit)	128MB	1.5TB	8GB
Debian Stretch 9 (32/64-bit)	256MB	1.5TB	10GB
Ubuntu 12.04 (32-bit)	128MB	32GB	8GB
Ubuntu 12.04 (64-bit)	128MB	128GB	8GB
Ubuntu 14.04 (32-bit)	512MB	64GB	8GB
Ubuntu 14.04 (64-bit)	512MB	192GB	8GB
Ubuntu 16.04 (32-bit)	512MB	64GB	10GB
Ubuntu 16.04 (64-bit)	512MB	1.5TB	10GB
CoreOS Stable (64-bit) *	1GB	512GB	8GB
NeoKylin Linux Advanced Server 6.5 (64-bit)	1GB	128GB	8GB
NeoKylin Linux Advanced Server 7.2 (64-bit)	1GB	1.5TB	10GB
NeoKylin Linux Security OS V5.0 (64-bit)	1GB	128GB	8GB
Asianux Server 4.2 (64-bit)	1GB	128GB	8GB
Asianux Server 4.4 (64-bit)	1GB	128GB	8GB
Asianux Server 4.5 (64-bit)	1GB	128GB	8GB
GreatTurbo Enterprise Server 12.2 (64-bit)	1GB	128GB	8GB
Linx Linux v6.0 (64-bit)	1GB	900GB	10GB

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Linx Linux v8.0 (64-bit)	1GB	900GB	10GB
Yinhe Kylin 4.0 (64-bit)	1GB	900GB	10GB

*Latest tested version is 1632.3.0.

Important:

RHEL, OL, and CentOS 5.x guest operating systems with the original kernel will fail to boot on XenServer 7.5. Before attempting to upgrade XenServer hosts to 7.5, customers should update the kernel to version 5.4 (2.6.18-164.el5xen) or later. Customers running these guests that have already upgraded their XenServer host to 7.5 should refer to the Citrix Knowledge Base article, CTX134845 for information on upgrading the kernel.

Note:

If you want to create VM of a newer minor update of a Red Hat Enterprise Linux (RHEL) release than is currently supported for installation by XenServer, install the VM 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.

Note:

Some 32-bit Windows operating systems can support more than 4 GB of RAM through the use of a special mode: physical address extension (PAE) mode. If you want to reconfigure a VM with greater than 4 GB of RAM, you must use the xe CLI, not XenCenter, as the CLI does not impose any upper bounds for `memory-static-max`.

3.2. Long-term Guest Support

XenServer includes a long-term guest support (LTS) policy for Linux VMs. The LTS policy enables all customers to consume minor version updates by either, installation from new guest media, or as an upgrade from an existing supported guest.

3.3. 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 7.5 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.

3.3.1. 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 Tools installs a special I/O driver that works in a similar way to Linux, except in a fully virtualized environment.

Chapter 4. Creating Windows VMs

Warning:

Running a Windows VM without installing the XenServer Tools is not a supported configuration. For more information, see Section 2.3, “XenServer Tools”.

Installing Windows VMs on the XenServer host requires hardware virtualization support (Intel VT or AMD-V).

4.1. 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 Tools (*I/O drivers* and the *Management Agent*)

4.2. 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, Windows Server 2003, and Windows Vista do not exist in XenServer 7.5. Customers who wish to create a Windows XP, Windows Server 2003, or Windows Vista VM should use the 'Legacy Windows' template and then run `xenlegacy.exe` from the XenServer Tools ISO to install XenServer 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).

Template Name	Description
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.
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 8 is no longer supported. Users who install Windows 8 are upgraded to Windows 8.1.

Warning:

Experimental guest operating systems have received limited testing, might not be present in future product releases, and must not be enabled on production systems. Citrix may not respond to support requests regarding experimental features.

4.2.1. 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. See Appendix C, *Creating ISO Images* for information on how to make an ISO image from a Windows install CD and make it available for use.

4.3. Using XenCenter to Create a VM

To create a Windows 7 (32-bit) VM:

Note:

The following procedure provides an example of creating Windows 7 (32-bit) VM. The default values may vary depending on the operating system that you choose.

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 Section 11.7, "Installing HVM VMs from Reseller Option Kit (BIOS-locked) Media". The option to set user-defined BIOS strings are not available for HVM VMs.

3. Enter a name and an optional description for the new VM.
4. Choose the source of the OS media to install on the new VM.

   Installing from a CD/DVD is the simplest option for getting started. 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 drop-down list.
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 wish 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 network interface card (NIC) and configurations, including an automatically-created unique MAC address for each NIC, or you may wish 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 Tools. See Section 4.3.1, "Installing XenServer Tools" for step-by-step instructions.

4.3.1. Installing XenServer Tools

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

XenServer Tools provide high performance I/O services without the overhead of traditional device emulation. XenServer Tools consists of I/O drivers (also known as Paravirtualized drivers or PV drivers) and the Management Agent. XenServer Tools must be installed on each Windows VM in order for the VM to have a fully-supported configuration. A VM will function without them, but performance will be significantly hampered. For more information about XenServer Tools, see Section 2.3, "XenServer Tools".

> **Note:**
>
> To install XenServer Tools on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.

To install XenServer Tools

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

   > **Note:**
   >
   > When you install XenServer Tools on your VM, you 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 Tools** to continue with the installation. This mounts the XenServer Tools ISO (guest-tools.iso) on the VM's CD/DVD drive.

   When prompted, select one of the following options to choose what happens with the XenServer Tools ISO:

   Click **Run Setup.exe** to begin XenServer 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. When you install XenServer 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 Tools using the following method:

   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 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 default settings. By default, the wizard displays the following settings:

   - Install I/O Drivers Now
   - Allow automatic management agent updates
   - Disallow automatic I/O drivers updates by the management agent
   - Send anonymous usage information to Citrix

   If you do not want to allow the automatic updating of the Management Agent, select **Disallow automatic management agent updates** from the drop-down list.

   If you would like to allow the Management Agent to update the I/O drivers automatically, select **Allow automatic I/O driver updates by the management agent**.

   Note:

   If you have chosen to receive I/O driver updates through the Windows Update mechanism, we recommend that you do not allow the Management Agent to update the I/O drivers automatically.

   If you do not wish to share anonymous usage information with Citrix, clear the **Send anonymous usage information to Citrix** check box. Note that the information transmitted to Citrix contains the UUID of the VM requesting the update. No other information relating to the VM is collected or transmitted to Citrix.

d. Click **Next** and then **Install** to begin the XenServer Tools installation process.

e. When prompted, perform any actions that are required to complete the installation process and click **Finish** to exit the wizard.

   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 Tools package to install the Management Agent, and to maintain supported configuration. For more information, see Section 2.3, “XenServer Tools” and Section 7.3, “Updating XenServer Tools”.

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 Tools ISO.

Customers who install the XenServer Tools or the Management Agent through RDP may not see the restart prompt as it only appears on the Windows console session. To ensure that you restart your VM (if 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.

4.3.1.1. Silent Installation

To silently install the XenServer 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 Tools are fully installed.

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

> **Note:**
>
> In order to install XenServer Tools on a Windows VM, the VM must be running the Microsoft .NET Framework Version 4.0 or later.
>
> **Warning:**
>
> Installing or upgrading the XenServer Tools can cause the friendly name and identifier of some network adapters to change. Any software which is configured to use a particular adapter may have to be reconfigured following XenServer Tools installation or upgrade.

4.4. 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*.

CITRIX

Chapter 5. Creating Linux VMs

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

When you want to create a new 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 chapter will focus on using the CLI.

> **Note:**
>
> Customers who wish to create VM of a newer minor update of a Red Hat Enterprise Linux (RHEL release, than is currently 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.

We recommend that you install the XenServer Tools immediately after installing the operating system. For more information, see Section 5.5, "Installing the Linux Guest Agent". For some operating systems, the XenServer Tools includes a kernel specific to XenServer, which replaces the kernel provided by the vendor. Other operating systems, such as RHEL 5.x require you to install a specific version of a vendor provided kernel.

The overview for creating a Linux VM is as following:

1. Create the VM for your target operating system using XenCenter or the CLI.
2. Install the operating system using vendor installation media.
3. Install the XenServer Tools (recommended).
4. Configure the correct time and time zone on the VM and VNC as you would in a normal non-virtual environment.

XenServer supports the installation of many Linux distributions as VMs. There are three installation mechanisms:

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 will be created as HVM guests, which may mean that some Linux VMs will use slower emulated devices rather than the higher performance I/O drivers.

For information regarding specific Linux distributions, see Section 5.6, "Additional Installation Notes for Linux Distributions".

PV Linux Distributions

The supported PV Linux distributions are:

Distribution	Vendor Install from CD	Vendor Install from network repository	Notes
Debian Squeeze 6 (32-/64-bit)	X	X	
Debian Wheezy 7 (32-/64-bit)	X	X	
Red Hat Enterprise Linux 5.x (32-/64-bit)	X	X	Supported provided you use the 5.4 or later kernel.
Red Hat Enterprise Linux 6.x (32-/64-bit)	X	X	
CentOS 5.x (32-/64-bit)	X	X	
CentOS 6.x (32-/64-bit)	X	X	
Oracle Linux 5.x (32-/64-bit)	X	X	
Oracle Linux 6.x (32-/64-bit)	X	X	
Scientific Linux 6.6 - 6.9 (32-/64-bit)	X	X	
SUSE Linux Enterprise Server 11 SP3, SP4 (32-/64-bit)	X	X	
SUSE Linux Enterprise Server 12, 12 SP1, 12 SP2 (64-bit)	X	X	
SUSE Linux Enterprise Desktop 11 SP3 (64-bit)	X	X	
SUSE Linux Enterprise Desktop 12, 12 SP1, 12 SP2 (64-bit)	X	X	
Ubuntu 12.04 (32-/64-bit)	X	X	
NeoKylin Linux Advanced Server 6.5 (64-bit)	X	X	
Asianux Server 4.2 (64-bit)	X	X	
Asianux Server 4.4 (64-bit)	X	X	
Asianux Server 4.5 (64-bit)	X	X	
GreatTurbo Enterprise Server 12.2 (64-bit)	X	X	
NeoKylin Linux Security OS V5.0 (64-bit)	X	X	

Distributions not present in the above list 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.

Note:

Running 32-bit PV Linux VMs on a host that has more than 128GB of memory is not supported.

Note:

XenServer hardware security features can reduce the overall performance of 32-bit PV VMs. If you are impacted by this issue, you can do one of the following things:

- Run a 64-bit version of the PV Linux VM
- Boot Xen with the `no-smep no-smap` option.

  We do not recommend this option as it can reduce the depth of security of the host

HVM Linux Distributions

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

The supported HVM Linux distributions are:

Distribution	Vendor Install from CD	Vendor Install from network repository	Notes
Debian Jessie 8 (32-/64-bit)	X	X	
Debian Stretch 9 (32-/64-bit)	X	X	
Red Hat Enterprise Linux 7.x (64-bit)	X	X	
CentOS 7.x (64-bit)	X	X	
Oracle Enterprise Linux 7.x (64-bit)	X	X	
Scientific Linux 7.x (64-bit)	X	X	
SUSE Linux Enterprise Server 12 SP3 (64-bit)	X	X	
SUSE Linux Enterprise Desktop 12 SP3 (64-bit)	X	X	
Ubuntu 14.04 (32-/64-bit)	X	X	
Ubuntu 16.04 (32-/64-bit)	X	X	
CoreOS Stable (64-bit)	X	X	
Linx Linux V6.0 (64-bit)	X	X	
Linx Linux V8.0 (64-bit)	X	X	
Yinhe Kylin 4.0 (64-bit)	X	X	

Distributions not present in the above list 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.

5.1. 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.

5.2. 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>
```

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

5.3. 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.

5.3.1. 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://*<server>*/*<path>*

- **FTP**
  ftp://*<server>*/*<path>*
- **NFS**
  nfs://*<server>*/*<path>*
- **NFS**
  nfs:*<server>*:/*<path>*

See your vendor installation instructions for information about how to prepare for a network-based installation, such as where to unpack the ISO.

> **Note:**
>
> Note that 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 will begin 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.

5.4. Advanced Operating System Boot Parameters

When creating a new VM, you can specify advanced operating system boot parameters using XenCenter or the xe CLI. Specifying advanced parameters may be particularly 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.

5.5. 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 Chapter 7, *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 Tools** option in XenCenter.
2. Mount the image onto the guest by running the command:

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

Note:

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

```
blkid -t LABEL="XenServer 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 12.04 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.

5.6. 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 Appendix B, *Linux VM Release Notes*.

Linux Distribution	Installation 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 Linux* 7.x (32-/64-bit)	The new template for these guests specifies 2GB RAM. This is a requirement for a successful install of v7.4. For v7.0 - v7.3, the template will specify 2GB RAM, but as with previous versions of XenServer, 1GB 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 2GB memory, set the boot parameter `crashkernel=no` to turn off the crashkernel. The VM does not reboot successfully unless 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 when creating a new VM 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.
Asianux Server 4.5	Installation must be performed with a graphical installer. In the **Installation Media** tab, add "VNC" in the Advanced OS boot parameters field.

Linux Distribution	Installation Notes

Linx Linux V6.0	• Supports upto 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 which 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/control-alt-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.
	OR
	• Ensure that the following two lines are enabled in `/etc/init/control-alt-delete.conf` file of the guest OS:
	`start on control-alt-delete`
	`exec /sbin/shutdown -r now "Control-Alt-Delete pressed"`
	• By default **Selinux** is enabled in the OS. So, the user cannot login 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.

*Refers to both Red Hat and Red Hat deriviatives.

5.6.1. Additional Debian Notes

5.6.1.1. 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 will create a partial or full mirror of a Debian repository. Either of these tools can be installed into a VM.

5.7. 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. For instructions for specific supported Linux distributions, see Section B.1, “Release Notes”.

5.7.1. 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.

5.7.2. 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 will assign 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.

5.7.3. 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 `eth`*<n>* interface, which is particularly 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.

Chapter 6. VM Migration with XenMotion and Storage XenMotion

This chapter discusses migrating running VMs using *XenMotion* and *Storage XenMotion* and how to move a VMs Virtual Disk Image (VDI) without any VM downtime.

6.1. XenMotion and Storage XenMotion

The following sections describe the compatibility requirements and limitations of XenMotion and Storage XenMotion.

6.1.1. 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 levelling, infrastructure resilience, and the upgrade of server software, without any VM downtime.

> **Note:**
>
> Storage can only be shared between hosts in the same pool. As a result VMs can only be migrated to hosts in the same pool.
>
> Virtual GPU and Intel GVT-g are not compatible with XenMotion, Storage XenMotion or VM Suspend. However, VMs using GPU Pass-through or vGPU can still be started any host that has the appropriate resources. For information about NVIDIA vGPU compatibility with these features, see the Configuring Citrix XenServer for Graphics Guide.

6.1.2. Storage XenMotion

> **Important:**
>
> Storage XenMotion must **not** be used in XenDesktop deployments.
>
> **Note:**
>
> Storage XenMotion cannot be used on VMs that have changed block tracking enabled. Disable changed block tracking before attempting Storage XenMotion.

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 as well as the historical performance metrics, such as CPU and network usage.

6.1.3. 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 Tools must be installed on each Windows VM that you wish to migrate. The version of XenServer 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 one snapshot cannot be migrated.
- VM with checkpoint cannot be migrated.
- 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.

6.1.4. 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.

6.2. 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** drop-down list, select a standalone server or a pool.
3. From the **Home Server** drop-down list, select a server to assign as the home server for the VM and click **Next**.
4. In the **Storage** tab, specify the storage repository where you would like to place the migrated VM's virtual disks, and then click **Next**.
   - The **Place all migrated virtual disks on the same SR** radio button is selected by default and displays the default shared SR on the destination pool.
   - Click **Place migrated virtual disks onto specified SRs** to specify an SR from the **Storage Repository** drop-down list. This option allows you to select different SR for each virtual disk on the migrated VM.
5. From the **Storage network** drop-down list, 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.

6.3. 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.

6.3.1. 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.
- If you perform live VDI migration on a VM that has a vGPU, vGPU XenMotion is used. The host must have enough vGPU space to make a copy of the vGPU instance on the host. If the pGPUs are fully utilised, VDI migration may not be possible.

6.3.2. 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.

CITRIX

Chapter 7. Updating VMs

This chapter discusses updating Windows VMs with updated operating systems, reinstalling XenServer 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 Tools on each VM.
- Suspend/Resume operation is not supported on Windows VMs until the XenServer Tools are upgraded.
- The use of certain anti-virus and firewall applications can crash Windows VMs, unless the XenServer Tools are upgraded.

7.1. Updating Windows Operating Systems

> **Warning:**
>
> Before updating Windows operating systems you must uninstall the XenServer Tools. If they are present during the attempt to update, the update will fail.

Windows installation disks typically provide an upgrade option if you boot them on a server which has an earlier version of Windows already installed.

You can update the operating system of Windows VMs in a similar way.

To uninstall the XenServer Tools

1. From the **Start** button, select **Control Panel**.
2. Select **Programs**, and then select **Programs and Features**.
3. Select all of the following items (the list depends on your operating system and the version of XenServer Tools installed on your VM):
   a. Citrix XenServer Windows Management Agent
   b. Citrix Tools for Virtual Machines
   c. Citrix XenServer Tools Installer
   d. Citrix XenServer Windows Guest Agent
   e. Citrix XenServer Xen Windows x64 PV Drivers
   f. Citrix XenServer Xen Windows x86 PV Drivers
   g. Citrix XenServer VSS Provider
4. Select **Uninstall**.

   This removes the XenServer Tools. When the operation completes a message is displayed. Click **OK** to close the message box.

Once the operating system update is complete, reinstall the XenServer Tools just as you would after installing a fresh Windows VM. See Section 7.2, “Reinstalling XenServer Tools” for details.

For information about applying updates to XenServer Tools, see Section 7.3, “Updating XenServer Tools”.

7.2. Reinstalling XenServer Tools

The XenServer Tools are available in XenCenter on the built-in `guest-tools.iso`. On the **VM** menu, select **Install XenServer Tools**; this attaches the CD image containing the XenServer Tools to the VM.

If AutoPlay is enabled for the VM's CD/DVD drive, installation will start automatically after a few moments. The process installs the I/O drivers and the Management Agent. Restart the VM when prompted to get your VM to an optimized state.

If AutoPlay is not enabled, the XenServer Tools installer displays the installation options. Click **Install XenServer Tools** to continue with the installation. This mounts the XenServer Tools ISO (guest-tools.iso) on the VM's CD/DVD drive. Click **Run setup.exe** to begin XenServer Tools installation and restart the VM when prompted to get your VM to an optimized state.

7.3. Updating XenServer 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.

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

7.3.1. 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 7.5 with Enterprise Edition , or have access to XenServer through XenApp/XenDesktop entitlement
- You have created a Windows VM using XenCenter issued with XenServer 7.5

  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 Tools ISO.

  Note:

  Customers can also receive I/O driver updates automatically through the automatic Management Agent update mechanism. You can configure this setting during XenServer Tools installation. See Section 4.3.1, “Installing XenServer Tools” for details.

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.

7.3.2. 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 Tools installation. See Section 4.3.1, "Installing XenServer 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 7.5, you can get the Management Agent updates automatically, provided:

- You are running XenServer 7.5 with Enterprise Edition or have access to XenServer through XenApp/ XenDesktop entitlement
- You have installed XenServer 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 7.5 Enterprise Edition, or those who have access to XenServer 7.5 through XenApp/XenDesktop entitlement.
- Updates to XenServer Tools can also be issued through the standard XenServer update (hotfix) mechanism. Such hotfixes contain updates to both I/O drivers and the Management Agent. There is no licensing restriction to update XenServer Tools issued as a hotfix.

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.

7.3.3. Managing Automatic Updates

Managing Automatic Updates using CLI

XenServer enables you to use command line to manage the automatic updating of the I/O drivers and the Management Agent. You can run `setup.exe` or `msiexec.exe` with the arguments listed in the following table to specify whether the I/O drivers and the Management Agent will be automatically updated. For information about installing XenServer Tools using `setup.exe` or `msiexec.exe`, see Section 4.3.1.1, "Silent Installation".

Argument	Values	Description
ALLOWAUTOUPDATE	YES|NO	Allow/disallow auto updating of the Management Agent
ALLOWDRIVERINSTALL	YES|NO	Allow/disallow the XenServer Tools installer to install I/O drivers

Argument	Values	Description
ALLOWDRIVERUPDATE	YES|NO	Allow/disallow the Management Agent to automatically update the I/O drivers
IDENTIFYAUTOUPDATE	YES|NO	Allow/disallow the auto update mechanism to send anonymous usage information to Citrix

For example:

```
setup.exe  /passive /forcerestart ALLOWAUTOUPDATE=YES ALLOWDRIVERINSTALL=NO \
 ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Or

```
msiexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES ALLOWDRIVERINSTALL=NO \
ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

Redirecting the Management Agent 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.

To redirect the Management Agent updates:

1. Download the updates.latest.tsv file from https://pvupdates.vmd.citrix.com/updates.latest.tsv .
2. Download the Management Agent MSI files referenced in the updates.latest.tsv file.
3. Upload the MSI files to an internal web server which can be accessed by your VMs.
4. Update the updates.latest.tsv file to point to the MSI files on the internal web server.
5. Upload the updates.latest.tsv file to the web server.

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

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

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

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

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

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 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 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>
```

Sending anonymous usage information to Citrix

During XenServer Tools installation, you can specify whether you would like to send anonymous usage information to Citrix. If you would like to update this setting after completing the XenServer Tools installation process, perform the following steps:

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

```
reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \
IDENTIFYAUTOUPDATE /d <YES/NO>
```

7.4. 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 (see Section 5.5, "Installing the Linux Guest Agent").

For `yum`-enabled distributions CentOS 5.x, RHEL 5.x and higher, `xe-guest-utilities` installs a `yum` configuration file to enable subsequent updates to be done using `yum` in the standard manner.

For Debian, `/etc/apt/sources.list` is populated to enable updates using apt by default.

When upgrading, Citrix recommends that you always re-run `Linux/install.sh`. This script automatically determines if your VM needs any updates and installs if necessary.

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

Customers who wish to upgrade *existing* Linux guests to versions which now operate in **HVM** mode (for example, 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.

Chapter 8. Bromium Secure Platform

8.1. Overview

XenServer supports Bromium Secure Platform on Windows VMs. This feature protects your enterprise from breaches while enabling users to perform any operations without compromising security.

> **Note:**
>
> The minimum supported Bromium version is 4.0.4.

Using this feature, you can:

- Protect your enterprise against known and unknown threats.
- Detect and monitor threat activity in real-time.
- Respond to a real-time visualization of the attack and view the remedial measures taken.

8.2. Compatibility Requirements and Caveats

XenServer supports Bromium on:

- **CPU**: Intel Core i3, i5, i7 v3 (Haswell) or later with Intel Virtualization Technology (Intel VT) and Extended Page Tables (EPT) enabled in the system BIOS.

  > **Note:**
  >
  > AMD CPUs are not supported.

- **VMs**: Windows 7 SP1 (32-bit and 64-bit), Windows 8.1 (64-bit), and Windows 10 (64-bit).
- **VM resources**: At least 2 vCPUs, 4GB RAM and 32GB disk space.

For VMs that are running Bromium, XenServer does not support and prevents the use of the following features:

- Any form of VM motion (for example: XenMotion, Storage XenMotion).
- Use of Dynamic Memory Control (DMC).

> **Note:**
>
> It is possible to use PCI pass-through and vGPU for a VM with enabled Nested Virtualization. However, such configurations are currently not supported by Citrix.
>
> **Important:**
>
> Bromium Secure Platform makes use of nested-virtualization support. This is supported by Citrix for use with Bromium Secure Platform only and not under normal circumstances and cases. For nested-virtualization, you must run XenServer 7.5 with Enterprise Edition or have access to XenServer through XenApp/XenDesktop entitlement.

8.3. Configuration

To prepare your XenServer system for use with Bromium Secure Platform, perform the following steps:

1. On each host, force the use of software VMCS shadowing by running the following command at the command prompt:

   ```
   /opt/xensource/libexec/xen-cmdline --set-xen force_software_vmcs_shadow
   ```

2. Reboot the host.

3. On each VM, enable nested-virtualized support using the following commands:
   a. `VM=`xe vm-list name-label='<vm name>' --minimal``
   b. `xe vm-param-set uuid=$VM platform:nested-virt=1`

      Note:

      For XenDesktop deployments, nested-virtualization should be done on the gold image.
4. Install Bromium Secure Platform in the VM by following its installation instructions.

CITRIX

Chapter 9. Container Management

XenServer includes two new features to enhance deployments of Docker™ Containers on XenServer

- Support for CoreOS Linux VMs and configuring Cloud Config Drives
- Container Management for CoreOS, Debian 8, Ubuntu 14.04 and RHEL/CentOS/OEL 7
- Preview of Container Management for Windows Server Containers on Windows Server 2016 Technology Preview

CoreOS is a minimalist Linux distribution which has become popular for hosting Docker™ applications. The CoreOS Cloud Config Drive allows the customization of various operating system configuration options. When Container Management is enabled on a VM, XenServer becomes aware of any Docker containers running in the VM.

> **Note:**
>
> For information on how to install CoreOS guests, configure Cloud-Config parameters, and manage Docker containers, 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 Section 9.2, “Container Management Supplemental Pack” for more information.

9.1. 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 userspace on the host operating system, sharing the kernel and base filesystem with other containers. For more information, refer to: https://www.docker.com/whatisdocker.

> **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.

9.2. 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.

9.3. 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 7.5.
2. Install the XenCenter shipped with XenServer 7.5.
3. Install the Container Management Supplemental pack available from the Citrix websiteCitrix 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 migrate a Container Managed VM between pools, Container Management stops working for the VM. This is because Container Management is implemented using a pool-specific key. To enable Container Management functionality again for the VM, update the Cloud Config Drive configuration in the VM preferences.

9.4. 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 Tools installed, and that the VM network is configured as described in Section 9.7, "Network Requirements and Security".
2. Install Docker, ncat and SSHD inside the VM.

   For Ubuntu 14.04: `apt-get install docker.io nmap openssh-server`

   For RHEL/CentOS/OEL 7.x: `yum install docker nmap openssh-server`
3. Enable autostart for docker.service:

   ```
   systemctl enable docker.service
   ```
4. Start docker.service

   ```
   systemctl start docker.service
   ```

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

5. Prepare the VM for container management; run the following command on the control domain (dom0) on one of the hosts in the pool:

   ```
   xscontainer-prepare-vm -v <vm-uuid> -u <username>
   ```

   Where *<vm-uuid>* is the VM to be prepared, and *<username>* is the username on the VM that the Container Management will use for management access.

The preparation script will guide you through the process and automatically enable container management for this VM.

> **Note:**
>
> If you migrate a Container Managed VM between pools, Container Management stops working for the VM. This is because Container Management is implemented using a pool-specific key. To enable Container Management functionality again for the VM, run the `xscontainer-prepare-vm` command again on the VM. Even afer running this command, the original XenServer pool might keep access to the VM.

9.5. Accessing Docker Container Console and Logs

For Linux VMs, XenCenter enables customers to access the container console and view logs in order 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 username and password.

> **Note:**
>
> Customers can automate the authentication process by configuring their public/private SSH keys. See the following section for details.

9.5.1. 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, 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`.

9.6. 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 Tools installed, and that the VM network is configured as described in Section 9.7, "Network Requirements and Security".
2. Install Windows Server Container support inside the VM as described in Microsoft Documentation. Note that 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 could 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. Note that 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.

9.7. 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). In order 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.

9.7.1. Network Partitioning and Firewalls

As with other VMs, container managed VMs should not be connected directly to XenServer's management network in order 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 and/or Docker TLS connections initiated by dom0.

9.7.2. 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 will attempt to reach Container Managed VMs through any of the IP addresses advertised by the XenServer Tools running inside the VM. After an initial connection, XenServer stores the public key of container managed VMs and validates that the key matches on any subsequent connection. 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.

9.7.3. 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, 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.

9.8. Notes

When using XenServer Container Management and Docker, be aware of the following behaviors:

- 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 may mean that XenServer may 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.

Chapter 10. vApps

A **vApp** is a logical group of one or more related Virtual Machines (VMs) which can be started up as a single entity. When a vApp is started, the VMs contained within the vApp will 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 particularly 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.*

10.1. 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.

Modifying vApps

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

10.2. Creating vApps

To group VMs together in a vApp follow the procedure:

Creating a vApp using XenCenter

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 usually 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**.

Value	Description
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 new vApp and close the wizard.

Note:

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

10.3. Deleting vApps

To delete a vApp follow the procedure:

Deleting vApps using XenCenter:

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.

10.4. 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 shut down will be attempted on all VMs; if this is not possible, then a forced shut down will be performed.

Note:

A soft shut down performs a graceful shut down of the VM, and all running processes are halted individually.

A forced shut down performs a hard shut down 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 shut down should only be used when a soft shut down is not possible.

10.5. Importing and Exporting vApps

vApps can be imported and exported as OVF/OVA packages. See Chapter 13, *Importing and Exporting VMs* for more details.

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 Section 13.5.1, “Exporting VMs as OVF/OVA”.

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 Section 13.4.1, “Importing VMs from OVF/OVA”.

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

Chapter 11. Advanced Notes for Virtual Machines

This chapter provides some advanced notes for Virtual Machines.

11.1. 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.

11.1.1. Persist (XenDesktop - Private Desktop Mode)

This is the default behaviour 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
```

11.1.2. 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

11.2. 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
```

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

The ISO should be attached to an appropriate Windows template.

11.3. Windows Volume Shadow Copy Service (VSS) provider

The Windows tools also include a VSS provider for XenServer that is used to quiesce the guest filesystem in preparation for a VM snapshot. The VSS provider is installed as part of the PV driver installation, but is not enabled by default.

To enable the Windows XenServer VSS provider

1. Install the Windows PV drivers.
2. Navigate to the directory where the drivers are installed (by default `c:\Program Files\Citrix\XenTools`, or the value of *`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\Install_dir`* in the Windows Registry).
3. Double-click the `install-XenProvider.cmd` command to activate the VSS provider.

   Note:

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

11.4. 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 Tools and follow the procedure below to enable it in each VM that you want to connect using Remote Desktop:

To Enable Remote Desktop on a Windows VM

1. Open **System** by clicking the **Start** button, right-click on **Computer**, and then select **Properties**
2. Click **Remote settings**. If you're prompted for an administrator password, type the password you created during the VM setup.
3. In the **Remote Desktop** area, click the check box labeled **Allow connections from computers running any version of Remote Desktop** (Windows 7).
4. 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 usernames. 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**.

11.5. 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 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.

11.6. Time Handling in Linux VMs

The time handling behavior of Linux VMs in XenServer depends on whether the VM is a PV guest or an HVM guest.

In addition to the behavior defined by XenServer, operating system settings and behaviors can affect the time handling behavior of your Linux VMs. 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 Section B.1, “Release Notes” for specific distribution instructions).

11.6.1. Time Handling in PV Linux VMs

There are two *wallclock* behaviors for paravirtualized Linux distributions – *dependent* and *independent*.

Dependent wallclock: 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 wallclock: 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 wallclock behavior of the VM.

The following table lists wallclock behavior for PV Linux VMs:

Guest OS	Default wallclock 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 6.x (32-/64-bit)	Independent	
SLES 11 SP3, SP4 (32-/64-bit)	Independent	Yes (No-op)
SLES 12 SP1, SP2 (64-bit)	Independent	Yes (No-op)
SLED 11 SP3, SP4 (64-bit)	Independent	Yes (No-op)
SLED 12 SP1, SP2 (64-bit)	Independent	Yes (No-op)
Debian 6 (32-/64-bit)	Independent	
Debian 7 (32-/64-bit)	Independent	
Ubuntu 12.04 (32-/64-bit)	Independent	
NeoKylin Linux Advanced Server 6.5 (64-bit)	Independent	
Asianux Server 4.2 (64-bit)	Dependent	Yes
Asianux Server 4.4 (64-bit)	Dependent	Yes
Asianux Server 4.5 (64-bit)	Dependent	Yes
GreatTurbo Enterprise Server 12.2 (64-bit)	Dependent	Yes
NeoKylin Linux Security OS V5.0 (64-bit)	Dependent	Yes

For PV Linux VMs where the `independent_wallclock` setting is available, you can use this setting to define whether the VM has dependent or independent wallclock behavior.

> **Important:**
>
> Citrix recommends using the `independent_wallclock` setting to enable independent wallclock 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.

11.6.2. 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.

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

There are two types of HVM VMs: BIOS-generic and BIOS-customized. 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. Alternatively, advanced users can set user-defined values to the BIOS strings.

11.7.1. BIOS-generic

The VM has generic XenServer BIOS strings.

> **Note:**
>
> 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.

11.7.2. BIOS-customized

HVM VMs support customization of BIOS in two ways, namely: Copy-Host BIOS strings and User-Defined BIOS strings.

11.7.2.1. Copy-Host BIOS Strings

The VM has a copy of the BIOS strings of a particular server in the pool. To install the BIOS-locked media that came with your host, follow the procedures given below.

Using XenCenter

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

Using the CLI

1. Run the `vm-install copy-bios-strings-from` command 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.
```

Note:

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.

11.7.2.2. User-Defined BIOS Strings

The user has option to set custom values in selected BIOS strings using CLI/API. To install the media in HVM VM with customized BIOS, follow the procedure given below.

Using the CLI

1. Run the `vm-install` command (without `copy-bios-strings-from`):

```
xe vm-install template=<template name> sr-name-label=<name of sr> \
  new-name-label=<name for new VM>
```

This returns the UUID of the newly created VM.

For example:

```
xe vm-install template="win7sp1" sr-name-label=Local\ storage  \
  new-name-label=newcentos
7cd98710-bf56-2045-48b7-e4ae219799db
```

2. To set user-defined BIOS strings, run the following command before starting the VM for the first time:

```
xe vm-param-set uuid=<VM_UUID> bios-strings:bios-vendor=<VALUE> \
bios-strings:bios-version=<VALUE> bios-strings:system-manufacturer=<VALUE> \
bios-strings:system-product-name=<VALUE> bios-strings:system-version=<VALUE> \
bios-strings:system-serial-number=<VALUE> bios-strings:enclosure-asset-
tag=<VALUE>
```

For example:

```
xe vm-param-set uuid=<7cd98710-bf56-2045-48b7-e4ae219799db> \
bios-strings:bios-vendor=<"vendor name"> \
bios-strings:bios-version=<2.4> \
bios-strings:system-manufacturer=<"manufacturer name"> \
bios-strings:system-product-name=<guest1> \
bios-strings:system-version=<1.0> \
bios-strings:system-serial-number=<"serial number"> \
bios-strings:enclosure-asset-tag=<abk58hr>
```

Note:

- Once the user-defined BIOS strings are set in a single CLI/API call, they cannot be modified.
- You can decide on the number of parameters you wish to provide to set the user-defined BIOS strings.

Warning:

It is your responsibility to:

- Comply with any EULAs and standards for the values being set in VM's BIOS.
- Ensure that the values you provide for the parameters are working parameters. Providing incorrect parameters can lead to boot/media installation failure.

11.8. Preparing for Cloning a Windows VM Using Sysprep

The only supported way to clone a windows VM is by using the Windows utility **sysprep** to prepare the VM.

sysprep 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:

Cloning Windows VMs

1. Create, install, and configure the Windows VM as desired.
2. Apply all relevant Service Packs and updates.
3. Install the XenServer Tools.
4. Install any applications and perform any other configuration.
5. Run **sysprep**. This 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)

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

XenServer allows you to assign a physical GPU in the 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 www.citrix.com/ready/hcl 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 wish 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 xe CLI:

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

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

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

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

To ensure that the GPU group has been attached, run the **xe vgpu-list** command.

4. Start the VM by using the **xe vm-start** command.
5. Once the VM starts, install the graphics card drivers on the VM.

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

   Note:

   If you try to start a VM with GPU Pass-Through on the 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.

Chapter 12. Importing the Demo Linux Virtual Appliance

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 Tools are pre installed in the Demo Linux Virtual Appliance and it also includes pre-configured networking connectivity as well as 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.

12.1. 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 web page 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 on 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 Web Page, 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.

Chapter 13. Importing and Exporting VMs

XenServer allows you to import VMs from and export them to a number of 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 Section 13.2, “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 Section 13.3, “The Transfer VM”.

You can also use the xe CLI to import VMs from and export them to XenServer XVA format.

13.1. 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 VM(s).
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 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 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

13.1.1. 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 VM(s). 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:**
>
> In order 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:

Attribute	Description
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 additional disk space on the XenServer host in order 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.

13.1.1.1. 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.

13.1.2. 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.

13.1.3. 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 filename extension is .xva.

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

13.1.4. 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 extension is ova.xml.

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

13.2. 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 the XenServer host.

XenCenter includes an advanced hypervisor interoperability feature — Operating System Fixup — which aims to ensure a basic level of interoperability for VMs that you import into XenServer. 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 the XenServer environment. This feature is not designed to perform conversions from one platform to another.

> **Note:**
>
> This feature requires an ISO storage repository with 40 MB of free space and 256 MB of virtual memory.

Operating System Fixup is supplied as an automatically booting ISO image that is attached to the DVD drive of the imported VM. It performs the necessary repair operations when the VM is first started, and then shuts down the VM. The next time the new VM is started, the boot device is reset, and the VM starts normally.

To use Operating System Fixup on imported disk images or OVF/OVA packages, 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, additional 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.

13.3. 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 the 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. Backup 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.

13.4. Importing VMs

When you import a VM, you effectively create a new 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.

13.4.1. Importing VMs from OVF/OVA

> **Note:**
>
> In order 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 new VM in XenCenter: nominating a host, and then configuring storage and networking for the new VM. When importing OVF and OVA files, additional 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 Section 13.2, “Operating System Fixup”.
- It is necessary to configure networking for the Transfer VM used to perform the import process. For more information, see Section 13.3, “The 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** drop-down list.

   To assign each VM a home XenServer host, select a server from the list in the **Home Server**. If you wish 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 the 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 Section 13.2, “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 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
  ```

13.4.2. 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** drop-down list.

   To assign each VM a home XenServer host, select a server from the list in the **Home Server**. If you wish 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 Section 13.2, "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 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
  ```

13.4.3. 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 extension) or XVA Version 1 format (with the ova.xml file 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 wish 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.

13.5. 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.

13.5.1. 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 wish 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** drop-down list. 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 wish to add. Once you have added the file, you can view the document by selecting it from the **EULA files** list and then clicking **View**.

   EULAs can provide the legal terms and conditions for using the appliance and/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 a 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 Section 13.1.1, “Open Virtualization Format (OVF and OVA)”.

   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 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 on the **Logs** tab, find the export in the list of events, and click the **Cancel** button.

13.5.1.1. 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 the 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 wish 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** drop-down list. Click **Next** to continue.
4. From the list of available VMs, select the VM that you want to export, and then click **Next** to continue.

5. Review the export settings.

   To have the wizard verify the exported package, select the **Verify export on completion** check box. Click **Finish** to begin the export process and close the wizard.

   Note:

   Exporting a VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection.

The export progress is displayed in the status bar at the bottom of the XenCenter window and on the **Logs** tab. To cancel an export in progress, click on 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 filename. 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.

CITRIX

Appendix A. Windows VM Release Notes

A.1. 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.

A.1.1. General Windows Issues

- When installing Windows VMs, start off with no more than three virtual disks. Once the VM and XenServer 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 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 hotplugged 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 backend 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 backend 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.

A.1.2. 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.

A.1.3. Windows 8

We no longer support Windows 8 guests. If you install a Windows 8 VM, it is upgraded to Windows 8.1.

A.1.4. 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.

Appendix B. Linux VM Release Notes

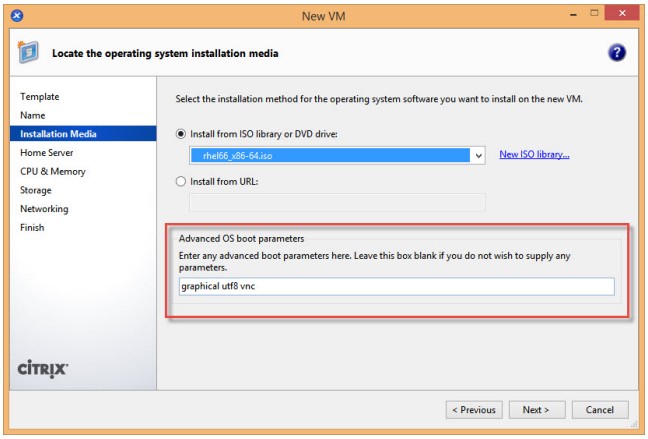
B.1. Release Notes

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

B.1.1. 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 will use 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 will displayed in the top right corner of the XenCenter window.

B.1.2. 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 will fail to boot on XenServer 7.5. Before attempting to upgrade the XenServer host to version 7.5, customers should update the kernel to version 5.4 (2.6.18-164.el5xen) or later. Customers running these guests who have already upgraded their host to XenServer 7.5, should refer to CTX134845 for information on upgrading the kernel.
- 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 wish 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 to 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 64GiB RAM or higher configured. Applying the Red Hat RHEL 5.4 kernel onwards resolves this issue. [EXT-30]

- In RHEL 5.0 to 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. Consequently, XenServer no longer includes a RHEL 5 specific kernel.

B.1.2.1. Preparing a RHEL 5 guest for cloning

To prepare a RHEL 5.x guest for cloning (see Section 5.7.3, "MAC address"), 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).

B.1.3. 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.

B.1.4. Red Hat Enterprise Linux 7

After performing a migration or suspend operation, RHEL 7.x guests may freeze during resume. For more information, see Red Hat Bugzilla 1141249.

B.1.5. CentOS 5

Please refer to Section B.1.2, "Red Hat Enterprise Linux 5" for the list of CentOS 5.x release notes.

B.1.6. CentOS 6

Please refer to Section B.1.3, "Red Hat Enterprise Linux 6" for the list of CentOS 6.x release notes.

B.1.7. CentOS 7

Please refer to Section B.1.4, "Red Hat Enterprise Linux 7" for the list of CentOS 7.x release notes.

B.1.8. Oracle Linux 5

Please refer to Section B.1.2, "Red Hat Enterprise Linux 5" for the list of Oracle Linux 5.x release notes.

B.1.9. Oracle Linux 6

Oracle Linux 6.x guests that 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.

For OEL 6.9 VMs with more that 2GB memory, set the boot parameter `crashkernel=no` to turn off the crashkernel. The VM does not reboot successfully unless this parameter is set. If you use an earlier version of OEL 6.x, set this boot parameter before updating to OEL 6.9. For more information, see Section 5.6, "Additional Installation Notes for Linux Distributions"

Please refer to Section B.1.3, "Red Hat Enterprise Linux 6" for a list of OEL 6.x release notes.

B.1.10. Oracle Linux 7

Please refer to Section B.1.4, "Red Hat Enterprise Linux 7" for the list of Oracle Linux 7.x release notes.

B.1.11. Scientific Linux 6

Please refer to Section B.1.3, "Red Hat Enterprise Linux 6" for the list of Scientific Linux 6.x release notes.

B.1.12. Scientific Linux 7

Please refer to Section B.1.4, "Red Hat Enterprise Linux 7" for the list of Scientific Linux 7.x release notes.

B.1.13. SUSE Linux Enterprise 12

SUSE Linux Enterprise 12 VMs are supported in the following modes by default:

PV mode:

- SUSE Linux Enterprise Desktop 12, 12 SP1, and 12 SP2
- SUSE Linux Enterprise Server 12, 12 SP1, and 12 SP2

HVM mode:

- SUSE Linux Enterprise Desktop 12 SP3
- SUSE Linux Enterprise Server 12 SP3

B.1.14. 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 Section 5.7.3, "MAC address"):

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.

B.1.15. 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.

B.1.16. 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 in order to fix this issue. For more information, see Ubuntu Launchpad 1350373.

Appendix C. 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 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.

On a Windows computer

- 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.

CITRIX

Appendix D. Enabling VNC for Linux VMs

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 X is based on Red Hat Enterprise Linux X.

D.1. 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 Section 5.5, "Installing 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 filename 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**.

D.2. 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 Section 5.5, “Installing 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 a number of subsequent procedures in this section.

Note:

For information on enabling VNC for RHEL, CentOS, or OEL 6.x VMs, see Section D.2.5, “Enabling VNC for RHEL, CentOS, or OEL 6 VMs”.

D.2.1. Determining the Location of your VNC Configuration File

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

D.2.2. 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 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:

   - `0=Standard`

     Modify it to read:

     `0=VNC`

   - If you are using Red Hat Linux 5.x or greater, add the above line just below the `[servers]` section and before the `[server-VNC]` section.

4. Save and close the file.

Restart GDM for your change in configuration to take effect, by running the command **/usr/sbin/gdm-restart**.

Note:

Red Hat Linux uses runlevel 5 for graphical startup. If your installation 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). See Section D.4, "Checking Runlevels" for further details.

D.2.3. Firewall Settings

The firewall configuration by default does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, 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 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 additional services to the outside world and reduce the overall security of your VM.

D.2.4. 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 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 GDM configuration file with your preferred text editor. See Section D.2.1, "Determining the Location of your VNC Configuration File" for information about determining the location of this file.
2. Find the `[server-VNC]` section you added above.
3. Edit the command line to read, for example:

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

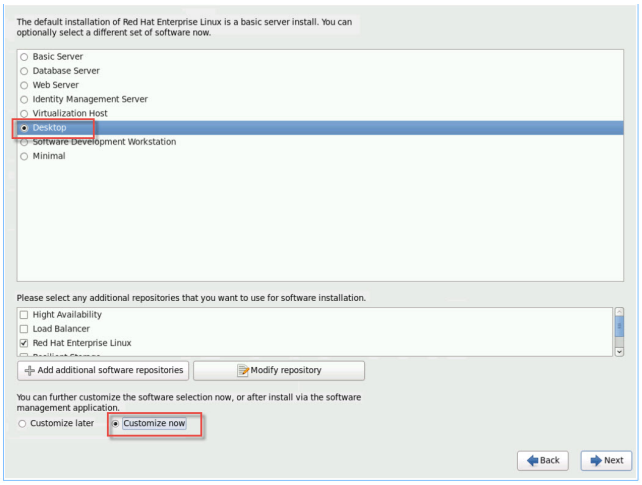
   where the value of the *`geometry`* parameter can be any valid screen width and height.
4. Save and close the file.

D.2.5. Enabling VNC for RHEL, CentOS, or OEL 6 VMs

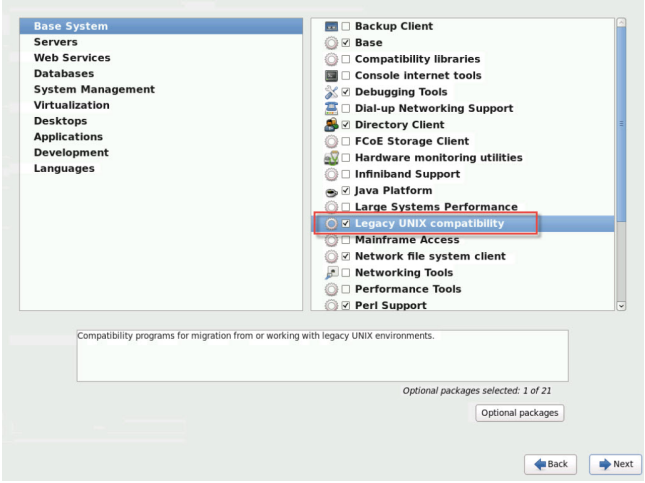
If you are using Red Hat Linux version 6.x, the GDM configuration file is `/etc/gdm/custom.conf`. This is a split configuration file that contains only user-specified values that override the default configuration. This type of file is used by default in newer versions of GDM, as included in these versions of Red Hat Linux.

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

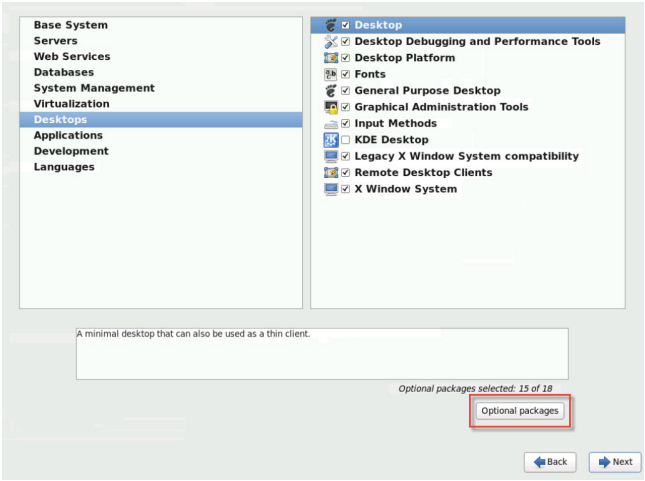
To do this, on the RHEL installation screen, select **Desktop**, **Customize now** and then click **Next**:



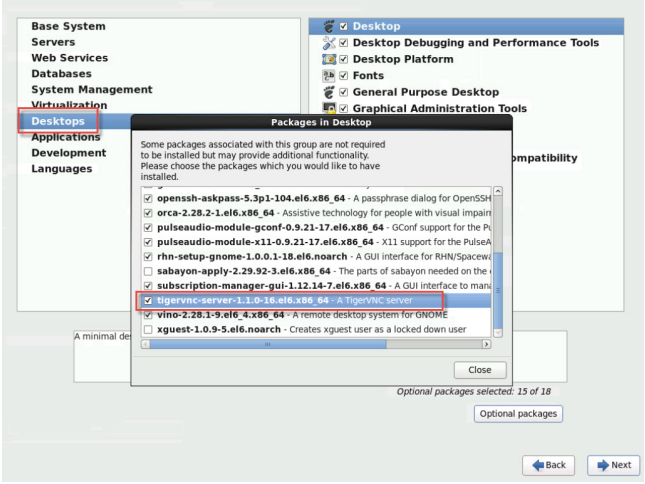
This displays the Base System screen, ensure that **Legacy UNIX compatibility** is selected:



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. Note that 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). See Section D.4, "Checking Runlevels" for further details.

D.3. 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 Section 5.5, "Installing 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.

D.3.1. 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
```

D.3.2. 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**.

D.3.3. 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. Refer to Section D.4, “Checking Runlevels” for details.

D.3.4. Firewall Settings

By default the firewall configuration does not allow VNC traffic to go through. If you have a firewall between the VM and XenCenter, 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`, etc. 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 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.

D.3.5. 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
   ```

D.4. 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.

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.

Appendix E. Troubleshooting VM Problems

Citrix provides two forms of support: free, self-help support on the Citrix Support website and paid-for Support Services, which you can purchase from the Support Site. With Citrix Technical Support, you can open a Support Case online or contact the support center by phone if you experience technical difficulties.

The Citrix Support site hosts a number of 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 chapter 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 chapter 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.

E.1. 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.

E.1.1. Controlling Linux VM Crashdump Behavior

For Linux VMs, the crashdump behavior can be controlled through the `actions-after-crash` parameter. The following are the possible values:

Value	Description
preserve	leave the VM in a paused state (for analysis)
restart	no core dump, 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 dumpcore on dom0. For example, run:

```
xl dump-core <domid> <filename>
```

E.1.2. Controlling Windows VM Crashdump Behaviour

For 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**.

E.2. Troubleshooting Boot Problems on Linux VMs

There 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. Run the command

```
xe vm-list
```

to ensure that the VM in question is shut down (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.