CiTRIX®

Citrix XenServer ® 5.6 Service Pack 2 Virtual Machine Installation Guide

Citrix XenServer ® 5.6 Service Pack 2 Virtual Machine Installation Guide

Copyright © 2011 Citrix Systems. Inc. All Rights Reserved.
Version: 5.6 Service Pack 2

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

CiTRIX

Contents

CITRIX

CITRIX

CITRIX

About this Document

Overview

This is a guide to creating Virtual Machines (VMs) with XenServer™, the platform virtualization solution from Citrix®. It describes the various methods of getting VMs up and running on XenServer hosts for each of the supported guest operating systems.

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
- Creating and using ISO images of vendor media for installing VMs
- Setting up a network repository of vendor media for installing VMs
- Troubleshooting problems with VMs

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 Installation 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 Guide* is a comprehensive user guide to the vSwitch and 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

Virtual Machines - Overview

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.

Overview

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 ParaVirtualised (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.

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

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

Other Methods of VM Creation

In addition to creating VMs from the provided templates, 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

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.

CİTRIX

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 the section called "Preparing for Cloning a Windows VM using VSS" for Windows and the section called "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.

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.

When importing a VM, you can choose to preserve the MAC address on any virtual network interfaces associated with it. If you choose to generate a new MAC address, be sure to follow the appropriate preparation procedure for the imported VM. See the section called "Preparing for Cloning a Windows VM using VSS" for Windows and the section called "Preparing to Clone a Linux VM" for Linux.

Importing an exported VM may take some time, depending on the size of the VM and the speed and bandwidth of the network connection between the XenServer host and XenCenter.

On VM import, XenServer re-attaches the VM virtual network interface (VIF) to the network that has the same *name* as the network on the server from which the VM was exported. If no matching network is found, the VM VIFs are attached to a new private network.

Exporting a VM

When you export a VM, a complete copy of the VM (including disk images) is stored as a single file on your local machine, with a **.xva** file extension. An existing VM can be exported using XenCenter or the XenServer Command Line Interface (CLI) . Additional instructions for using XenCenter, are available in the XenCenter online Help.

CİTRIX

The following procedure assumes that you have multiple XenServer hosts and that you are administering them using the CLI on a separate machine (that is, a machine that is not one of the XenServer hosts) where you can maintain a library of export files. Citrix recommends not exporting a VM to a XenServer host filesystem.

To Export a VM using XenCenter

1. In the **Resources** pane, select the VM, then right click and select **Shut Down**.

2. Right click on the VM, and select **Export to File**.

3. Enter a name for the export file and specify the folder where you want it to be saved.

4. Click **Save** to begin exporting the file.

    The export progress is displayed in the status bar at the bottom of the XenCenter window and also on the **Logs** tab.

5. The saved file has a *.xva extension.

    Note:

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

To Export a VM using the CLI

1. Shut down the VM that you want to export.

2. Run the following commands to export the VM:

    ```
    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 attempt to import it using XenCenter, it might fail to recognize the file as a valid XVA file.

Importing a VM

An exported VM file can be imported using XenCenter or the CLI.

To Import a VM using XenCenter

1. In the **Resources** pane, select a host or a Pool, then right-click and select **Import**.

2. Follow the Import wizard.

3. Importing a VM, template or snapshot involves the same steps as creating and provisioning a new VM using the New VM wizard, that is, nominating a home server, and configuring storage and networking for the new VM.

    Note:

    The import progress is displayed in the status bar at the bottom of the XenCenter window and also on the **Logs** tab. The import process may take some time, depending on the size of the VM and the speed and bandwidth of the network connection between XenCenter and the destination server. When the newly-imported VM is available, it appears in the **Resources** pane.

    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 a VM using the CLI

1. To import the VM to the default SR on the target XenServer host:

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

   You can import the VM to another SR on the target XenServer host by adding 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>
   ```

   You can also preserve the MAC address of the original VM by adding the optional $preserve$ parameter set to $true$:

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

2. Import process may take some time, depending on the size of the VM and the speed and bandwidth of the network connection. When finished, the command prompt returns the UUID of the newly-imported VM.

CITRIX·

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

- 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 the section called "XenServer Tools"

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

CITRIX

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.

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	Disk space
Windows 7 (32 bit)	1GB	4GB	Minimum 16GB, 40GB or more recommended
Windows 7 (64 bit)	2GB	32GB	Minimum 20GB
Windows Server 2008 R2 SP1 (64 bit)	512MB	32GB	Minimum 32GB
Windows Server 2008 R2 (64 bit)	512MB	32GB	Minimum 32GB
Windows Server 2008 (32/64 bit)	512MB	32GB	Minimum 10GB, 40GB or more recommended
Windows Server 2003	256MB	32GB	2GB
Windows Vista (32 bit)	1GB	4GB	16GB
Windows XP SP3	256MB	32GB	1.5GB
CentOS 4.5, 4.6, 4.7	256MB	16GB	800MB
CentOS 5.0, 5.1, 5.2, 5.3, 5.4	512MB	16GB	800MB
CentOS 5.5 (32/64 bit)	512MB	16GB	800MB
Red Hat Enterprise Linux 4.5, 4.6, 4.7, 4.8	256MB	16GB	800MB
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4	512MB	16GB	800MB

![CITRIX]

Operating System	Minimum RAM	Maximum RAM	Disk space
Red Hat Enterprise Linux 5.5 (32/64 bit)	512MB	16GB	800MB
Red Hat Enterprise Linux 6.0 (32/64 bit)	512MB	16GB	800MB
SUSE Linux Enterprise Server 9 SP2/3/4	256MB	32GB	1GB
SUSE Linux Enterprise Server 10 SP1/2	512MB	32GB	1.5GB
SUSE Linux Enterprise Server 11 SP1 (32/64 bit)	512MB	32GB	1.5GB
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4	512MB	16GB	800MB
Oracle Enterprise Linux 5.5 (32/64 bit)	512MB	16GB	800MB
Debian Lenny	128MB	32GB	4GB
Debian Squeeze 6.0 (32/64 bit)	128MB	32GB	4GB

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*.

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[*]	8
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 8 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

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

Creating Windows VMs

Warning:

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

XenServer allows you to install Windows Server 2008 R2, Windows Server 2008 (32/64 bit), Windows Server 2003 (32/64 bit), Windows 7 (32/64 bit), Windows Vista, and Windows XP SP3 on to a VM. Installing Windows VMs on a XenServer host requires hardware virtualization support (Intel VT or AMD-V).

Basic Procedure for Creating a Windows VM

The process of installing a Windows on to a VM can be broken down into three steps:

• selecting the appropriate Windows template

• installing the Windows operating system

• installing the *paravirtualized device drivers* known as the XenServer Tools

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
Windows Server 2008 (x86), optimized for Citrix XenApp	Used to install all editions of Windows Server 2008 (x86). This template is specially tuned to optimize XenApp performance.
Windows Server 2008 (x64), optimized for Citrix XenApp	Uused to install all editions of Windows Server 2008 (x64). This template is specially tuned to optimize XenApp performance.
Windows Server 2008 R2 (x64), optimized for Citrix XenApp	Used to install all editions of Windows Server 2008 R2 64-bit. This template is specially tuned to optimize XenApp performance.
Windows Server 2003 (x86), optimized for Citrix XenApp	Used to install Windows Server 2003 32-bit SP0, SP1, SP2, and R2. The Server, Enterprise, Data Centre, and SBS editions are supported. This template is specially tuned to optimize XenApp performance.
Windows Server 2003 (x64), optimized for Citrix XenApp	Used to install Windows Server 2003 32-bit. The Server, Enterprise, Data Centre, and SBS editions are supported. This template is specially tuned to optimize XenApp performance.
Windows Server 2008 x32/x64	Used to install Windows Server 2008 32-bit/64-bit
Windows Server 2008 R2 x64	Used to install Windows Server 2008 R2, 64-bit.
Windows Server 2003	Used to install Windows Server 2003 32-bit SP0, SP1, SP2, and R2. The Server, Enterprise, Data Centre, and SBS editions are supported.

CITRIX

Template Name	Description
Windows Server 2003 x64	Used to install Windows Server 2003 64-bit. The Server, Enterprise, Data Centre, and SBS editions are supported.
Windows 7 (x86)	Used to install Windows 7, 32-bit.
Windows 7 (x64)	Used to install Windows 7, 64-bit.
Windows Vista (x86)	Used to install Windows Vista 32-bit. The *Enterprise* edition is supported.
Windows XP SP3 (x86)	Used to install Windows XP Service Pack 3, 32-bit. Earlier service packs are not supported.

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.

Using XenCenter to Create a VM

To create a VM:

1. On the XenCenter toolbar, click the **New VM** button to open the New VM wizard.

   The New VM wizard allows you to configure the new VM, adjusting various parameters for CPU, storage and networking resources.

2. Select a VM template.

   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 the section called "Installing a VM from Reseller Option Kit (BIOS-locked) Media"

3. Enter a name for and optional description of the new VM.

4. Choose the source of the OS media to install on the new VM.

   Installing from a CD/DVD is the simplest option for getting started. 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. The default of 1 virtual CPU and 512 MB of RAM to initially allocate to the new VM are appropriate for getting started. 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 (8 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.

    The following shows a sample a Windows 7 (32-bit) installation from DVD/CD.

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 will need to install XenServer Tools for each VM. Running VMs without XenServer Tools is *not* supported. For more information on XenServer Tools see the section called "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. In the Setup wizard, accept the License Agreement, and then choose a destination folder. Click **Install**.

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

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.

CITRIX

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.

Creating Linux VMs

Warning:

Running a VM without installing the XenServer Tools is not a supported configuration, so install the tools immediately after Operating System installation. For more information, see the section called "XenServer Tools".

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.

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.

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

Installing Linux VMs requires the Linux Pack to be installed onto the XenServer host. Without the Linux Pack, the Linux VM templates are not available.

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.

For information regarding specific Linux distributions the section called "Linux Distribution Notes""

CİTRIX

The supported Linux distributions are:

Distribution	Vendor Install from CD	Vendor Install from network repository	Notes
Demo Linux VM			Built-in
Debian Lenny 5.0	X	X	
Red Hat Enterprise Linux 4.5, 4.6, 4.7, 4.8	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 32-bit	X	X	Supported provided they use the 5.4 or later kernel.
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 64-bit	X	X	Supported provided they use the 5.4 or later kernel.
Red Hat Enterprise Linux 6.0 32-bit/64-bit	X	X	
SUSE Linux Enterprise Server 9 SP4		X	
SUSE Linux Enterprise Server 10 SP1, SP2 32-bit/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 32-bit/64-bit	X	X	
CentOS 4.5, 4.6, 4.7, 4.8	X	X	
CentOS 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 32-bit	X	X	
CentOS 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 64-bit	X	X	
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 32-bit	X	X	
Oracle Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5 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.

CITRIX

Installing the Demo Linux VM Template

The Demo Linux VM template provided with XenServer can be used to create a VM running Linux without the need for vendor installation media. This can be useful for testing purposes. For example, Demo Linux VMs allow quick and simple VM creation for use with XenServer product features such as XenMotion, Dynamic Memory Control, and High Availability.

> **Warning:**
>
> Demo Linux VMs should not be used for running production workloads.

The VMs are instantiated by running the **vm-install** command on the CLI, or by cloning the template using XenCenter. For example, using the CLI on Linux:

```
xe vm-install template="Demo Linux VM"  new-name-label=<demo>
```

When you first boot the VM you are prompted for a root password, a VNC password (for graphical use), and a hostname. You will need to add a network interface if you installed the VM using the CLI.

> **Note:**
>
> The Demo Linux VM template is only available if you install the separate Linux pack (that is, the linux.iso).

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 Lenny example, by installing the OS from an internet repository.

Example: Installing a Debian Lenny VM from a network repository

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

   ```
   xe vm-install template=<template-name> new-name-label=<lenny-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. Start the VM; it boots straight into the Debian installer:

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

4. Follow the Debian Installer procedure to install the VM in the configuration you require.

5. See below for instructions on how to install the guest utilities and how to configure graphical display.

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

This section shows the CLI procedure for creating a Linux VM, using a Debian Lenny example, by installing the OS from a physical CD/DVD.

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

1. Create a VM from the Debian Lenny 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 Lenny 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.

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://server/RedHat/5.0` as the URL of the vendor media:

```
xe vm-param-set uuid=<vm_uuid> \
other-config:install-repository=<http://server/redhat/5.0>
```

5. Start the VM

```
xe vm-start uuid=<vm_uuid>
```

6. Connect to the VM console using XenCenter or VNC and perform the OS installation.

Network Installation Notes

The XenServer guest installer allows you to install an operating system from a network-accessible ISO image onto a VM. To prepare for installing from an ISO, make an exploded network repository of your vendor media (*not* ISO images) and export it over NFS, HTTP or FTP so that it is accessible to the XenServer host administration interface. 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**
  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.

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 *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 /dev/xvdd /mnt`

3. Execute the installation script as the root user:

   `/mnt/Linux/install.sh`

4. 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 `/dev/xvdd` 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.

Linux Distribution Notes

This section describes some vendor specific configuration points.

Debian Lenny/Squeeze Notes

Debian Lenny/Squeeze is installed using the standard Debian installer, which supports installation into a VM. Use XenCenter or the xe CLI to install Debian Lenny/Squeeze from either a CD, ISO library, or from a network repository over FTP or HTTP.

Before installing Debian Lenny from a network repository, follow the Debian instructions for preparing for network installations, including how to set up a mirror. 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.

Information on installing Debian Lenny using XenCenter is available in the XenCenter help — to get started, run the **New VM** wizard. The rest of this section provides information about installing Debian Lenny using the CLI.

For detailed Debian Lenny release notes see the section called "Debian Lenny 5.0"

   > **Note:**
   >
   > If you want to perform a Debian Lenny installation from the DVD, then you must obtain a suitable Debian Lenny DVD image that is compatible with XenServer. The standard images Debian provides are not compatible with XenServer. For details on how to obtain this DVD image, see the Debian Lenny article on the Citrix Developer Network (http://community.citrix.com/display/xs/Debian+Lenny). If you want to perform a Debian Squeeze installation, use the multiarch.iso from the official Debian mirror - (http://www.debian.org/mirror/official).

Automated Installation of Debian Lenny

Installation of Debian Lenny uses the standard Debian installer — you can use the usual Debian pre-seed mechanism to support automated installation.

1. Create a pre-seed file. Information about pre-seed files is available in the appendices of the Debian user guide.

2. Set the kernel command-line correctly for the VM before starting it. This can be done using 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>
```

Apt Repositories and Lenny

For infrequent or one-off installations of Lenny, 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.

Red Hat, CentOS, Oracle Enterprise, and SUSE Enterprise Linux Notes

This section provides an overview of installing Red Hat, CentOS, Oracle Enterprise, and SUSE Enterprise.

For information about the general Linux VM installation process, see *Creating Linux VMs*.

RHEL 5.x/CentOS/OEL 5.x

When you want to create a RHEL 5.x/CentOS/OEL 5.x VM, you must ensure the operating system will use the RHEL 5.4 kernel (2.6.18-164.el5) or higher, which is available from the distribution vendor.

1. Create the VM using the New VM wizard or the CLI.
2. Install the RHEL operating system using vendor installation media.
3. Upgrade to the 5.4 or later kernel using the vendor's normal kernel upgrade procedures.
4. Follow the process for installing the Linux Guest Agent. See the overview *Creating Linux VMs*.

> **Note:**
>
> Enterprise Linux (EL) kernel versions prior to 5.4 contain issues that prevent proper operation as a XenServer VM. In previous XenServer releases, Citrix provided a 5.x kernel with fixes for those issues and required its installation. Since the required fixes are now available in 5.4 (2.6.18-164.el5) and later kernels, Citrix no longer supplies a 5.x kernel. Instead, Citrix requires use of a 5.4 or later kernel.

For detailed RHEL 5.x release notes see the section called "Red Hat Enterprise Linux 5"

For detailed CentOS 5.x release notes see the section called "CentOS 5"

For detailed OEL 5.x release notes see the section called "Oracle Enterprise Linux 5"

RHEL 4.5 to 4.8

When you want to create a RHEL 4.5 to 4.8 VM, you must install the Citrix-provided RHEL 4.8 kernel after installing the operating system. Citrix includes this kernel in the XenServer Tools for VMs, and it fixes issues in the RHEL kernel which prevents XenServer from running correctly.

Installing RHEL 4.5 to 4.8 requires using the following process:

1. Create the VM using the New VM wizard or the CLI.
2. Install the RHEL operating system using Red Hat installation media.
3. Install XenServer Tools for VMs on the new VM. This automatically installs the Citrix-provided RHEL 4.8 kernel on the VM.
4. Follow the process for installing the Linux Guest Agent. See the overview *Creating Linux VMs*.

For detailed RHEL 4.x release notes see the section called "Red Hat Enterprise Linux 4.5 to 4.8"

For detailed CentOS 4.x release notes see the section called "CentOS 4"

Red Hat, CentOS, Oracle Enterprise, and SUSE Enterprise Linux from Vendor Media

XenServer supports the installation of the following Linux operating systems from vendor media in the XenServer host DVD/CD-ROM drive:

- Red Hat Enterprise Linux 5.0-5.4, 32-bit
- Red Hat Enterprise Linux 5.0-5.4, 64-bit
- CentOS 4.5-4.6
- CentOS 5.0-5.4, 32-bit
- CentOS 5.0-5.4, 64-bit
- Oracle Enterprise Linux 5.0-5.4, 32-bit
- Oracle Enterprise Linux 5.0-5.4, 64-bit
- SUSE Enterprise Linux, 10, SP1, SP2, 32-bit
- SUSE Enterprise Linux, 10, SP1, SP2, SP3, 64-bit
- SUSE Enterprise Linux, 11, 32-bit
- SUSE Enterprise Linux, 11, 64-bit

Other Linux operating systems need to be installed from a network installation server. See the section called "Network Installation Notes".

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

Installing RHEL Using a Kickstart File

When you are installing RHEL through New VM wizard in XenCenter, you can automate the installation by using a *Red Hat Kickstart* file. 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`.

To Install RHEL Linux Using a Custom Kickstart File (from XenCenter)

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/fileksdevice=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`.

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.

CÏTRIX®

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 the section called "Release Notes".

Machine Name

A cloned VM is another computer, and like any new computer in a network, it must have a unique name within the network domain it is part of.

IP address

A cloned VM must have a unique IP address within the network domain it is part of. Generally, this is not a problem if DHCP is used to assign addresses; when the VM boots, the DHCP server 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.

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.

CİTRIX

Updating VMs

This chapter discusses updating VMs updated Windows operating systems updates to XenServer Tools drivers and VM utilities, 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.

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 the section called "XenServer Tools" for details.

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.

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 the section called "Installing the Linux Guest Agent"). From time to time, Citrix also supplies updated RHEL 4.x Linux kernels for supported distributions on its Web site (http://

updates.vmd.citrix.com/XenServer/5.6.0/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 the section called "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.

CİTRIX

Advanced Notes for Virtual Machines

This chapter details some advanced notes for Virtual Machines.

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.

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.

CİTRIX

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.

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.

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**.

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).

Time Handling in Linux VMs

By default, the clocks in a Linux VM are synchronized to the clock running on the control domain, and cannot be independently changed. This mode is a convenient default, since only the control domain needs to be running the NTP service to keep accurate time across all VMs. Upon installation of a new Linux VM, make sure you change the time-zone from the default UTC to your local value (see the section called "Release Notes" for specific distribution instructions).

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.

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.

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. Refer to the Microsoft KnowledgeBase article 314828, "The Microsoft policy for disk duplication of Windows installations," for more information.

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?

CITRIX®

Importing and Exporting Appliances

You can import and export VMs as an *appliance package*, which is a collection of one or more VMs, as well as disk images, using the XenServer OVF Appliance wizards in XenCenter.

When you export VMs in an appliance, they are exported as the configuration data along with the virtual hard disks of with each VM. When the appliance is exported, an OVF file is created that explains how to the wizard should reassemble the VMs in the package. The OVF file describes the way these virtual hard disks join together to form a VM and the resource settings (CPU, memory, disk space) associated with that VM.

When you import the appliance, the wizard reads the OVF file to determine the resource requirements for the VMs in the appliance and what virtual disks are associated with each VM and then reconstitutes them.

XenServer OVF Appliance Wizards

The XenServer OVF Appliance wizards include the Export Appliance wizard, Import Appliance wizard, and Disk Image Import wizard.

To start one of the OVF Appliance wizards, go to the **Tools** menu, point to **Virtual Appliance Tools** and then select either **Import Appliance**, **Export Appliance** or **Disk Image Import**.

The OVF Appliance Import wizard supports importing OVF appliance packages. However, due to subtle incompatibilities, the Appliance Import Wizard cannot import all OVF content. See the section called "XenServer OVF Appliance Wizards Requirements" for a list of tested OVF content.

The OVF Appliance Export wizard allows you to export packages in OVF and OVA format. For example, you could export a complete XenApp farm that you have already prepared for deployment with Sysprep, the System Preparation Utility by Microsoft for Windows deployments.

XenServer OVF Appliance Wizards Requirements

The XenServer OVF Appliance wizards support importing OVF content produced from the following utilities:

• VMware OVF versions 0.9, 1.0

• Citrix Kensho 1.*x*

• VirtualBox

• Citrix XenConvert 2.1 and higher

• XenServer OVF Appliance Wizard (this tool)

The XenServer OVF Appliance Wizard requires the following:

• To run the XenServer OVF Appliance Wizard, 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 XenServer OVF Appliance Wizard requires local storage on the server on which you are running it.

• When importing from non-XenServer sources, you may want to run the Operating System Fixups while importing the appliance. For more information about Operating System Fixups, see the section called "Operating System Fixups".

Understanding OVF and OVA Formats

Both OVF and OVA formats are appliance-package standards defined by the Distributed Management Task Force (DMTF). However, the times when you would use them differ significantly. This topic provides an overview of the OVF and OVA formats and why you would choose one over the other.

Open Virtualization Format (OVF)

OVF is an open standard for packaging and distributing software to be run in virtual machines. This standard describes the metadata of one or more virtual machines. An OVF Package consists of a descriptor file (*.ovf) and any other files representing the following attributes of the package:

- **Signature**. Digital signature used by a public key certificate in the X.509 format to authenticate the producer of the package.

- **Manifest**. An SHA-1 digest of every file in the package to verify its contents by detecting any corruption.

- **Virtual disks**. Files comprising virtual disks in the format defined by the virtualization product that exported the virtual disks. VMware products export a virtual disk in the Stream-Optimized VMDK format for an OVF Package. XenServer products export a virtual disk in the Dynamic VHD format for an OVF Package.

  Note:

  A virtual disk can contain a Windows or Linux operating system.

However, it also supports other non-metadata related capabilities, such as encryption, compression, archiving, EULA attachment, and annotations among other capabilities.

Open Virtualization Appliance (OVA)

An OVA package is a single archive file, in the Tape Archive (tar) format, containing the files that comprise an OVF Package.

More Information

For more information about OVF and OVA formats, see the following:

- Knowledge Base Article CTX121652: [] Overview of the Open Virtualization Format
- [] (Open Virtualization Format Specification

Selecting a Package Format

OVF packages contain a series of uncompressed files.

OVA packages are simply one archive file of an OVF package. OVA is useful for specific applications where 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 option lengthens both the export and import processes.

OVF Best Practices

Consider the following best practices when importing or exporting VMs, appliances, and disk images using the XenServer OVF Appliance wizards:

- When creating an appliance package you intend to import into XenServer, remove any vendor-specific tools from the VMs' operating systems before exporting the package. This is particularly helpful when importing VMware packages into XenServer.
- Citrix does not recommend manually editing the OVF XML file.
- Only use OVA as an option to make the package easier to manage. Using this option lengthens both the Export and Import process.
- Before importing OVF files, make sure all files are in the same folder and that folder is unique to the package. Importing OVF files (in one package) from multiple locations is not supported.

CITRIX

Exporting VMs as an Appliance

You can use the XenServer OVF Appliance Export wizard to export one or more VMs as a virtual appliance package. A VM must be shut down before exporting it. It cannot be hibernating or in a suspended state.

You can export an individual VM or all shutdown VMs in a host or pool. You can also export all shutdown VMs associated with all hosts currently connected to XenCenter.

Creating appliance packages consists of five major tasks, which you perform using the XenServer OVF Appliance Export wizard:

1. Defining the name and destination of the appliance package.

2. Selecting the VMs for export.

3. Including one or more EULAs to protect the software inside the appliance package. (Optional.)

4. Configuring security for the exported package. (Optional.)

5. Configuring compression and other advanced export options, such as creating an OVA TAR file for the appliance.

Each task corresponds with a wizard page. Errors may appear on the Progress page if the export is unsuccessful.

Importing Appliances

The OVF Appliance Import wizard lets you import appliances from OVF or OVA packages. When you import the appliance, it recreates the VMs described in the package in the target location you specify. These newly recreated VMs are configured with the same resources as the original VMs.

> **Important:**
>
> 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.

Importing appliance packages consists of seven major tasks, which you perform with the XenServer OVF Appliance Wizard:

1. Selecting the package to import.

2. Reviewing (and accepting) the EULAs associated with the software in that appliance package.

3. Selecting the Home Server for the VMs.

4. Selecting the target location that you want to use as storage for the VMs in the package.

5. Selecting the network for the VMs in the package.

6. Providing responses for security settings in the package.

7. Running Operating System Fixups (enabled by default), a XenServer utility that fixes potential issues in the operating systems on the imported VMs.

Each task corresponds with a wizard page. Errors may appear on the Progress page if the import is unsuccessful.

Operating System Fixups

Using OVF as a packaging method does not guarantee that VMs created with one hypervisor will be compatible with another. For example, sometimes after the initial import, VM appliances and disk images imported from non-XenServer hypervisors fail to boot correctly on XenServer.

VMs may not boot or operate correctly for a variety of reasons including different interpretations of the OVF specification, guest operating system devices, and drivers specific to a particular hypervisor.

CITRIX

To help resolve these issues, XenCenter includes an automatically booting ISO image known as the *Operating System Fixups* feature, which is an option in the OVF Appliance Import and Disk Image Import wizards. This option is enabled by default. This option is often required when you import Windows and Linux VMs from third-party OVF packages, such as ones from VMware products. When importing XenServer or certain WIM content, enabling this option is optional.

The Operating System Fixup feature attempts to repair specific problems with the imported system that might prevent the operating system of the VM from booting. Operating System Fixups creates a basic level of interoperability for OVF packages and disk images that originated on non-XenServer platforms.

When Operating System Fixups runs, the OVF Appliance Import and Disk Image Import wizards attach a bootable ISO to the DVD drive of the imported system. After import, when the VM is started, the ISO performs the repairs and then shuts down the VM. When the next time you start the VM, the VM starts normally.

Depending on the guest operating system and original hypervisor host, additional configuration changes, driver installation, or other actions may be required following using the fixup option.

> **Tip:**
>
> See CTX124961, *Operating System Fixup in the XenCenter 5.6 OVF Appliance Plug-in* for additional troubleshooting information.

Requirements

To run Operating System Fixups, you must have an ISO SR configured at the target XenServer or XenServer pool. If you do not have an ISO SR configured, you are prompted to configure and specify one.

> **Note:**
>
> XenServer does not support sharing a single ISO SR among many non-pooled XenServer hosts. It is preferred that your XenServer hosts are in a pool and the ISO SR is created to be used by all hosts in that pool. Importing a multi-VM OVF package into a group of non-pooled XenServer hosts may result in failed import due to the Fixup ISO not being found on each XenServer. It is important to ensure that when using non-pooled XenServer hosts, that each host has a configured ISO SR with a Fixup ISO in the ISO SR.

1. Create an NFS or CIFS (Windows) share from a file server host.

2. Have a user account that has read/write access to this share.

3. Create an ISO SR (using the user account and share from above) using the CLI or XenCenter.

Importing Disk Images

The Disk Image Import wizard lets you import a disk image into one of your resource pools or into a specific host as a VM. When you import the disk image, the wizard creates a VM for it.

You might want to use this wizard when only a virtual disk image is available, and there is no OVF metadata associated with it. Situations when this might occur include:

• Migrating content from a XenDesktop VMware hosting infrastructure to a XenDesktop XenServer hosting infrastructure.

• The OVF metadata is not readable. However, it is still possible to import the disk image.

• You have a virtual disk that is not defined in an OVF package.

• You are moving from a platform that does not let you create an OVF appliance (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 MS Virtual Server 2005 content into XenServer.

When available, Citrix recommends importing appliance packages that contain OVF metadata and not just importing an individual disk image. The OVF data provides information the wizard needs to reconstitute a VM from its disk image, including the number of disk images associated with the VM, the processor, storage, network, and memory requirements and so on. Without this information, it can be much more complex and error-prone when trying to recreate the VM.

Importing disk images consists of two major tasks, which you perform with the XenServer Disk Image Import wizard:

1. Selecting a disk image to import.

2. Enter information for XenCenter to use to create the VM after the image is imported (that is, "defining" the VM).

> **Note:**
>
> Running Fixups on disk images may or may not be required. It is impossible to account for every potential device driver or other component installed and required by the original hardware platform (virtual or bare metal). In some cases, Fixups may not be able to ensure the disk imported will successfully boot as a XenServer VM. See CTX124961, *Operating System Fixup in the XenCenter 5.6 OVF Appliance Plug-in* for additional information regarding Fixup, operating systems and disk import types.

Supported Disk Image Formats

The Disk Image Import wizard supports importing the following formats:

• **Virtual Hard Disk (VHD)** is a universal virtual hard-disk file format that contains items similar to a physical hard drive, such as files, folders, and partitions. Often, VHD is used as the hard disk of a virtual machine.

• **Virtual Machine Disk (VMDK)**. The VMware virtual appliance file format for VMware products.

• **Virtual Disk Image (VDI)**. The Oracle default storage format for Virtual Box containers.

• **Windows Imaging Format (WIM)**. The Microsoft file-based disk image format used for its more recent operating systems (Windows 7, Windows Server 2008).

> **Tip:**
>
> If you are importing a WIM disk image, consider reading the following Citrix Knowledge Center article: *How to Build a Reference Virtual Machine for Deployment from WIM*. It is important to understand that the most recent Windows versions auto-detect hardware changes and do not need to run Fixups where as Windows Server 2003 and earlier do not have this capability. In these cases, you must know what type of disk controller the WIM has to know if Fixups are required. For WIM with IDE interfaces, Fixups should not be necessary. For WIM with SCSI interfaces, Fixups are required.

CITRIX®

Appendix A. Windows VM Release Notes

Release Notes

There are many versions and variations of Windows with different levels of support for the features provided by XenServer. This section lists notes and errata for the known differences.

General Windows Issues

- When installing Windows VMs, start off with no more than three virtual disks. Once the VM and XenServer 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 2 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 NIC will actually perform at the same rate as the physical NIC.

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.

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.

Windows 7

No known issues

Windows Vista

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

Windows 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

Release Notes

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

Debian Lenny 5.0

XenServer support for Debian Lenny makes use of support from the distribution to perform an installation into a virtual machine, in a similar manner to the other supported Linux distributions. This provides a more customizable configuration and native support for automation of the installation, and so on. Making use of these features is documented later in this guide. However this does mean that some configuration of VNC may have to be done manually if you want a graphical console.

> **Note:**
>
> Network installation support is provided by the distribution so HTTP and FTP installation is supported. Installation from a CD or DVD is also supported. Only 32-bit Debian Lenny is supported due to the upstream limitations.

To avoid receiving the message `There is no public key available for the following key IDs` when running **apt-get update**, run the following command to download the appropriate key:

```
wget -O - http://updates.vmd.citrix.com/XenServer/5.6 Service Pack 2/GPG-KEY \
| sudo apt-key add -
```

Red Hat Enterprise Linux 4.5 to 4.8

XenServer includes the RHEL 4.8 kernel with additional bug fixes and expanded Xen support. This kernel is installed with the XenServer Tools installation, but is not included if you install the Red Hat default RHEL 4.5 to 4.7 installations.

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)
- 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.
- 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]

- 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]

- 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]

Preparing a RHEL 4.5 to 4.8 guest for cloning

To prepare a RHEL 4.5 to 4.8 guest for cloning (see the section called "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).

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.

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]

When you install the XenServer `xe-guest-utilities` RPM, an entry is added to the yum configuration, allowing you to pick up kernel updates provided by Citrix when they become available.

> **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

Preparing a RHEL 5.x guest for cloning

To prepare a RHEL 5.x guest for cloning (see the section called "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).

CentOS 4

Please refer to the section called "Red Hat Enterprise Linux 4.5 to 4.8" for the list of CentOS 4 release notes.

Unlike RHEL4, CentOS includes a third-party updates mechanism known as yum. The `xe-guest-utilities` RPM will install a XenServer entry for `yum`, allowing you to pick up kernel updates provided by Citrix using the standard update mechanism as they become available.

CentOS 5

Please refer to the section called "Red Hat Enterprise Linux 5" for the list of CentOS 5 release notes.

Oracle Enterprise Linux 5

Please refer to the section called "Red Hat Enterprise Linux 5" for the list of Oracle Enterprise Linux 5 release notes.

SUSE Enterprise Linux 9

XenServer uses a SUSE-provided kernel. (Earlier versions of XenServer included a Citrix-provided version of the SLES9 which had a more mature version of the hypervisor, but which was out of date with the SUSE version, particularly with regard to security updates.) SUSE Enterprise Linux 9 VMs, with multiple VPCUs, are unable to use the suspend, resume and XenMotion functionality.

> **Note:**
>
> On upgrade from XenServer 5.5 to XenServer 5.6 we recommend that you should upgrade to the latest kernel from Novell.

To prepare a SUSE Linux guest for cloning (see the section called "MAC address"), edit `/etc/sysconfig/network/config` and edit the line:

`FORCE_PERSISTENT_NAMES=yes`

to

CITRIX

```
FORCE_PERSISTENT_NAMES=no
```

SUSE Enterprise Linux 10 SP1

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

- A maximum of 3 virtual network interfaces is supported.

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

SUSE Enterprise Linux 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.

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.

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.

Enabling a graphical console on Debian Lenny VMs

The graphical console for Debian Lenny 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 Lenny 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):

    ```
    aptitude install vnc4server
    ```

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]` section as follows:

    ```
    [servers]
    0=VNC

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

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

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

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

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

> **Note:**
>
> Before setting up your Red Hat VMs for VNC, be sure that you have installed the Linux guest agent. See the section called "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.

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.

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 the section called "Checking runlevels" for further details.

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.

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 the section called "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.

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 the section called "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.

Checking for a VNC Server

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

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

```
rpm -q tightvnc
```

Enabling Remote Administration

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

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

   ```
   yast
   ```

2. Use the arrow keys to select **Network Services** in the left menu, then **Tab** to the right menu and use the arrow keys to select **Remote Administration**. Press **Enter**.

3. In the **Remote Administration** screen, **Tab** to the **Remote Administration Settings** section. Use the arrow keys to select **Allow Remote Administration** and press **Enter** to place an X in the check box.

4. **Tab** to the **Firewall Settings** section. Use the arrow keys to select **Open Port in Firewall** and press **Enter** to place an X in the check box.

5. **Tab** to the **Finish** button and press **Enter**.

6. A message box is displayed, telling you that you will need to restart the display manager for your settings to take effect. Press **Enter** to acknowledge the message.

7. The original top-level menu of `YaST` appears. **Tab** to the **Quit** button and press **Enter**.

Modifying the xinetd Configuration

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

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

   The file contains sections like the following:

   ```
   service vnc1
   {
   socket_type = stream
   protocol    = tcp
   wait        = no
   user        = nobody
   server      = /usr/X11R6/bin/Xvnc
   server_args = :42 -inetd -once -query localhost -geometry 1024x768 -depth 16
   type        = UNLISTED
   port        = 5901
   }
   ```

2. Edit the `port` line to read

   ```
   port = 5900
   ```

3. Save and close the file.

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

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

SUSE Linux uses runlevel 5 for graphical startup. If your remote desktop does not appear, verify that your VM is configured to start up in runlevel 5. Refer to the section called "Checking runlevels" for details.

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:

CITRIX®

```
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
    ```

Alternatively, you can disable the firewall until the next reboot by running the **rcSuSEfirewall2 stop** command, or permanently by using `YaST`. This can of course expose additional services to the outside world and reduce the overall security of your VM.

VNC Screen Resolution

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

1. Open the `/etc/xinetd.d/vnc` file with your preferred text editor and find the `service_vnc1` section (corresponding to `displayID` 1).

2. Edit the `geometry` argument in the `server-args` line to the desired display resolution. For example,

    ```
    server_args  = :42 -inetd -once -query localhost -geometry 800x600 -depth 16
    ```

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

3. Save and close the file.

4. Restart the VNC server:

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

Checking runlevels

Red Hat and SUSE Linux VMs use runlevel 5 for graphical startup. This section describes how to verify that your VM is configured to start up in runlevel 5 and how to change it if it is not.

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

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.

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.

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
```

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.

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.

CITRIX

Appendix F. Troubleshooting VM Problems

If you experience odd behavior, application crashes, or have other issues, 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.

Citrix provides two forms of support: you can get free self-help support on the Support site, or you may purchase our Support Services and directly submit requests by filing an online Support Case. Our free web-based resources include product documentation, a Knowledge Base, and discussion forums.

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 to send the crash dumps to Citrix.

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)
coredump_and_restart	record a core dump, then reboot the VM
coredump_and_destroy	record a core dump, leave VM halted
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=coredump_and_restart
    ```

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**.

CITRIX

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.

CITRIX

Index

C

Cloning VMs, 3, 21
Configuring VNC
    firewall settings, RHEL, 42
    firewall settings, SLES, 44
    for Red Hat VMs, 41
    for SUSE VMs, 43
Creating an ISO image, 40
Creating VMs
    From pre-configured template, 2
    installing OS from a CD or ISO, 2
    overview, 2
    Windows, 2

D

Drivers, Windows paravirtualized, 25

I

Importing VMs, 3
Installation server, for installing Red Hat VMs, 46

L

Limits, virtual disk space, 7
Linux
    guest agent, 18
    runlevels, 45

N

NFS server, mounting ISO from, 25

P

P2V
    Windows, 2
    XenConvert, 2
Physical to virtual conversion (see P2V)

R

Release notes
    Linux VMs, 36
    Windows VMs, 35
Remote Administration, SUSE Linux, 43

S

Sysprep, for preparing Windows VM for cloning
    sysprep, 28

T

Template
    definition of, 2
    pre-configured (Debian), 2
    Windows VMs, 2
Time handling, in Linux VMs

    time handling, in VMs, 27
Troubleshooting
    Linux VM boot problems, 49
    Linux VM general problems, 48
    Windows VM general problems, 48

V

Virtual devices, limitations on, 8
VMs
    installing by P2V, 2
    non-paravirtualized (Windows), 10
    Paravirtualized, 18, 21
    paravirtualized, 19
    Remote Desktop, 26

W

Windows
    multi-processor HAL, 10
    SMB/CIFS share, mounting ISO from, 25

X

XenConvert, 2