CİTRIX

Citrix XenServer ® 6.1.0 Virtual Machine User's Guide

CiTRIX

Citrix XenServer ® 6.1.0 Virtual Machine User's Guide

Copyright © 2012 Citrix Systems. Inc. All Rights Reserved.
Version: 6.1.0

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

CiTRIX

Contents

CÍTRIX®

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
- 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:

- *Release Notes* cover 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 a 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 XenServer deployment, 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 Knowledge Center.

CITRIX

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.

XenServer supports guests with any combination of IPV4 or IPv6 configured addresses

2.1. Creating VMs

2.1.1. 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. Linux templates create ParaVirtualized (PV) guests, whereas Windows templates create Hardware Virtual Machine (HVM) guests. 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 VM.

• Installing an operating system from a CD or an ISO image onto the appropriate provided template.

You install operating systems onto VMs from either a vendor installation CD, or from an ISO repository, or can choose use a complete pre-configured OS instance.

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.

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

2.2.1. 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 is transferred, instantiated, and started as a VM on the XenServer host.

For existing physical instances of Windows servers, use *XenConvert*. XenConvert runs on the physical Windows machine and converts it live into a VHD-format disk image or an XVA template suitable for importing into a XenServer host. The physical host does not need to be restarted during this process, and device drivers automatically modify to run in a virtual environment. For more information, please refer to the XenConvert documentation for installation and usage guidelines.

CITRIX

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 9.8, "Preparing for Cloning a Windows VM Using VSS" 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 and is only supported for file-backed VMs. 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.

2.2.3. 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 a XenServer host that is in another resource pool.

For details and procedures on importing and exporting VMs, see Chapter 11, *Importing and Exporting VMs*.

2.3. XenServer Tools

XenServer Tools must be installed for each Virtual Machine (Windows and Linux) 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). A Windows VM will function without them, but performance will be significantly hampered unless the tools are installed.

Without the tools being installed, you cannot:

• Cleanly shut down a VM

• Cleanly reboot a VM

• Suspend a VM

• Migrate a running VM (XenMotion)

• Use the checkpoint and roll back feature

CİTRIX

- Dynamically adjust the number of vCPUs assigned to a running Linux VM- Windows VMs require a reboot for this to take effect

For further information about XenServer Tools see Section 9.2, "XenServer Tools"

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

CITRIX

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.

> **Note:**
>
> 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, Windows 7 SP1 (32-bit)	1GB	4GB	24GB (40GB or more recommended)
Windows 7, Windows 7 SP1 (64-bit)	2GB	128GB	24GB (40GB or more recommended)
Windows Server 2008 R2, Windows Server 2008 R2 SP1 (64-bit)	512MB	128GB	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	128GB	24GB (40GB or more recommended)
Windows Server 2003 SP2 (32-bit)	256MB	64GB	8GB (16GB or more recommended)
Windows Server 2003 SP2 (64-bit)	256MB	128GB	8GB (16GB or more recommended)
Windows Vista SP2 (32-bit)	1GB	4GB	24GB (40GB or more recommended)
Windows XP SP3 (32-bit)	256MB	4GB	8GB, (16GB or more recommended)
CentOS 4.5, 4.6, 4.7, 4.8 (32-bit)	256MB	16GB	8GB
CentOS 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-/64-bit)	512MB	16GB	8GB

CiTRIX

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
CentOS 6.0, 6.1 (32-bit)	512MB	8GB	8GB
CentOS 6.0, 6.1 (64-bit)	512MB	32GB	8GB
CentOS 6.2 (32-bit)	512MB	16GB	8GB
CentOS 6.2 (64-bit)	512MB	128GB	8GB
Red Hat Enterprise Linux 4.5, 4.6, 4.7, 4.8 (32-bit)	256MB	16GB	8GB
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-/64-bit)	512MB	16GB	8GB
Red Hat Enterprise Linux 6.0, 6.1 (32-bit)	512MB	8GB	8GB
Red Hat Enterprise Linux 6.0, 6.1 (64-bit)	512MB	32GB	8GB
Red Hat Enterprise Linux 6.2 (32-bit)	512MB	16GB	8GB
Red Hat Enterprise Linux 6.2 (64-bit)	512MB	128GB	8GB
SUSE Linux Enterprise Server 10 SP1, SLES 10 SP2, SLES 10 SP3, SLES 10 SP4 (32-bit)	512MB	16GB	8GB
SUSE Linux Enterprise Server 10 SP1, SLES 10 SP2, SLES 10 SP3, SLES 10 SP4 (64-bit)	512MB	128GB	8GB
SUSE Linux Enterprise Server 11, SLES 11 SP1 (32-bit)	512MB	16GB	8GB
SUSE Linux Enterprise Server 11 SP1, SLES 11 SP1 (64-bit)	512MB	128GB	8GB
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-bit)	512MB	64GB	8GB
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (64-bit)	512MB	128GB	8GB
Oracle Enterprise Linux 6.0, 6.1 (32-bit)	512MB	8GB	8GB
Oracle Enterprise Linux 6.0, 6.1 (64-bit)	512MB	32GB	8GB
Oracle Enterprise Linux 6.2 (32-bit)	512MB	16GB	8GB
Oracle Enterprise Linux 6.2 (64-bit)	512MB	128GB	8GB
Debian Squeeze 6.0 (32-/64-bit)	128MB	32GB	8GB
Ubuntu 10.04 (32-bit)	128MB	512MB	8GB
Ubuntu 10.04 (64-bit)	128MB	32GB	8GB
Ubuntu 12.04 (32-bit)	128MB	32GB	8GB

CITRIX

Operating System	Minimum RAM	Maximum RAM	Minimum Disk Space
Ubuntu 12.04 (64-bit)	128MB	128GB	8GB

Important:

RHEL, OEL, and CentOS 5.0 guest operating systems with the original kernel will fail to boot on XenServer 6.1.0. Before attempting to upgrade a XenServer host to version 6.1.0, 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 version 6.1.0, should refer to the Citrix Knowledge Base article CTX134845 for information on upgrading the kernel.

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`.

For more information on how to set the memory static max, please refer to the Dynamic Memory Control chapter, in the *XenServer Administrator's Guide*.

3.2. Experimental Guests

The following table lists the experimental guest operating systems in XenServer 6.1.0.

Operating System
Windows 8 (32-bit)
Windows 8 (64-bit)
Windows Server 2012 (64-bit)
Ubuntu Maverick Meerkat 10.10 (32-bit)
Ubuntu Maverick Meerkat 10.10 (64-bit)
Solaris 10

Warning:

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

3.3. Deprecated Guests

The following table lists the deprecated guest operating systems in XenServer 6.1.0.

Operating System
Debian Lenny 5.0 (32-bit)
SUSE Linux Enterprise Server 9 SP4 (32-bit)

Operating System
Windows Server 2008 (base release) (32-bit)
Windows Server 2008 (base release) (64-bit)
Windows Server 2003 (base release), Windows Server 2003 SP1 (32-bit)
Windows Server 2003 (base release), Windows Server 2003 SP1 (64-bit)
Windows Vista (base release), Windows Vista SP1 (32-bit)

> **Note:**
>
> There will be no option to engage Citrix's product development resources, and technical workarounds may be limited or not possible for customers on unsupported guest operating systems. If the support incident requires escalation to development for further guidance, requires a hotfix, or requires a security update, customers will be asked to upgrade to a supported service pack.

3.4. XenServer Product Family Virtual Device Support

The current version of the XenServer product family has the following general limitations on virtual devices for VMs. Note that specific guest operating systems may have lower limits for certain features. The individual guest installation section notes the limitations.

Virtual device	Linux VMs	Windows VMs
Number of virtual CPUs	32[*]	16
Number of virtual disks	7 (including virtual CD-ROM)	7 (including virtual CD-ROM)
Number of virtual CD-ROM drives	1	1
Number of virtual NICs	7[†]	7

[*]A maximum of 16 vCPUs are supported by XenCenter.

[†]except for SLES 10 SP1 and RHEL 4.x, which support 3. RHEL 5.0/5.1/5.2 support 3, but can support 7 when the kernel is patched with the XenServer Tools. The same applies for Oracle and CentOS 5.0/5.1/5.2.

3.4.1. 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 PV driver that works in a similar way to Linux, except in a fully virtualized environment.

CITRIX

Chapter 4. Creating Windows VMs

Warning:

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

Installing Windows VMs on a 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 *paravirtualized device drivers* known as the XenServer Tools

4.2. Available Windows 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.

The available Windows templates are listed below:

Template Name	Description
Citrix XenApp on Windows Server 2003 (32-bit)	Used to install Windows Server 2003 SP2 (32-bit). The Server, Enterprise, Data Centre, and SBS editions are supported. This template is specially tuned to optimize XenApp performance.
Citrix XenApp on Windows Server 2003 (64-bit)	Used to install Windows Server 2003 SP2 (64-bit). The Server, Enterprise, Data Centre, and SBS editions are supported. This template is specially tuned to optimize XenApp performance.
Citrix XenApp on Windows Server 2008 (32-bit)	Used to install Windows Server 2008 SP2 (32-bit). All editions are supported. This template is specially tuned to optimize XenApp performance.
Citrix XenApp on Windows Server 2008 (64-bit)	Used to install Windows Server 2008 SP2 (64-bit). All editions are supported. This template is specially tuned to optimize XenApp performance.
Citrix XenApp on Windows Server 2008 R2 (64-bit)	Used to install Windows Server 2008 R2 and Windows Server 2008 R2 SP1 (64-bit). All editions are supported. This template is specially tuned to optimize XenApp performance.
Windows 7 (32-bit)	Used to install Windows 7 and Windows 7 SP1 (32-bit).
Windows 7 (64-bit)	Used to install Windows 7 and Windows 7 SP1 (64-bit).
Windows Server 2003 (32-bit)	Used to install Windows Server 2003 SP2 (32-bit). The Server, Enterprise, Data Centre, and SBS editions are supported.
Windows Server 2003 (64-bit)	Used to install Windows Server 2003 SP2 (64-bit). The Server, Enterprise, Data Centre, and SBS editions are supported.

CÏTRĮX®

Template Name	Description
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 Vista (32-bit)	Used to install Windows Vista SP2 (32-bit). The Enterprise edition is supported.
Windows XP SP3 (32-bit)	Used to install Windows XP SP3 (32-bit). Earlier service packs are not supported.

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

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 9.7, "Installing a VM from Reseller Option Kit (BIOS-locked) Media"

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

6. For a Windows 7 VM, the default is 1 virtual CPU and 2048 MB of RAM. You may also choose to modify the defaults. Select **Next** to continue.

7. 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**.

8. 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**.

9. Review settings, and then click **Finish** 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.

10. Follow the OS installation screens and make your selections.

11. Once the OS installation completes and the VM reboots, install the XenServer Tools.

   XenServer Tools provide high-speed I/O for enhanced disk and network performance. XenServer Tools must be installed on each VM in order for the VM to have a fully-supported configuration. A VM will function without them, but performance will be significantly hampered. XenServer Tools also enable certain functions and features, including cleanly shutting down, rebooting, suspending and live migrating VMs.

   Warning:

   You must install XenServer Tools for each VM. Running VMs without XenServer Tools is *not* supported. For more information on XenServer Tools see Section 9.2, "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. If a VM is running Windows 2003, you need to install the Windows Imaging Component (see your vendor documentation for details) before installing XenServer Tools.

   To install XenServer Tools:

   a. On the **Resources** pane, select the XenServer host and then the **Search** tab.

The **XenServer Tools not installed** blue status text appears next to the new VM.

b. Click the text to open the XenServer Tools setup wizard on the VM console.

c. Click the **Install XenServer Tools** button, and then **Run Xensetup.exe**.

d. When prompted, click **Yes** to allow the program to make changes to the computer.

e. Accept the License Agreement, and click **Next** to continue.

f. Choose a destination folder and click **Install**.

g. Select **Reboot now**, and then **Finish** to complete the installation.

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*.

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:**
>
> The templates for **Red Hat Enterprise Linux 5** do not currently support RHEL 5.7 or later for CD install. Customers who wish to install RHEL 5.7 or later should either use a network install or install from a version 5.6 CD image and then use 'yum update' to bring the VM up to date. This also applies to RHEL derivatives such as CentOS and OEL.

You will need to install the XenServer Tools immediately after installing the operating system. For some operating systems, the XenServer Tools includes a XenServer specific kernel, which replaces the kernel provided by the vendor. Other operating systems, such as RHEL 5.x require you to install a specific version of a vendor provided kernel.

> **Warning:**
>
> Running a VM without installing the XenServer Tools is not a supported configuration, so Citrix recommends that you install the tools immediately after Operating System installation. For more information, see Section 2.3, "XenServer Tools".

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.
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 meant 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.
>
> Note that VMs created using the **Other install media** template will be created as HVM guests, which means that the Linux VMs created using this template will not be able to use the native high-performance drivers (PV drivers) included in modern kernels.

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

CITRIX

The supported Linux distributions are:

Distribution	Vendor Install from CD	Vendor Install from network repository	Notes
Debian Squeeze 6.0 (32-/64-bit)	X	X	
Red Hat Enterprise Linux 4.5, 4.6, 4.7, 4.8 (32-bit)	X	X	Requires installing XenServer Tools after installing RHEL to apply the Citrix RHEL 4.8 kernel.
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-/64-bit)	X	X	Supported provided you use the 5.4 or later kernel.
Red Hat Enterprise Linux 6.0, 6.1, 6.2 (32-/64-bit)	X	X	
SUSE Linux Enterprise Server 10 SP1, SLES 10 SP2, SLES 10 SP4 (32-/64-bit)	X	X	
SUSE Linux Enterprise Server 10 SP3 (32-bit)			Supported only if upgrading from SLES 10 SP2
SUSE Linux Enterprise Server 10 SP3 (64-bit)	X	X	
SUSE Linux Enterprise Server 11, SLES 11 SP1 (32-/64-bit)	X	X	
CentOS 4.5, 4.6, 4.7, 4.8 (32-bit)	X	X	
CentOS 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-/64-bit)	X	X	
CentOS 6.0, 6.1, 6.2 (32-/64-bit)	X	X	
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (32-/64-bit)	X	X	
Oracle Enterprise Linux 6.0, 6.1, 6.2 (32-/64-bit)	X	X	
Ubuntu 10.04 (32-/64-bit)		X	
Ubuntu 12.04 (32-/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 5 (for example Fedora Core 6) might be successfully installed using the same template.

> **Note:**
>
> Creating 32-bit Linux VMs on a host that has more than 128GB of memory is not supported.

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.

CİTRIX®

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 bootable:

```
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. See Appendix E, *Setting Up a Red Hat Installation Server* for information on how to copy a set of installation CDs to a network drive.

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**

CİTRIX

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/file 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 command to the **Advanced OS boot parameters** text box. For example, for RHEL 5.4, this command would be `ks=nfs:telos:/linux/distros/auto-install/rhel54.cfg`.

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. This additional information includes:

- Linux distribution name and version (major, minor revision).
- Kernel version (`uname`).
- IP address of each Ethernet interface.
- Total and free memory within the VM.

It is important to install this agent and keep it 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 `xs-tools.iso` CD image, or alternatively can be installed by using the **VM > 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 10.10 and later) instead of as `/dev/cdrom` as you might expect. This is because they are not true CD-ROM devices, but normal devices. When the CD is ejected by either XenCenter or the CLI, it hot-unplugs the device from the VM and the device disappears. This is different from Windows Virtual Machines, where the CD remains in the VM in an empty state.

CITRIX

5.6. Additional Installation Notes for Linux Distributions

This section describes additional, vendor-specific configuration information that you should be aware of before creating Linux VMs. It covers each Linux distribution supported in this release of XenServer.

Important:

For detailed release notes on all distributions, see Appendix B, *Linux VM Release Notes*.

Linux Distribution	Installation Notes
CentOS 4.5, 4.6, 4.7, 4.8 (32-bit)	For a CentOS 4.x VM, you must install the XenServer Tools, which includes the CentOS 4.8 kernel and fixes issues in the CentOS kernel that prevent XenServer from running correctly.
CentOS 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (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.
CentOS 6.0, 6.1, 6.2 (32-/64-bit)	None.
Red Hat Enterprise Linux 4.5, 4.6, 4.7, 4.8 (32-bit)	For a RHEL 4.x VM, you must install the XenServer Tools, which includes the RHEL 4.8 kernel and fixes issues in the RHEL kernel that prevent XenServer from running correctly.
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (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 6.0, 6.1, 6.2 (32-/64-bit)	None.
SUSE Linux Enterprise Server 10 SP1, SLES 10 SP2, SLES 10 SP 3 (32-/64-bit)	None.
SUSE Linux Enterprise Server 11, SLES 11 SP1 (32-/64-bit)	None.
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 (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. • With OEL 5.6 64-bit, the Unbreakable Enterprise Kernel does not support the Xen platform. If you use the Unbreakable Enterprise Kernel with this operating system, the kernel fails to boot properly.

Linux Distribution	Installation Notes
Oracle Enterprise Linux 6.0, 6.1, 6.2 (32-/64-bit)	None.
Debian Squeeze 6.0 (32-/64-bit)	When a private mirror is specified in XenCenter this is only used to retrieve the installer kernel. Once the installer is running you will again need to enter the address of the mirror to be used for package retrieval.
Ubuntu 10.04 (32-/64-bit)	For Ubuntu 10.04 VMs with multiple vCPUs, Citrix strongly recommends that you update the guest kernel to "2.6.32-32 #64". For details on this issue, see the Knowledge Base article CTX129472 Ubuntu 10.04 Kernel Bug Affects SMP Operation.
Ubuntu 12.04 (32-/64-bit)	None.

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 Workload Balancing (WLB), 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.

6.1.2. Storage XenMotion

> **Note:**
>
> Storage XenMotion feature is only available in Citrix XenServer Advanced Edition or higher. To learn more about upgrading XenServer, click here.
>
> Storage XenMotion must **not** be used in XenDesktop deployments.

Storage XenMotion additionally allows VMs to be moved from one host to another, where the VMs are **not** located on storage shared between the two hosts. As a result, VMs stored on local storage can be migrated without downtime and VMs can be moved from one pool to another. This enables system administrators to:

- rebalance VMs between XenServer pools (for example from a development environment to a production environment).
- upgrade and update standalone XenServer hosts without any VM downtime.
- upgrade XenServer host hardware.

> **Note:**
>
> Moving a VM from one host to another preserves the VM *state*. The state information includes information that defines and identifies the VM 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 new VM host must meet the following compatibility requirements in order for the migration to proceed:

- XenServer Tools must be installed on each VM that you wish to migrate.
- The target host must have the same or a more recent version of XenServer installed as the source 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.

- 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 (for the VM and its snapshot) available for the incoming VMs. If there is not enough space, the migration will fail to complete.

6.1.4. Limitations and Caveats

XenMotion and Storage XenMotion are subject to the following limitations and caveats:

- VMs with VDIs located on Integrated StorageLink (iSL) SRs cannot be migrated.

- VMs using PCI pass-thru cannot be migrated.

- VM performance will be reduced during migration.

- For Storage XenMotion, pools protected by High Availability (HA) or Work Load Balancing (WLB) should have HA and WLB 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:

   - Right-click and on the shortcut menu, point to **Migrate to Server** and then select **Migrate VM wizard.**

   - On the **VM** menu, point to **Migrate to Server** and then select **Migrate VM wizard.**

   - In **Folder View**, drag the VM onto the destination server.

     Note:

     You must be in **Folder View** to be able to migrate a VM by dragging and dropping it in the Resources pane.

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

Note:

The Live VDI Migration feature is available in Citrix XenServer Enterprise Edition or higher. To learn more about the features available in different XenServer Editions, click here.

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

- There must be sufficient disk space available on the target repository.

- VDIs located on Integrated StorageLink (iSL) SRs cannot be migrated.

- VDIs with more than one snapshot cannot be migrated.

- IPv6 Linux VMs require a Linux Kernel greater than 3.0.

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, updating XenServer Tools, and updating VMs with new Linux kernel revisions.

Upgrades to VMs are typically required when moving to a new version of XenServer. The following are current issues involving upgrading VMs running on XenServer to this version:

• XenMotion of Windows VMs is not supported until the XenServer Tools are upgraded.

• Suspend/Resume of Windows VMs is not supported until the XenServer Tools are upgraded.

• The use of certain anti-virus and firewall applications can crash the Windows VM 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. In Windows XP, 2000, or 2003, select **Add or Remove Programs**.

    In Windows 7 and Vista, select **Programs**, then select **Programs and Features**.

3. Select select **Citrix Tools for Virtual Machines**.

4. In Windows XP, 2000, or 2003, click the **Remove** button.

    In Windows 7 and Vista, from the toolbar above the list of programs, 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 9.2, "XenServer Tools" for details.

7.2. Updating XenServer Tools for Windows VMs

The XenServer Tools are available in XenCenter on the built-in `xs-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 CD drive, installation will be started automatically after a few moments. If Autoplay is not enabled, double-click on the CD drive, and select `xensetup.exe` to begin the XenServer Tools installation. Follow the on-screen prompts to install the new drivers, which will automatically deactivate and upgrade the old drivers.

7.3. Updating Linux Kernels and Guest Utilities

The Linux guest utilities can be updated by rerunning the `Linux/install.sh` script from the built-in `xs-tools.iso` CD image (see Section 5.5, "Installing the Linux Guest Agent"). From time to time, Citrix also supplies updated RHEL 4.x Linux kernels for supported distributions on the website, http://updates.vmd.citrix.com/

XenServer/6.1.0/rhel4x/. Because Citrix no longer provides RHEL 5.x kernels, you should obtain updates to RHEL 5.4 and higher kernels directly from Red Hat.

Rerunning the `Linux/install.sh` script from the built-in `xs-tools.iso` is particularly important for CentOS versions prior to 5.3, where you will get the upstream kernel by default, which has certain limitations (see Section B.1, "Release Notes").

For `yum`-enabled distributions (CentOS 4 and 5, RHEL 5.4 and higher), `xe-guest-utilities` installs a `yum` configuration file to enable subsequent updates to be done using `yum` in the standard manner.

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

When upgrading, Citrix recommends that you always rerun `Linux/install.sh` when you upgrade. This script automatically determines if your VM needs a kernel update and installs it if necessary.

> **Note:**
>
> SLES is also supported, but Citrix does not provide an updated kernel.

CITRIX

Chapter 8. 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 dependant 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.*

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

8.5. Importing and Exporting vApps

vApps can be imported and exported as OVF/OVA packages. See Chapter 11, *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 11.5.1, "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 11.4.1, "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 9. Advanced Notes for Virtual Machines

This chapter details some advanced notes for Virtual Machines.

9.1. 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 smbfs -o username=myname/myworkgroup
```

The `unc_path` argument should have back-slashes replaced by forward-slashes. `-t cifs` can be used for CIFS instead of SMB. For example:

```
xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
xe-mount-iso-sr //server2/iso_share -t smbfs -o username=alice
```

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.

9.2. XenServer Tools

The Citrix paravirtualized network and SCSI drivers (XenServer Tools) provide high performance I/O services without the overhead of traditional device emulation. 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.

If you are working with a VM that does not have XenServer Tools installed, a **Tools not installed** message in red text will be visible on the **General** tab in the properties pane. A message will also be displayed here if XenServer has been updated and the VM has an older version of XenServer Tools from an earlier release. In this case, the message displayed is **Tools out of date (version x.y installed)**. For a Windows VM, you can double-click on this text to switch to the VM console, load the Tools ISO, and launch the Tools installation wizard; for Linux VMs, you can double-click on this text to switch to the VM console and load the Tools ISO (however, you must mount the ISO and manually run the installation).

After Windows is installed, install the XenServer Tools. These are on an ISO available to the virtual CD-ROM drive of the Virtual Machine.

> **Note:**
>
> While a Windows VM functions without them, performance is significantly hampered unless these drivers are installed. Running Windows VMs without these drivers is *not* supported.

Some features, such as live relocation across physical hosts, will only work with the PV drivers installed and active.

Attach the Windows PV drivers ISO to the VM by using the **Install Tools** menu in XenCenter, or by directly attaching the built-in `xs-tools.iso` ISO image on the VM using the CLI. Once the ISO is attached, double-click on the `xensetup.exe` installer executable and follow the on-screen prompts.

> **Note:**
>
> To silently install the XenServer Tools and prevent the system from rebooting afterwards, use the `/S` and `/norestart` options:
>
> `<install_dir>/xensetup.exe /S /norestart`

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

The XenServer Tools can also be installed on a provisioned Windows machine by running the executable `windows-pvdrivers-xensetup.exe`, located in the `client_install/` directory of the installation CD.

> **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. If a VM is running Windows 2003, you need to install the Windows Imaging Component (see your vendor documentation for details) before installing XenServer Tools.

9.3. Windows Volume Shadow Copy Service (VSS) provider

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

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.

9.4. 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 (PV drivers) 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) or **Enable Remote Desktop on this computer** (Windows 2003 Server).

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**.

9.5. 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 highly recommends running a reliable NTP service in the control domain and all Windows VMs.

So 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. Note that changing the control domain time-zone does not affect VM time-zones or offset. It is only the hardware clock setting which is used by XenServer to synchronize the guests.

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).

9.6. Time Handling in Linux VMs

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

Dependent wallclock: Clocks in 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: Clocks in Linux VMs are **not** synchronized to the clock running on the control domain and can be altered. The control domain time is used to set the initial time when the VM boots.

CITRIX

The following table lists wallclock settings for Linux VMs:

Guest OS	Dependent wallclock	Independent wallclock
CentOS 4.x	Default	Optional
CentOS 5.x (32-/64-bit)	Default	Optional
CentOS 6.x (32-/64-bit)	Not supported	Default
Red Hat Enterprise Linux 4.x (32-bit)	Default	Optional
Red Hat Enterprise Linux 5.x (32-/64-bit)	Default	Optional
Red Hat Enterprise Linux 6.x (32-/64-bit)	Not supported	Default
OEL 5.x (32-/64-bit)	Default	Optional
OEL 6.x (32-/64-bit)	Not supported	Default
SLES 10.x (32-/64-bit)	Default	Optional
SLES 11.x (32-/64-bit)	Default	Optional
Debian 6.0 (32-/64-bit)	Not supported	Default
Ubuntu 10.04 (32-/64-bit)	Not supported	Default
Ubuntu 12.04 (32-/64-bit)	Not supported	Default

Important:

- For Linux guests that support dependent wallclock, Citrix recommends enabling independent wallclock setting and using NTP inside the VM.
- For Linux guests that support independent wallclock, Citrix highly recommends running a reliable NTP service on the Linux VMs.

Refer to the following section to set the independent wallclock time.

To set individual Linux VMs to maintain independent times

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* may also be passed as a boot parameter to the 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).

9.7. Installing a VM from Reseller Option Kit (BIOS-locked) Media

A XenServer VM can be:

- BIOS-generic: the VM has generic XenServer BIOS strings;

- BIOS-customized: the VM has a copy of the BIOS strings of a particular server in the pool;

- without BIOS strings: immediately after its creation. If a VM does not have BIOS strings set when it is started, the standard XenServer BIOS strings will be inserted into it, and the VM will become BIOS-generic.

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

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

9.8. Preparing for Cloning a Windows VM Using VSS

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

Computers running Windows operating systems are uniquely identified by a Security ID (SID). When cloning a Windows VM, it is important to take steps to ensure the uniqueness of the SID. Cloning an installation without taking the recommended system preparation steps can lead to duplicate SIDs and other problems. Because the SID identifies the computer or domain as well as the user, it is critical that it is unique. For more information,

refer to the Microsoft Knowledge Base article 314828, "The Microsoft policy for disk duplication of Windows installations".

sysprep modifies the local computer SID to make it unique to each computer. The **sysprep** binaries are on the Windows product CDs in the `\support\tools\deploy.cab` file.

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. Copy the contents of `\support\tools\deploy.cab` from the Windows product CD to a new `\sysprep` folder in the VM.

6. Run **sysprep**. This will shut down the VM when it completes.

7. Using XenCenter convert the VM into a template.

8. Clone the newly created template into new VMs as required.

9. 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, sysprepped 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 websites:

Windows 7- The Windows Automated Installation Kit (AIK) for Windows 7

Windows XP - How to use the Sysprep tool to automate successful deployment of Windows XP

Windows Server 2003 - What Is Sysprep?

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

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

> **Important:**
>
> GPU Pass-Through is available to Citrix XenServer Enterprise editions and higher.

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 or WLB 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.

CiTRIX

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. For any further questions regarding the hardware compatibility list, e-mail xenserver.hcl@citrix.com.

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 a XenServer host without an available GPU in the appropriate GPU group, XenServer prints an error message.

To detach a Windows VM from a GPU using XenCenter:

1. Shut down the VM.

2. Open the VM properties: right-click the VM and select **Properties**.

3. Detach the GPU from the VM: Select **GPU** from the list of VM properties, and then select **None** as the GPU type. Click **OK**.

CiTRIX

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.

CiTRIX

Chapter 10. 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 **My Citrix**. 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 XenServer area of My Citrix.

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

10.1. 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.

CITRIX

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.

CITRIX·

Chapter 11. 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 11.2, "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 11.3, "The Transfer VM".

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

11.1. 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

CİTRIX

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

11.1.1. 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.

CITRIX

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.

11.1.1.1. 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.

11.1.2. 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.

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

CITRIX

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

11.2. 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 a XenServer host.

XenCenter includes an advanced hypervisor interoperability feature — Operating System Fixup — which aims to ensure a basic level of interoperability for VMs that you import into XenServer. You need to use Operating System Fixup when importing VMs from OVF/OVA packages and disk images created on other virtualization platforms.

The Operating System Fixup process addresses the operating system device and driver issues inherent when moving from one hypervisor to another, attempting to repair boot device-related problems with the imported VM that might prevent the operating system within from booting in a XenServer environment. This feature is not designed to perform conversions from one platform to another.

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

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

To use Operating System Fixup on imported disk images or OVF/OVA packages, you must enable the feature on the Advanced Options page of the XenCenter Import wizard and then specify a location where the Fixup ISO should be copied so that XenServer can use it.

What Does Operating System Fixup do to the VM?

The Operating System Fixup option is designed to make the minimal changes possible to enable a virtual system to boot. Depending on the guest operating system and the hypervisor of the original host, 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.

11.3. 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 a XenServer storage repository.

One Transfer VM runs for each import or export of a disk image. When importing or exporting a virtual appliance with more than one disk image, only one disk image transfers at a time.

Running one Transfer VM has the following requirements:

Virtual CPU	1
Virtual Memory	256 MB
Storage	8 MB
Network	Reachable by the XenServer host; static or dynamic IP address (dynamic, recommended)

The default transfer protocol is iSCSI. In which case, the Transfer VM requires an iSCSI Initiator on the XenServer host. An alternate transfer protocol is RawVDI.

To use the RawVDI transfer protocol:

1. 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.

11.4. 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.

11.4.1. 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 11.2, "Operating System Fixup".

- It is necessary to configure networking for the Transfer VM used to perform the import process. For more information, see Section 11.3, "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 11.2, "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 Vista, Server 2008, and later, set the `platform` parameter to `device_id=0002`. For example:

  ```
  xe vm-param-set uuid=<VM uuid> platform:device_id=0002
  ```

- For all other versions of Windows, set the `platform` parameter to `viridian=true`. For example:

  ```
  xe vm-param-set uuid=<VM uuid> platform:viridian=true
  ```

11.4.2. 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 11.2, "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 Vista, Server 2008, and later, set the `platform` parameter to `device_id=0002`. For example:
>
> ```
> xe vm-param-set uuid=<VM uuid> platform:device_id=0002
> ```
>
> • For all other versions of Windows, set the `platform` parameter to `viridian=true`. For example:
>
> ```
> xe vm-param-set uuid=<VM uuid> platform:viridian=true
> ```

11.4.3. 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:

CiTRIX

- 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, 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.

11.5. 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.

11.5.1. 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.

CİTRIX

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 11.1.1, "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.

11.5.1.1. 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 a XenServer host, on which you can maintain a library of export files (for example, to the machine running XenCenter).

> **Warning:**
>
> It may not always be possible to run an imported VM that was exported from another server with a different CPU type. For example, a Windows VM created on a server with an Intel VT Enabled CPU, then exported, may not run when imported to a server with an AMD-VTM CPU.

To Export VM(s) as XVA Files using XenCenter:

1. Shut down or suspend the VM that you 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.

![CITRIX]

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 PV 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 Server 2008

Quiesced snapshots taken on Windows Server 2008 guests will not be directly bootable. Attach the snapshot disk to an existing Windows Server 2008 VM to access files for restoration purposes.

A.1.3. Windows Server 2003

Windows Server 2003 32-bit does not boot successfully if any virtual disks larger than 2TB (terabytes) in size are attached to the VM. See this article in the Windows Hardware Developer Central website.

A.1.4. Windows 7

No known issues

A.1.5. Windows Vista

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

A.1.6. Windows XP SP3

Windows XP does not support disks larger than 2TB (terabytes) in size. See this article in the Windows Hardware Developer Central website.

CITRIX

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. Red Hat Enterprise Linux 4.5 to 4.8

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

- The Xen kernel in RHEL 4.8 can occasionally enter tickless mode when an RCU is pending. When this triggers, it is usually in `synchronize_kernel()` which means the guest essentially hangs until some external event (such as a `SysRQ`) releases it (Red Hat Bugzilla 427998)

- Live migration can occasionally crash the kernel under low memory conditions (Red Hat Bugzilla 249867)

- Guest kernel can occasionally hang due to other XenStore activity (Red Hat Bugzilla 250381)

- RHEL 4.7 contains a bug which normally prevents it from booting on a host with more than 64GiB of RAM (Red Hat Bugzilla 311431). For this reason XenServer RHEL 4.7 guests are only allocated RAM addresses in the range below 64GiB by default. This may cause RHEL 4.7 guests to fail to start even if RAM appears to be available, in which case rebooting or shutting down other guests can cause suitable RAM to become available. If all else fails, temporarily shut down other guests until your RHEL 4.7 VM can boot.

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

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

  to remove the memory restriction.

- On some hardware (generally newer systems), the CPU will generate occasional spurious page faults which the OS should ignore. Unfortunately all versions of RHEL 4 fail to ignore the spurious fault and it causes them to crash (Red Hat Bugzilla 465914).

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

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

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

- In RHEL 4.5 to 4.7, if a xenbus transaction end command fails it is possible for the suspend_mutex to remain locked preventing any further xenbus traffic. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-5]

- In RHEL 4.5 to 4.8, use of the XFS filesystem can lead to kernel panic under exceptional circumstances. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-16]

- In RHEL 4.5 to RHEL 4.8, the kernel can enter no tick idle mode with RCU pending; this leads to a guest operating system lock up. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-21]

- In RHEL 4.7, 4.8, VMs may crash when a host has 64GiB RAM or higher configured. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-30]

- In RHEL 4.5 to 4.8 and 5.0 to 5.3, the network driver contains an issue that can, in rare circumstances, lead to a kernel deadlock. Applying the Citrix RHEL 4.8 kernel resolves this issue. [EXT-45]

Additional Notes:

- RHEL 4.7, 4.8, sometimes when there are many devices attached to a VM, there is not enough time for all of these devices to connect and startup fails. [EXT-17]

- If you try to install RHEL 4.x on a VM that has more than two virtual CPUs (which RHEL 4.x does not support), an error message incorrectly reports the number of CPUs detected.

B.1.1.1. Preparing a RHEL 4.5 to 4.8 guest for cloning

To prepare a RHEL 4.5 to 4.8 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.1.1.2. RHEL Graphical Network Install Support

To perform a graphical installation, add `VNC` to the list of advanced OS boot parameters when creating the VM:

```
graphical utf8 vnc
```

You will be prompted to provide networking configuration for the new VM so that VNC communication can be enabled. The standard graphical installer will then be displayed.

B.1.2. Red Hat Enterprise Linux 5

XenServer requires that you run the RHEL 5.4 kernel or higher. These kernels have the following known issues:

- 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).

- 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.x 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).

CITRIX

B.1.3. CentOS 4

Please refer to Section B.1.1, "Red Hat Enterprise Linux 4.5 to 4.8" for the list of CentOS 4 release notes.

B.1.4. CentOS 5

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

B.1.5. Oracle Enterprise Linux 5

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

B.1.6. SUSE Enterprise Linux 10 SP1

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

• A maximum of 3 virtual network interfaces is supported.

• Disks sometimes do not attach correctly on boot. (Novell Bugzilla 290346).

B.1.7. SUSE Enterprise Linux 10 SP3

Due to a defect in the packaging of Novell SUSE Linux Enterprise Server 10 SP3 (32-bit) edition, users will not be able to create a new VM of this edition. As a workaround, you must install SLES 10 SP2 and then upgrade it to SLES SP3 using, for example, "yast" within the VM. For more information, please refer to the Novell documentation 7005079.

B.1.8. SUSE Enterprise Linux 11

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

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

B.1.9. 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.

CİTRİX

B.1.10. Ubuntu 10.04

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

B.1.11. Upgrading from Debian Lenny 5. 0 (32-/64-bit) to Squeeze 6.0 (32-/64-bit)

Due to a PV bootloader limitation, users will not be able to use the chainload option while upgrading from Debian Lenny to Debian Squeeze. When presented with an option during the upgrade to chainload from menu.lst, you must select **No**.

After completing the upgrade process and before rebooting your VM:

- Execute the command, `upgrade-from-grub` to switch to GRUB 2.
- Enter the command, `rm -f /boot/grub/menu.lst` to remove legacy GRUB files.

Please refer to the Debian release notes, Upgrading from Debian 5.0 Lenny for more information.

CITRIX

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.

    One simple and free utility is ISO Recorder. It works on Windows XP SP2/SP3, and Windows Server 2003. Once installed, right-click on a CD/DVD drive and select **Create image from CD** from the context menu.

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 4 is based on Red Hat Enterprise Linux 4, and CentOS 5 is based on Red Hat Enterprise Linux 5.

D.1. Enabling a Graphical Console on Debian Squeeze VMs

> **Note:**
>
> Before enabling a graphical console on your Debain 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
```

CiTRIX

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.x VMs".

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

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

If you are using Red Hat Linux version 5 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 3 and 4, this should be added above the `[server-Standard]` section.

    • With configuration files on Red Hat Linux 5, this should be added into the empty `[servers]` section.

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

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

```
0=Standard
```

Modify it to read:

```
0=VNC
```

- If you are using Red Hat Linux 5 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 4 and 5, 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.

CITRIX

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

If you are using Red Hat Linux version 6, 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.

Before making configuration changes, verify that you have a VNC server installed. Login as root on the text CLI in the VM, and run the command **rpm -q tigervnc-server gdm**. The package names `tigervnc-server` and `gdm` should appear, with their version numbers specified.

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.

Follow the instructions below to enable graphical console on your RHEL 6.x VMs:

1. Enter the following command to install the `inetd` service:

    ```
    # yum install -y xinetd
    ```

2. 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
    ```

3. Create the xinetd.d 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
    }
    ```

4. Enter the following command to start the `inetd` service:

    ```
    # service xinetd start
    ```

5. 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
    ```

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

    ```
    # service iptables restart
    ```

7. 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 a SLES-based 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, **Tab** to the **Firewall Configuration: Settings** section. Use the arrow keys to select the **Allowed Services** in the left menu.

4. **Tab** to the **Firewall Configuration: Allowed Services** fields on the right. Use the arrow keys to select the **Advanced** button (near the bottom right, just above the **Next** button) and press **Enter**.

5. In the **Additional Allowed Ports** screen, enter *5900* in the **TCP Ports** field. **Tab** to the **OK** button and press **Enter**.

6. **Tab** back to the list of screens on the left side and use the arrow keys to select **Start-Up**. **Tab** back to the right and **Tab** to the **Save Settings and Restart Firewall Now** button and press **Enter**.

7. **Tab** to the **Next** button and press **Enter**, then in the **Summary** screen **Tab** to the **Accept** button and press **Enter**, and finally on the top-level `YaST` screen **Tab** to the **Quit** button and press **Enter**.

8. Restart the display manager and `xinetd` service with the following commands:

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

CITRIX

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.

CiTRIX

Appendix E. Setting Up a Red Hat Installation Server

This chapter explains how to set up a server as an installation server for Red Hat Linux.

For a server to act as a Red Hat Linux network installation server, you need space on your server to copy the entire contents of each CD onto your server. This is typically the number of CDs or ISO images multiplied by 650MB.

Ensure that the space you intend to use is formatted with your chosen filesystem and is mounted. You can check this space with the command:

df -h

E.1. Copying Installation Media

1. First create a directory to contain the installation files, for example `/install`

2. Mount your CD. Refer to your operating system documentation for assistance if needed. This example assumes that it is mounted at `/mnt/cdrom`:

   ```
   mount /mnt/cdrom
   ```

3. Copy the data from the CD to the installation directory:

   ```
   cp -var /mnt/cdrom/RedHat /install
   ```

4. Unmount the CD:

   ```
   umount /mnt/cdrom
   ```

5. Remove the first CD, put in the next one, and repeat for each of the CDs you have.

   > **Note:**
   >
   > Copying the subsequent disks will overwrite some files, but these are generic files such as `license.txt` that appear on each CD, and this is not a problem.

E.2. Enable Remote Access

Next, make your installation data available to other machines on the network. You can use NFS, HTTP, or FTP protocols. You can enable all three services on your server or any subset of the three.

E.2.1. NFS

To install over NFS you must meet certain conditions on the server:

- The installation directory must be exported

  To export your installation directory, edit the `/etc/exports` file and add an entry for `/install` to it:

  ```
  /install *(ro)
  ```

  Save the edited exports file and make the NFS daemon reread its configuration file:

  ```
  exportfs -r
  ```

  This configures the most basic read-only export to all hosts on our network. If you want to include more advanced options in your export, such as exporting to certain hosts only, or on a certain subnet only, see the man page for the exports file: `exports (5)`.

- NFS needs to be installed and running

To check, type the command:

```
showmount -e hostname
```

Running the **showmount** command without the hostname parameter will check the local system.

If NFS is not active, you will see a message similar to

```
showmount: ServerA: RPC: Program not registered
```

- `portmap` must be running. Run the following command to check this:

```
service portmap status
```

E.2.2. FTP

To enable installation over FTP, you must allow FTP access to the installation directory on the server. This can be either anonymous FTP access or access through a named account with a password.

If you want anonymous FTP to point to a different directory, you can use symlinks to point to the installation directory on the server.

E.2.3. HTTP

If you have a web server running and want to enable HTTP access to your installation server, add symlinks from your document root to the installation server directory to grant access.

The installation server is now ready to use. Record the server name or IP address and the directory path to the installation directory you created.

Appendix F. 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 Knowledge Center hosts a number of resources that may be helpful to you if you experience odd behavior, crashes, or other problems. Resources include: Support Forums, Knowledge Base articles and product documentation.

If you experience odd VM behavior, this chapter is meant to help you solve the problem if possible and, failing that, describes where the 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.

F.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.

F.1.1. Controlling Linux VM Crashdump Behaviour

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 command:

   ```
   xe vm-list name-label=<name> params=uuid --minimal
   ```

2. Change the `actions-after-crash` value using **xe vm-param-set**; for example:

   ```
   xe vm-param-set uuid=<vm_uuid> actions-after-crash=preserve
   ```

3. Crash the VM

   ```
   echo c | sudo tee /proc/sysrq-trigger
   ```

4. Execute the dumpcore on dom0. For example, run:

   ```
   /opt/xensource/libexec/dumpcore -domid <domid> -file <filename>
   ```

CiTRIX

F.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**.

F.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.