Xen Cloud Platform Virtual Machine Installation Guide

Release 0.1

0.1

Published October 2009

0.1 Edition

Xen Cloud Platform Virtual Machine Installation Guide: Release 0.1

Published October 2009

This product contains an embodiment of the following patent pending intellectual property of Xen.org:

1. United States Non-Provisional Utility Patent Application Serial Number 11/487,945, filed on July 17, 2006, and entitled “Using Writeable Page Tables for Memory Address Translation in a Hypervisor Environment”.
2. United States Non-Provisional Utility Patent Application Serial Number 11/879,338, filed on July 17, 2007, and entitled “Tracking Current Time on Multiprocessor Hosts and Virtual Machines”.

Contents

Chapter 1. About this document

Overview

This document is a guide to creating Virtual Machines with Xen Cloud Platform™, the platform virtualization solution from Xen.org®. It describes the various methods of getting VMs up and running on Xen Cloud Platform hosts for each of the supported 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 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

How this Guide relates to other documentation

This document is primarily aimed at system administrators who need to set up deployments of Xen Cloud Platform VMs. Other documentation shipped with this release includes:

- *Xen Cloud Platform Installation Guide* provides step-by-step instructions on installing Xen Cloud Platform hosts;
- *Xen Cloud Platform Administrator's Guide* describes the tasks involved in configuring a Xen Cloud Platform deployment -- how to set up storage, networking and resource pools, and how to administer Xen Cloud Platform hosts using the xe command line interface (CLI).
- *Xen Cloud Platform Software Development Kit Guide* presents an overview of the Xen Cloud Platform SDK -- a selection of code samples that demonstrate how to write applications that interface with Xen Cloud Platform hosts.
- *XenAPI Specification* provides a programmer's reference guide to the Xen Cloud Platform API.
- *Release notes* provide a list of known issues that affect this release.

Chapter 2. Creating VMs

This chapter provides an overview of how VMs are created and lists virtual memory and virtual disk size minimums, describes the differences in virtual device support for the members of the Xen Cloud Platform product family. This chapter also discusses physical to virtual conversion (P2V), cloning templates, and importing previously-exported VMs.

Overview

VMs are created from *templates*. A template is a "gold image" that contains all the various configuration settings to instantiate a specific VM. Xen Cloud Platform ships with a base set of templates, which range from generic "raw" VMs that can boot an OS vendor installation CD or run an installation from a network repository to complete pre-configured OS instances.

Different operating systems require slightly different settings in order to run at their best. Xen Cloud Platform templates are tuned to maximize operating system performance.

The Linux templates create Pure Virtual (PV) guests, as opposed to the HVM guests created by the Windows and Other Install Media templates. Other Install Media template Linux installations are not supported.

There are three basic methods by which VMs are created using templates:

- using a complete pre-configured template.
- Installing from a CD or an *ISO image* onto the appropriate template.
- Installing from vendor media on a network installation server directly onto a template.

See Chapter 4, *Installing Linux VMs* to find out which methods are supported for which Linux flavor operating systems. Windows VMs can be installed from a CD or an ISO image.

Creating VMs by installing Windows operating systems onto the appropriate templates is described in Chapter 3, *Installing Windows VMs*.

Creating VMs by installing Linux operating systems onto the appropriate templates is described in Chapter 4, *Installing Linux VMs*.

Additionally, VMs can be created by:

- performing a physical to virtual (P2V) conversion on an existing physical server.
- importing an existing, exported VM
- converting an existing VM to a template

These methods are described in this chapter.

Virtual memory and disk size limits

In general, when installing VMs, be sure to follow the memory and disk space guidelines of the operating system and any relevant applications that you want to run when allocating resources such as memory and disk space.

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

Operating System	Minimum RAM	Maximum RAM	Disk space
Windows Server 2008 32-bit/64-bit	512MB minimum supported, 2GB or more recommended	32GB	Minimum 10GB, 40GB or more recommended
Windows Vista 32-bit	512MB minimum supported, 768MB or more recommended	32GB	16GB
Windows 2003	128MB minimum supported; 256MB or more recommended	32GB	2GB
Windows XP SP2/3	128MB minimum supported; 256MB or more recommended	32GB	1.5GB
Windows 2000 SP4	128MB minimum supported; 256MB or more recommended	32GB	2GB
CentOS 4.5, 4.6, 4.7	256MB	16GB	800MB
CentOS 5.0, 5.1, 5.2, 5.3	512MB	16GB	800MB
Red Hat Enterprise Linux 3.6	64MB	32GB	1.5GB
Red Hat Enterprise Linux 4.5, 4.6, 4.7	256MB	16GB	800MB
Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3	512MB	16GB	800MB
SUSE Linux Enterprise Server 9 SP2/3/4	256MB	32GB	1GB
SUSE Linux Enterprise Server 10 SP1/2, 11	512MB	32GB	1.5GB
Debian Etch	128MB	32GB	4GB
Debian Lenny	128MB	32GB	4GB

Xen Cloud Platform product family virtual device support

The current version of the Xen Cloud Platform 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. These limitations are noted in the individual guest installation section.

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

*except for SLES 10 SP1 and RHEL 3.x and 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 Citrix Tools for Virtual Machines. The same applies for Oracle and CentOS 5.0/5.1/5.2

Physical to Virtual Conversion (P2V)

Physical to Virtual Conversion(P2V) is the process by which an existing operating system on a physical server -- its filesystem, configuration, and so on -- is turned into a virtualized instance of the same operating system and filesystem, transferred, instantiated, and started as a VM on the Xen Cloud Platform 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 are automatically modified to make them able to run in a virtual environment. For more information, please refer to the XenConvert documentation for installation and usage guidelines.

For existing physical instances of Linux servers P2V conversion is accomplished by booting from the Xen Cloud Platform installation CD and choosing the **P2V** option. The filesystem is copied across the network onto a Xen Cloud Platform host, where it appears as a normal VM. Xen.org recommends that you perform P2V operations during off-peak hours because the process involves transferring a large amount of data, which could impact the performance of other Virtual Machines running on the Xen Cloud Platform host.

The P2V tool requires a 64-bit capable CPU by default. If you have an existing Linux instance on an older machine that you want to transfer using P2V, you can boot the CD using the *p2v-legacy* option at the initial prompt. This does require at least a PAE-enabled machine (Physical Address Extension), so for very old machines you can physically move the hard drive to a PAE-enabled machine and perform the operation from there.

To P2V an existing Linux server directly to a Xen Cloud Platform host

1. Reboot the physical server that you want to convert and boot from the Xen Cloud Platform installation CD. If the boot fails, start again and use the `p2v-legacy` option.
2. After the initial boot messages, the installer does some hardware detection and initialization, then presents a screen asking you to select which keyboard keymap you want to use for the installation. In this and the screens that follow, use **Tab** or **Alt+Tab** to move between elements, **Space** to select, and **F12** to move to the next screen.

   Select the desired keymap and choose **OK** to proceed.
3. Next, the **Welcome to Xen Cloud Platform** screen is displayed. Select **Convert an existing OS on this machine to a VM (P2V)** and click **OK** to proceed.
4. The **Welcome to XenServer P2V** screen is displayed. Click **OK** to proceed, and follow the on-screen prompts.

When the P2V process is complete and the new VM is created, you need to create and attach a VIF for it to have external network connectivity. Similarly, extra disks may also be added to take advantage of additional storage capacity available to the Xen Cloud Platform host.

Since the VM has new virtual network hardware, the MAC addresses it sees will also be different. Follow the Linux cloning guidelines (see the section called “Preparing to clone a Linux VM”) for customizing the configuration files to make the VM re-run any hardware detection scripts at startup.

General Guidelines for Virtualizing Physical Servers

When considering how to best begin virtualizing a collection of physical servers, it is best to gain some comfort level and experience with virtualizing servers that are more simply configured, moving later to servers with more complex configurations.

Good candidates typically include servers that are used for test and development environments, and servers used for in-house IT infrastructure (intranet web servers, DNS, NIS, other network services, and so on). Typically servers that are running CPU-intensive workloads (sophisticated mathematical modeling, video rendering) or are I/O-intensive (high-traffic commercial web sites, highly-used database servers, streaming audio/video servers) are not the best candidates for virtualization.

Once you have identified some physical servers that seem reasonable to work on first, examine how you are currently using them. What applications are they hosting? How I/O intensive are they? How CPU-intensive are they?

To make a reasonable assessment, gather a reasonable amount of data on the current physical servers that you are considering virtualizing. Look at system monitoring data for disk usage, CPU usage, memory usage, and network traffic, and consider both peak and average values.

Good candidates for virtualization are:

- servers whose CPU and memory usage and NIC and disk throughput are low will be more likely to coexist as a VM on a Xen Cloud Platform host with a few other VMs without unduly constraining its performance.

- servers that are a few years old - so their performance as VMs hosted on a newer server would be comparable to their existing state.
- servers that do not use any incompatible hardware which cannot be virtualized, such as dongles, serial or parallel ports, or other unsupported PCI cards (serial cards, cryptographic accelerators, and so on).

Once you have identified a set of machines that you want to virtualize, you should plan the process to accomplish the task. First, provision the physical servers that will serve as your Xen Cloud Platform hosts. The chief constraint on the number of VMs you can run per Xen Cloud Platform host is system memory.

Next, plan how you will create the VMs. Your choices are to P2V an existing server, install a fresh server from network-mounted vendor media, or install a base operating system using a pre-existing template.

If you P2V an existing server, it is best to P2V a test instance of the server, and run it in parallel with the existing physical server until you are satisfied that everything works properly in the virtual environment before re-purposing the existing physical machine.

Next, plan how to arrange the desired VMs on the Xen Cloud Platform hosts. Assign VMs to specific Xen Cloud Platform hosts, giving consideration to complementary resource consumption (mixing CPU-intensive and I/O-intensive workloads) and complementary peak usage patterns (for instance, assigning overnight batch processing and daytime interactive workloads to the same Xen Cloud Platform host).

For configuring individual VMs themselves, keep these guidelines in mind:

- assign only one core to a VMs unless the VM is serving a multi-threaded application that will perform demonstrably better with a second virtual CPU.
- when you configure the memory settings for a VM, consult the documentation of the guest operating system you plan to run on that VM and the documentation of the applications you plan to run on them.

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, but be sure to follow the appropriate preparation procedure for the VM (see the section called “Preparing to clone a Windows VM” for Windows and the section called “Preparing to clone a Linux VM” for Linux). Templates cannot be used as normal VMs.

Xen Cloud Platform has two mechanisms for cloning VMs: a full copy, or a faster Copy-on-Write (CoW) mode which only writes modified blocks to disk. The CoW mode 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, but 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.

Resource pools introduce some complexities around creating custom templates and cloning them. If you create a template on a server in a pool, and all virtual disks of the source VM are on shared storage repositories, the operation of cloning that template will be forwarded to any server in the pool that can see those shared SRs. However, if you create the template from a source VM that has any virtual disks on a local SR, then the 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 way to create additional VMs of a certain configuration. 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 Xen Cloud Platform host that 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 to clone a Windows VM” 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.

When VMs are imported Xen Cloud Platform re-attaches the VM VIFs to any network that has the same name as the network on the server that the VM was exported from. If no matching network can be found a new private network is created and the VM VIFs are attached to that.

Exporting a VM

An existing VM can be exported using the CLI. This section describes using the CLI.

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

To export a VM using the CLI

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

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

3. The export process might take some time to complete. When finished, the command prompt returns.

Importing a VM

An exported VM file can be imported using the CLI. This section describes using the CLI.

The following procedure assumes that you are administering the Xen Cloud Platform host using the CLI on a separate machine (that is, a machine that is not one of your Xen Cloud Platform hosts) where you maintain a library of export files.

To import a VM using the CLI

1. To import the VM to the default SR on the target Xen Cloud Platform 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 Xen Cloud Platform 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. The import process might take some time to complete. When finished, the command prompt returns the UUID of the newly-imported VM.

VM Block Devices

In the para-virtualized (PV) Linux case, block devices are passed through as PV devices. Xen Cloud Platform 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, Xen Cloud Platform emulates an IDE bus in the form of an `hd*` device. When using Windows, installing the Xen.org Tools for Virtual Machines installs a special PV driver that works in a similar way to Linux, except in a fully virtualized environment.

Chapter 3. Installing Windows VMs

Xen Cloud Platform allows you to install Windows 2000 SP4, Windows Server 2003 (32-/64-bit), Windows Server 2008, Windows XP SP2/3, or Windows Vista as a VM. Installing Windows VMs on a Xen Cloud Platform host requires hardware virtualization support (Intel VT or AMD-V).

The process of installing a Windows VM can be broken down into two main steps:

- installing the Windows operating system
- installing the *paravirtualized device drivers* known as the Xen.org Tools for Virtual Machines

Windows VMs are installed by cloning an appropriate template using the CLI. 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:

- **Windows Server 2008**
  can be used to install Windows Server 2008 32-bit.
- **Windows Server 2008 x64**
  can be used to install Windows Server 2008 64-bit.
- **Windows Server 2003**
  can be used to install Windows Server 2003 32-bit SP0, SP1, SP2, and R2. The Server, Enterprise, Data Centre, and SBS editions are supported.
- **Windows Server 2003 x64**
  can be used to install Windows Server 2003 64-bit. The Server, Enterprise, Data Centre, and SBS editions are supported.
- **Windows Server 2003, optimized for Citrix XenApp**
  can be 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**
  can be used to install Windows Server 2003 64-bit. The Server, Enterprise, Data Centre, and SBS editions are supported. This template is specially tuned to optimize XenApp performance.
- **Windows 2000 SP4**
  can be used to install Windows 2000 Server Service Pack 4. Earlier service packs are not supported.
- **Windows Vista**
  can be used to install Windows Vista 32-bit. The *Enterprise* edition is supported.
- **Windows XP SP3**

can be used to install Windows XP Service Pack 3. Earlier service packs are not supported.

- **Windows XP SP2**
  can be used to install Windows XP Service Pack 2. Earlier service packs are not supported.

The Windows VM can be installed either from an install CD in a physical CD-ROM on the Xen Cloud Platform host, or from an ISO image of your Windows media. See Appendix A, *Creating ISO images* for information on how to make an ISO image from a Windows install CD and make it available for use.

Making the ISO available to Xen Cloud Platform hosts

To make an ISO library available to Xen Cloud Platform 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.

Connect to the host console and run the command:

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

Additional arguments to the mount command may be passed in, for advanced use.

If making a Windows SMB/CIFS share available to the Xen Cloud Platform host, connect to the host console and run the command:

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

The *unc_path* argument should have back-slashes replaces by forward-slashes. *-t cifs* can be used for CIFS instead of SMB. Examples:

```
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 ISOs in it should be available by name from CD images from the CLI commands. The ISO should be attached to an appropriate Windows template.

Copying ISOs to local storage

In Xen Cloud Platform 3.2 and earlier, ISOs could be copied directly to the control domain into the `/opt/xensource/packages/iso` directory. In Xen Cloud Platform 0.1 hosts, this directory is reserved for use of the built-in ISO images, and is *not intended for general use*. This directory is considered to be identical across hosts in a resource pool, and CD images may fail to attach if the contents are modified.

To use local ISO storage from the control domain

1. Log onto the host console.
2. Create a directory to copy the local ISOs into:

   ```
   mkdir -p /var/opt/xen/iso_import
   ```

3. Create an ISO storage repository:

```
xe sr-create name-label=<name> type=iso \
device-config:location=/var/opt/xen/iso_import/<name> \
device-config:legacy_mode=true content-type=iso
```

4. Copy the ISO images into this directory, taking care not to fill up the control domain filesystem.
5. Verify that the ISO image is available for use by using the **xe vdi-list** command.

Warning

Be extremely careful with copying ISOs directly onto the control domain filesystem, as it has limited space available. A network share is a much safer mechanism for storing large numbers of ISO images. If the control domain does fill up, unpredictable behavior will result.

Windows paravirtualized drivers

The Xen.org paravirtualized network and SCSI drivers (Xen.org Tools for Virtual Machines) provide high performance I/O services without the overhead of traditional device emulation. During the installation of a Windows operating system, Xen Cloud Platform 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.

After Windows is installed, install the Xen.org high-speed PV drivers. These are on an ISO available to the virtual CD-ROM drive of the Virtual Machine. These drivers replace the emulated devices and provide high-speed transport between Windows and the Xen Cloud Platform product family software.

Note

While a Windows VM functions without them, performance is significantly hampered unless these drivers are installed. Running Windows VMs without these drivers is *not* supported. Some features, such as live relocation across physical hosts, will only work with the PV drivers installed and active.

Attach the Windows PV drivers ISO 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 Xen.org Tools for Virtual Machines and prevent the system from re-booting 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 Xen.org Tools for Virtual Machines 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 Xen Cloud Platform 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 Xen Cloud Platform 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 reinstallation. They can be uninstalled separately from the PV drivers by using `uninstall-XenProvider.cmd` in the same directory.

Preparing to clone a Windows VM

Use the Windows utility **sysprep** to prepare a Windows VM for cloning. This is the only supported way to clone a Windows 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 162001, "Do not disk duplicate installed versions of Windows," 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 Xen.org Tools for Virtual Machines.

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. 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**, refer to the Microsoft TechNet page Windows System Preparation Tool.

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. Xen.org 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 (e.g. using a time-zone offset within the VM), then it will remember that. 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 Xen Cloud Platform to synchronize the guests.

When performing suspend/resume operations or live relocation using XenMotion, it is important to have up-to-date Windows PV drivers installed, as they notify the Windows kernel that a time synchronization is required after resuming (potentially on a different physical host).

Release Notes

There are many versions and variations of Windows with different levels of support for the features provided by Xen Cloud Platform. 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 Xen.org Tools for Virtual Machines 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 Xen.org Tools for Virtual Machines.

- 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 2003 Server

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 2008 Server

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 XP SP3

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

Windows 2000 Server

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.

Chapter 4. Installing Linux VMs

Xen Cloud Platform supports the installation of many Linux distributions as PV VMs. There are four installation mechanisms:

- complete distributions provided as built-in templates
- Physical-to-Virtual (P2V) conversion of an existing native instance (see the section called "Physical to Virtual Conversion (P2V)")
- using the vendor media in the server's physical DVD/CD drive
- using the vendor media to perform a network installation.

Installing Linux VMs requires the Linux Pack to be installed onto the Xen Cloud Platform host.

The supported Linux distributions are:

Distribution	Built-in	P2V	Vendor Install from CD	Vendor Install from network repository
Debian Lenny 5.0				X
Debian Etch 4.0	X			
Red Hat Enterprise Linux 3.6-3.8		X		
Red Hat Enterprise Linux 4.5-4.7			X	X
Red Hat Enterprise Linux 5.0-5.3 32-bit			X	X
Red Hat Enterprise Linux 5.0-5.3 64-bit			X	X
SUSE Linux Enterprise Server 9 SP1/2/3		X		
SUSE Linux Enterprise Server 9 SP4		X	X	X
SUSE Linux Enterprise Server 10 SP1/2 32-bit/64-bit			X	X
SUSE Linux Enterprise Server 11 32-bit/64-bit			X	X
CentOS 4.5, 4.6			X	X

Distribution	Built-in	P2V	Vendor Install from CD	Vendor Install from network repository
CentOS 4.7				X
CentOS 5.0-5.3 32-bit			X	X
CentOS 5.0-5.3 64-bit			X	X
Oracle Enterprise Linux 5.0-5.2 32-bit			X	X
Oracle Enterprise Linux 5.0-5.2 64-bit			X	X

Note

Distributions which use the same installation mechanism as Red Hat Enterprise Linux 5 (for example Fedora Core 6) might be successfully installed using the same template. However, distributions not present in the above list are *not* supported.

Installing Debian Etch

The template provided with Xen Cloud Platform can be used to directly create a VM running Debian Linux 4.0 (Etch) without the need for vendor installation media and without performing a P2V conversion of an existing physical server.

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

```
xe vm-install template=Debian\ Etch\ 4.0 new-name-label=<ExampleVM>
```

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.

Installing Debian Lenny

Debian Lenny is installed using the standard Debian installer, which supports installation into a PV VM (performance optimized). Use the xe CLI to install Debian Lenny either from a CD, or from a network repository over FTP or HTTP.

Installing a Debian Lenny VM using the xe CLI

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

```
xe vm-install template=Debian\ Lenny\ 5.0 new-name-label=<lenny-vm>
```

2. Specify the installation repository — this should be a standard 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 Xen.org recommends using a local mirror or apt proxy to avoid generating excessive network traffic or load on the central repositories.

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.

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 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.

Installing Red Hat, CentOS, and Oracle Linux from vendor media

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

- Red Hat Enterprise Linux 5.0-5.3, 32-bit
- Red Hat Enterprise Linux 5.0-5.3, 64-bit
- CentOS 4.5-4.6

- CentOS 5.0-5.3, 32-bit
- CentOS 5.0-5.3, 64-bit
- Oracle Enterprise Linux 5.0-5.2, 32-bit
- Oracle Enterprise Linux 5.0-5.2, 64-bit

Other Linux operating systems need to be installed from a network installation server. See the section called “Installing Linux from a network installation server to a VM”.

To install a supported Linux VM from vendor media using the CLI

1. Insert the vendor installation CD into the CD drive on the Xen Cloud Platform host.
2. Run the command **xe template-list** to find the name of the template corresponding to the OS you want to install.
3. Run the command:

   ```
   xe vm-install template="<template_name>" new-name-label=<name_for_vm>
   ```

   This command returns the UUID of the new VM.
4. Get the UUID of the root disk of the new VM:

   ```
   xe vbd-list vm-uuid=<vm_uuid> userdevice=0 params=uuid --minimal
   ```
5. Using the UUID returned, set the root disk to not be bootable:

   ```
   xe vbd-param-set uuid=<root_disk_uuid> bootable=false
   ```
6. Get the name of the physical CD drive on the Xen Cloud Platform host:

   ```
   xe cd-list
   ```

   The result of this command should give you something like SCSI 0:0:0:0 for the *name-label* field.
7. Add a virtual CD-ROM to the new VM using the Xen Cloud Platform 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
   ```
8. 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
   ```
9. Make the VBD of the virtual CD bootable:

   ```
   xe vbd-param-set uuid=<cd_drive_uuid> bootable=true
   ```
10. Set the install repository of the VM to be the CD drive:

    ```
    xe vm-param-set uuid=<vm_uuid> other-config:install-repository=cdrom
    ```
11. Start the VM

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

12. Open an SSH terminal and follow the steps to perform the OS installation.

Installing Linux from a network installation server to a VM

The Xen Cloud Platform guest installer allows you to install an operating system from a network-accessible copy of vendor media onto a VM. In preparation for installing from vendor media, you need to make an exploded network repository of your vendor media (*not* ISO images), exported over NFS, HTTP or FTP accessible to the Xen Cloud Platform host administration interface. See Appendix B, *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 Xen Cloud Platform 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>* or nfs://*<server>*/*<path>*

Using the CLI as per the instructions below, the appropriate form must be chosen manually. In the case of SUSE-based distributions this is the `nfs://<server>/<path>` style, and in the case of Red-Hat based distributions this is `nfs:<server>:/<path>`.

The Xen Cloud Platform **New VM** wizard provides an additional step for vendor-installable templates which prompts 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.

Note

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.

To install a Linux VM from a network-accessible copy of vendor media using the CLI

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. VNC and perform the OS installation.

Installing RHEL Linux using a Custom Kickstart File

1. Specify the kickstart file to use as a kernel command-line argument in the new VM wizard, exactly as it would be specified in the PXE config file, for example:

```
ks=http://server/fileksdevice=eth0
```

2. 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">
```

3. Set the repository location so Xen Cloud Platform 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>
```

Physical-to-Virtual Installation of a Linux VM

Older Linux distributions such as Red Hat Linux Enterprise 3.6 do not support Xen Cloud Platform directly, and are typically legacy installations which benefit from virtualization for the purposes of server consolidation or hardware upgrades. The Xen Cloud Platform P2V feature analyzes existing installations and converts them into VMs.

When an installation is converted into a VM using P2V (see the section called “Physical to Virtual Conversion (P2V)”), the kernel used is also automatically switched to a Xen Cloud Platform PV kernel. Xen Cloud Platform contains ports of the Red Hat Enterprise Linux 3/4 and SUSE Enterprise Linux 9 kernels to support the native Xen hypervisor interface directly. These kernels are present in the built-in `xs-tools.iso` image in the default CD list.

Warning

While a VM is in the process of being installed using P2V, do not attempt to perform any operations on it.

Guest Installation Network

During the installation of a VM using P2V, a special network is used to assign a temporary IP address to the VM to enable the installation to proceed. It is possible that the range of IP addresses used might conflict with real IP addresses already in use in your network. The default range of IP addresses is `192.168.128.1` to `192.168.128.254`, and the default netmask is `255.255.255.0`.

To change the guest installer network values

1. Open a console on the Xen Cloud Platform host.
2. Find the guest installer network:

   ```
   xe network-list
   ```

   The command returns the list of networks available to the Xen Cloud Platform host. The to use has the name-label *Guest installer network*.
3. Examine the *`other-config`* parameters of the guest installer network:

   ```
   xe network-param-list uuid=<guest_installer_network_uuid>
   ```

   The command returns a subset of the guest installer network parameters, including the *other-config* parameter. If the values are set to the default described above, you will see the line:

   ```
   other-config (MRW): is_guest_installer_network: true;
   ip_begin: 169.254.0.1; \
   ip_end: 169.254.255.254; netmask: 255.255.0.0
   ```
4. To change the IP address range the guest installer network will use, edit the *`ip_begin`*, *`ip_end`*, and *`netmask`* values as follows:

   ```
   xe network-param-set uuid=<guest_installer_network_uuid> \
   other-config:ip_begin=<desired_ip_range_beginning> \
   other-config:ip_end=<desired_ip_range_end> \
   other-config:netmask=<desired_netmask>
   ```

   Do *not* change the value of the parameter *`is_guest_installer_network`*.

Installing the Linux guest agent

Although all the supported Linux distributions are natively paravirtualized (and therefore do not need special drivers for full performance), Xen Cloud Platform includes a guest agent

which provides additional information about the VM to the host. This additional information includes:

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

It is important to install this agent and keep it up-to-date (see Chapter 5, *Updating VMs*) as you upgrade your Xen Cloud Platform host.

To install the guest agent

1. The files required are present on the built-in `xs-tools.iso` CD image.
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 reasonably expect. This is because they are not true CD-ROM devices, but normal devices. When the CD is ejected by 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.

Preparing to clone a Linux VM

When a Linux VM is cloned, some virtual hardware parameters are changed in the new VM. 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. This is not a problem in general 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

In some cases, the MAC address of the virtual network interface of a cloned VM is recorded in the network configuration files. After the VM is cloned, the new cloned VM has a different MAC address. Therefore, when started, the network does not come up automatically.

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. Meanwhile the VM is deliberately forcing this to be `eth1`. The result is that networking does not work.

If the VM uses persistent names, the best thing to do is to turn these rules off. If for some reason you do not want to turn persistent names off, be aware that you will need to reconfigure networking inside the VM in the usual way.

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.

Configuring VNC for VMs

With the exception of VMs based on the Debian Etch template, VMs might not be set up to support VNC by default. Before you can connect with a management 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 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:

```
/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 3 or 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 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 management console, 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 3, use **redhat-config-securitylevel-tui**.

   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 other management consoles, 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 checkbox.

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 checkbox.
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 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 management console, you need to allow traffic over the port that the VNC connection uses. By default, a VNC server listens for connections from a VNC viewer on TCP port `5900 + n`, where n is the display number (usually just zero). So a VNC server setup for Display-0 will listen on TCP port `5900`, Display-1 is `TCP-5901`, etc. Consult your firewall documentation to make sure these ports are open.

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

To open the VNC port on a SLES-based VMs firewall

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

```
yast
```

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

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

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
```

Setting up Debian Etch VMs for VNC

The built-in Debian Etch template comes pre-configured with VNC set up and ready use. However, the default VNC configuration in Debian does not permit the root administrator to log in by default. To log in through VNC, you can either:

- Log in to the text console and create a new, unprivileged user by running the **adduser** command. This is the recommended course of action.
- At the graphical console login prompt, select **Actions**, **Configure the Login Manager**, type in your root password, then select **Security**, **Allow local system administrator login**, and finally select **Close**.

If you need to reset the VNC password, run the command:

```
vnc4passwd /etc/vncpass
```

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.

Release Notes

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

Debian Lenny 5.0

Xen Cloud Platform 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, unlike Debian Etch, 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/0.1/GPG-KEY \
| sudo apt-key add -
```

Debian Etch 4.0

Xen Cloud Platform includes a custom Xen kernel for Debian VMs installed using the built-in template to provide full performance optimizations.

When a Debian VM is first booted, you are prompted for details such as hostname and root passwords. This prevents a freshly installed Debian guest from rebooting until the requested information is entered. In order to bypass the first-boot scripts and boot non-interactively, you must pass the *noninteractive* flag to the kernel arguments.

After installation, the time-zone in a Debian VM defaults to UTC (see the section called “Time handling in Linux VMs”). You can change the local value using the **tzconfig** command.

To prepare a Debian guest for cloning (see the section called “MAC address”), Ethernet name persistence must be disabled. For Debian Sarge and Etch VMs, name persistence is controlled through `/etc/udev/rules.d/z45_persistent-net-generator.rules`, which is used to generate `/etc/udev/rules.d/z25_persistent-net.rules`. To prepare an Etch VM for cloning, remove `/etc/udev/rules.d/z25_persistent-net.rules`:

```
rm -f /etc/udev/rules.d/z25_persistent-net.rules
```

Persistence is re-enabled on reboot. To permanently disable persistence, remove `/etc/udev/rules.d/z45_persistent-net-generator.rules`.

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://updatesv.vmd.citrix.com/XenServer/5.5.0/GPG-KEY \
| sudo apt-key add -
```

Red Hat Enterprise Linux 3

Xen Cloud Platform includes a custom port of the RHEL3.8 kernel with native Xen PV VM support. This kernel is installed during the P2V process for RHEL3.6-3.8 guests. Because the kernel is based on Linux 2.4, the following limitations apply:

- A maximum of 3 virtual network interfaces is supported.
- VMs with multiple VCPUs cannot be suspended. To suspend these VMs, reduce the number of VCPUs to 1 while the VM is halted.

Before performing a P2V conversion from an existing RHEL3 installation, ensure that the `/etc/fstab` file in the VM contains an entry for the `/boot` mount point. This partition contains the files which are changed by the P2V process to give the resulting VM a PV kernel.

Red Hat Enterprise Linux 4

Xen Cloud Platform includes the RHEL 4.7 kernel with additional bug fixes and expanded Xen support. This kernel is installed with the Xen.org Tools for Virtual Machines installation, but not in the RHEL 4.5/4.6/4.7 default installations.

The following issues have been reported upstream 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):

- 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. (Red Hat Bugzilla 429103).)
- The NetFront driver in the RHEL 4.5 and 4.6 kernel has issues with the `iptables` firewall due to the use of checksum offloading. To work around this issue, either install the Xen.org Tools for Virtual Machines or disable checksum offload on the VIF associated with the device in the control domain of the Xen Cloud Platform host on which your RHEL 4.6 VM runs. First determine the UUID of the VIF, by:

```
xe vif-list vm-name-label=examplevm
```

  Then disable checksum offload on the VIF:

```
xe vif-param-set uuid=<vif_uuid> other-config:ethtool-tx=off
```

- A maximum of 3 virtual network interfaces is supported.
- The Xen kernel in versions 4.5, 4.6 and 4.7 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)
- Occasional kernel crash on boot in `queue_work()` (Red Hat Bugzilla 246586)
- Incorrect network device initialization order can cause kernel panic on boot. (456653)
- Disks sometimes do not attach correctly on boot (Red Hat Bugzilla 247265)

- 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 2 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 Xen Cloud Platform 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 Xen.org Tools for Virtual Machines 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 Xen.org-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
```

Preparing a RHEL 4.x guest for cloning

To prepare a RHEL4 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).

Preparing a RHEL 4.x server for P2V

Before performing a P2V conversion from an existing RHEL4 installation, ensure that the `/etc/fstab` file on the VM contains an entry for the `/boot` mount point. This partition

contains the files which are changed by the P2V process to give the resulting VM a PV kernel.

After a successful P2V, some modifications may be needed in older Red Hat Linux 4.x distributions. To get LVM working on `xvd*` devices, add the following line under the `devices {` line in `/etc/lvm/lvm.conf`:

```
types = ["xvd", 16]
```

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

Xen Cloud Platform includes the RHEL 5.3 kernel with additional bug fixes and expanded Xen support. This kernel is installed with the Xen.org Tools for Virtual Machines installation, but not in the RHEL 5 default installations.

- 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. (Red Hat Bugzilla 429102).
- After resuming a suspended VM, it might crash with the message kernel BUG at mm/rmap.c:590! (Red Hat Bugzilla 294811)
- A maximum of 3 virtual network interfaces is supported in versions below 5.2. For 5.2 and above, 7 virtual network interfaces are supported.
- Random segmentation faults on loading ELF binaries (Red Hat Bugzilla 247261)
- Disks sometimes do not attach correctly on boot (Red Hat Bugzilla 247265). This has been fixed in Red Hat Enterprise Linux 5.1.
- Soft lockup messages after suspend/resume or live migration (Red Hat Bugzilla 250994). These messages are harmless, but there may be a period of inactivity in the guest during live migration as a result of the lockup.
- Network blackout during live relocation for up to a minute (Red Hat Bugzilla 251527). After migration is complete, the kernel sends a gratuitous ARP to cause ARP caches to be refreshed and minimize network downtime. However, carrier detect is delayed in the kernel and so there is a network blackout until the ARP caches expire or the guest generates an ARP for some other reason.
- RHEL 5.2 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 Xen Cloud Platform RHEL 5.2 guests are only allocated RAM addresses in the range below 64GiB by default. This may cause RHEL 5.2 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 5.2 VM can boot.

Once you have succeeded in booting your RHEL 5.2 VM, install the Xen.org Tools for Virtual Machines 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.

- When installing the Xen Cloud Platform PV tools you may encounter a warning such as `Header V3 DSA signature: NOKEY, key ID 37017186`. Installing the PV tools can cause one or more packages signed by Red Hat to be installed but by default Red Hat do not include the key used to sign their packages in the RPM database. To resolve this you can import the Red Hat release key using:

```
rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

before installing the tools. See the section titled *New RPM GPG Signing keys* in the RHEL release notes (i386, x86_64) for more information on Red Hat release signing keys.

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

CentOS 4

Please refer to the section called “Red Hat Enterprise Linux 4” 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 Xen Cloud Platform entry for `yum`, allowing you to pick up kernel updates provided by Xen.org 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

Xen Cloud Platform uses a SUSE-provided kernel. (Earlier versions of Xen Cloud Platform included a Xen.org-provided version of the SLES9 which had a more mature version of the hypervisor, but which was out of date with SUSE's version, particularly with regard to

security updates.) As a result, suspending and resuming a VM, and XenMotion, are not 100% reliable, especially with multiple VCPUs.

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

```
FORCE_PERSISTENT_NAMES=no
```

When you P2V a SLES 9 server, the networking configuration files that were present on the physical server will remain on the VM. You may wish to move these aside, or update them accordingly, when you add virtual interfaces to the VM.

SUSE Enterprise Linux 10 SP1

Xen Cloud Platform 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

Xen Cloud Platform 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 a future kernel update from Novell will resolve this issue.

Chapter 5. Updating VMs

This chapter discusses updating VMs with new Linux kernel revisions, updating Windows operating systems, applying Windows Service Packs, and updates to Xen Cloud Platform PV drivers and VM utilities.

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

- XenMotion of Windows VMs is not supported until the PV drivers are upgraded.
- Suspend/Resume of Windows VMs is not supported until the PV drivers are upgraded.
- The use of certain anti-virus and firewall applications can crash the Windows VM unless the PV drivers are upgraded.

Updating Windows operating systems

Warning

Before updating Windows operating systems you must uninstall the PV device drivers. 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. So if, for example, you have a Windows 2000 server, and you wish to update it to Windows 2003, you can insert the Windows 2003 installation CD in the CD drive and run the setup program to update it.

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

To uninstall the PV drivers

1. Select **Control Panel** from the **Start** menu.
2. In Windows XP, 2000, or 2003, select **Add or Remove Programs**.

   In Windows Vista, select **Programs**, then select **Programs and Features**.
3. A list of programs installed on the computer is displayed. Scroll down if necessary and select **Xen.org Xen Cloud Platform Windows PV drivers Add-on**.
4. In Windows XP, 2000, or 2003, click the **Remove** button.

   In Windows Vista, select **Uninstall** from the toolbar above the list of programs.

   This removes the PV drivers add-on. When the operation completes a message is displayed. Click **OK** to close the message box.

Once the operating system update is complete, reinstall the PV drivers just as you would after installing a fresh Windows VM. See the section called “Windows paravirtualized drivers” for details.

Updating Linux kernels and guest utilities

The Linux guest utilities can be updated by re-running the `Linux/install.sh` script from the built-in `xs-tools.iso` CD image (see the section called “Installing the Linux guest agent”). From time to time, Xen.org also supplies updated Linux kernels for supported distributions.

The updates are posted online at: http://www.xen.org/.

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

Note

RHEL 4 in particular does not use `yum`.

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

Note

SLES is also supported, but Xen.org does not provide an updated kernel.

Appendix A. Creating ISO images

Xen Cloud Platform 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, Windows 2000, and Windows Server 2003. Once installed, right-click on a CD/DVD drive and select **Create image from CD** from the context menu.

Appendix B. 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.

Appendix C. 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 you track and resolve the issue.

Troubleshooting of installation issues is covered in the *Xen Cloud Platform Installation Guide*. Troubleshooting of Xen Cloud Platform host issues is covered in the *Xen Cloud Platform Administrator's Guide*.

Xen.org provides various types of support: Support site.

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 Xen.org.

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 Xen Cloud Platform 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**.

Troubleshooting boot problems on Linux VMs

There is a utility script named **xe-edit-bootloader** in the Xen Cloud Platform 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.

Index

R

S

T

V

W

X