Orchestration Installation Guide

Cloud Manager 2.1.5

January 31, 2012

Legal Notice

Contents

About This Guide

This guide provides instructions for installing and configuring a NetIQ Cloud Manager system. It includes the following sections:

Intended Audience

This information is intended for anyone who is assigned the Cloud Administrator role for a NetIQ Cloud Manager system. Consumers of this information should be experienced Linux and Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Additional Documentation

For other NetIQ Cloud Manager documentation, see the NetIQ Cloud Manager 2.*x* documentation site (https://www.netiq.com/documentation/cloudmanager2/).

Formatting Conventions

Cloud Manager product documentation uses consistent formatting conventions to help you recognize and differentiate items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Italics	◆ Titles or menu items from the user interface ◆ Book and CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value]*	◆ Optional parameters of a command
Braces, such as *{value}*	◆ Required parameters of a command
Logical OR, such as *value1|value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. We want to hear your comments and suggestions about this manual and the other documentation included with this product.

- Please use the *User Comments* feature at the bottom of each page of the online documentation to provide specific feedback about the content on that page. A documentation representative will contact you via e-mail with a resolution to the documentation problem within five business days.
- If you have more general suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Orchestration Components Preinstallation Tasks

Before you install the NetIQ Cloud Manager Orchestration components, you need to prepare the environment where those are to be installed:

- Section 1.1, “Gathering Certificate and License Information,” on page 11
- Section 1.2, “Preparing the Server When Multiple NICs and DNS Addresses Exist,” on page 11

1.1 Gathering Certificate and License Information

Before you install NetIQ Cloud Manager, you need to have the following information available:

- A license key (90-day evaluation license or a full license) is required to use the Cloud Manager Orchestration Server. You should have received this key from NetIQ, then you should have subsequently copied it to the network location that you identify during the pattern installation. Be sure to include the name of the license file in the path.

  If you install or configure Orchestration components by using a trial key, the product behaves normally for 90 days, although the trial key controls the number of users and managed nodes you can configure. For fully supported functionality, product components require a purchased license key. Contact your NetIQ Sales Representative or a Certified NetIQPartner for purchase information.
- (Optional) Certificate authority information (internal, or signed certificate, private key, and public certificate).

1.2 Preparing the Server When Multiple NICs and DNS Addresses Exist

If your anticipated Cloud Manager Orchestration Server has multiple network interfaces and multiple DNS addresses, you need to edit the `/etc/hosts` file on the server to change the default (127.0.0.1 or 127.0.0.2) address to the actual IP address of the server. This is necessary because at server startup, the Orchestration Server tries to determine the `matrix.hostname.full` fact. If the IP address of the hostname is found to be a loopback address (for example, 127.0.0.2), it is skipped and subsequently configured incorrectly.

If this change is not made, the *Install Agent* action performed on a VM misconfigures the VM to point to the wrong address (because the grid’s `matrix.hostname.full` fact is incorrect), resulting in no connection to the server.

2 Installing Cloud Manager Orchestration Components

The RPMs in the Orchestration install patterns must be installed to a supported version of SUSE Linux Enterprise Server (SLES) 11.

Some Cloud Manager RPMs have dependencies on SLES patterns that might not have been previously installed on the SLES server. For this reason, we recommend that you mount the SLES install media in a CD ROM drive on the server while you install the Cloud Manager packages, either from another CD ROM drive on the same server or from a downloaded ISO image.

- Section 2.1, “SLES 11 Standard Installation,” on page 14
- Section 2.2, “Alternative Installation Methods for the Orchestration Agent,” on page 15
- Section 2.3, “Alternative Installation Methods for the Orchestration Console and Clients,” on page 19
- Section 2.4, “Alternative Installation Methods for the Cloud Manager Monitoring Agent,” on page 22

After the initial installation and configuration, installers for some Cloud Manager Orchestration components for other operating systems become available in the Orchestration file system. For more information about these alternative post-installation methods, see Section 2.2, “Alternative Installation Methods for the Orchestration Agent,” on page 15, Section 2.3, “Alternative Installation Methods for the Orchestration Console and Clients,” on page 19, and Section 2.4, “Alternative Installation Methods for the Cloud Manager Monitoring Agent,” on page 22.

NetIQ recommends that you install and configure the Cloud Manager Orchestration components before continuing with the installation and configuration of Cloud Manager components. For more information, see the *NetIQ Cloud Manager 2.1.5 Application Server Installation Guide*.

For information about automated methods you can use to install the Orchestration Agent see Appendix A, “Advanced Agent Installation Methods,” on page 91.

For information about uninstalling Cloud Manager components, see Appendix C, “Uninstalling Orchestration Component Patterns from a SLES Server,” on page 99.

For advanced configuration tasks and methods for optimizing the Cloud Manager Orchestration components, see the *NetIQ Cloud Manager 2.1.5 Orchestration Administrator Reference*.

2.1 SLES 11 Standard Installation

The steps for installing Cloud Manager Orchestration components on a SLES 11 server, including the Orchestration Server, Orchestration Agent, the Orchestration Console (accompanied by other Orchestration clients), and the Cloud Manager Monitoring Server and Monitoring Agent are included in this section.

You should have already decided which SLES file packages you want to install, and on which machines. If not, the information in "Choosing the Installation Packages and Where to Install Them" in the *NetIQ Cloud Manager 2.1.5 Installation Planning Guide* can help you make that decision.

1 Log in to the target SLES server as `root`, then open YaST or YaST2. You should install the Orchestration Server on a dedicated server for optimal performance.

2 Download the appropriate NetIQ Cloud Manager ISO to the SLES server.

or

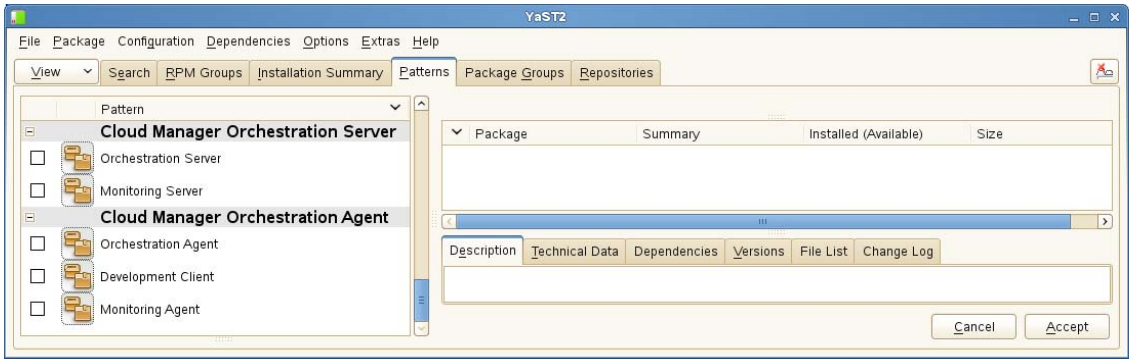
Load the NetIQ Cloud Manager DVD on the SLES server.

3 Define the NetIQ Cloud Manager ISO or DVD as an add-on product:

3a In the YaST Control Center, click *Software,* then click *Add-On Products*.

3b Click Add, select *Local ISO Image* or *DVD*, then follow the prompts to add the product.

4 Read and accept the license agreement, then click *Next* to display the Software Selection and System Tasks dialog box.



Cloud Manager Orchestration Server
- □ Orchestration Server
- □ Monitoring Server

Cloud Manager Orchestration Agent
- □ Orchestration Agent
- □ Development Client
- □ Monitoring Agent

5 Select the installation pattern that contains the Orchestration component packages you want to install on this server.

You should have previously decided which packages to install. For more information, see "Choosing the Installation Packages and Where to Install Them" in the *NetIQ Cloud Manager 2.1.5 Installation Planning Guide*.

6 Click *OK* to install the packages.

7 When package installation is complete, click *OK* to close the Installed Add-On Products dialog box.

2.2 Alternative Installation Methods for the Orchestration Agent

If you install the Cloud Manager Orchestration Server and the Cloud Manager Application Server, you also need to install the Orchestration Agent on a supported virtual or physical machine so that you can discover resources on such machines and then manage them by using either the Cloud Manager Web console or a Cloud Manager Mobile Client. This section includes information about the installation methods you can use that differ from the standard installation on a SLES machine.

The alternative agent installation methods vary depending on the platform you are installing to. You can install the agent on most SLES 11 servers, on most RHEL 5 or RHEL 6 servers, on most Windows 2003 or 2008 servers or the Windows 7 desktop. For exact requirements, see "Cloud Manager Orchestration Agent Requirements" in the *NetIQ Cloud Manager 2.1.5 Installation Planning Guide*.

Agents can be automatically installed on multiple computing resources or groups of computing resources by using your favorite configuration management software. For Windows installation, you can also build your own silent install script. For details about the installation options available for this kind of installation, see Appendix A, "Advanced Agent Installation Methods," on page 91

Windows Installation Source: The Windows installation program for the agent is located on the install media at `\Windows\zosagent_windows_3_1_5_with_jre.exe`. For information about installing the clients on a Windows machine, see Section 2.3.2, "Installing the Console and Clients on Windows," on page 21.

You can copy this file from the install media to the network, then copy it again to a supported Windows machine where you can run the installation program, or you can open the Administrator Information `.html` page in a Web browser. On this page, you can either run the program or download it to copy and run elsewhere. For more information about the Administrator Information page, see Section 2.2.1, "Obtaining the Agent Installer and Supporting Files from the Administrator Information Page," on page 16.

NOTE: Installation of the Orchestration Agent on a Windows machine does not install the Cloud Manager Monitoring Agent (gmond).

For Monitoring Agent installation information, see Section 2.4.2, "Installing the Cloud Manager Monitoring Agent On Windows Machines," on page 23.

Linux Installation Source: The manual installation procedure for the agent files on Linux depends on the operating system where you want to install them. For information about installing the clients on a Linux machine, see Section 2.3.2, "Installing the Console and Clients on Windows," on page 21.

This section includes the following information:

- Section 2.2.1, "Obtaining the Agent Installer and Supporting Files from the Administrator Information Page," on page 16
- Section 2.2.2, "Installing the Agent on Windows Machines," on page 17
- Section 2.2.3, "Manually Installing the Agent Packages on SLES Machines," on page 17
- Section 2.2.4, "Manually Installing the Agent Linux Packages on RHEL Machines," on page 18

2.2.1 Obtaining the Agent Installer and Supporting Files from the Administrator Information Page

After you install and configure the Orchestration Server on the network, you can launch the Administrator Information page. The page has links to various installer programs that you can use to install required Cloud Manager software on the computing resources that you will be utilizing in the grid system.

The following browsers support the Orchestration Server Administrator's Web page applications:

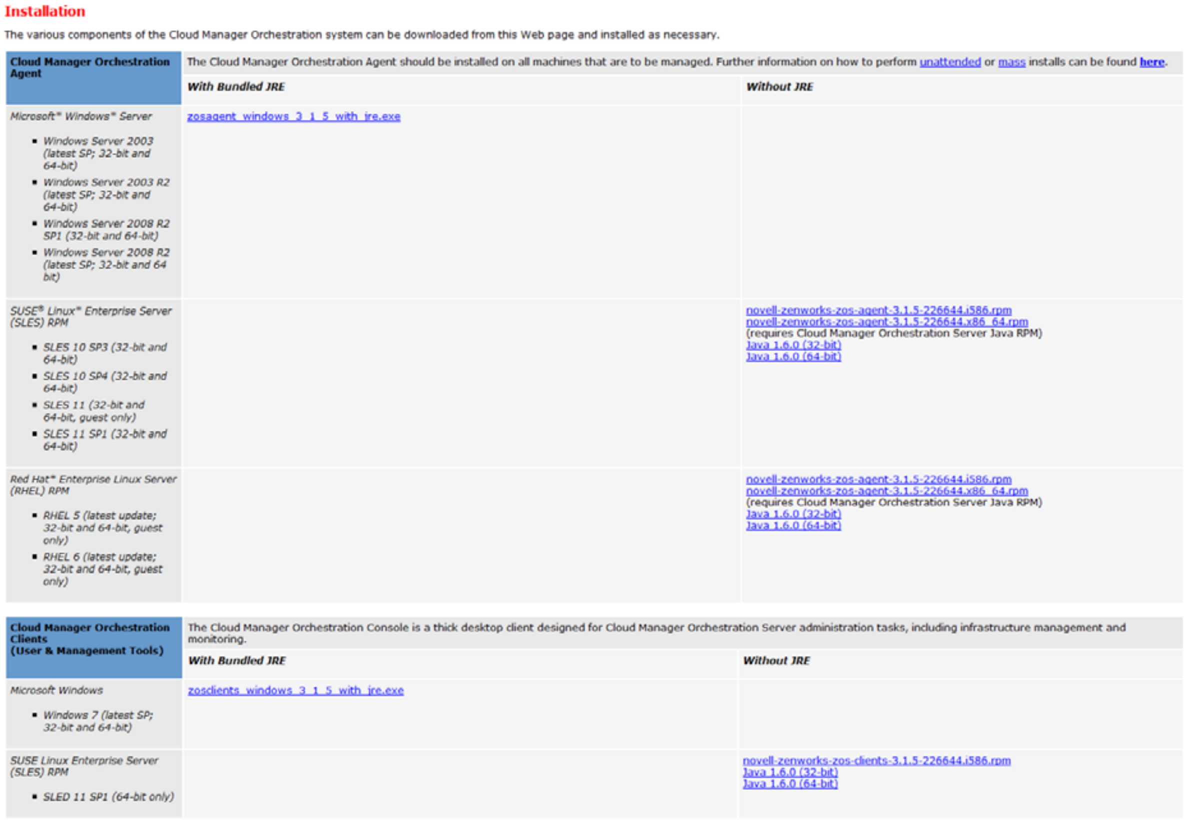
- Internet Explorer, version 6.0 or higher
- Netscape Navigator, version 6.0 or higher
- Firefox, version 1.5 or higher

Using a supported browser, enter the following URL to access the Administrator Information from the server:

```
http://Orchestration_Server_name:8001/
```

This URL is the DNS name (or IP address) of Orchestration Server. Be sure to use Port 8001 in the address to access and display the page, as shown in the following illustration:

Figure 2-1 *Administrator Information Page*



Installation

The various components of the Cloud Manager Orchestration system can be downloaded from this Web page and installed as necessary.

Cloud Manager Orchestration Agent	The Cloud Manager Orchestration Agent should be installed on all machines that are to be managed. Further information on how to perform unattended or mass installs can be found **here**.	
	With Bundled JRE	***Without JRE***
Microsoft® Windows® Server ▪ *Windows Server 2003 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2003 R2 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2008 R2 SP1 (32-bit and 64-bit)* ▪ *Windows Server 2008 R2 (latest SP; 32-bit and 64 bit)*	zosagent_windows_3_1_5_with_jre.exe	
SUSE® Linux® Enterprise Server (SLES) RPM ▪ *SLES 10 SP3 (32-bit and 64-bit)* ▪ *SLES 10 SP4 (32-bit and 64-bit)* ▪ *SLES 11 (32-bit and 64-bit, guest only)* ▪ *SLES 11 SP1 (32-bit and 64-bit)*		novell-zenworks-zos-agent-3.1.5-226644.i586.rpm novell-zenworks-zos-agent-3.1.5-226644.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)
Red Hat® Enterprise Linux Server (RHEL) RPM ▪ *RHEL 5 (latest update; 32-bit and 64-bit, guest only)* ▪ *RHEL 6 (latest update; 32-bit and 64-bit, guest only)*		novell-zenworks-zos-agent-3.1.5-226644.i586.rpm novell-zenworks-zos-agent-3.1.5-226644.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

Cloud Manager Orchestration Clients (User & Management Tools)	The Cloud Manager Orchestration Console is a thick desktop client designed for Cloud Manager Orchestration Server administration tasks, including infrastructure management and monitoring.	
	With Bundled JRE	***Without JRE***
Microsoft Windows ▪ *Windows 7 (latest SP; 32-bit and 64-bit)*	zosclients_windows_3_1_5_with_jre.exe	
SUSE Linux Enterprise Server (SLES) RPM ▪ *SLED 11 SP1 (64-bit only)*		novell-zenworks-zos-clients-3.1.5-226644.i586.rpm Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

The page includes links to information for Cloud Manager Orchestration Server administrators, including product documentation and the installers for the Orchestration Agent.

2.2.2 Installing the Agent on Windows Machines

Cloud Manager requires computing resources in order to run applications. The Orchestration Agent must be installed on each managed device to add that computing resource to the grid where the Orchestration Server can manage it.

Use the following steps to install the agent on a Windows computing resource:

1. At the location where you copied the Windows agent installer file (`zosagent_windows_3_1_5_with_jre.exe`), double-click the filename to run the installer.

   When you launch the installer on Windows XP or Windows Vista, a Security Warning for an Unknown Publisher is displayed. You can ignore this warning and run the installer without a problem.

   The welcome page of the Orchestration Agent Setup Wizard is displayed.
2. Click *Next* to display the Select Destination Directory dialog box.
3. Accept the default location, then click *Next* to display the Select Start Menu Folder page of the Setup Wizard.
4. Enter the path to the folder where you want the wizard to set up shortcuts to the Agent or select *Next* to accept the default and to display the Windows Services page.
5. Select the services you want to install (at a minimum, you must select *Install Service Orchestration Agent*), then click *Next* to display the Identify Orchestration Server page.
6. Enter the *Orchestration_Server_name* in the *Orchestration Server* field.

   You might find it easier to click *Discover* so that the installer searches for and finds the Orchestration Server on the network. If the installer discovers several servers, make sure you select the server you previously associated with this agent.
7. Click *Next* to display the Agent Configuration page.

   You can accept the defaults on this page of the Setup Wizard, or you can customize it according to your needs.
8. Click *Next* to run the Orchestration Agent installation until the Agent Setup Wizard completion page is displayed:.
9. Click *Finish* to exit the setup.
10. Register the agent to the Orchestration Console.

    For more information on how to register the agent, see Chapter 5, "Creating a Resource Account," on page 37.

2.2.3 Manually Installing the Agent Packages on SLES Machines

1. In the Orchestration Agent section, download:

```
novell-zenworks-zos-agent-3.1.5-<build_number>.i586.rpm
```

   - Java 1.6.0 (64-bit) RPM

2. Install the Java 1.6.0 RPM by entering the one of the following commands (as applicable):

   ```
   rpm -ivh novell-zenworks-zos-java-1.6.0_sun_update14-1.x86_64.rpm
   ```

   or

   ```
   rpm -ivh novell-zenworks-zos-java-1.6.0_sun_update14-1.i586.rpm
   ```
3. Install the Orchestration Agent by entering the following command:

```
rpm -ivh novell-zenworks-zos-agent-3.1.5-<build_number>.i586.rpm
```

4 Edit `/opt/novell/zenworks/zos/agent/agent.properties` to set the value of `zos.agent.server` to the IP address of the Orchestration Server where you want to register the agent.

5 Start the agent by entering the following command:

```
/etc/init.d/novell-zosagent start
```

2.2.4 Manually Installing the Agent Linux Packages on RHEL Machines

Because you won't be using the YaST utility to install Orchestration packages on RHEL machines, the information in this section can help you manually install those files on RHEL 5 or RHEL 6.

- "Required Agent Installation Files for RHEL Machines" on page 18
- "Manually Installing Orchestration Agents on RHEL 5" on page 18
- "Manually Installing Orchestration Agents on RHEL 6" on page 19

Required Agent Installation Files for RHEL Machines

The table below lists Orchestration Agent packages that you need to install on RHEL 5 or RHEL 6 servers. You can find them on the downloaded 32-bit or 64-bit ISO in the `/RHEL5` or `/RHEL6` directories.

Table 2-1 *Required RHEL Installation Packages for the Orchestration Agent*

Platform	Installation Package Name

RHEL 5 (64-bit)	`novell-zenworks-orch-config-3.1.5-<build_number>.noarch.rpm`
	`novell-zenworks-orch-config-gui-3.1.5-<build_number>.noarch.rpm`
	`novell-zenworks-zos-agent-3.1.5-<build_number>.x86_64.rpm`
	`novell-zenworks-zos-java-1.6.0_sun_update14-1.x86_64.rpm`

RHEL 6 (64-bit)	`novell-zenworks-orch-config-3.1.5-<build_number>.noarch.rpm`
	`novell-zenworks-orch-config-gui-3.1.5-<build_number>.noarch.rpm`
	`novell-zenworks-zos-agent-3.1.5-<build_number>.x86_64.rpm`
	`novell-zenworks-zos-java-1.6.0_sun_update14-1.x86_64.rpm`

Manually Installing Orchestration Agents on RHEL 5

To install the four packages required for the Orchestration Agent on RHEL 5:

1 Download the pertinent 64-bit Add-On ISO from the DVD.

2 Mount the ISO as a loopback device.

For example, if you are mounting a 64-bit SLES 11 ISO, the command is:

```
$ mount -o loop Cloud_Manager_Orchestration-3.1.5-SLE11.x86_64.iso /mnt
```

3 Change your working directory to the location of the RHEL package:

```
$ cd /mnt/RHEL5
```

4 Use the package manager included in RHEL to install the Orchestration Agent packages. (Missing dependencies are met by using RHN):

```
$ yum localinstall *.rpm
```

5 Run the configuration script:

```
$ /opt/novell/zenworks/orch/bin/config
```

See Section 3.3, "Configuring the Orchestration Agent," on page 28 for an explanation of the configuration for the Orchestration Agent.

Manually Installing Orchestration Agents on RHEL 6

To install the four packages of the Orchestration Agent on RHEL 6:

1 Download the pertinent 64-bit Add-On ISO from the DVD.

2 Mount the ISO as a loopback device.

For example, if you are mounting a 64-bit SLES 11 ISO, the command is:

```
$ mount -o loop Cloud_Manager_Orchestration-3.1.5-SLE11.x86_64.iso /mnt
```

3 Change your working directory to the location of the RHEL package:

```
$ cd /mnt/RHEL6
```

4 Use the package manager included in RHEL to install the Orchestration Agent packages. (Missing dependencies are met by using RHN):

```
$ yum localinstall *.rpm
```

5 Run the configuration script:

```
$ /opt/novell/zenworks/orch/bin/config
```

See Section 3.3, "Configuring the Orchestration Agent," on page 28 for an explanation of the configuration for the Orchestration Agent.

2.3 Alternative Installation Methods for the Orchestration Console and Clients

You can use the Cloud Manager Orchestration Console to administer the Orchestration Server from any SLES 11 server or Windows 7 desktop.

Windows Installation Source: The Windows installation program for the console and clients is located on the install media at `\Windows\zosclients_windows_3_1_5_with_jre.exe`. For information about installing the clients on a Windows machine, see Section 2.3.2, "Installing the Console and Clients on Windows," on page 21.

You can copy this file from the install media to the network, then copy it again to a supported Windows machine where you can run the installation program, or you can open the Administrator Information `.html` page in a Web browser. On this page, you can either run the program or download it to copy and run elsewhere.

Linux Installation Source: The manual installation procedure for the client files on Linux depends on the operating system where you want to install them. For information about installing the clients on a Linux machine, see Section 2.3.3, "Installing the Console and Clients on a SLES Server," on page 22.

2.3.1 Obtaining Installers from the Administrator Information Page

After you install the Orchestration Server on the network, you can launch the Administrator Information page. The page has links to various installer programs that you can use to install required Cloud Manager software on the computing resources that you will be utilizing in the grid system.

The following browsers support the Orchestration Server Administrator's Web page applications:

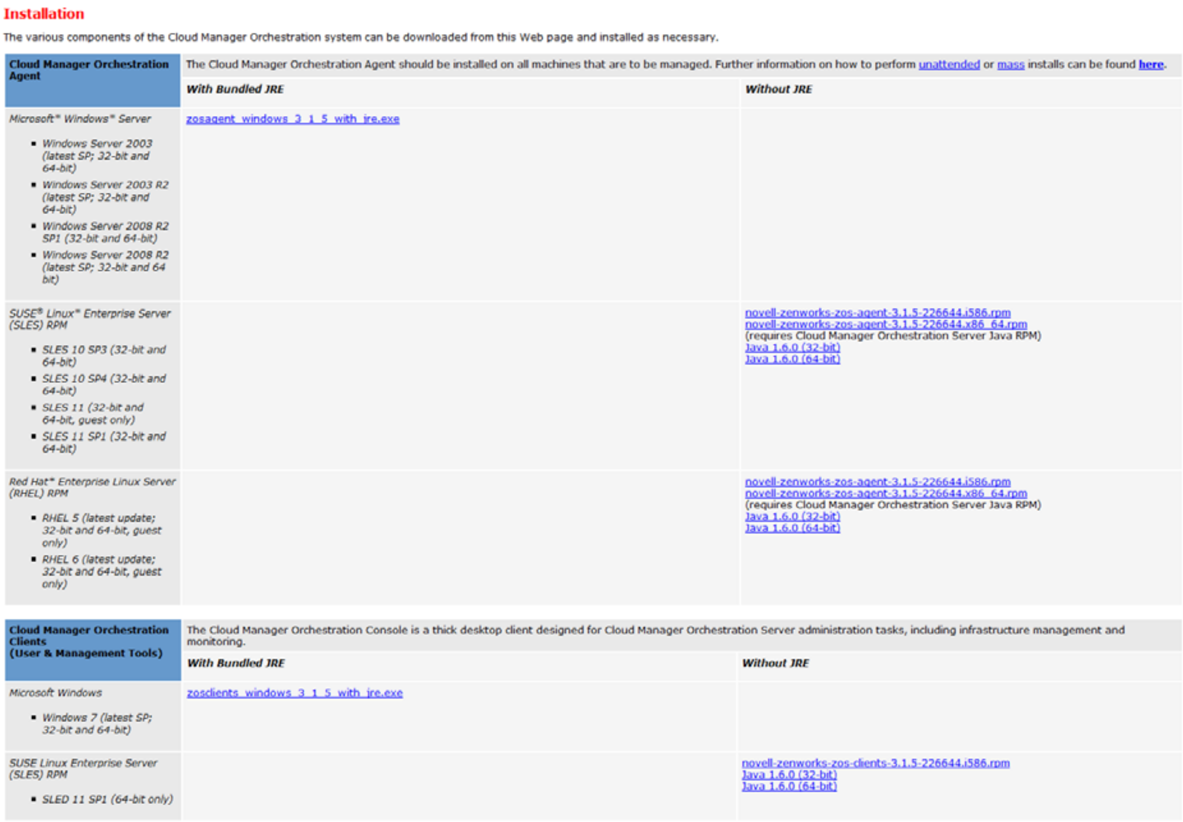
- Internet Explorer, version 6.0 or higher
- Netscape Navigator, version 6.0 or higher
- Firefox, version 1.5 or higher

Using a supported browser, enter the following URL to access the Administrator Information from the server:

`http://Orchestration_Server_name:8001/`

This URL is the DNS name (or IP address) of Orchestration Server. Be sure to use Port 8001 in the address to access and display the page, as shown in the following illustration:

Figure 2-2 *Administrator Information Page*



Installation

The various components of the Cloud Manager Orchestration system can be downloaded from this Web page and installed as necessary.

Cloud Manager Orchestration Agent	The Cloud Manager Orchestration Agent should be installed on all machines that are to be managed. Further information on how to perform unattended or mass installs can be found **here**.	
	With Bundled JRE	***Without JRE***
Microsoft® Windows® Server ▪ *Windows Server 2003 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2003 R2 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2008 R2 SP1 (32-bit and 64-bit)* ▪ *Windows Server 2008 R2 (latest SP; 32-bit and 64 bit)*	zosagent_windows_3_1_5_with_jre.exe	
SUSE® Linux® Enterprise Server (SLES) RPM ▪ *SLES 10 SP3 (32-bit and 64-bit)* ▪ *SLES 10 SP4 (32-bit and 64-bit)* ▪ *SLES 11 (32-bit and 64-bit, guest only)* ▪ *SLES 11 SP1 (32-bit and 64-bit)*		novell-zenworks-zos-agent-3.1.5-226644.i586.rpm novell-zenworks-zos-agent-3.1.5-226644.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)
Red Hat® Enterprise Linux Server (RHEL) RPM ▪ *RHEL 5 (latest update; 32-bit and 64-bit, guest only)* ▪ *RHEL 6 (latest update; 32-bit and 64-bit, guest only)*		novell-zenworks-zos-agent-3.1.5-226644.i586.rpm novell-zenworks-zos-agent-3.1.5-226644.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

Cloud Manager Orchestration Clients (User & Management Tools)	The Cloud Manager Orchestration Console is a thick desktop client designed for Cloud Manager Orchestration Server administration tasks, including infrastructure management and monitoring.	
	With Bundled JRE	***Without JRE***
Microsoft Windows ▪ *Windows 7 (latest SP; 32-bit and 64-bit)*	zosclients_windows_3_1_5_with_jre.exe	
SUSE Linux Enterprise Server (SLES) RPM ▪ *SLED 11 SP1 (64-bit only)*		novell-zenworks-zos-clients-3.1.5-226644.i586.rpm Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

The page includes links to Orchestration information for data center administrators, including links to product documentation and to the installers for the Orchestration Console and clients

2.3.2 Installing the Console and Clients on Windows

1 At a Windows 7 location where you downloaded the client installer file for Windows, double-click the `zosclients_windows_3_1_5_with_jre.exe` icon to run the installer.

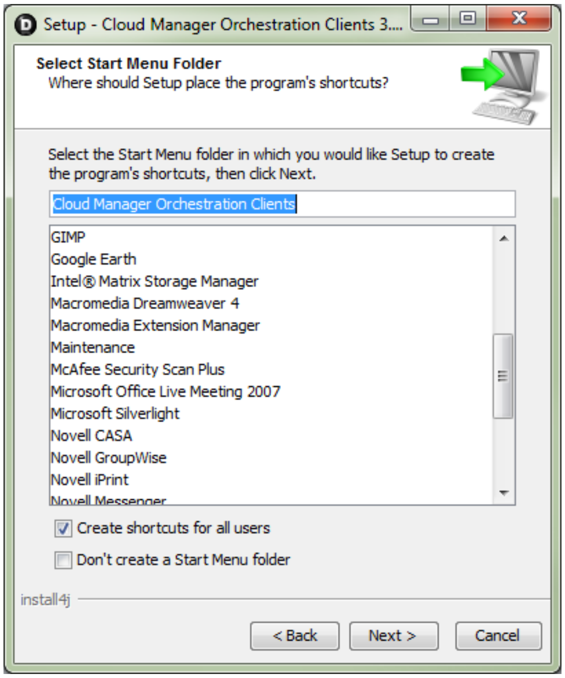
When you launch the installer, a Security Warning for an Unknown Publisher is displayed. You can ignore this warning and run the installer without a problem.

The first page of the Cloud Manager Orchestration Tools Setup Wizard is displayed.

2 Click *Next* to display the License Agreement page.

3 Accept the license agreement, then click *Next* to display the Select Destination Directory page.

4 Select the folder where you want to install the clients, then click *Next* to display the Select Start Menu folder page.



Select Start Menu Folder

Where should Setup place the program's shortcuts?

Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

Cloud Manager Orchestration Clients

GIMP
Google Earth
Intel® Matrix Storage Manager
Macromedia Dreamweaver 4
Macromedia Extension Manager
Maintenance
McAfee Security Scan Plus
Microsoft Office Live Meeting 2007
Microsoft Silverlight
Novell CASA
Novell GroupWise
Novell iPrint
Novell Messenger

☑ Create shortcuts for all users

□ Don't create a Start Menu folder

5 Select the Start Menu folder where you want the install program to create the client shortcuts, then click *Next* to begin the installation. The file extraction and copy process proceeds until the Cloud Manager Orchestration Tools Setup Completion page is displayed.

The following items are installed on the Windows machine:

- **Custom Orchestration Tools:** This includes the zos command line tool and a `.jar` file used to develop custom clients. The zos command line tool provides a non-Web method for a user to access the server.

  For more information, see the *NetIQ Cloud Manager 2.1.5 Orchestration Server Command Line Reference*.

- **Orchestration Console and Command Line:** This includes the Cloud Manager Orchestration Console, which is a thick client console for administrators. It also installs the zosadmin command line tool for administrators. Both of these tools require administrator login.

  For more information, see the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference* and the *NetIQ Cloud Manager 2.1.5 Orchestration Server Command Line Reference*.

6. Click *Finish* to exit the setup.

   Installing these components on a Windows workstation adds several items to the program group available from *Start* > *All Programs* > *Novell* > *ZOS* > *Clients*. One of these programs is the Orchestration Server Command Prompt. The PATH is preset in this prompt to run the zos and zosadmin commands.

2.3.3 Installing the Console and Clients on a SLES Server

1. In the Orchestration Clients section of the Administrator Information page, download:
   - `novell-zenworks-zos-clients-3.1.5-<build_number>.i586.rpm`
   - The Java 1.6.0 (64-bit) RPM
2. Install the Java 1.6.0 RPM by entering the following command:

```
rpm -ivh novell-zenworks-zos-java-1.6.0_sun_update14-1.x86_64.rpm
```

3. Install the Orchestration Console by entering the following command:

```
rpm -ivh novell-zenworks-zos-clients-3.1.5-<build_number>.i586.rpm
```

2.4 Alternative Installation Methods for the Cloud Manager Monitoring Agent

The Cloud Manager Monitoring Agent can be installed on a server where any other Orchestration pattern is installed or independently on a SLES or Windows server. The agent installation lays down the Ganglia Agent on each monitored node to collect performance metrics and send the data to the Cloud Manager Monitoring Server.

If you need to install Cloud Manager Monitoring Agent files without using the standard SLES installation script, the information in this section can help you identify the installation source files and give you some direction on how to install them to Linux or Windows machines.

- Section 2.4.1, “Installing the Cloud Manager Monitoring Agent on Linux Servers,” on page 22
- Section 2.4.2, “Installing the Cloud Manager Monitoring Agent On Windows Machines,” on page 23

For more information about agent installation, see Appendix A, “Advanced Agent Installation Methods,” on page 91.

2.4.1 Installing the Cloud Manager Monitoring Agent on Linux Servers

This section can help you identify the correct installation files for the Cloud Manager Monitoring Agent on the Cloud Manager product ISO and provide you with some installation instructions for installing those files on SLES or RHEL servers.

- “Cloud Manager Monitoring Agent Installation Files for Linux Servers” on page 22

Cloud Manager Monitoring Agent Installation Files for Linux Servers

The Cloud Manager Monitoring Agent uses both the agent program files

Table 2-2 Monitoring Agent Installation Pattern Files for Linux

Operating System	Installation File
SLES 11 SP2 (64-bit)	`<cd>/suse/setup/descr/zw_mon_agent-3.1.3-0.x86_64.pat`
RHEL 6 (latest update, 64-bit)	`<cd>/RHEL6/novell-zenworks-monitor-gmond-3.0.4-67.1.x86_64.rpm`
RHEL 5 (latest update, 64-bit)	`<cd>/RHEL5/novell-zenworks-monitor-gmond-3.0.4-67.1.x86_64.rpm`

2.4.2 Installing the Cloud Manager Monitoring Agent On Windows Machines

Installing the Cloud Manager Orchestration Agent on Microsoft Windows Server 2003 or Windows Server 2008 (see Section 2.2.2, "Installing the Agent on Windows Machines," on page 17) does not automatically install the Cloud Manager Monitoring Agent.

A separate installation package is available for installing the Monitoring Agent on Windows platforms where you have installed the Orchestration Agent.

This section includes the following information:

- "Installing the Cloud Manager Monitoring Agent for Windows" on page 23
- "Configuring the Monitoring Agent for Windows" on page 24

Installing the Cloud Manager Monitoring Agent for Windows

- "Hardware and Software Requirements" on page 23
- "Installing the Monitoring Agent" on page 23
- "Starting and Stopping the Monitoring Agent" on page 24
- "Uninstalling the Monitoring Agent" on page 24

Hardware and Software Requirements

The Cloud Manager Monitoring Agent (gmond) can be installed only on Windows Server 2003 or Windows Server 2008 machines where the Orchestration Agent is also installed. Only a 32-bit version of gmond is provided, but it will run normally on 64-bit systems. It requires the same minimum hardware configuration as the Orchestration Agent. Port 8649 must be available for gmond to communicate with the agent.

Installing the Monitoring Agent

Use these steps to install the Monitoring Agent as a service on a local Windows Server 2003 or Windows Server 2008 machine.

1. Download the pertinent Add-On ISO from the product DVD.
2. Create a CD from the ISO or use ISOBuster (or a similar tool) to mount the ISO.
3. Browse to the `Windows/` folder and search for the Cloud Manager Monitoring Agent.
4. Double-click the Monitoring Agent icon (`gmondsetup.exe`) and follow the wizard through the setup:

NOTE: You must be logged on as Administrator to run the installation program. If you are installing on Windows Server 2008, click *Accept* in the User Account Control dialog box to allow the installation to proceed as system administrator.

Starting and Stopping the Monitoring Agent

If you are logged on as the Windows administrator, you can start and stop the gmond service by using the Windows Services Control Panel.

1 From the desktop, click *My Computer*, select *Manage*, expand *Services and Applications*, expand *Services*, then right-click the gmond service object and choose the *Start* or *Stop* option as needed.

Uninstalling the Monitoring Agent

You can uninstall gmond by using the Add/Remove Programs utility in the Windows Control Panel. Uninstalling gmond automatically shuts down the gmond service prior to uninstalling.

Configuring the Monitoring Agent for Windows

This version of the Monitoring Agent uses the open source gmond 3.1.7 code. It is preconfigured to run only on a Windows local machine. It does not support multicasting. The installation includes a preconfigured `gmond.conf` that works only on the local host. You can manually edit `gmond.conf` for a different configuration, but your changes are not supported by Novell.

If you choose to customize an unsupported configuration for your needs, you can test the configuration by stopping the gmond service and then restarting gmond from the Windows command line prompt. Use the `-d` (debug) and `-f` (foreground) options to capture any error messages generated by the new configuration.

3 Configuring Cloud Manager Orchestration Components

This section discusses the basic configuration of all NetIQ Cloud Manager Orchestration components after each is installed. Component configuration is done either with a text-based configuration tool or with a GUI Wizard configuration tool.

The text-based configuration script detects which RPM patterns are installed, but the GUI Configuration Wizard requires that you specify the components to be configured, whether the patterns have been installed on the server or not.

It is possible to execute the text-based configuration file Orchestration components from the Cloud Manager configuration utility, but this occurs only if you install Cloud Manager Application components on the same server as the Cloud Manager Orchestration components, which is only likely if you are setting up your system for a demonstration.

Both the text-based tool and the GUI Wizard tool produce a configuration file that can be used to automatically reconfigure your system after an upgrade. If you use the tools to reconfigure your server after the original configuration has been done, make sure you reconfigure all of the components that are installed on the system (this is the default).

NOTE: Remember that the Cloud Manager Orchestration components are version 3.0. This might cause confusion because they are to be used with Cloud Manager Application components, which are version 2.0.

Some Considerations When Configuring with the GUI Wizard

If you have only a keyboard to navigate through the pages of the GUI Configuration Wizard, use the Tab key to shift the focus to a control you want to use (for example, a *Next* button), then press the Spacebar to activate this control.

When you have finished answering the configuration questions in the wizard, the Cloud Manager Orchestration Configuration Summary page displays. Although this page of the wizard lets you navigate by using the Tab key and the Spacebar, you need to use the Ctrl+Tab combination to navigate past the summary list. Click *Back* if you accidentally enter the summary list, and re-enter the page to navigate to the control buttons.

By default, the *Configure now* check box on the page is selected. If you accept this default, the wizard starts the Orchestration Server and applies the configuration settings. If you deselect the check box, the wizard writes out the configuration file to `/etc/opt/novell/novell_zenworks_orch_install.conf` without starting the Orchestration Server or applying the configuration settings.

You can use this `.conf` file to start the Orchestration Server or Agent and apply the settings either manually or with an installation script. Use the following command to run the configuration:

```
/opt/novell/zenworks/orch/bin/config -rs
```

This section includes the following information:

- Section 3.1, "Configuring the Orchestration Server," on page 26
- Section 3.2, "Configuring the Monitoring Server and Monitoring Agent," on page 28
- Section 3.3, "Configuring the Orchestration Agent," on page 28
- Section 3.4, "Validating and Optimizing the Orchestration Configuration," on page 30
- Section 3.5, "Configuring the Orchestration Server," on page 30
- Section 3.6, "Configuring the Monitoring Server and Monitoring Agent," on page 32
- Section 3.7, "Configuring the Orchestration Agent," on page 33

When the installation and configuration are complete, you need to validate and optimize the configuration. You can them proceed to register the resources to be managed by the Cloud Manager system. Refer to Chapter 5, "Creating a Resource Account," on page 37 for detailed information about getting resources to manage in the Cloud Manager system.

3.1 Configuring the Orchestration Server

Because so much of Cloud Manager's operations depends on the Orchestration Server, we recommend that you configure it before you configure any other Cloud Manager component.

1 Make sure you are ready with the information that you'll be prompted for during the configuration procedure (GUI or text-based):

Server Configuration Requirement	**Explanation and Action**
Configuration Type	Your answer here determines whether this configuration takes place on a standard installation or on a High Availability installation. This section discusses standard installation, so specify `s` (for `standard`) or press Enter to accept the default. For more information about High Availability configuration, see the *NetIQ Cloud Manager 2.1.5 Orchestration Server High Availability Configuration Guide*.
Server IP Address	You need to know the IP address of this server if you have multiple network interfaces. If specified, the server uses the specified hostname or IP address for binding RMI connections.
Grid Name	A grid is an administrative domain container holding all of the objects in your network or data center. The Orchestration Server monitors and manages these objects, including users, resources, and jobs. The grid name you create here is displayed as the name for the container placed at the root of the tree in the Explorer panel of the Orchestration Console.
Administrator User	The name you specify here is required when you access the Orchestration Console or the `zosadmin` command line interface. You should remember this username for future logins.
Administrator Password	The password you specify here is required when you access the Orchestration Console or the `zosadmin` command line interface. You should remember this username for future logins.

Server Configuration Requirement	Explanation and Action
Auditing Database JDBC URL	If you answer `yes` to this question, you need access to a relational database management system. We recommend that this database be installed on a different server from where you installed Cloud Manager. NetIQ has tested and supports only the PostgreSQL relational database as the audit database for this release of Cloud Manager. If you use a different RDBMS, no support or documentation is available from NetIQ. For more information, see "Configuring the Orchestration Server to Use an Audit Database" in the *NetIQ Cloud Manager 2.1.5 Orchestration Administrator Reference*.
Path to License File	A license key (90-day evaluation license or a full license) is required to use this product. You should have received this key from Novell, then you should have subsequently copied it to the network location that you specify here. Be sure to include the name of the license file in the path.
User Portal	This utility is no longer supported. Select the default and continue.
Admin Info Port	Port 8001 on the Orchestration Server provides access to an Administrator Information page that includes links to product documentation, agent and client installers, and product tools to help you understand and use the product. Specify another port number if 8001 is reserved for another use on this server.
Orchestration Agent Port	Port 8100 is used for communication between the Orchestration Server and the Orchestration Agent. Specify another port number if 8100 is reserved for another use. If your Orchestration Server communicates with ESX servers, we recommend you configure port 8101. This requires that you configure all other Orchestration Agents communicating with this server to use port 8101. This configuration parameter is considered an advanced setting for the Orchestration Server in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, you have the option of changing the default values. If you leave the check box deselected the setting is configured with normal defaults.
(Optional) Path to TLS Server Certificate and TLS Server Private Key	A PEM-encoded TLS certificate and key is needed for secure communication between the Orchestration Server and Orchestration Agent. If you do not want the Orchestration Server to generate a certificate and key for authentication, you need to provide the location of an existing certificate and key. This configuration parameter is considered an advanced setting for the Orchestration Server in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, this parameter is listed, but default values are provided only if the previous value is manually set to *no*.

2 At the computer where you installed the Cloud Manager Orchestration Server pattern, run the Cloud Manager Orchestration configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration.

3.2 Configuring the Monitoring Server and Monitoring Agent

The Cloud Manager Monitoring Server leverages open source (Ganglia) monitoring of the performance of certain data on network resources in a time period you define. The network resources being monitored must have the Cloud Manager Monitoring Agent installed.

1 Make sure you are ready with the information that you are prompted for during the Monitoring Server configuration procedure (GUI or text-based):

Server Configuration Requirement	Explanation and Action
Is this computer to be a Monitoring Server or a Monitored Node?	If you chose to install the Monitoring Server pattern, the Monitoring Agent pattern is installed on the same computer by default. You can also install the Monitoring Agent pattern independent of the Monitoring Server, but you should install it on the same node where you install an Orchestration Agent. The configuration lets you choose not to configure this computer as a Monitoring Server.
Hostname or IP Address of the Monitoring Server	You need to know the hostname or IP address of the server if you configured as the Cloud Manager Monitoring Server. Monitored nodes send their metrics to this address.
Monitored Computer Name	The descriptive name you designate appears in the monitoring interface as the name or location of the monitored node.

2 At the computer where you installed the Cloud Manager Monitoring Server or Cloud Manager Monitoring Agent pattern, run the configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration of the Monitoring Server or the Monitoring Agent.

3.3 Configuring the Orchestration Agent

The Cloud Manager Orchestration Agent manages the life cycle of VMs in your hypervisor environment under the direction of the Orchestration Server. You install the agent on computers where those VMs reside.

1 Make sure you are ready with the information that you'll be prompted for during the Monitoring Server configuration procedure (GUI or text-based):

Server Configuration Requirement	Explanation and Action
Configuration Type	Your answer here determines whether this configuration takes place on a standard installation or on a High Availability installation. This section discusses standard installation, so specify `s` (for `standard`) or press Enter to accept the default. For more information about High Availability configuration, see the *NetIQ Cloud Manager 2.1.5 Orchestration Server High Availability Configuration Guide*.
Agent Name	The Orchestration Agent requires a name to authenticate to the Orchestration Server.
Orchestration Server Hostname or IP Address	The DNS name or IP address of the Orchestration Server that this agent binds to.
Always Implement the Orchestration Server Certificate and Key?	The Agent relies on the Orchestration Server's TLS certificate as verification that it is communicating with the correct Orchestration Server. Decide whether you want to always trust the server certificate after the agent initially downloads it from the server, or if you want to exercise the certificate and key every time the agent connects to the server.
Is the Node a Physical or a Virtual Machine?	If the computer where you installed the agent is actually a VM, the Cloud Manager Server approaches its management in a unique way.
Agent Port	Port 8100 is used for communication between the Orchestration Server and the Orchestration Agent. Specify another port number if 8100 is reserved for another use. For an Agent installed on ESX, configure port 8101.
(Optional) Agent IP Address	You can specify a local bind address for the agent if you want to. If you specify an address, the agent tries to use this address locally when it connects to the Orchestration Server. If you don't specify an address, the operating system automatically sets the local address for each connection.
Path to Server Certificate	Specify the path to the Orchestration Server certificate file. The default path is `/root/zos_server_cert.pem`. **NOTE:** This configuration parameter is considered an advanced setting for the Orchestration Agent in the GUI Configuration Wizard, but only if you set *Provide Existing Orchestration Server Certificate* to *yes*.

2 At the computer where you installed the Cloud Manager Orchestration Agent pattern, run the configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration of the Orchestration Agent.

NOTE: Some configuration parameters for the agent are considered "advanced setting" in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, the setting is configured with normal defaults. Leaving the check box deselected lets you have the option of changing the default value.

You can also configure the agent as part of the silent installation procedure. See Section A.1, “Silent Installation of the Orchestration Agent,” on page 91.

3.4 Validating and Optimizing the Orchestration Configuration

1. Open the configuration log file (`/var/opt/novell/novell_zenworks_orch_install.log`) to make sure that the components were correctly configured.
2. Access the Administrator Information Page to verify that the Orchestration Server is installed and running. Use the following URL to open the page in a Web browser:

```
http://DNS_name_or_IP_address_of_Orchestration_Server:8001
```

   The Administrator Information page includes links to separate installation programs (installers) for the Orchestration Agent and the Orchestration Clients. The installers are used for various operating systems. You can download the installers and install the agent or the clients on any supported machine you choose. For more information, see Section 2.2.3, “Manually Installing the Agent Packages on SLES Machines,” on page 17.

If you installed the Orchestration Tools, you can increase the heap size that the JVM handles. This enables the console to manage a larger number of objects.

1. Open the `zoc` bash shell script at `/opt/novell/zenworks/zos/server/bin`.

   On Microsoft Windows, the path to the console is `program files\novell\zos\clients\bin\zoc.bat`. For more information, see Section 2.2.3, “Manually Installing the Agent Packages on SLES Machines,” on page 17.
2. Inside the script, find the following line where the JVM parameters are defined:

   ```
   JVMARGS="-Xmx256m -Xms256m -Xmn64m -XX:NewSize=64m -XX:MaxNewSize=64m"
   ```

   The `-Xmx` argument specifies the maximum heap size for the JVM. Increasing the heap size prevents a JVM out of memory condition.
3. Change the value in the `-Xmx` argument from 256MB to 512MB.

If you want to reconfigure the components of a Cloud Manager Orchestration system that you previously installed and configured, you can rerun the configuration script or the GUI Configuration Wizard and change your responses during the configuration process.

3.5 Configuring the Orchestration Server

Because so much of Cloud Manager’s operations depends on the Orchestration Server, we recommend that you configure it before you configure any other Cloud Manager component.

1. Make sure you are ready with the information that you’ll be prompted for during the configuration procedure (GUI or text-based):

Server Configuration Requirement	Explanation and Action
Configuration Type	Your answer here determines whether this configuration takes place on a standard installation or on a High Availability installation. This section discusses standard installation, so specify `s` (for `standard`) or press Enter to accept the default. For more information about High Availability configuration, see the *NetIQ Cloud Manager 2.1.5 Orchestration Server High Availability Configuration Guide*.
Server IP Address	You need to know the IP address of this server if you have multiple network interfaces. If specified, the server uses the specified hostname or IP address for binding RMI connections.
Grid Name	A grid is an administrative domain container holding all of the objects in your network or data center. The Orchestration Server monitors and manages these objects, including users, resources, and jobs. The grid name you create here is displayed as the name for the container placed at the root of the tree in the Explorer panel of the Orchestration Console.
Administrator User	The name you specify here is required when you access the Orchestration Console or the `zosadmin` command line interface. You should remember this username for future logins.
Administrator Password	The password you specify here is required when you access the Orchestration Console or the `zosadmin` command line interface. You should remember this username for future logins.
Auditing Database JDBC URL	If you answer `yes` to this question, you need access to a relational database management system. We recommend that this database be installed on a different server from where you installed Cloud Manager. NetIQ has tested and supports only the PostgreSQL relational database as the audit database for this release of Cloud Manager. If you use a different RDBMS, no support or documentation is available from NetIQ. For more information, see "Configuring the Orchestration Server to Use an Audit Database" in the *NetIQ Cloud Manager 2.1.5 Orchestration Administrator Reference*.
Path to License File	A license key (90-day evaluation license or a full license) is required to use this product. You should have received this key from Novell, then you should have subsequently copied it to the network location that you specify here. Be sure to include the name of the license file in the path.
User Portal	This utility is no longer supported. Select the default and continue.
Admin Info Port	Port 8001 on the Orchestration Server provides access to an Administrator Information page that includes links to product documentation, agent and client installers, and product tools to help you understand and use the product. Specify another port number if 8001 is reserved for another use on this server.

Server Configuration Requirement	Explanation and Action
Orchestration Agent Port	Port 8100 is used for communication between the Orchestration Server and the Orchestration Agent. Specify another port number if 8100 is reserved for another use. If your Orchestration Server communicates with ESX servers, we recommend you configure port 8101. This requires that you configure all other Orchestration Agents communicating with this server to use port 8101. This configuration parameter is considered an advanced setting for the Orchestration Server in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, you have the option of changing the default values. If you leave the check box deselected the setting is configured with normal defaults.
(Optional) Path to TLS Server Certificate and TLS Server Private Key	A PEM-encoded TLS certificate and key is needed for secure communication between the Orchestration Server and Orchestration Agent. If you do not want the Orchestration Server to generate a certificate and key for authentication, you need to provide the location of an existing certificate and key. This configuration parameter is considered an advanced setting for the Orchestration Server in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, this parameter is listed, but default values are provided only if the previous value is manually set to *no*.

2 At the computer where you installed the Cloud Manager Orchestration Server pattern, run the Cloud Manager Orchestration configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration.

3.6 Configuring the Monitoring Server and Monitoring Agent

The Cloud Manager Monitoring Server leverages open source (Ganglia) monitoring of the performance of certain data on network resources in a time period you define. The network resources being monitored must have the Cloud Manager Monitoring Agent installed.

All of the monitoring data is available for viewing in the Cloud Manager VM Client. You need to install the VM Client to make use of the monitoring data.

1 Make sure you are ready with the information that you are prompted for during the Monitoring Server configuration procedure (GUI or text-based):

Server Configuration Requirement	Explanation and Action
Is this computer to be a Monitoring Server or a Monitored Node?	If you chose to install the Monitoring Server pattern, the Monitoring Agent pattern is installed on the same computer by default. You can also install the Monitoring Agent pattern independent of the Monitoring Server, but you should install it on the same node where you install an Orchestration Agent. The configuration lets you choose not to configure this computer as a Monitoring Server.
Hostname or IP Address of the Monitoring Server	You need to know the hostname or IP address of the server if you configured as the Cloud Manager Monitoring Server. Monitored nodes send their metrics to this address.
Monitored Computer Name	The descriptive name you designate appears in the VM Client monitoring interface as the name or location of the monitored node.

2 At the computer where you installed the Cloud Manager Monitoring Server or Cloud Manager Monitoring Agent pattern, run the configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration of the Monitoring Server or the Monitoring Agent.

3.7 Configuring the Orchestration Agent

The Cloud Manager Orchestration Agent manages the life cycle of VMs in your hypervisor environment under the direction of the Orchestration Server. You install the agent on computers where those VMs reside.

1 Make sure you are ready with the information that you are prompted for during the Monitoring Server configuration procedure (GUI or text-based):

Server Configuration Requirement	Explanation and Action
Configuration Type	Your answer here determines whether this iconfiguration takes place on a standard installation or on a High Availability installation. This section discusses standard installation, so specify `s` (for `standard`) or press Enter to accept the default. For more information about High Availability configuration, see the *NetIQ Cloud Manager 2.1.5 Orchestration Server High Availability Configuration Guide*.
Agent Name	The Orchestration Agent requires a name to authenticate to the Orchestration Server.
Orchestration Server Hostname or IP Address	The DNS name or IP address of the Orchestration Server that this agent binds to.

Server Configuration Requirement	Explanation and Action
Always Implement the Orchestration Server Certificate and Key?	The Agent relies on the Orchestration Server's TLS certificate as verification that it is communicating with the corrrect Orchestration Server. Decide whether you want to always trust the server certificate after the agent initially downloads it from the server, or if you want to exercise the certificate and key every time the agent connects to the server.
Is the Node a Physical or a Virtual Machine?	If the computer where you installed the agent is actually a VM, the Cloud Manager Server approaches its management in a unique way.
Agent Port	Port 8100 is used for communication between the Orchestration Server and the Orchestration Agent. Specify another port number if 8100 is reserved for another use. For an Agent installed on ESX, configure port 8101.
(Optional) Agent IP Address	You can specify a local bind address for the agent if you want to. If you specify an address, the agent tries to use this address locally when it connects to the Orchestration Server. If you don't specify an address, the operating system automatically sets the local address for each connection.
Path to Server Certificate	Specify the path to the Orchestration Server certificate file. The default path is `/root/zos_server_cert.pem`. **NOTE:** This configuration parameter is considered an advanced setting for the Orchestration Agent in the GUI Configuration Wizard, but only if you set *Provide Existing Orchestration Server Certificate* to *yes*.

2 At the computer where you installed the Cloud Manager Orchestration Agent pattern, run the configuration utility:

```
/opt/novell/zenworks/orch/bin/config
```

or

```
/opt/novell/zenworks/orch/bin/guiconfig
```

3 Follow the prompts to complete the configuration of the Orchestration Agent.

NOTE: Some configuration parameters for the agent are considered "advanced setting" in the GUI Configuration Wizard. If you select the *Configure Advanced Settings* check box in the wizard, the setting is configured with normal defaults. Leaving the check box deselected lets you have the option of changing the default value.

You can also configure the agent as part of the silent installation procedure. See Section A.1, "Silent Installation of the Orchestration Agent," on page 91.

4 Launching the Orchestration Console and Logging in to the Orchestration Server

When you have installed and configured the Orchestration Server, you can launch and log in to the Orchestration Server Console.

- Section 4.1, "Launching the Orchestration Console," on page 35
- Section 4.2, "Logging In Explicitly to a Named Server," on page 36

NOTE: The Orchestration Server Console uses TCP port 1099 for its initial connection and then selects a port in the ephemeral port range (ports 32768-65535) for additional communications. If you have problems connecting to the orchestration console, ensure that these ports on the server are reachable from the client.

4.1 Launching the Orchestration Console

When the Orchestration Console is launched, it broadcasts throughout the network to discover all of the Orchestration Servers that have been previously installed. The server or servers are displayed at the root of the Explorer panel in the Orchestration Console.

To launch the Orchestration Console:

1. Navigate to the location where the Orchestration Console was installed:
   - **SLES:** Change to the following directory:

     ```
     /opt/novell/zenworks/zos/server/bin
     ```
   - **Windows:** In the *Start* menu, click *All Programs* > *Novell* > *ZOS* > *Clients*.
2. Launch the Orchestration Console:
   - **SLES:** Use the following command to launch the Orchestration Console:

     ```
     ./zoc
     ```
   - **Windows:** In the *Start* menu, click *Programs* > *Cloud Manager Orchestration Clients* submenu, then click *Cloud Manager Orchestration Console*.
3. In the Orchestration Console, log in to the Orchestration Server by selecting a server in the Explorer tree.

IMPORTANT: If you are not operating in a broadcast-capable network and you have installed the Orchestration Console on a machine with a different subnet from the server, the console might not be able to discover your Orchestration Server. See "Logging In Explicitly to a Named Server" on page 36 for the login procedure in this scenario.

4.2 Logging In Explicitly to a Named Server

If you do not see the Orchestration Server you want to log into in the Explorer tree, you must log in explicitly to the server you want.

1 In the Orchestration Console, click *Server,* then click *Login* to display the Remote Connection dialog box.

  Orchestrate supports multiple servers on the same network.

  This login option allows you to select the server before you enter the administrator name and password.

2 In the dialog box, specify the IP address of the Orchestration Server in the *Server Address* field, then click *OK* to display the login dialog box.

3 Specify the administrator name (created during the install) in the *Username* field, specify the administrator password in the *Password* field, then click *OK* to log in to the server.

5 Creating a Resource Account

After being installed on a computing node, having its credentials defined, and associating itself with the computing node, the Orchestration Agent begins broadcasting the availability of its host as a potential computing resource. Before the Orchestration Server can allow an agent to authenticate and establish ongoing communication, you need to create a resource account for the agent on the Orchestration Server. When this account is created or "registered," the agent's host node can be discovered and recognized as a computing resource that can perform the jobs assigned to it.

It is also possible to create a resource account for an agent before that agent is actually installed on a computing node.

You can create a resource account on the Orchestration Server and have it waiting in an offline state in anticipation of agent installation and login.

This section includes the information you need to create a resource account on the Orchestration Server:

- Section 5.1, "Opening the Resources Monitor," on page 38
- Section 5.2, "Automatically Registering a Resource," on page 38
- Section 5.3, "Selecting a Resource for Manual Registration," on page 39

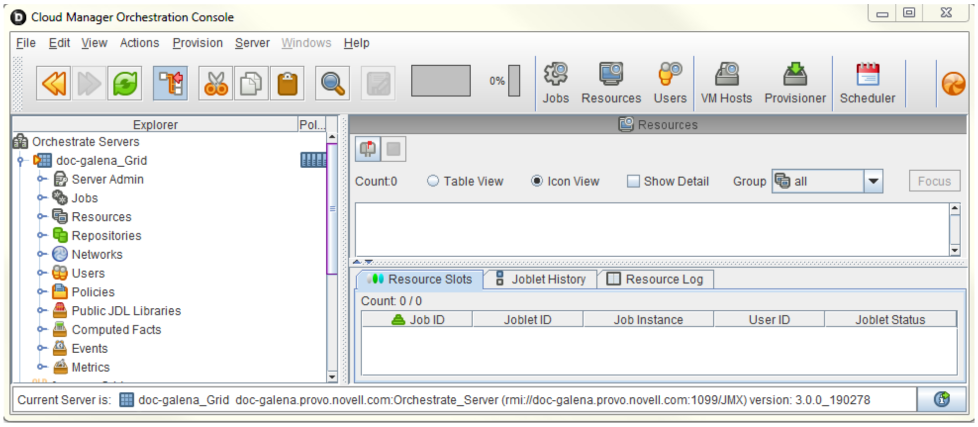
When resources are created, connected to the Orchestration Server and online, a provisioning adapter job deploys and runs a discovery process on its own.

For information about manually configuring a resource account, see Appendix B, "Manually Registering a Resource in the Orchestration Console," on page 95.

5.1 Opening the Resources Monitor

Now that you have installed an Orchestration Server and launched the Orchestration Console, you can begin to create resource accounts.

1 Open the Orchestration Console and click *Resources* to open the Resources Monitor in the admin view of the Orchestration Console.



Current Server is: doc-galena_Grid doc-galena.provo.novell.com:Orchestrate_Server (rmi://doc-galena.provo.novell.com:1099/JMX) version: 3.0.0_190278

From this monitor, you can see the resources that are connected to the server and what they are doing in the grid.

If an agent is installed but has not been registered (that is, no account is created for it), it attempts a server login every 90 seconds. If this is the case (as in the figure above), the Resource Registration icon has a "flag up" status, meaning that an agent is waiting to register. If the icon has a "flag down" status, either no Orchestration Agents have been installed in the network or all active agents are logged in, so none are waiting to register.

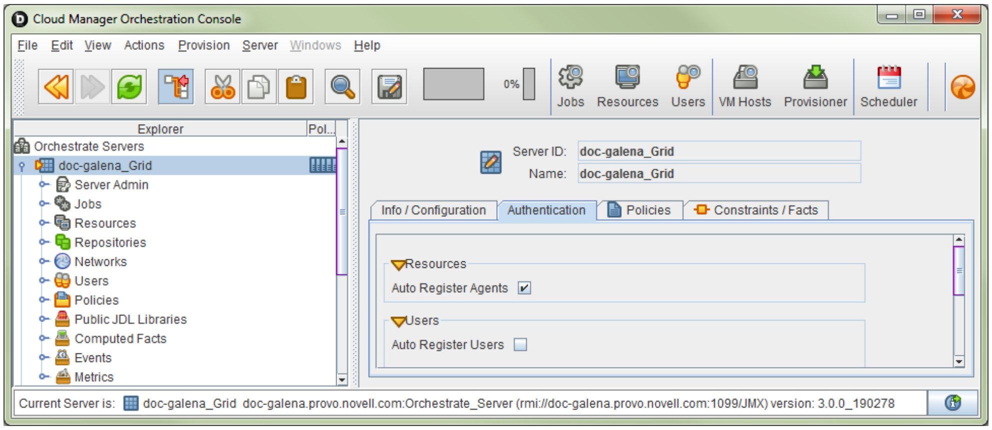
The Resources Monitor has many features to help you manage resources when they are registered, including the jobs and joblets assigned to individual resources. For more detailed information about the Resources Monitor, see "Monitoring Server Resources" in the *NetIQ Cloud Manager 2.1.5 Orchestration Administrator Reference*.

5.2 Automatically Registering a Resource

If your network environment does not require a high level of security (such as in a development and testing environment) and you want a quick way to create a resource account, you can do so at the Orchestration Console.

1 In the Orchestration Console, select the grid object in the Explorer tree to open the *Authentication* page in the admin view.

2 In the *Resources* section of the page, select the *Auto Register Agents* check box, then click the Save icon in the toolbar to save the setting.



Server ID: doc-galena_Grid
Name: doc-galena_Grid

Resources
Auto Register Agents ☑

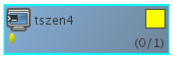
Users
Auto Register Users □

Current Server is: doc-galena_Grid doc-galena.provo.novell.com:Orchestrate_Server (rmi://doc-galena.provo.novell.com:1099/JMX) version: 3.0.0_190278

The resource object is created and registered in the Orchestration Server, although it is offline (the object is dimmed in the tree of the Explorer panel) until it the agent tries to log in.

The next time the agent tries to log in, it is automatically authenticated and the Orchestration Server creates a a new resource account.

When the resource is online, the Resources Monitor displays a labeled box representing the registered agent. This box includes information about the agent, including the number of available slots it has and a status color indicating its state of readiness for Cloud Manager jobs.



The status color window can be white (inactive), green (available for use), or blue (in use). If the color changes from green to blue, a job is running on this resource. To find out what kind of job is running, you can click the *Jobs* monitor button on the toolbar.

5.3 Selecting a Resource for Manual Registration

If you do not select the *Auto Register Agents* check box on the grid object's *Authentication* page, you have the option of explicitly accepting or denying the login attempts of a resource, thus preventing it from creating an account.

The following steps assume that you have already created a resource in your grid.

1 In the Resources Monitor, click the Resource Registration (mailbox) icon to open the Resource Registration Monitor dialog box.

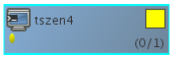
  This dialog box lets you preview the Orchestration Agents that are installed in the network and trying to log in to the server. The top row of radio buttons is a mass selector for all listed agents, allowing you the choice to accept, deny, or ignore automatic registration for all agents, both those currently listed and those that might try to log in later.

  If you want to choose the agents that can be allowed to auto register, you can visually identify the agent by name and select how you want to handle that agent's request for registration the next time it tries to log in.

2 For this example, select the *Accept* radio button adjacent to the agent you want to register, then click *OK*.

3 From the Orchestration Console, open the Resources Monitor to observe the resource object you created change from offline to online. When the object is no longer dimmed, the agent has logged in as a resource and is registered.

When the resource is online, the Resources Monitor displays a labeled box representing the registered agent. This box includes information about the agent, including the number of available slots it has and a status color indicating its state of readiness for Orchestrate jobs.



The status color window can be white (inactive), blue (in use), green (available for use), or blue (in use). If the color changes from green to blue, a job is running on this resource. To find out what kind of job is running, you can click on the *Jobs* monitor button on the toolbar.

6 Configuring Orchestration Provisioning Adapters

You can complete the configuration of the Cloud Manager Orchestration system by preparing it to receive information about the VMs it discovers in your installed hypervisor environment. This VM discovery is made possible when you configure the Orchestration provisioning adapter jobs for each hypervisor environment. This section discusses how to configure the pre-packaged provisioning adapters to discover VMs.

- Section 6.1, "Configuring the vsphere Provisioning Adapter," on page 41
- Section 6.2, "Configuring the Citrix XenServer Provisioning Adapter," on page 54
- Section 6.3, "Configuring the Hyper-V Provisioning Adapter," on page 60
- Section 6.4, "Configuring the SUSE Xen Provisioning Adapter," on page 62
- Section 6.5, "Configuring the KVM Provisioning Adapter," on page 63

6.1 Configuring the vsphere Provisioning Adapter

- Section 6.1.1, "Configuring the vSphere Provisioning Adapter to Discover VMs," on page 41
- Section 6.1.2, "Discovering Enterprise Resources in Multiple vSphere Environments," on page 50

6.1.1 Configuring the vSphere Provisioning Adapter to Discover VMs

The content of this section includes information to help you configure the vsphere provisioning adapter job, which authenticates to a VMware hypervisor environment and then discovers VMs in that environment.

The information is organized in the following sections:

- "Initial Configuration" on page 42
- "Policy Configuration Summary for the vSphere Provisioning Adapter" on page 43
- "Assigning a vSphere VM to a Resource Pool" on page 44
- "Setting Up Orchestration VNC for a VM Managed by vSphere" on page 45
- "Setting Up Orchestration to Accommodate VMware DRS Clustering and Updates" on page 47
- "Constraining vSphere VMs to Their Assigned Resource Pools" on page 50

Initial Configuration

Before you can provision and manage VMs with the vsphere provisioning adapter job, you must perform some initial steps to configure it in order to get it running.

1. Make sure that the Orchestration Agent is installed and started on a supported host.

   For more information, see Chapter 2, “Installing Cloud Manager Orchestration Components,” on page 13.

   If you are installing the agent to a vSphere environment, you can install the agent either locally on the vCenter Server (the vCenter appliance is not supported), or on a dedicated system (virtual or physical) as long as the OS in that system is supported for the Orchestration Agent.
2. In the Cloud Manager Orchestration Console, log in to the Orchestration Server that you want to use to manage vSphere VMs.
3. In the Explorer tree of the Orchestration Console, select the Orchestration Server or “grid” object, then select the *Authentication* tab in the admin view to open the Authentication page.
4. Create a credential to authenticate to the vCenter Server. In most cases, the credential is for “administrator” account of the Windows machine where the vCenter Server is running.

   4a On the Authentication page, scroll to the Credential Manager (consisting of the *Stored Credentials* panel and the *Stored Certificates* panel), then click *Add Credential* to display the *Edit Credential* dialog box.

   4b Fill in the fields of the dialog box:

   - **Name:** Enter a value in that identifies the vCenter Web service to log in to.
   - **User:** Enter the user name used to connect to the vCenter Web service.
   - **Secret:** Enter the password of the vCenter Web service user.
   - **Type:** (Optional) Enter any string that lets you categorize similar credentials into a category or group. For example, for the vsphere provisioning adapter you might enter a “type” called `vsphere`.

   For more information, see “Authentication Page” in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

   4c Click *Add*.
5. In the Explorer tree, expand the *Jobs* container, then expand the *provisionAdapters* container to expose all of the provisioning adapter jobs.
6. In the Explorer tree, select the *vsphere* job to open the Admin view.
7. In the Admin view, select the *Job Configuration* tab to open the Job Configuration page, then expand the Accounts table on this page.
8. On the Accounts table, select *Add* to open the Add a New Account dialog box.

   8a Fill in the fields of the dialog box:

   - **Account Name:** Enter the name you wish to use to refer to this vCenter serveras within Orchestrator. This name can be any value, but once selected, it should not be changed.
   - **vSphere Webservice URL:** Enter the URL of the vCenter Web Service server.

     Syntax: `https://address-of-vcenter-server/sdk`

     Example: `https://vcenter.server.test/sdk`, where `vcenter.server.test` is the fully qualified domain name (FQDN) of the vCenter server. You could also use the IP address rather than the FQDN.
   - **Credential Name:** Enter the name of the credential from the Credential Manager that you want to use for logging in to the vCenter Web service server.

- **Auto Portgroup Creation:** (Optional) If selected and the `vsphere_ignoreNetwork` policy is used, port groups are automatically created on a host if it does not have access to the specified network.
- **Auto Portgroup Disconnect:** (Optional) If selected, the vNIC on a VM is disconnected when it is shut down.
- **Auto Portgroup Deletion:** (Optional) If selected, when the VM is shut down, it checks for port groups on the VM host that has no VMs associated with it and deletes them, if possible. This setting is best used with *Auto Portgroup Creation* and *Auto Portgroup Disconnect*.

9 Associate the `vsphere_client` policy to the resource that will access the vCenter Server.

When the vsphere provisioning adapter job starts, this policy constrains the resource for the job to run the Web service commands.

9a In the Explorer tree, expand the *Resources* group, select the client resource that is to access the vCenter Web Service server, then select the *Policies* tab in the admin view to open the *Policies* page.

9b On the Policies page, click *Choose* to open the Policy Selection dialog box, then in the *Source Policies* list, select the *vsphere_client* policy, click *Add*, then click *OK* to associate this policy with this resource. For more information, see “Resource Policies Page” in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

If you want to connect multiple vCenter Servers, refer to Section 6.1.2, “Discovering Enterprise Resources in Multiple vSphere Environments,” on page 50.

10 Discover the VM images on the vCenter Server and populate the Orchestration Console Explorer tree.

10a From the main menu, select *Provision* > *Select VM Hosts and Repositories* to display the Discover VM Hosts and Repositories dialog box.

10b In the Discover VM Hosts and Repositories dialog box, select the *vsphere* job, then click *OK*.

TIP: Ensure that this job completes before proceeding to Step 10c: Repositories where VMs might reside must be discovered prior to any attempt to discover VM images residing there.

10c From the main menu, select *Provision* > *Discover VM Images...* to open the Discover VM Images dialog box.

10d In the Source Repositories table of the Discover VM Images dialog box, select the repositories where vSphere images are stored, click *Add* to move the repositories to the Target Repositories table, then click *OK* to run the image discovery.

Policy Configuration Summary for the vSphere Provisioning Adapter

The following table provides detailed information about other policies associated with the vSphere provisioning adapter that are used to manage the vSphere hosts and the VMs in the grid. The policy settings are applied to all the VMware VMs in the grid.

Table 6-1 *Virtual Machine Management Policies for vSphere*

Policy Name	Description	Additional Details
vsphere	Contains the constraints used to select the vCenter Server resources.	Do not modify this policy.

Policy Name	Description	Additional Details
vsphere_assignPool	If you need to assign the VMs to a certain cluster (for example, a cluster root pool), or if you want to assign VMs to pools "owned" by your customers, use this policy.	When applied this policy allows the VM to reside only on VM hosts that have access to the assigned resource pool (`resource.vm.pool`).
vsphere_client	Contains the settings used to run the vsphere job on the associated vSphere resource.	You need to associate the vsphere_client policy to a vSphere resource before the discovery works. For more information, see Step 9 on page 43.
vsphere_ignoreNetwork	Includes special facts that allow VMs to consider a VM host despite a missing required Network.	If ignoreNetworkCheck is set, a vBridge (portgroup) can be dynamically created on a VM power-on event. This works in conjunction with the auto_portgroups_creation fact found in the vpshere.policy. Make sure that you set the `auto_portgroups_creation` fact to true or else the portgroup will not be created during the VM power-on event.
vspherePA	Includes the basic constraints for the vsphere provisioning adapter.	Do not modify this policy.
vSphereUpdate	Includes settings for the vsphereUpdateDaemon job. The policy can be modified directly or the user can edit job args in the schedule that is created by default installation of the Cloud Manager Orchestration Server.	For more information, see "Configuring the vSphere Update Client" on page 48.
vsphereVmHostVnc	Includes port settings to identify a range of ports to be used for remote connections on a specified VM host.	When applied, this policy defines a range of port numbers to be used for remote connections. As VMs are provisioned, they are assigned a port number within the configured range for remote access. This applies only when the VNC mode is *automatic* (the default) as defined in the vsphereVnc policy.
vsphereVnc	Includes a setting to allow remote desktop connections to vSphere VMs.	For more information, see "Setting Up Orchestration VNC for a VM Managed by vSphere" on page 45.

Assigning a vSphere VM to a Resource Pool

All VMs managed by vSphere are assigned to either the default (named "Resources") or a named resource pool. When vSphere VM images are discovered by the Orchestration Agent, the `resource.vm.pool` fact for each VM is set with what is known by vSphere as a "pool assignment."

If you do not need to restrict VMs based on resource pool assignment, then no policy configuration is necessary and you can provision the VMs as usual, but if you need to assign the VMs to a certain cluster (for example, the cluster root pool), or if you want to assign VMs to pools "owned" by your customers, you can configure the `vsphere_assignPool` policy to accomplish this.

Use the following steps to ensure that the Orchestration Server always provisions a VM to the resource pool where that VM resides.

1. Assign the `vsphere_assignPool` policy to the VM or a group of VMs. No changes to the actual policy file are necessary.

   During provisioning of the VM, the Orchestration Server verifies and relocates the VM (as necessary) to maintain the validity of the pool assignment.

2. (Conditional) If the VM does not reside in the correct resource pool, look up the ID of the resource pool in vCenter and modify the `resource.vm.pool` fact to reflect the correct pool assignment. The Orchestration Server relocates the VM to the specified resource pool at the next provision.

   Alternatively, use vSphere to move the resource to the proper pool and re-run the VM discovery process.

Setting Up Orchestration VNC for a VM Managed by vSphere

When you right-click a VM resource, you have the option of launching a remote virtual network computing (VNC) session console of that VM's desktop. This section provides information about setting up the Orchestration Server to accommodate a VNC session for a VM.

ESX 4.*x* servers managed by vSphere might have a firewall in place to protect some ports from being open or closed. The vsphere provisioning adapter opens the appropriate ports to accommodate VNC connections from a remote console. These ports are opened when the Orchestration Server discovers the servers. This is not true for ESX 5.*x* servers managed by vSphere, where the ports require manual opening. For more information, see Appendix D, "Enabling VNC Access to vSphere 5 VM Guest Consoles," on page 101.

Use the following steps to set up VNC session connectivity for the VM managed by the vsphere provisioning adapter job.

NOTE: Although you can change these settings at any time, they take effect for a vSphere VM after a non-running VM is provisioned, or after you perform an *Apply Config* action on a running VM.

1. In the Explorer tree of the Orchestration Console, select the Grid Server object where you are logged in, then select the *Authentication* tab to open the server's authentication page.

2. In the *Stored Credentials* panel (also known as the "Credential Manager") of the Authentication page, click *Add Credential* to open the Add Credential dialog box.

3. In the Add Credential dialog box, specify a credential that includes the VNC password you want to use, then click *Add*. List the credential type as `vnc`.

   Although a user is required when you create the credential, this value is not used in the remote session. Only the *secret* field is used when making the connection.

4. Configure the vsphereVNC policy.

   4a In the Explorer tree, expand the Policies folder to display the list of policies, then select *vsphereVNC* policy to open the Policy Editor.

   4b In the Policy Editor, modify the `vnc.credential` fact value to be the name of the credential you created in Step 3, then click the *Save* icon.

   Modifying this policy is not necessary unless you want to assign the same credential to every vSphere VM or groups of vSphere VMs. Otherwise, you can select the credential on a per-VM basis from the *VNC Credential* drop-down list on the Resource Information panel of the VM's Info/Groups page.

5. (Conditional) Configure the vsphereVmHostVnc policy for a VM host.

Modifying this policy is not necessary unless the `resource.vnc.mode` fact of the vsphereVNC policy is set to *automatic*. When the ports defined in this range have been consumed, further vSphere VM provisioning fails.

The default port range in the policy is 5900-5964. If you want to provide remote capabilities to more than 65 VMs on a host or cluster, you need to alter the policy configuration to add more ports to the range. You can also reconfigure the policy to use a different range of ports.

5a In the Explorer tree, expand the Policies folder to display the list of policies, then select *vsphereVmHostVnc* policy to open the Policy Editor.

5b In the Policy Editor, modify the `vpshere.port.min` fact value as the lower end of the range of ports you want to be used as remote connections for this VM host.

5c In the Policy Editor, modify the `vpshere.port.max` fact value as the upper end of the range of ports you want to be used as remote connections for this VM host, then click the *Save* icon.

6 Associate the vsphereVNC policy to a VM Resource Group or VM.

6a In the Explorer tree, select the VM Resource Group (or an individual VM) managed by the vsphere provisioning adapter, then in the admin view, select the *Policies* tab to open the Policies page for this group.

6b On the Policies page, select *Choose* to open the Policy Selection dialog box.

6c In the *Source Policies* list of the Policy Selection dialog box, select the *vsphereVnc* policy, click *Add* to move it to the associated *Policies* list, then Click *OK*.

7 Associate the vsphereVmHostVnc policy to a VM host.

7a In the Explorer tree, select the VM host managed by the vsphere provisioning adapter, then in the admin view, select the *Policies* tab to open the Policies page for this group.

7b On the Policies page, select *Choose* to open the Policy Selection dialog box.

7c In the *Source Policies* list of the Policy Selection dialog box, select the *vsphereVMHostVnc* policy, click *Add* to move it to the associated *Policies* list, then Click *OK*.

8 On the Orchestration Console Menu Bar, click *Provision* > *Discover VM Hosts and Repositories*.

In vSphere 4.*x* environments, this action opens or closes the firewall on the VM hosts to allow VNC access. This access is based on the `vsphere.openVncFirewallPort` fact in the vsphere policy.

For ESX 5.*x* servers managed by vSphere, the ports require manual opening. For more information, see Appendix D, “Enabling VNC Access to vSphere 5 VM Guest Consoles,” on page 101.

9 (Conditional: For VMs that are running) From the Explorer tree, right-click a vSphere-managed VM, then select *Apply Config*.

If the VM for which you want to open a VNC session is not running, simply reprovision the VM.

10 If the vSphereUpdate Client is running for your vCenter server, refresh the Orchestration Console.

or

If the vSphereUpdate Client is not running for your vCenter server, right-click the VM object and select *Resync State*.

If you don’t want to resync before using the VNC console, make sure you configure the vSphere Update Client beforehand. For more information, see “Configuring the vSphere Update Client” on page 48.

11. Right-click the VM object and select *Launch Remote Desktop* to open the login dialog box for the VNC session.
12. In the login dialog box, enter the VNC password that you created in the Credential Manager in Step 3.

The following table lists the VNC-related facts in the vsphere provisioning adapter and provides a description of each of those facts.

Table 6-2 *vSphere VNC Facts*

Fact Name	Description
`resource.vnc.ip`	The IP address of the VM host where the VM is running
`resource.vnc.port`	The port currently assigned to the VM. The value is -1 if VNC is disabled for the VM.
`resource.vnc.credential`	The credential containing the VNC password. This is the name of the credential itself, not the username or the password contained in the credential.
`resource.vnc.mode`	Determines how VNC port assignments are handled. This value must be `automatic`, `manual`, or `off`. ◆ If mode = `automatic`: the Orchestration Server attempts to select the next available VNC port. ◆ If mode = `manual`: The port value specified in the VM's `resource.vnc.port` fact is used. ◆ If mode = `off`: The VNC console is disabled.
`resource.remotedesktop`	Controls enabling or disabling the Launch Remote Desktop action in the Orchestration Console.

NOTE: With the vSphere 5 release, VMware removed *VNC Server* as a service than can be directly administered by using the VMware Client or the VMware Client libraries and APIs. Although the VNC functionality still works on ESXi servers, the firewall must be opened to allow access.

For information about enabling VNC access for ESXi 5 servers, see Appendix D, "Enabling VNC Access to vSphere 5 VM Guest Consoles," on page 101.

Setting Up Orchestration to Accommodate VMware DRS Clustering and Updates

The Orchestration Server supports the discovery of VMware vSphere clusters used for high availability in a VMware environment or managed by the VMware Distributed Resource Scheduler (DRS) after an Orchestration Agent has been deployed into such an environment. In this scenario, Cloud Manager Orchestration also allows you to verify when actions have taken place outside of Cloud Manager, such as when DRS moves a VM to an alternate host in the cluster or when an administrator moves a VM into a different resource pool.

Any vSphere clusters discovered by Cloud Manager and managed by DRS are listed in the Orchestration Console as members of a convenience group (for example, a group named `clusters_`*`vsphere`*).

You can learn about the read-only cluster-related facts for these discovered clusters in the following Orchestration documentation references:

- "Orchestration Server Facts in a VM Host Residing in a Cluster" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*
- "Orchestration Server Facts in the VM Host Cluster Object" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*
- "Orchestration Server Facts in VMs Hosted in Clusters" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*

The Cloud Manager Orchestration update infrastructure consists of two main components:

- A vSphere Update Client component, which is executed by the Orchestration Agent
- The vSphereUpdate monitor job, which starts the Update Client component and ensures that it runs when necessary

Configuring the vSphere Update Client

To configure the vSphere Update Client:

1 Create a proxy user:

1a In the Orchestration Console, click *Actions* > *Create User* to open the Create a New User dialog box.

1b In the *Source Groups* list, select administrators, then click *Add* to move the administrators user group to the *Target Group* list.

1c In the *New User Name* field, specify a user name, click *Create*, then click *Close*.

This is the proxy user. The username must contain the word "proxy," for example, *my_proxy*, or *proxy1*.

2 Modify the vSphereUpdate.policy (or modify the jobargs in the scheduler) so that `zos.proxy.user` contains the name of the user created in Step 1c:

2a In the Explorer Tree, select the *Policies* group to expand the list of policies included on this grid.

2b Select the *vSphereUpdate* policy to open the Policy Editor view.

2c Find the `zos.proxy.user` fact in the policy, then specify the name of the proxy user you created in Step 1c as the value for this fact.

3 Run the vSphereUpdate schedule and job:

3a In the toolbar of the Orchestration Console, select *Scheduler* to open the Orchestration Server Job Scheduler.

3b Select the *vSphereUpdate* schedule, click *Enable*, then click *Run Now*.

4 (Optional) Verify that the update job has run.

4a In the Orchestration Console main menu, select *Jobs* to open the Jobs admin view.

4b In the admin view, locate the VsphereUpdate job that ran last, then select its *Job Log* tab.

You should see something similar to the following in the log:

```
[vrack-vc] checking pid: 5276
[vrack-vc] pid '5276' is still alive
```

The "pid" reference in the log refers to the `javaw.exe` process running on the resource that accesses the vCenter software. You can verify that this process is running in the Windows Task Manager on the VCenter host machine.

The vSphereUpdate Monitor Job

The vSphereUpdate monitor job is located in the "all" jobs group. It is associated with both the vsphere policy (for VCenter configuration information) and the vSphereUpdate policy. The vSphereUpdate policy specifies the following cluster-related facts. You can modify these facts to accommodate your environment.

Table 6-3 *Cluster-Related Facts in the vSphereUpdate Policy*

Fact Name	Type	Description
`jobargs.zos.proxy.user`	String	An administrative user used by the Orchestration Console to log in to the Orchestration Server in order to perform update operations there. You must create an administrative user for this purpose, if you have not already done so. The name of this user must contain the word "proxy," for example, *my_proxy*, or *proxy1*. When you change the value of this fact, you must restart the Orchestration Server. For information about configuring the vSphere Update Client, see "Configuring the vSphere Update Client" on page 48.
`jobargs.zos.proxy.passwd_validity`	Integer	The amount of time (measured in seconds) that the `zos.proxy.user` password is valid. **Example:** 86400 (1 day). Although the default value (-1) implies that the password is valid forever, the actual validity time is limited to the uptime of the Orchestration Server. When the password expires, the Orchestration Console is automatically restarted with a new password the next time that the monitor job runs.
`jobargs.debug`	Boolean	Specifies whether you want extra verbose debug logging sent to a job log. **NOTE:** The client logs its output to the `log.txt` and `err.txt` files located in `<`*`agent_install_dir`*`>/node.default/.vSphereUpdate/<`*`hostname`*`>/<`*`vcenterId`*`>`.
`jobargs.verbose`	Boolean	Specifies whether you want verbose logging sent to a job log. This fact is implicitly set when `jobargs.debug` is set.

Fact Name	Type	Description
`jobargs.mode`	String	The value for this fact can be optionally set to “clear.” This resets the passwd_validity and forces a restart on the next invocation where the mode is not set. The value can also be set to “stop” to stop all running update clients.

Configuring the Orchestration Server to Limit Datastore Visibility in vSphere Clusters

If you want to limit the number of datastores (that is, Repositories that are modeled in the Orchestration Server) that are available to a vSphere cluster, you can assign a policy similar the policy below to the undesired repository or repositories:

```
<policy>
  <repository>
    <fact name="enabled" type="Boolean" value="False" />
    <fact name="provisioner.jobs">
      <array type="String">
      </array>
    </fact>
  </repository>
</policy>
```

This disables the repository for use with the cluster.

Constraining vSphere VMs to Their Assigned Resource Pools

To assign the VMs to a certain cluster (for example, the cluster root pool), or if you want to assign VMs to a pool “owned” by your customers, configure the vsphere_assignPool policy to to a VM or a group of VMs.

1. In the Orchestration Console tree view, select the VM or Group of VMs that you wish to constrain to their assigned resource pool.
2. In the admin view, select *Policies* to open the Policies page.
3. On the Policies page, select *Choose* to display the Policy Selection dialog box.
4. In the Source Policies list, select *vsphere_assignPool*, click *Add* to move it to the Associated Polices list, then click *OK*.

6.1.2 Discovering Enterprise Resources in Multiple vSphere Environments

A data center administrator running VMware products might organize the virtual resources in his or her enterprise into several different vSphere environments. The Cloud Manager Orchestration Server lets you discover and manage all of these enterprise VMs, discovering each relevant VM host, network, repository, and VM within the several vSphere environments and modeling them as objects in the Orchestration Console.

- “Creating Accounts for Each vCenter Environment” on page 51
- “Configuring the vsphere.vcenters Fact to Include All Accounts Representing a vCenter Server” on page 51
- “Optionally Specifying an Authentication Certificate for Each vCenter Server” on page 53
- “Running Discovery” on page 54

Creating Accounts for Each vCenter Environment

1. In the Explorer tree, select the *vsphere* provisioning adapter job to open the Admin view of this job.
2. Select the *Job Configuration* tab to open the Job Configuration page, then expand the Accounts table on this page.
3. On the Accounts table, select *Add* to open the Add a New Account dialog box.

   3a Fill in the fields of the dialog box:

   - **Account Name:** This should match the name of the VCenter environment you are connecting to.
   - **vSphere Webservice URL:** Enter the URL of the vCenter Web Service server.
   - **Credential Name:** Enter the name of the credential from the Credential Manager that you want to use for logging in to the vCenter Web service server.
   - **Auto Portgroup Creation:** (Optional) If selected and the `vsphere_ignoreNetwork` policy is used, port groups are automatically created on a host if it does not have access to the specified network.
   - **Auto Portgroup Disconnect:** (Optional) If selected, the vNIC on a VM is disconnected when it is shut down.
   - **Auto Portgroup Deletion:** (Optional) If selected, when the VM is shut down, it checks for port groups on the VM host that has no VMs associated with it and deletes them, if possible. This setting is best used with *Auto Portgroup Creation* and *Auto Portgroup Disconnect*.
4. Repeat Step 3 for every vCenter Server you want to connect to for VM discovery in that vSphere environment.

When you have created Orchestration accounts for each of the vCenter servers in your enterprise, you can continue with "Configuring the vsphere.vcenters Fact to Include All Accounts Representing a vCenter Server" on page 51.

Configuring the vsphere.vcenters Fact to Include All Accounts Representing a vCenter Server

The `vsphere.vcenters` fact can be set to include the definition for all the vCenter server accounts that you identified in "Creating Accounts for Each vCenter Environment" on page 51. This is required to ensure that only certain agents communicate with certain vSphere accounts. You can set this fact in the vsphere_client policy of the vsphere provisioning adapter or by using a policy to apply to the individual Orchestration Agents you installed in your respective vSphere environments.

- "Configuring the vsphere.vcenters Fact in the vsphere_client Policy" on page 52
- "Creating a Policy to Apply to Each Orchestration Resource in the Respective vSphere Environments" on page 52

When you have used one of these methods, continue with "Optionally Specifying an Authentication Certificate for Each vCenter Server" on page 53.

Configuring the vsphere.vcenters Fact in the vsphere_client Policy

You can associate the `vsphere.vcenters` fact in the vsphere_client policy to the resources that access the respective vCenter Servers. When the vsphere provisioning adapter job starts, the policy applies the `vsphere.vcenters` fact to constrain the identified resources for the job to run the Web service commands.

Use these steps to configure the `vsphere.vcenters` fact:

1. In the Explorer tree, expand the *Policies* group, then select the *vsphere_client* policy to open the *Policy Editor* page in the admin view.
2. In the Policy Editor, scroll to or search for the `vsphere.vcenters` fact, then uncomment it and enter a string value in the array, using the *Account Name* for each vCenter Server (identified in "Creating Accounts for Each vCenter Environment" on page 51) as a string value.
3. In the Explorer tree, expand the *Resources* group, select the client resource that is to access the vCenter Web Service server, then select the *Policies* tab in the admin view to open the *Policies* page.
4. On the Policies page, click *Choose* to open the Policy Selection dialog box, then in the *Source Policies* list, select the *vsphere_client* policy, click *Add*, then click *OK* to associate this policy with this resource. For more information, see "Resource Policies Page" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

   If you want to connect multiple vCenter Servers, make sure you modify the `vsphere.vcenters fact` of the vsphere_client policy as described in the policy comments.

Creating a Policy to Apply to Each Orchestration Resource in the Respective vSphere Environments

You can use separate resources to connect to and manage the different vCenter environments that you have configured. To do this, create a custom policy for each vCenter that you want to manage and assign these policies to the resources that you designate to manage the respective vCenters.

The content of the policy should be similar to the following:

```
<policy>
   <resource>
   <fact name=”vsphere.vcenters”>
      <array>
       <string>VCENTER1_NAME</string>
    </array>
   </fact>
  </resource>
</policy>
```

In this case, applying this policy along with the vsphere_client.policy to a resource would enable that resource to connect to and manage the vCenter with the name `VCENTER1_NAME`. This name must match the *Account Name* you configured in "Creating Accounts for Each vCenter Environment" on page 51.

Optionally Specifying an Authentication Certificate for Each vCenter Server

The vsphere provisioning adapter job automatically enables a secure SSL connection between your Orchestration Agent and the vCenter Server. This involves some security risk if a malicious user is impersonating your vCenter Server. To avoid this risk, you can explicitly configure the SSL certificate that the Orchestration Agent accepts from the vCenter Server.

We recommend that you review VMware documentation regarding gathering the certificate (http://pubs.vmware.com/vsphere-50/topic/com.vmware.wssdk.dsg.doc_50/sdk_sg_server_certificate_Appendix.6.4.html#991190) used by your vCenter Server's Web interface before you proceed further.

When you have gathered the certificate, use the following steps to explicitly configure the certificate:

1 Make sure that the Orchestration Agent is installed and started on a computer in each vCenter environment.

   For more information, see Chapter 2, "Installing Cloud Manager Orchestration Components," on page 13.

   If you are installing the agent to a vSphere environment, you can install the agent either locally on the vCenter Server (the vCenter appliance is not supported), or on a dedicated system (virtual or physical) as long as the OS in that system is supported for the Orchestration Agent.

2 In the Cloud Manager Orchestration Console, log in to the Orchestration Server that you want to use to manage vSphere VMs.

3 In the Explorer tree of the Orchestration Console, select the Orchestration Server or "grid" object, then select the *Authentication* tab in the admin view to open the Authentication page.

4 Create a credential to authenticate to a unique vCenter Server in your enterprise. In most cases, the credential is for "administrator" account of the Windows machine where the vCenter Server is running.

   4a On the Authentication page, scroll to the Credential Manager (consisting of the *Stored Credentials* panel and the *Stored Certificates* panel), then click *Add Certificate* to display the *Add Certificate* dialog box.

   4b Fill in the fields of the dialog box:

   - **Identifier:** Specify a value in that uniquely identifies the certificate associated with this unique vCenter Server. the identifier should be of the form `vsphere_<YOUR_VCENTER_NAME>`, where `<YOUR_VCENTER_NAME>` is the account name that you configured earlier for the vCenter Server.
   - **Location:** Specify the file location of the certificate you gathered previously.
   - **Group:** Enter `vsphere` as the group name.

   For more information, see "Authentication Page" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

   4c Click *Add*.

5 Repeat Step 4 for all of the vCenter Servers you want to connect to.

When you have completed the authentication configuration, continue with "Running Discovery" on page 54.

Running Discovery

When the Orchestration Server is properly configured, you can use the following steps to discover the VM images on each vCenter Server and populate the Orchestration Console Explorer tree.

1. From the main menu, select *Provision* > *Select VM Hosts and Repositories* to display the Discover VM Hosts and Repositories dialog box.
2. In the Discover VM Hosts and Repositories dialog box, select the *vsphere* job, then click *OK*.

   When you perform this discovery action, the Orchestration Server runs jobs that discover the VM hosts, repositories, and networks in each of the vSphere environments. On each discovered object, the server also generates a `*.vsphere.vcenter` fact that contains a vCenter ID from the hosting vSphere environment.

   After the objects are discovered in the vSphere environments, you can use the Orchestration Server to discover existing VMs in those environments.
3. From the main menu, select *Provision* > *Discover VM Images* to open the Discover VM Images dialog box.

   The Orchestration Agent discovers all of the VMs managed in the vSphere environments and places them in the Orchestration model for you to manage.
4. In the Source Repositories table of the Discover VM Images dialog box, select the repositories where vSphere images are stored, click *Add* to move the repositories to the Target Repositories table, then click *OK* to run the image discovery.

When a VM with a given name is discovered in two different vSphere environments, the second VM discovered is named in the form of `VMNAME_VCENTERID`, rather than named by appending an incremental number, as explained above. As with other such object names that are automatically generated, these VM names can be changed.

6.2 Configuring the Citrix XenServer Provisioning Adapter

If you manage a Citrix XenServer environment, you can use the NetIQ Cloud Manager XenServer provisioning adapter job to help you manage that environment. The xenserv provisioning adapter job is automatically deployed when you start the Orchestration Server.

For more information about the xenserv provisioning adapter policy, see “The Citrix XenServer Provisioning Adapter” in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*.

This section includes the following information:

- Section 6.2.1, “Deploying the Citrix XenServer Provisioning Adapter,” on page 55
- Section 6.2.2, “Configuring the Citrix XenServer Updater,” on page 57
- Section 6.2.3, “Configuring Orchestrator for Personalization with XenServer,” on page 57
- Section 6.2.4, “Using Xen VNC Proxy to Establish a Remote Desktop Connection to XenServer VMs,” on page 57

6.2.1 Deploying the Citrix XenServer Provisioning Adapter

The Citrix XenServer Provisioning Adapter uses the XenAPI management API to connect to and manage XenServer hosts. Unlike previous versions of the XenServer Provisioning Adapter, this adapter requires no additional software be installed on the XenServer host.

To configure the provisioning adapter, perform the following steps in the Cloud Manager Orchestration Console:

1 Create a XenServer credential for each user ID/password combination used for XenServer pool master hosts:

1a Navigate to the Grid object for the Orchestrator server in the explorer panel

1b Select the *Authentication* tab in the management panel

1c Under “Stored Credentials”, click *Add Credential*

1d Fill in the following fields:

Name: The name to refer to this credential as

User: Enter `root`

Secret: Enter the root account’s password for the XenServer pool master

Type: Select `xenserv` from the dropdown list

2 Create an account for each XenServer pool master host in the `xenserv` job:

2a Expand the *Jobs->provisionAdapters* branch of the Grid in the explorer panel

2b Select the *Job Configuration* tab in the management panel

2c Under “Accounts”, click *Add*

2d Fill in the following fields and save the job:

Account Name: The name to use for this account

VM Host IP/DNS Address: The IP or DNS address of the XenServer Pool master server.

Credential Name: The name of the credential entered in Step 1d

Use SSL: Check this option to encrypt the API calls over the network

NOTE: Using SSL is generally not necessary, and adds significant overhead to the traffic and processing. Only enable this option if encryption is necessary.

3 Associate the xenservClient policy with the system that will execute this job:

3a Expand the *Resources* branch of the Grid in the explorer panel and select the system that will execute the job

3b Select the *Policies* tab and click the *Choose* button

3c Select the `xenservClient` object in the *Source Policies* list and click the *Add* button

3d Click the *OK* button

4 Discover the XenServer hosts and repositories by clicking the *Provision* menu and selecting *Discover VM Hosts and Repositories...*

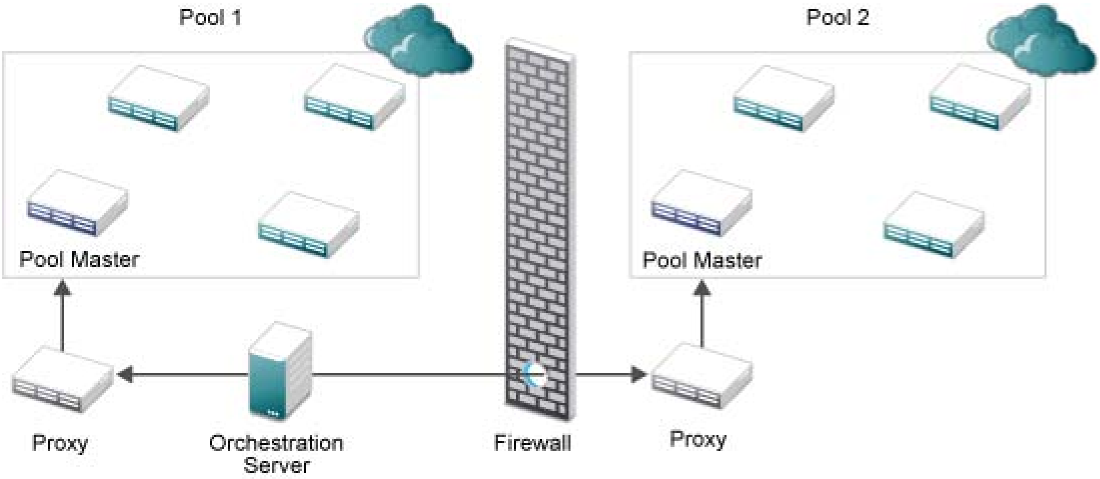
5 When the `Provision(xenserv)` job has completed, discover the VM images in the discovered hosts by clicking the *Provision* menu and selecting *Discover VM Images...*

NOTE: In order for VMs to be properly discovered, they must have the XenServer tools installed and the OS information populated prior to discovery.

If a single provisioning adapter is deployed within a single directly reachable network, nothing special needs to be done in order for the adapter to work. This applies both with multiple pools on the same network as well as a pool on one side of a firewall, as shown in Figure 6-1.

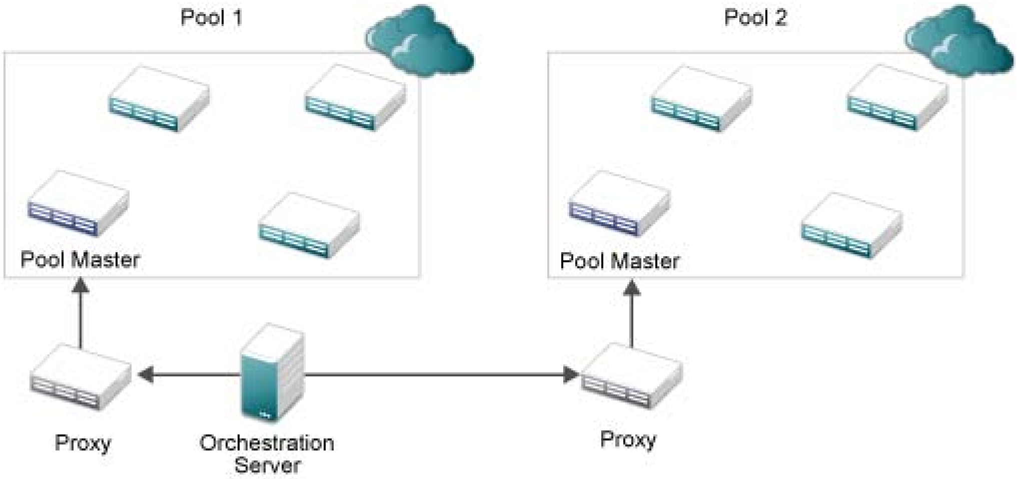
This type of configuration is typically used when multiple networks are separated by a firewall that limits communication between the networks.

Figure 6-1 *Single provisioning adapter per network*



If, as shown in Figure 6-2, multiple provisioning adapters are used within a single network, it is also necessary to define restrictions using the *xenservClientHostRestriction-Template* policy. These restrictions are used to limit which XenServer pool masters each provisioning adapter connects to.

Figure 6-2 *Multiple provisioning adapters per network*



To define these restrictions, perform the following steps:

1. Navigate to the *xenservClientHostRestrictions-Template* policy in the *Policies* tree.
2. Create a copy of the policy for the first instance of the provisioning adapter.
3. Modify the copy to list the account name or names that the client has access to, following the instructions in the comments in the policy.

4 Associate the policy with the host the provisioning adapter job is associated with.

5 Repeat Steps 2-4 for each provisioning adapter instance.

6.2.2 Configuring the Citrix XenServer Updater

To keep the discovered facts about VMs hosted on Citrix XenServer updated, you can enable the schedule for the XenServer Updater job. To do this:

1. Open the Scheduler view
2. Select the XenServer Updater schedule
3. Click the *Enable* button to enable the daemon
4. (Optional) To start the job immediately, click the *Run Now* button

Once the daemon is started, changes to the facts tracked by Orchestrator will be reflected as they are made to the VM.

6.2.3 Configuring Orchestrator for Personalization with XenServer

When using personalization with VMs hosted on Citrix XenServer 6.0 and later, it is necessary to have a shared ISO library configured. Orchestrator will upload a customizer LiveCD image to that library that will handle all the personalization (server name, DHCP/network configuration, autoprep/sysprep and other configuration) using that ISO.

For XenServer 5.6, it is necessary to manually upload the ISO to the ISO library:

1. Copy the CMOS_Customizer_LiveCD.i686-*x.y.z*.iso file from `/opt/novell/zenworks/zos/server/doc/install` directory into the shared ISO library
2. Rescan the ISO library in XenCenter to verify the upload has completed.
3. In the Orchestration Console, browse to the ISO library, right click, and select *Discover Disks*

Once these steps are completed, personalization of VMs on the XenServer host will run as expected.

6.2.4 Using Xen VNC Proxy to Establish a Remote Desktop Connection to XenServer VMs

NetIQ Cloud Manager uses the Xen VNC proxy (xvp) server to provide a password-based connection to the all of the guest VM consoles that are hosted on a single Citrix XenServer that is connected to a single Cloud Manager Orchestration Server.

This section includes information about how to install and configure xvp for use with Cloud Manager.

- "Installing the Xen VNC Proxy Packages" on page 58
- "Configuring Xvp Credentials in the Orchestration Server for the Citrix XenServer Environment" on page 58
- "Understanding How Xen VNC Proxy Works in the Orchestration Environment" on page 59
- "Cloud Manager Console Actions on XenServer VMs Configured To Use Xen VNC Proxy" on page 60
- "Known Issues with Xen VNC Proxy Remote Console Usage" on page 60

Installing the Xen VNC Proxy Packages

If you want a supported method of launching a remote console of a VM managed by Citrix XenServer, you need to install the xvp package provided by NetIQ on the Cloud Manager installation ISO.

To install xvp packages:

1. Mount the Cloud Manager installation ISO on a network computer running a supported version of SUSE Linux Enterprise Server (SLES). This computer should not be part of the existing Citrix Xen environment. It must also have the NetIQ Cloud Manager Orchestration Agent installed on it.
2. On the computer where you are installing xvp, start YaST and select *Software Management*.
3. In the YaST *Software Management* view, select the *Xen VNC Proxy* install pattern, then click *Accept* to install the packages. The pattern includes two xvp packages:
    - `libxenserver`
    - `xvp`
4. Start the Orchestration Agent on the SLES computer where you installed the xvp proxy.
5. In the Orchestration Console toolbar, select *Resources*, select the registration icon to open the Resource Registration Monitor dialog box, then click *Accept* > *OK* to register the new resource.

    When the resource is registered, it is automatically discovered as an xvp host.

Configuring Xvp Credentials in the Orchestration Server for the Citrix XenServer Environment

After the host discovery, you need to set up the credentials that allow xvp to open ports for the VNC sessions to the Citrix XenServer VMs.

- "Creating Credentials for Individual Citrix XenServer VMs" on page 58

Creating Credentials for Individual Citrix XenServer VMs

VMs are most commonly provisioned and given VNC credentials by Cloud Manager business owners, who own and control those VMs as managed workloads. These are saved in the Orchestration Server credential store.

If you want to create VNC credentials manually for Citrix XenServer VMs you manage with Cloud Manager Orchestration Console, you can use the following steps:

1. In the Explorer tree of the Orchestration Console, select the Grid object for the Orchestration Server that communicates with the Citrix Xen environment, then in the Admin view, select *Authentication* to open the Authentication page.
2. In the Stored Credentials subpanel, select *Add Credential* to open the Add Credential dialog box.
3. In the Add Credential dialog box, fill in the fields to create a new VNC credential set for a VM. computer.
    - **Name:** This is a required field. Provide a name that you want to use to identify this credential set.
    - **User:** This is a required field. Enter a username you want use in the VNC session for this VM.
    - **Secret:** This is a required field. Enter a password you want use in the VNC session for this VM.

IMPORTANT: This password must be no more than 10 characters. Passwords with more than 10 characters do not store properly.

- **Type:** Select *VNC* as the credential type.

4 Click *Add* to save the credential information.

5 In the Explorer tree, select a VM that is hosted by the Citrix XenServer computer “host”.

6 Apply the newly created VNC credential for this VM.

6a Select the Info/Facts tab to open the Info/Groups page for this VM.

6b On the Info/Groups page, scroll to the *VNC Credential* field in the *Resource Information* subpanel.

6c In the VNC Credential field, open the drop-down menu to list the configured credentials, then select the name of the credential that you created in Step 3.

6d Click *Save* to commit the change.

6e In the Explorer tree, right-click the VM to which you just added a credential, then click Apply Config or Save config to enable the credential.

This action populates the following facts on the VM:

- resource.vnc.port
- resource.vnc.ip

Understanding How Xen VNC Proxy Works in the Orchestration Environment

When the host discovery runs on the SLES resource where the Orchestrate Agent is running, it checks for the xvp service at `/etc/init.d/xvp`. If the service is present, four facts are created. The following table lists these facts, their values and purpose.

Table 6-4 *Facts for the Xvp Service Listed in the SLES Resource*

XVP Fact Name	Default Port Value	Purpose
`resource.xvp.beginport`	6901	◆ User configurable. ◆ Instructs the xvp computer which port to start using.
`resource.xvp.freeport`	6901	◆ User configurable. ◆ Informs the xvp machine which port to use for the next provisioned VM ◆ Value increments automatically. ◆ Ports assigned to destroyed VMs are stored in `var/xenservXVP_freeports.txt`, to be reused later.
`resource.xvp.vncportrange`	100	◆ User configurable. ◆ Provides information for the xvp computer regarding how many ports it should use for proxy connections.
`resource.xvpHost`	true	◆ Identifies the system as an xvp proxy server.

Cloud Manager Console Actions on XenServer VMs Configured To Use Xen VNC Proxy

The following table lists some of the actions you can perform on a Citrix XenServer VM that you have configured with xvp credentials for using a remote console session.

VM Action	Result
Apply Config or Save Config	The Orchestration Server makes an entry in the xvp configuration file for the selected VM.
Migrate or Move	The Orchestration Server moves the “VM configuration” information in the XVP configuration file to the XVP configuration file of the destination XenServer.
Destroy	The Orchestration Server deletes the “VM configuration” information in the xvp configuration file. If there are no such entries in the file, the server deletes the entire file, along with the corresponding entry from the main configuration file (`/etc/xvp.conf`).

Known Issues with Xen VNC Proxy Remote Console Usage

There are some known issues with Cloud Manager 2.1 remote console connections to Citrix XenServer VMs via xvp:

- Only one xvp proxy server can be registered on the Orchestration Server. If you determine that network traffic becomes too much for this single proxy to efficiently handle its remote connections, you can deploy another xvp, but you also need to deploy an additional Orchestration Server to manage it.
- Occasionally, a workload (that is, a Citrix XenServer VM) provisioned from the Cloud Manager Application Server Console fails to properly configure the `resource.vnc.ip` fact and the resource.vnc.port fact. Use the *Apply Config* action on the VM in the Orchestration Console to correct the configuration of these facts.

6.3 Configuring the Hyper-V Provisioning Adapter

The hyperv provisioning adapter job deploys the hyperv.policy with the job. This policy contains the facts and constraints that the hyperv provisioning adapter job uses for checking whether the Hyper-V server host is registered to the Orchestration Server, and whether that host is up and running. By default, the optimal values are preset for the configuration of the job and joblets in the policy. We strongly recommend that you do not edit this policy.

The following additional configuration information is included in this section:

- Section 6.3.1, “Ensuring that the Orchestration Server Discovers Hyper-V VMs,” on page 61
- Section 6.3.2, “Configuring the Provisioning Adapter to Discover iSCSI Target Repositories,” on page 61
- Section 6.3.3, “Configuring the Provisioning Adapter for Sysprep,” on page 61
- Section 6.3.4, “Enabling a Remote Console Session for a Hyper-V VM,” on page 61
- Section 6.3.5, “Configuring Hyper-V Linux VMs to Enable Visibility of Added vDisks,” on page 62

For information about troubleshooting the hyperv provisioning adapter job, see “Troubleshooting Hyper-V VM Provisioning Operations” in the *NetIQ Cloud Manager 2.1.5 Troubleshooting Reference*.

6.3.1 Ensuring that the Orchestration Server Discovers Hyper-V VMs

If you create a VM in your Hyper-V environment, but the path to that VM was not configured as the default path in the Hyper-V Manager, the Orchestration Server does not discover the VM until you edit the preferred path for the discovered repository where the VM resides. You can also create a new repository in the Orchestration Console with the preferred path to the Hyper-V VM.

6.3.2 Configuring the Provisioning Adapter to Discover iSCSI Target Repositories

If you are managing Windows VMs in a Hyper-V environment (clustered or non-clustered), the hyperv provisioning adapter must be configured to discover iSCSI target repositories in that environment if the VM is in a location other than `C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks`.

To configure the provisioning adapter for this use case:

1. In the Explorer tree of the Orchestration Console, select the *Repositories* group to expand the list of Repository Objects, select *hyperv*, then select the storage object associated to the Hyper-V cluster to open the admin view.
2. In the Info/Groups page of the admin view, find the *Preferred Storage Path* field (the `repository.preferredpath` fact).
3. In the *Preferred Storage Path* field, change the value to the path where the VM resides.

   Remember that this field considers the information in the *Root Location* field (that is `repository.location`).

   This is the location where the Orchestration Server searches for VM files for use in cloning and moving.Generally, it is a path like this:

   ```
   C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
   ```
4. Click the *Save* icon to save the new configuration.

NOTE: If your Hyper-V environment is a Cluster Storage Volumes (CSV) environment, the VMs on the CSVs are automatically discovered by the hyperv provisioning adapter as separate repositories. Executing the *Discover VM Images* action on these repositories discovers the VMs residing there.

6.3.3 Configuring the Provisioning Adapter for Sysprep

As with other VMs provisioned by the Orchestration Server, sysprep does not work on Hyper-V Windows VMs until you set a value for the Admin Password fact (`resource.provisioner.autoprep.sysprep.GuiUnattended.AdminPassword.value`). For information about this fact, see “Admin Password” in the *NetIQ Cloud Manager 2.1.5 Orchestration Installation Guide*.

6.3.4 Enabling a Remote Console Session for a Hyper-V VM

If you invoke the VNC console for a Hyper-V VM (referred to as a “workload”) from the Cloud Manager Web Client, the VNC console does not launch.

Installing the Orchestration Agent on the VM and executing the *Apply Config* action lets you launch a VNC session from Cloud Manager to the Hyper-V “workload” desktop.

To install the agent to the VM:

1. In Explorer tree of the Orchestration Console, select the VM that you want to observe in a remote session, then right-click and select *Shutdown*.
2. Right-click the now idle VM, then select *Install Agent*.
3. Right-click the VM, then select *Start*.
4. When the VM appears online again in the list of resources, right-click the VM again and select *Apply Config*.

6.3.5 Configuring Hyper-V Linux VMs to Enable Visibility of Added vDisks

If you plan to add an additional vDisk to the Hyper-V Linux VM at some point, you need to further configure the VM so that the vDisk is visible. To do this, you need to install Microsoft Linux Integration Components for Linux. See the Microsoft downloads site (http://download.microsoft.com/download/4/2/7/4273D9CF-3FC3-4A91-8204-9E0D4DE2027C/Linux%20Integration%20Components%20Read%20Me.pdf) for more information.

6.4 Configuring the SUSE Xen Provisioning Adapter

The xen provisioning adapter job has prepackaged policies that are deployed with the job. These policies run when the job is deployed and manage the Xen hosts and VMs in the grid. The policy settings are applied to all the VMs in the grid.

For more information about the provisioning adapter policies, see “The Xen Provisioning Adapter” in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*.

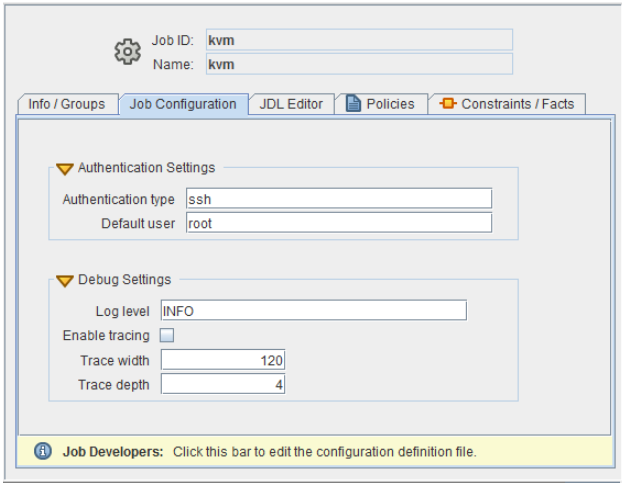
For information about troubleshooting the xen provisioning adapter job, see “Troubleshooting SUSE Xen VM Provisioning Actions” in the *NetIQ Cloud Manager 2.1.5 Troubleshooting Reference*.

6.5 Configuring the KVM Provisioning Adapter

If you manage a KVM (kernel based virtual machine) hypervisor environment where the hypervisor funs on a SUSE Linux Enterprise Server (SLES) 11 SP1 host machine, you can use the Orchestration KVM provisioning adapter to help manage its VMs and to expose guest OS machines to Cloud Manager.

The KVM provisioning adapter uses job configuration settings specified on the kvm job, which is automatically deployed when you start the Orchestration Server. You can select these settings when you select the kvm job and open the Job Configuration tab in the job admin view of the Orchestration Console.

Figure 6-3 *The Job Configuration Page of the KVM Provisioning Adapter Job*



Job ID: kvm
Name: kvm

Authentication Settings
Authentication type: ssh
Default user: root

Debug Settings
Log level: INFO
Enable tracing: □
Trace width: 120
Trace depth: 4

Job Developers: Click this bar to edit the configuration definition file.

The page includes two subpanels:

- Authentication Settings
- Debug Settings

There are additional `kvm.policy` file that are used by the provisioning adapter. You should retain the default values for these settings.

For more information about the how the KVM provisioning adapter works and for a list of the facts in the kvm provisioning adapter policy, see "The KVM Provisioning Adapter" in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*.

6.5.1 Authentication Settings

These settings relate to the type of authentication used between KVM hosts in your hypervisor's environment. You need to set up some form of authentication between KVM hosts so that migrate operations function correctly. The Orchestration Server also uses the authenticated channel to optimize how VM registrations are moved between hosts, though it falls back to a less-efficient method of running joblets on both resources, if necessary. The Authentication Settings subpanel includes the following fact settings:

- **Authentication Type:** The default type of authentication used by the libvirt libraries. This setting can be overridden on a per-host basis by setting the `vmhost.libvirt.authentication.type` fact. Valid values are `ssh` or `tls`.

The setting is listed in the Fact Editor as a String type, named `job.libvirt.authentication.type.default`.

- **Default User:** The default user to use to connect over a secure channel to the libvirt user on a given host. This setting can be overridden on a per-host basis by setting the `vmhost.libvirt.authentication.user` fact on any given host.

  The setting is listed in the Fact Editor as a String type, named `job.libvirt.authentication.user.default`.

You are responsible to set up the authentication channel and to advertise it to the Cloud Manager Orchestration Server (Cloud Manager does not attempt to automatically create these connections if they do not exist). For setup instructions for libvirt authentication on SUSE-based hosts, see *Chapter 7: Connecting and Authorizing (https://www.suse.com/documentation/sles11/book_kvm/data/cha_libvirt_connect.html)* in *Part II: Managing Virtual Machines with libvirt* of the *SLES 11 Virtualization with KVM Administration Guide*.

The SSHConfigure job can help you set up SSH authentication, but you must run it manually. The job:

- Sets up ssh keys for the root user on each kvm host.
- Imports public keys into the Credential Manager from each host.
- Propagates hosts' public keys to other hosts and makes them available for use.

Use the following steps to run the SSHConfigure job manually:

1 Create a Resource Group that includes each kvm host you want to configure for SSH.

2 In the Job Configuration page of the Orchestration Console admin view for the SSHConfigure job, edit the settings.

  2a Enter the desired group name for SSH keys. This is the group name for keys in the Credential Manager.

  2b Define the desired SSH user name.

  2c Enter the name of the group you created in Step 2a above into the *Desired Host Group* field.

3 Run the SSHConfigure job by using the SSHConfigure schedule.

6.5.2 Debug Settings

These settings control the amount of information that is reported to a job log. The Debug Settings subpanel includes the following fact settings:

- **Log level:** Specifies the level of verbosity for the information recorded in the job log. Values of “OFF”, “CRITICAL”, “ERROR”, “WARN”, “INFO”, “DEBUG”, “FINE”, “FINER”, and “FINEST” produce increasing detail.

  The setting is listed in the Fact Editor as a String type, named `job.debugLevel`.
- **Enable tracing:** Select this check box to log a TRACE statement to the job log each time an annotated job method is entered or exited. The only reason to enable this is to provide additional detail when reporting a bug.

  The setting is listed in the Fact Editor as a Boolean type, named `job.traceEnabled`.
- **Trace width:** Trace statements are formatted so that they do not exceed this line length. The default value is 120.

  The setting is listed in the Fact Editor as an Integer type, named `job.traceWidth`.

- **Trace depth:** Specifies how much argument and return value data is displayed on trace statements. A value of 0 (zero) suppresses method argument and return values from the job log. Larger values indicate how many levels of data should be logged if arguments are nested data structures.

  The setting is listed in the Fact Editor as an Integer type, named `job.traceDepth`.

7 Configuring Sysprep or Autoprep

When a Cloud Manager provisioning adapter discovers the VMs in your hypervisor, you need to configure those VMs for future provisioning. This section explains sysprep concepts and configuring sysprep for Windows VMs in the Orchestration Console. It also explains autoprep concepts and configuring autoprep for Linux VMs in the Orchestration Console.

- Section 7.1, "Understanding and Configuring Sysprep," on page 67
- Section 7.2, "Understanding and Configuring Autoprep," on page 81

7.1 Understanding and Configuring Sysprep

In the Orchestration Console, sysprep refers to the function of preparing unique settings for Windows VMs on VM hosts so that those VMs can be provisioned by the provisioning adapter without creating conflicts and personalizing other information.

As the administrator, you can set facts in the Orchestration Console that can later be automatically applied to a VM clone (by selecting the *Use Autoprep* check box) during a *Provision* or a *Clone* action from a VM template. The sysprep facts can also be manually applied to an existing VM by using the *Personalize* action.

Windows VMs managed by the xen provisioning adapter and the hyperv provisioning adapter can be "sysprepped" in the Orchestration Console. To do so, make sure that you have performed the following prerequisite tasks:

- Create a Windows VM by using the Xen hypervisor.
- Make sure the VM is discovered by the Orchestration Server.
- Configure the VM (or a template of the VM) by using the information in Section 7.1.2, "Setting Sysprep Facts in the Orchestration Console," on page 68 and in Section 7.1.3, "Using the Sysprep deploy.cab Files," on page 77.

When the prerequisites are met, you can proceed to sysprep the xen VM by using the information in Section 7.1.4, "Applying Sysprep Facts," on page 79.

This section includes the following information:

- Section 7.1.1, "How Sysprep Works," on page 68
- Section 7.1.2, "Setting Sysprep Facts in the Orchestration Console," on page 68
- Section 7.1.3, "Using the Sysprep deploy.cab Files," on page 77
- Section 7.1.4, "Applying Sysprep Facts," on page 79
- Section 7.1.5, "Example Sysprep Scenarios," on page 79
- Section 7.1.6, "Known Sysprep Limitations," on page 80

7.1.1 How Sysprep Works

This section includes the following information:

- "Sysprep on VMware VMs" on page 68
- "Sysprep On Xen VMs" on page 68

Sysprep on VMware VMs

Sysprep facts (see Section 7.1.2, "Setting Sysprep Facts in the Orchestration Console," on page 68) are translated by the vSphere provisioning adapter into a VMware image-customization specification. The provisioning adapter passes the specification to the vSphere client API, which does the customization work. The changes made are leveraged by the Windows sysprep facility to complete final reconfiguration.

The vsphere provisioning adapter requires the VMware Tools package installed and running on the target VM before sysprep can be done, because that is a requirement of the underlying VMware Image Customization functionality leveraged by the Orchestration Server.

NOTE: In order for sysprep to run, it must be installed on the vCenter server host. For information about the requirements, see Sysprep file locations and versions (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005593) in the VMware knowledge base.

Sysprep On Xen VMs

The xen provisioning adapter uses the settings specified in the sysprep facts to perform an "unattended mini-setup" to reconfigure the VMs' Windows guest operating system. The provisioning adapter directly modifies the VM image without need for any agent, so you can configure sysprep on a "cold" VM image in the same way as you can run the *Install Agent* action on that image.

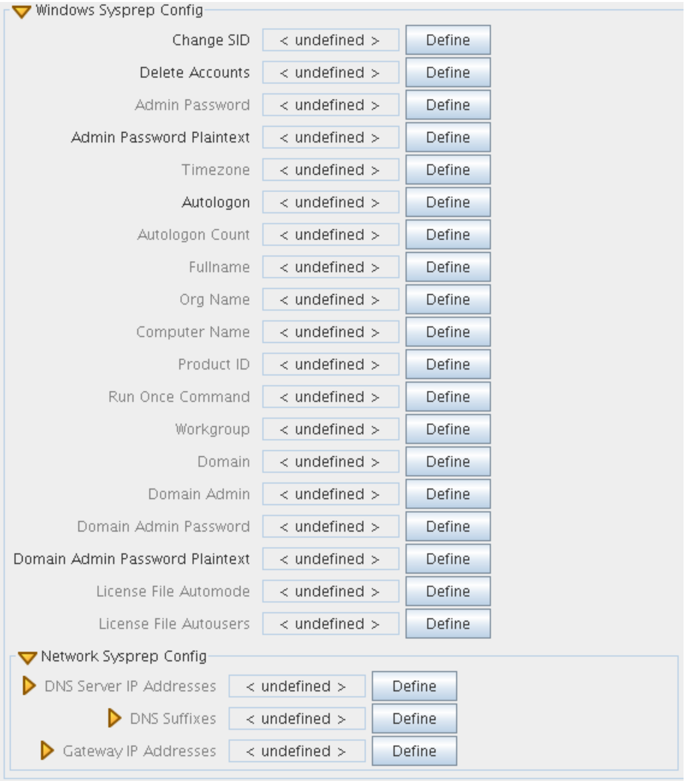
NOTE: You can perform the *Install Agent* and *Personalize* actions at the same time on a Xen Windows VM. The two operations cooperate and complete without conflict.

7.1.2 Setting Sysprep Facts in the Orchestration Console

You can use the Orchestration Console to configure the facts for sysprep of a VM. This section includes information about the Orchestration Console interface where those facts are set.

When you select a Windows VM object in the Explorer tree of the Orchestration Console, click the *Info/Groups* tab to open the Info Groups page, then scroll down to the *Provisioning Information* panel of this page. Open the *Windows Sysprep Config* subpanel and the *Network Sysprep Config* subpanel.

Figure 7-1 *The Sysprep Sections of the Info/Groups Page of a VM Template Object*



Windows Sysprep Config

Change SID	< undefined >	Define
Delete Accounts	< undefined >	Define
Admin Password	< undefined >	Define
Admin Password Plaintext	< undefined >	Define
Timezone	< undefined >	Define
Autologon	< undefined >	Define
Autologon Count	< undefined >	Define
Fullname	< undefined >	Define
Org Name	< undefined >	Define
Computer Name	< undefined >	Define
Product ID	< undefined >	Define
Run Once Command	< undefined >	Define
Workgroup	< undefined >	Define
Domain	< undefined >	Define
Domain Admin	< undefined >	Define
Domain Admin Password	< undefined >	Define
Domain Admin Password Plaintext	< undefined >	Define
License File Automode	< undefined >	Define
License File Autousers	< undefined >	Define

Network Sysprep Config

DNS Server IP Addresses	< undefined >	Define
DNS Suffixes	< undefined >	Define
Gateway IP Addresses	< undefined >	Define

Windows VMs that you clone can be personalized and prepared for provisioning by configuring the facts in this panel. Click *Define* on each field if the value has not been previously configured.

NOTE: You can trigger a sysprep for a Windows VM just by configuring the *Admin Password* field on this page. The provisioning adapter fills in the other required values with reasonable defaults if you don't specify them. For example, the value for the *Computer Name* field uses the VM name in the Orchestration Server by default.

When you finish changing the settings in this panel, right-click the VM and select *Personalize* for the changes to take effect. This sets up a pending customization that does not take place until the VM is powered on (provisioned) again.

IMPORTANT: On VMs managed by Xen and vSphere, running the *Personalize* action on a templated VM is not supported. Running this action results in failure because it is not supported in the underlying system. When you clone or provision from a templated VM, select the *Use Autoprep* check box.

This section also includes the following information:

- "Sysprep Facts" on page 69
- "Configuring vNIC Sysprep Facts" on page 76

Sysprep Facts

The following table lists the facts that are either required or optional for configuring sysprep.

Table 7-1 Required or Optional Facts for Sysprep Configuration

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Change SID	`<fact name="resource.provisioner.autoprep.options.changeSID" value="false" type="Boolean" />`	Automatic default value provided by the Orchestration Server[1]	The Windows Security ID. If this is marked as true, sysprep generates a new Security ID. If this is not selected, the Orchestration Server defaults the value to true, meaning a new SID is to be generated during sysprep. For newer (that is, unattended `.xml`-based) sysprep, unless this fact is defined and explicitly set to false, the SID is always changed. This is the desired behavior for cloning a Windows machine.
Delete Accounts	`<fact name="resource.provisioner.autoprep.options.deleteAccounts" value="false" type="Boolean" />`	Optional[2]	(Windows with vSphere VMs) When this check box is selected (it has a value of true), the Orchestration Server removes all user accounts from the destination VM; the Administrator account and other Windows “standard” accounts are left in place. If it is false, existing accounts from the source VM are retained. (Xen) This field is deprecated for Xen sysprep. Instead, ensure that the VM image has the required set of accounts from the beginning. No account deletion is done unless this fact is defined and set to true. Also, some versions of Windows sysprep do not support account deletion during sysprep, in which case this flag is ignored.
Admin Password	`<fact name="resource.provisioner.autoprep.sysprep.GuiUnattended.AdminPassword.value" value="" type="String" />`	Required[3]	The Admin password for this VM. **NOTE:** Only a plaintext admin password is currently supported. You should leave this field blank if *Admin Password Plaintext* is not selected. This fact must be specified or the personalization fails. Windows sysprep requires that this be specified.

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Admin Password Plaintext	`<fact name="resource.provisioner.autoprep.sysprep.GuiUnattended.AdminPassword.plainText" value="false" type="Boolean" />`	Automatic default value provided by the Orchestration Server[1]	When this check box is selected (it has a value of true) the *Admin Password* value is entered in plain text. If not set, this fact defaults to true, indicating that the AdminPassword fact is a plain text password. The Orchestration Server does not support automatic encryption of the password, so if you want to use an encrypted password, you need to know how to encrypt the password correctly for `sysprep.inf`, then enter it as `AdminPassword.value` with this flag set to false.
Timezone	`<fact name="resource.provisioner.autoprep.sysprep.GuiUnattended.TimeZone" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The time zone of the new VM. For sysprep on Windows versions prior to Vista, (that is, versions using `sysprep.inf`), numeric time zone codes are used. See the Microsoft sysprep documentation for values (for example, 04 indicates PST, 10 indicates MST, 20 indicates Central, 35 indicates EST as defined in the Windows sysprep documentation (http://technet.microsoft.com/en-us/library/cc749073.aspx)). **NOTE:** Make sure that you use the exact text string listed under the Time Zone column heading in the table included in this Microsoft article. For sysprep on Windows Vista and later (that is, versions using `unattend.xml`), full string time zone names are used. Refer to the Microsoft sysprep documentation for the relevant Windows version. If you do not set this fact, the default time zone for `sysprep.inf` (UTC or 85) is used.

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Autologon	`<fact name="resource.provisioner.autoprep.sysprep.GuiUnattended.AutoLogon" value="false" type="Boolean" />`	Optional[2]	When this check box is selected (it has a value of true) the VM automatically logs on to the Administrator account by using *AdminPassword*. If the value is false, logon is prompted. If no value is provided, the fact is set to false.
Autologon Count	`<fact name="resource.provisioner.autoprep.sysprep.GuiUnattended.AutoLogon" value="" type="Boolean" />>`	Optional[2]	The limit count for the VM to automatically log on with the Administrator account. *AutoLogon* must be true for this value to be accepted. If a value is not specified for this fact, but *Autologon* is set to true, the value defaults to 1.
Fullname	`<fact name="resource.provisioner.autoprep.sysprep.UserData.FullName" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The user's full name required by the Windows OS installer during installation.
Org Name	`<fact name="resource.provisioner.autoprep.sysprep.UserData.OrgName" value="" type="String" />`	Automatic default value provided by the Orchestrtation Server[1]	The organization name required by the Windows OS installer during installation. This fact is required by sysprep. If the value is not specified, the provided default is Organization Name. This fact is nonessential for Windows functionality.

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Computer Name	`<fact name="resource.provisioner.autoprep.sysprep.UserData.ComputerName" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The VM’s new host name. If you specify an asterisk (*) in this field, the Orchestration Server generates the name based on the source VM name. This fact is required by sysprep. If the value is not set, the default value is the name of the VM in the Orchestration Server. The name cannot be longer than 15 characters because of a Windows limitation on the length of the computer name. Values longer than 15 characters are not accepted. Because facts can be edited using methods other than the Admin view of the Orchestration Console, be aware that there are other restrictions regarding the characters you can use for the Computer Name. The following characters are not allowed: whitespace ` ! @ # $ ^ & * () + = [] {} \ | ; : ' " , <> / ? Other methods you could use to edit the computer name fact might not enforce any restrictions or constraints on the naming. If the naming is invalid, the VM might hang during sysprep.

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Product ID	`<fact name="resource.provisioner.autoprep.sysprep.UserData.ProductID" value="" type="String" />`	Effectively required[4]	The Windows product key. The ID is obtained from the Windows MSDN CD or from Microsoft. The value is used when building a new VM. This fact is optional for the Orchestration Server, but if the value is not specified, the Windows VM might stop at a user prompt on its console waiting for the entry of the Product ID. Certain versions of Windows, such Windows Server 2008, might not require a product key at installation, but will eventually require it (or a valid license server setup for product activation).
Run Once Command	`<fact name="resource.provisioner.autoprep.sysprep.GuiRunOnce.Command" value="" type="String" />`	Optional[2]	A list of commands separated by new line characters that run the first time a user logs on after the new VM is created. Commands are scheduled by using the `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce` registry key. The value does not need to be specified. It is passed to the sysprep answer file only if one or more commands are specified in the list.
Workgroup	`<fact name="resource.provisioner.autoprep.sysprep.Identification.JoinWorkgroup" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The Windows workgroup name. If the VM is joining a domain, use `JoinDomain`. Sysprep requires either a domain or a workgroup to be joined. This fact is ignored if the `Domain` fact and related facts are set, because domain joining takes priority over Workgroup joining. If no domain is being joined, and this fact is not specified, the default value becomes WORKGROUP (default with Windows).

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
Domain	`<fact name="resource.provisioner.autoprep.sysprep.Identification.JoinDomain" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The Windows domain name. If the VM is joining a workgroup, use `JoinWorkgroup`. For joining a domain, `DomainAdmin` and `DomainAdminPassword` must be defined. No default value is provided if this value is not set. Instead, a workgroup is joined with the default name WORKGROUP if no `Workgroup` fact was set. See also: Domain Admin Password (required if a value is set for this fact).
Domain Admin	`<fact name="resource.provisioner.autoprep.sysprep.Identification.DomainAdmin" value="" type="String" />`	Required[3]	Provide a value for this fact when the `Domain` fact has a value. Configuring this fact allows sufficient privileges to the Windows sysprep program to add the new server or workstation to the domain. Normally, this is the Administrator account for the domain. If the `Domain` fact does not have a value, this fact is ignored.
Domain Admin Password	`<fact name="resource.provisioner.autoprep.sysprep.Identification.DomainAdminPassword.value" value="" type="String" />`	Required[3]	Provide a value for this fact when the `Domain` fact has a value. Configuring this fact allows sufficient privileges to the Windows sysprep program to add the new server or workstation to the domain. Normally, this is the Administrator password for the domain. If the `Domain` fact does not have a value, this fact is ignored.
Domain Admin Password Plaintext	`<fact name="resource.provisioner.autoprep.sysprep.Identification.DomainAdminPassword.plainText" value="false" type="Boolean" />`	Automatic default value provided by the Orchestration Server[1]	When this check box is selected (it has a value of true), `DomainAdminPassword` is in plaintext. The value defaults to true if it is not set. The value is currently ignored for sysprep, because there are no fields to accept this flag in `sysprep.inf` or `unattend.xml`.

String in Orchestration Console UI	Fact Name	Required/ Optional	Description and Information
License File Automode	`<fact name="resource.provisioner.autoprep.sysprep.LicenseFilePrintData.AutoMode" value="" type="String" />`	Automatic default value provided by the Orchestration Server[1]	The value in this field is either PerServer or PerSeat. If it is set to PerServer, the `AutoUsers` fact must be set. A value for this fact is required for sysprep on Windows Server products. The provided default is PerServer.
License File Autousers	`<fact name="resource.provisioner.autoprep.sysprep.LicenseFilePrintData.AutoUsers" value="200" type="Integer" />`	Automatic default value provided by the Orchestration Server[1]	Specify value between 1 and 9999, representing the number of client licenses per seat. A value for this fact is required for sysprep on Windows Server products. The provided default is 5.

[1] Facts with automatic default values must be set in the `sysprep.inf` or `unattend.xml` answer file, but the vmprep job provides useful "generic" defaults if any of these facts are not specified. In general, a VM can be successfully personalized using only an Admin Password and Product ID. Some versions of Windows do not require the Product ID if their activation timeout for Windows Product Activation has not yet expired.

[2] Optional facts are never required. They are not placed in `sysprep.inf` or `unattend.xml` if a value is not specified. For the purpose of this documentation, "optional" also means that sysprep continues to function if these facts are not specified; however, optional facts might be needed as part of a Domain join or a similar function.

[3] There is no way to provide default values for required facts, and sysprep fails ungracefully if they are not specified. The vmprep job fails a Personalization action if these facts are not set by the user.

[4] For sysprep, this is the only fact that is "effectively" required. Some versions of Windows can be installed or sysprepped without this value, but most versions stop during sysprep and await user interaction at a Product Key prompt if this value is not specified in `sysprep.inf` or `unattend.xml`.

Configuring vNIC Sysprep Facts

VMs can be prepared for provisioning by configuring the facts in either the *Autoprep Network Adapter* subpanel (Windows VMs) of the vNIC *Info/Groups* panel or the *Sysprep Network Adapter* subpanel (Linux VMs). For more information, see "Defining Autoprep/Sysprep Network Adapter Facts on the vNIC Object" on page 84.

Virtual NIC sysprep facts are always optional. If they are not specified, Windows chooses "typical system" values, including setting vNICS to use DHCP.

7.1.3 Using the Sysprep deploy.cab Files

By default, Microsoft does not include the `sysprep.exe` or `setupcl.exe` utilities needed for sysprep on Windows Server 2003, Windows XP, or any previous version. To provide sysprep functionality for VMs running these Windows versions, the Orchestration Server must have access to compatible `deploy.cab` files from Microsoft. These files can usually be copied directly from the Windows installation CD, or they can be downloaded from Microsoft.

For Windows Vista, Windows Server 2008, and later releases, Microsoft includes the needed sysprep tools on the OS installation and uses a different "answer file" format and utility syntax. For these newer versions of Windows, there is no need to download additional files from Microsoft, or to copy them from the installation CD.

The following instructions apply only if you want to perform sysprep-based personalization on Windows 2003 VMs, Windows XP VMs, or earlier versions of Windows VMs. The instructions include the following:

- ".cab File Installation Locations" on page 77
- "Detailed Instructions for Downloading .cab Files From Microsoft" on page 78
- "Detailed instructions for Copying deploy.cab from the Windows Installation CD or DVD" on page 78

.cab File Installation Locations

Assuming a normal install of the Orchestration Server, the server's datagrid file tree is located in the `/var/opt/novell/zenworks/zos/server/datagrid/` directory. Copy the `.cab` files to one of the following locations (leaving off the fully qualified portion of the path before `"/datagrid`") as appropriate for the Windows server operating system:

```
dataGrid/files/sysprep/winserver2003_sp1/x86/deploy.cab
dataGrid/files/sysprep/winserver2003_r2/x86/deploy.cab
dataGrid/files/sysprep/winserver2003/x86/deploy.cab
dataGrid/files/sysprep/windowsxp/x86/deploy.cab
dataGrid/files/sysprep/windowsxpx64/x86_64/deploy.cab
dataGrid/files/sysprep/winserver2003x64/x86_64/deploy.cab
dataGrid/files/sysprep/winserver2003x64_r2/x86_64/deploy.cab
```

Notice that the files are named according to the `resource.os.type` fact, the `resource.os.arch` fact, and (optionally) whether the VM's operating system is SP1, R2, or something similar. The file tree in the list above covers all of the common releases of Windows.The sysprep job looks for the datagrid file in the following path:

```
grid:///sysprep/<resource.os.type>_<servicepack>/<resource.os.arch>/deploy.cab
```

If the Orchestration Server cannot find the `.cab` file in this path, it looks for the datagrid file in the following path:

```
grid:///sysprep/<resource.os.type>/<resource.os.arch>/deploy.cab
```

If you want to install the precise version of `deploy.cab` from your Windows CD, use the above convention to copy it to the `/datagrid` directory.

Through testing, NetIQ has determined that only two unique `.cab` files are required to support the most common Windows versions. See the Download Instructions exceptions on the Microsoft site for details. This method works because the Orchestration Server uses only the `sysprep.exe` and `setupcl.exe` executables from the `.cab` files. The other utilities are not used because their purpose is to manually build `sysprep.inf`. the Orchestration Server automatically builds its own answer file as part of the VM personalization process.

Detailed Instructions for Downloading .cab Files From Microsoft

Use the following steps to download the `.cab` files from Microsoft that you need for sysprep for Xen and Hyper-V VMs.

TIP: You can deploy the `.cab` files using any user account that has admin rights.

1 (Conditional) Download the Windows 2003 `.exe` file containing `deploy.cab`.

- **1a** From a Web browser, navigate to the Microsoft Download Center page entitled *System Preparation tool for Windows Server 2003 Service Pack 2 Deployment* (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=93f20bb1-97aa-4356-8b43-9584b7e72556&displaylang=en), then download the Windows 2003 sysprep tool, `WindowsServer2003-KB926028-v2-x86-ENU.exe`.
- **1b** Copy the `.exe` file to a suitable location on a Windows physical or virtual machine, then run the executable with the `/x` flag (which specifies file extraction only) to extract `deploy.cab` from the executable bundle.
- **1c** Navigate to the extracted directory where `deploy.cab` is located.
- **1d** Copy `deploy.cab` to the appropriate locations on the Orchestration Server:

2 (Conditional) Download the Windows XP `.cab` file:

- **2a** From a Web browser, navigate to the Microsoft Download Center page entitled *Windows XP Service Pack 2 Deployment Tools* (http://www.microsoft.com/downloads/en/details.aspx?FamilyId=3E90DC91-AC56-4665-949B-BEDA3080E0F6&displaylang=en) , then download the Windows XP sysprep tool, `WindowsXP-KB838080-SP2-DeployTools-ENU.cab`.
- **2b** Run the `.cab` file on a Windows physical or virtual machine to extract `deploy.cab`.
- **2c** Navigate to the extracted directory where `deploy.cab` is located.
- **2d** Copy `deploy.cab` to the appropriate locations on the Orchestration Server:

VM personalization testing using the two versions of `deploy.cab` files listed above has determined that they are suitable for common versions of Windows. When you have placed copies of the `deploy.cab` file in the proper directories of the Orchestration Server machine, you can perform sysprep personalization on pre-Vista versions of Windows.

You can download other, potentially newer, `deploy.cab` files from Microsoft, but be sure you are familiar with how to use the Microsoft sysprep tools and that the version you download matches the version of your VMs. Make sure you use the file and directory naming conventions explained in this section, so that the personalization system uses the correct `deploy.cab` for the VM being personalized.

Detailed instructions for Copying deploy.cab from the Windows Installation CD or DVD

If the version of `deploy.cab` you download from Microsoft is not suitable for the Windows version on your Windows VMs, you can copy `deploy.cab` for the version of Windows server you need directly from the Microsoft installation CD or DVD. The file is normally located in the following path relative to the CD's root directory:

```
support/tools/deploy.cab
```

Copy `deploy.cab` to the correct location in the datagrid file tree of the Orchestration Server according your Windows version (see ".cab File Installation Locations" on page 77). For example, if your CD is the x86_64 version of Windows 2003 Server SP2, copy it to the following location on the Orchestration Server computer:

```
dataGrid/files/sysprep/winserver2003x64_sp2/x86_64/deploy.cab
```

You can also copy `deploy.cab` to the alternate location used for fall back:

```
dataGrid/files/sysprep/winserver2003x64/x86_64/deploy.cab
```

NOTE: If the `.cab` file you download from Microsoft (see "Detailed Instructions for Downloading .cab Files From Microsoft" on page 78) causes problems with sysprep on your VM images, using the method of coping `deploy.cab` described in this section might correct compatibility problems.

7.1.4 Applying Sysprep Facts

For vSphere VMs, the vmprep.job is not used. Instead, the Orchestration Server uses VMware Image Customization through the vsphere provisioning adapter's vi-client facility. For more information, see "Sysprep on VMware VMs" on page 68.

For Xen VMs, the Orchestration Server applies the sysprep facts by launching the vmprep job when the facts are defined. This job runs automatically and applies the appropriate facts to a VM in the following situations:

- When you run a *Personalize* action on any non-templated VM. (See "Right-Click VM Commands" in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*).

  On VMs managed by Xen and vSphere, running the *Personalize* action on a templated VM is not supported. Running this action results in failure because it is not supported in the underlying system. When you clone or provision from a templated VM, select the *Use Autoprep* check box.
- When you create a VM clone by initiating the *Clone* action on a VM template.

  You must select the *Use Autoprep* check box in the Orchestration Console if autoprep facts are to be used when the *Clone* action is initiated.

You need to make sure that the VM template is set up according to your needs before you clone or provision it, so that the resulting clone meets your needs.

7.1.5 Example Sysprep Scenarios

Scenario 1: You want to create 25 dynamic VM instances to test job provisioning. You will never use these instances again, so you will not personalize them.

You create a VM template by right-clicking a VM, then you select *Create Template*. When the VM Template is created in the Explorer Tree, you define its sysprep facts in the *Info/Groups* page by specifying an asterisk in the *MAC Address* field, then you select the *Use DHCP* check box. This lets the Orchestration Console autogenerate the MAC address and retrieve network data from the DHCP server. For information about setting sysprep facts on each vNIC, see "Virtual NIC Info Panel" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

When the sysprep facts are defined, you provision this template. You right-click the template object and select *Provision*, then in the Provision VM dialog box, you specify that you want to provision (create) 25 new VM instances from this template. Provisioning automatically applies the sysprep facts from the template.

Scenario 2: You have created three VM clones in your grid and you want to provision those clones. You want to ensure that the MAC address and other key network information for each clone is unique, even though each clone is a copy of the same OS image. These clones are to be detached later and used for such things as mail servers and Web servers. When the clones were first created, sysprep facts were applied, but now you have changed those facts by adding static IP addresses, subnet masks, and gateway addresses for each. Each clone must be "personalized" because of this change to basic network identifiers.

To personalize, you select each Clone object, then define the adapter-specific settings on the *Info/ Groups* page by entering IP addresses, subnet masks, and gateway addresses for each adapter. When you have defined the sysprep facts on each VM clone, you right-click each Clone object in turn and select *Personalize* to apply the new network configuration.

For more information, see "Changing a Virtual Machine Template Clone to an Instance" and "Personalize" in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*.

7.1.6 Known Sysprep Limitations

There are some limitations that you need to be aware of when you use sysprep on VMs:

- When a VM is sysprepped on vSphere, two reboots are required after the VM is first started in order for Windows to apply VMware and sysprep reconfigurations. Windows VMs managed by Xen and syspreppred also require two reboots.
- Before performing a sysprep operation on a vSphere VM, you must first configure the VM to have the VMware Tools guest OS package installed. The VMware administrator must also have configured the Virtual Center server to allow sysprep. For more information, see the VMware vSphere Online Library (http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=admin/c_installing_the_microsoft_sysprep_tools.html).
- When a VM is sysprepped in vSphere, it goes into a "customization pending" state that is not cleared until the VM successfully starts and the prep is complete. This means that subsequent attempts to sysprep fail until the VM reboots and the previous prep completes. There is no way to directly reverse customization in vSphere.
- When you create a template of a VM with the Windows Server 2008 R2 OS, make sure that you configure the sysprep settings for all of its network interfaces using a DHCP connection, not an IP address. This is necessary because of a problem in Windows sysprep that does not remove old IP addresses from the template. The guest OS must not have an IP configured when it is sysprepped.

  When the template has been prepared to use DHCP, subsequent syspreps of the clones of that template can use an IP address.
- Testing has shown that personalizing VMs that have pre-Vista Windows operating systems does not properly configure some network settings. This is a sysprep limitation. The issue is manifest when vNIC-specific settings from sysprep facts on the VM's vNICs are not configured in the VM after personalization.

  To work around this issue, personalize by using DHCP settings. You can do this by leaving the fields blank. DHCP is the default for network settings.
- If a Hyper-V VM is running during the discover process, it fails to discover the `resource.os.family` fact. This prevents the Orchestration Console from displaying the *Sysprep* and *Autoprep* options section on the *Info/Groups* tab for the VM.

  NOTE: If the VM not running when the discovery occurs, the hyperv provisioning adapter discovers `resource.os.family` itself.

If you create a template from this VM, the `resource.os.family` fact is discovered and populated on the VM template admin view.

To display the sysprep/autoprep settings on a Hyper-V VM use the following steps:

1. Shut down the Hyper-V VM that has the problem.
2. In the Explorer Tree, right-click the VM you have shut down, then select *Resync State.*
3. In the Orchestration Console, Shift+click the Refresh 🔄 icon or restart the Orchestration Console to refresh all of the objects and their facts in the Resource admin view.

- Sysprep does not work on Windows VMs until you set a value for the `Admin Password` fact: `resource.provisioner.autoprep.sysprep.GuiUnattended.AdminPassword.value`.

  For information about this fact, see "Admin Password" on page 70.

- If you clone a Windows Server 2003 VM template originally created in the hypervisor environment, the administrator password for the VM template base image must be blank (no value), or the original VM administrator password is retained and you cannot log in to the cloned VM with the new password.

  Attempting to change an old password value by using the the `AdminPassword` entry in `sysprep.inf` does not work, but if the original password value was blank, you can use the `AdminPassword` entry in `sysprep.inf` to provide the password value and log in with that password. The value is applied from the `resource.provisioner.autoprep.sysprep.GuiUnattended.AdminPassword.value` sysprep fact when you select the *Use Autoprep* check box while creating a clone.

- Some sysprep problems have been noted with Windows Product Activation (WPA) functionality, particularly with versions of Wndows that require product activation by the end user.

  On Windows Server 2003 SP1, if you have a VM that has passed the initial activation deadline, and you sysprep it, sysprep is applied correctly, but that VM immediately changes to "limited functionality" mode and requires user intervention to reactivate it. Sysprep seems to remove activation and require that the VM be reactivated.

  Further, although there is a Boolean value (AutoActivate) that you can set in the "unattended" section of `sysprep.inf`, setting the value does not always result in auto activation of a VM.

  To avoid this situation, we recommend that you consider volume licensing or similar licensing solutions available from Microsoft that don't require manual activation by an actual user. For versions of Windows prior to Windows Vista, this would be a VLK (Volume License Key). For Windows Vista or later, Microsoft has license server-based solutions available to handle volume licensing.

In using sysprep on Windows VMs managed by Xen, no special agent or tools are needed for sysprep because of the method used by the xen provisioning adapter. See "Sysprep On Xen VMs" on page 68 for more information.

7.2 Understanding and Configuring Autoprep

In the Cloud Manager Orchestration Console, "autoprep" refers to the function of preparing unique network settings for a Linux VM so that VM can be provisioned by its provisioning adapter without creating network conflicts and without customizing other network-related settings.

As the administrator, you can set facts in the Orchestration Console that can later be applied to a VM clone during a *Provision* or a *Clone* action from a VM template. You can also use the *Personalize* action to manually apply autoprep facts to an existing VM.

This section includes the following information:

- Section 7.2.1, “How Autoprep Works,” on page 82
- Section 7.2.2, “Setting Autoprep Facts in the Orchestration Console,” on page 82
- Section 7.2.3, “Applying Autoprep Facts,” on page 86
- Section 7.2.4, “Example Autoprep Scenarios,” on page 86
- Section 7.2.5, “Known Autoprep Limitations,” on page 87

7.2.1 How Autoprep Works

The vmprep job always runs when you clone or provision from a VM template. The job prepares the root disk image of the VM with the defined autoprep settings. On a Linux system, the global autoprep settings for a VM are stored in various configuration files in the `/etc` directory. For example, the hostname is stored in `/etc/HOSTNAME`. Global network properties are stored in `/etc/sysconfig/network/config` and in `/etc/sysconfig/network/dhcp`. Per-NIC properties are written to the various `/etc/sysconfig/network/ifcfg.*` scripts, with one for each virtual NIC.

The vmprep job attempts to identify the disk image with the root partition, then mounts that partition and starts scanning the configuration files to make the necessary changes to the VM configuration file settings.

If the *Use Autoprep* check box in the Orchestration Console is not selected, the vmprep job still runs, but only to change the name of the Orchestration Agent (if installed) on the VM.

If you want a full autoprep with system config changes when cloning or provisioning from template, you need to select *Use Autoprep* check box in the Orchestration Console.

For Linux VMs, autoprep mounts the VM image’s root disk image and edits the appropriate files in the `/etc/` directory to make the desired configuration changes. This might include adding network interface configurations to the network configuration scripts. The changes take effect when the VM starts again.

IMPORTANT: If you plan to prepare virtual machines that use LVM as their volume manager on a SLES VM host, and if that VM host also uses LVM as its volume manager, you cannot perform autoprep if the VM has an LVM volume with the same name as one already mounted on the VM host. This is because LVM on the VM Host can mount only one volume with the same name.

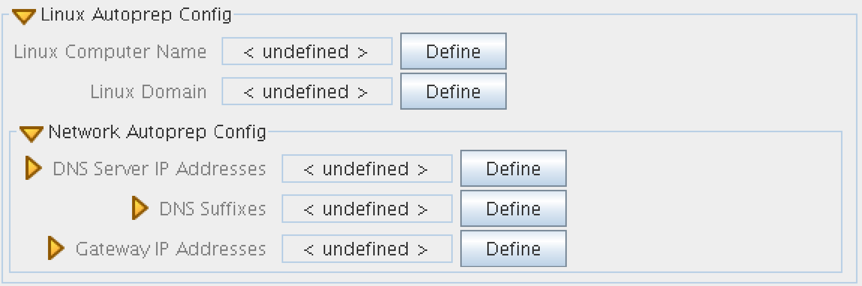
To work around this issue, ensure that the volume names on the VM hosts and virtual machines are different.

7.2.2 Setting Autoprep Facts in the Orchestration Console

You can use the Orchestration Console to configure the facts for autoprep of a VM. This section includes information about the Orchestration Console interface where those facts are set.

When you select a Linux VM object in the Explorer tree of the Orchestration Console, click the *Info/Groups* tab to open the Info Groups page, then scroll down to the *Provisioning Information* panel of this page. Open the *Linux Autoprep Config* panel and the *Network Autoprep Config* panels.

Figure 7-2 *The Autoprep Sections of the Info/Groups Page of a VM Template Object*


Linux Autoprep Config

Linux Computer Name: < undefined >

Linux Domain: < undefined >

Network Autoprep Config

DNS Server IP Addresses: < undefined >

DNS Suffixes: < undefined >

Gateway IP Addresses: < undefined >

Linux VMs that you clone can be personalized and prepared for provisioning by configuring the facts in this panel. Click *Define* on each field if the value has not been previously configured.

NOTE: When you change any of the settings in this panel, you need to right-click the VM and select *Personalize* for the changes to take effect. This action is in contrast to right-clicking a template, which can apply these settings during a provision or clone operation.

This section also contains this information:

- "Linux Autoprep Config" on page 83
- "Network Autoprep Config" on page 84
- "Defining Autoprep/Sysprep Network Adapter Facts on the vNIC Object" on page 84

Linux Autoprep Config

The settings located in the *Linux Autoprep Config* panel are global to a configuration of a Linux VM and are not specific to a particular network adapter.

NOTE: It is not mandatory to define these facts. If they are left undefined, they are not applied to the "autoprepped" VM.

- **Linux Computer Name:** The network host name of the new VM. If you specify an asterisk (*), the current Grid object ID (`resource.id`) of the new VM is used.

  The Linux Computer Name should be the unqualified computer name without the DNS domain suffix, such as webserver instead of webserver.acme.com.

  In the Fact Editor, this fact is listed as `resource.provisioner.autoprep.linuxglobal.ComputerName`:

  ```
  <fact name="resource.provisioner.autoprep.linuxglobal.ComputerName" value=""
  type="String" />
  ```
- **Linux Domain:** The network domain name where the new VM is a member.

  This field should contain the default DNS domain for the host, such as acme.com.

  In the Fact Editor, this fact is listed as `resource.provisioner.autoprep.linuxglobal.Domain`:

  ```
  <fact name="resource.provisioner.autoprep.linuxglobal.Domain" value=""
  type="String" />
  ```

Network Autoprep Config

This section includes the following fields:

- **DNS Server IP Addresses:** The list of DNS Servers for name for lookup. This setting is only for cloning/personalize actions. For Linux, it should be set only in the VM facts, not in the vNIC facts.

  In the Fact Editor, this fact is listed as an array:

  ```
  <fact name="resource.provisioner.autoprep.DNSServers">
    <array>
      <string></string>
    </array>
  </fact>
  ```

- **DNS Suffixes:** The list of suffixes to append to a name for lookup. This setting is only for cloning/personalize actions. For Linux, it should be set only in the VM facts, not in the vNIC facts.

  ```
  <fact name="resource.provisioner.autoprep.DNSSuffixes">
    <array type="String">
    </array>
  </fact>
  ```

- **Gateway IP Addresses:** The list of Internet gateways available to this VM. This setting is only for cloning/personalize actions. For Linux, it should be set only in the VM facts, not in the vNIC facts.

  In the Fact Editor, this fact is listed as an array:

  ```
  <fact name="resource.provisioner.autoprep.Gateways">
    <array>
      <string></string>
    </array>
  </fact>
  ```

Defining Autoprep/Sysprep Network Adapter Facts on the vNIC Object

VMs can be prepared for provisioning by configuring the facts in either the *Autoprep Network Adapter* subpanel (Windows VMs) of the vNIC *Info/Groups* panel or the *Sysprep Network Adapter* subpanel (Linux VMs). Click *Define* on each field if the value has not been previously configured.

NOTE: When you change any of the settings in this panel, you need to right-click the VM and select *Personalize* for the changes to take effect.

- **MAC Address:** The MAC address of the interface. Specify an asterisk (*) or specify no setting at all to generate a new MAC address. If the value is not set, the existing `vnic.mac` is used.

  IMPORTANT: An unset *MAC Address* fact generates a new MAC address. This is contrary to the current tool tip text.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.MACAddress`:

  ```
  <fact name="vnic.provisioner.autoprep.MACAddress" value="" type="String" />
  ```

- **Use DHCP:** When this check box is selected (it has a value of true), the VM is configured to retrieve its network settings from a DHCP server. If the check box is not selected (it has value of false), you should make sure that the IP address, subnet mask, and gateway address facts are defined. In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.UseDHCP`:

```
<fact name="vnic.provisioner.autoprep.UseDHCP" value="false" type="Boolean" />
```

- **IP Address:** The IP address for the adapter.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.IPAddress`:

  ```
  <fact name="vnic.provisioner.autoprep.IPAddress" value="" type="String" />
  ```

- **Subnet Mask:** The subnet mask for this adapter.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.subnetMask`:

  ```
  <fact name="vnic.provisioner.autoprep.subnetMask" value="" type="String" />
  ```

- **Gateway IP Addresses:** (Windows only) A list of the gateway IP addresses available to the interface.

  In the Fact Editor, this fact is listed as an array:

  ```
  <fact name="vnic.provisioner.autoprep.Gateways">
    <array type="String">
    </array>
  </fact>
  ```

  You can edit this array by clicking the ··· button to open an array editor. In this dialog box, you can add or remove the IP address or change its order in the array of element choices.

- **DNS from DHCP:** When this check box is selected (it has a value of true), the SUSE VM is configured to retrieve its DNS server settings from DHCP.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.DNSFromDHCP`:

  ```
  <fact name="vnic.provisioner.autoprep.DNSFromDHCP" value="false"
  type="Boolean" />
  ```

- **DNS Server IP Addresses:** (Windows VM only) The adapter's list of DNS servers used for name lookup.

  In the Fact Editor, this fact is listed as an array:

  ```
  <fact name="vnic.provisioner.autoprep.DNSServers">
    <array type="String">
    </array>
  </fact>
  ```

- **DNS Domain:** (Windows VM only) The adapter's DNS domain name.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.DNSDomain`:

  ```
  <fact name="vnic.provisioner.autoprep.DNSDomain" value="" type="String" />
  ```

- **Primary WINS Server:** (Windows VM only) The name of the adapter's primary WINS server.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.primaryWINS`:

  ```
  <fact name="vnic.provisioner.autoprep.primaryWINS" value="" type="String" />
  ```

- **Secondary WINS Server:** (Windows VM only) The name of the adapter's secondary WINS server.

  In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.secondaryWINS`:

  ```
  <fact name="vnic.provisioner.autoprep.secondaryWINS" value="" type="String" />
  ```

- **NetBIOS:** (Windows VM only) The NetBIOS options for this VM. Options include:
  - *EnableNetBIOSviaDhcp*
  - *EnableNetBIOS*
  - *DisableNetBIOS*

In the Fact Editor, this fact is listed as `vnic.provisioner.autoprep.netBIOS`:

```
<fact name="vnic.provisioner.autoprep.netBIOS" value="" type="String" />
```

NOTE: Although you can define individual static settings to be applied to these adapters, autoprep can be useful for provisioning multiple clones with unique, autogenerated MAC addresses and DHCP-defined IP addresses (even though the VM clones are copies of the same VM template OS image) by coupling the autoprep settings on the VM with the autoprep settings on the vNIC object associated with the VM, thus avoiding network conflicts. For more information about vNIC autoprep settings, see "Defining Autoprep/Sysprep Network Adapter Facts on the vNIC Object" on page 84.

7.2.3 Applying Autoprep Facts

The Orchestration Server applies the autoprep facts by launching the vmprep job when the facts are defined. This job runs automatically and applies the appropriate facts to a VM in the following situations:

- When a *Personalize* action is run on any non-template VM. (See "Right-Click VM Commands" in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*).

  On VMs managed by Xen and vSphere, running the *Personalize* action on a templated VM is not supported. Running this action results in failure because it is not supported in the underlying system. When you clone or provision from a templated VM, select the *Use Autoprep* check box.
- When a VM clone is created by initiating the *Clone* action on a VM template.

  Selectthe *Use Autoprep* check box in the Orchestration Console if autoprep facts are to be used when the *Clone* action is initiated.
- When a VM clone is created by initiating a *Provision* action on a VM template.

  Select the *Use Autoprep* check box in the Orchestration Console if autoprep facts are to be used when the *Clone* action is initiated.

7.2.4 Example Autoprep Scenarios

Scenario 1: You want to create 25 dynamic VM instances to test job provisioning. You will never use these instances again.

You create a VM template by right-clicking a VM, then you select *Create Template*. When the VM Template is created in the Explorer Tree, you define its autoprep facts in the *Info/Groups* page of the vNIC object by specifying an asterisk in the *MAC Address* field, then you select the *Use DHCP* check box. This lets the Orchestration Console autogenerate the MAC address and retrieve network data from the DHCP server. For information about setting autoprep facts on each vNIC, see "Virtual NIC Info Panel" in the *NetIQ Cloud Manager 2.1.5 Orchestration Console Reference*.

When the autoprep facts are defined, you provision this template. You right-click the template object and select *Provision*, then in the Provision VM dialog box, you specify that you want to provision (create) 25 new VM instances from this template. Provisioning automatically applies the autoprep facts from the template if the *Use Autoprep* check box is selected.

Scenario 2: You have created three VM clones in your grid and you want to provision those clones. You want to ensure that the MAC address and other key network information for each clone is unique, even though each clone is a copy of the same OS image. These clones are to be detached later and used for such things as mail servers and Web servers. When the clones were first created, autoprep facts were applied, but now you have changed those facts by adding static IP addresses, subnet masks, and gateway addresses for each. Each clone must be "personalized" because of this change to basic network identifiers.

To personalize, you select each Clone object, then define the adapter-specific settings on the *Info/ Groups* page of each of the VM's vNICs by entering IP addresses, DNS suffixes, and gateway addresses for each vNIC in the *Network Autoprep Config* subpanel. When you have defined the autoprep facts on each VM clone, you right-click each Clone object in turn and select *Personalize* to apply the new network configuration.

For more information, see "Changing a Virtual Machine Template Clone to an Instance" and "Personalize" in the *NetIQ Cloud Manager 2.1.5 VM Orchestration Reference*.

7.2.5 Known Autoprep Limitations

There are some limitations that you need to be aware of when you use autoprep:

- Currently, the *Gateway IP Addresses* setting in the *Info/Groups tab* for a VM object is available in a list box.

  Because the Linux VM OS accepts only one default gateway, it accepts only the first setting in the list as the actual gateway IP address. The other settings are ignored.
- Before performing an autoprep operation on a vSphere VM, you must first configure the VM to have the VMware Tools guest OS package installed. The VMware administrator must also have configured the Virtual Center server to allow sysprep. For more information, see the VMware vSphere Online Library (http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=admin/c_installing_the_microsoft_sysprep_tools.html).
- When a VM is autoprepped in vSphere, it goes into a "customization pending" state that is not cleared until the VM successfully starts and the prep completes. This means that subsequent attempts to autoprep fail until the VM reboots and the previous prep completes. There is no way to directly reverse customization in vSphere.
- Customization of a vSphere VM for autoprep does the following with regard to the MAC address:
  - If the MAC address field in the Orchestration Console autoprep subpanel is empty (or if an asterisk is entered), the Orchestration Server auto-generates a new MAC address.
  - If the MAC address value is in the range `00:50:56:00:00:00` ? `00:50:56:3f:ff:ff`, the Orchestration Server statically assigns the MAC address.
  - If the MAC address value is not empty and is outside the defined range, the Orchestration Server attempts to assign the MAC address, but it might be reassigned by vSphere if it is determined to be duplicate.

  For more information, see VMware Data Object - VirtualEthernetCard (http://www.vmware.com/support/developer/vc-sdk/visdk400pubs/ReferenceGuide/vim.vm.device.VirtualEthernetCard.html) documentation.
- The vsphere provisioning adapter checks the setting for the host name. If the host name is not set, the setting defaults to the VM name in the Orchestration Server.
- If a Hyper-V VM is running during the discover process, it fails to discover the `resource.os.family` fact. This prevents the Orchestration Console from displaying the *Sysprep* and *Autoprep* options section on the *Info/Groups* tab for the VM.

  NOTE: If the VM not running when the discovery occurs, the hyperv provisioning adapter discovers `resource.os.family` itself.

  If you create a template from this VM, the `resource.os.family` fact is discovered and populated on the VM template admin view.

  To display the sysprep/autoprep settings on a Hyper-V VM:

  1. Shut down the Hyper-V VM that has the problem.

2. From the Explorer Tree, right-click the VM you shut down, then select *Resync State*.
3. In the Orchestration Console, Shift+click the Refresh 🔄 icon or restart the Orchestration Console to refresh all of the objects and their facts in the Resource admin view.

8 Configuring Connections to the Cloud Manager Application Server

The Cloud Manager Orchestration Server requires an HTTP connection to each Cloud Manager Application Server that you want to define as a zone in your Cloud Manager system. This connection can be secure (SSL) or non-secure (no SSL).

The following sections provide instructions for enabling secure and non-secure connections. You must complete the instructions for each Cloud Manager Orchestration Server that you plan to define as a Cloud Manager zone.

- Section 8.1, "Enabling a Secure Connection," on page 89
- Section 8.2, "Enabling a Non-Secure Connection," on page 90

8.1 Enabling a Secure Connection

A secure connection requires certificate authentication between the Cloud Manager Application Server and the Cloud Manager Orchestration Server.

The first time it is started, the Cloud Manager Web Service creates a keystore, generates a public/private key pair, and exports the public key to a certificate. The Web Service is started automatically as part of the Cloud Manager Orchestration Server startup or manually by using the following command:

```
/etc/init.d/novell-pso-ws start
```

To complete the configuration of the secure connection, you need to import the Cloud Manager Web Service's public certificate to the Cloud Manager Application Server trust store and configure the secure port for the Cloud Manager Web Service. The following sections provide instructions:

- Section 8.1.1, "Configuring the Cloud Manager Web Service Secure Port," on page 89

8.1.1 Configuring the Cloud Manager Web Service Secure Port

By default, the Cloud Manager Web Service listens on port 8443. You can change this port if necessary.

1. On the Cloud Manager Orchestration Server, open the `jetty-ssl.xml` file:

   ```
   /etc/opt/novell/pso-ws/jetty/jetty-ssl.xml
   ```

2. Locate the `<Call name ="addConnector">` section. It will look similar to the section shown below:

```
<Call name="addConnector">
  <Arg>
    <New class="org.mortbay.jetty.security.SslSocketConnector">
      <Set name="Port">8443</Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="handshakeTimeout">2000</Set>
      <Set name="keystore"><SystemProperty name="jetty.home" default="."
        />/etc/keystore</Set>
      <Set name="password">OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4</Set>
      <Set name="keyPassword">OBF:1u2u1wml1z7s1z7a1wnl1u2g</Set>
      <Set name="truststore"><SystemProperty name="jetty.home"
        default="." />/etc/keystore</Set>
      <Set name="trustPassword">OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4</Set>
      <Set name="handshakeTimeout">2000</Set>
    </New>
  </Arg>
</Call>
```

3. In the `<Set name="Port">` directive, change the port number.

   When adding the Cloud Manager Orchestration Server as a zone in the Cloud Manager Application Console, you specify this port as the server port.

4. Save the `jetty-ssl.xml` file.

5. Restart the Cloud Manager Web Service:

   ```
   /etc/init.d/novell-pso-ws restart
   ```

8.2 Enabling a Non-Secure Connection

1. On the Cloud Manager Orchestration Server, open the `jetty.xml` file:

   ```
   /etc/opt/novell/pso-ws/jetty/jetty.xml
   ```

2. Uncomment the `<Call name =”addConnector”>` section that enables the non-secure port.

3. If you want the Cloud Manager Web Service, which handles the connection for the server, to listen on a port other than 8080, change the port number.

   When adding the Cloud Manager Orchestration Server as a zone in Cloud Manager, you specify this port as the server port.

4. Save the `jetty.xml` file.

5. Restart the Cloud Manager Web Service:

   ```
   /etc/init.d/novell-pso-ws restart
   ```

A Advanced Agent Installation Methods

This section includes information you can use if you find that the standard and manual methods for installing the Orchestration Agent in your datacenter are inadequate.

- Section A.1, "Silent Installation of the Orchestration Agent," on page 91
- Section A.2, "Using an Orchestration Job to Install the Orchestration Agent on a VM Host," on page 93
- Section A.3, "Automatically Installing the Agent on a VM," on page 93

A.1 Silent Installation of the Orchestration Agent

In a large data center, it might not be practical to perform an interactive configuration of the Orchestration Agent on the multiple servers that you intend to use for Cloud Manager resources. The information in this section provides information that can help you perform a silent installation and configuration of the agent.

- Section A.1.1, "Silent Install and Configuration of the Orchestration Agent for Windows," on page 91
- Section A.1.2, "Silent Installation and Configuration of the Orchestration Agent RPM," on page 92

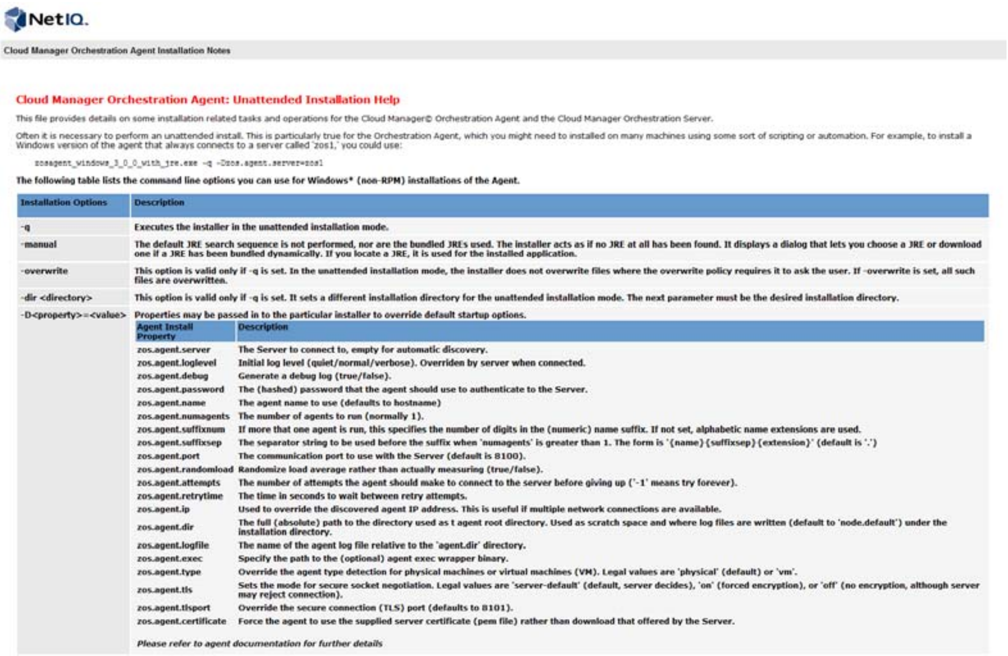
A.1.1 Silent Install and Configuration of the Orchestration Agent for Windows

The Cloud Manager Orchestration Server includes an installation help page that provides tips for installing the Windows Orchestration Agent on many machines when you want to use scripting or automation to perform a silent installation.

The page is accessed from the Orchestration Server IP address:

```
http://IP_address:8001/install.html
```

Figure A-1 *Orchestration Agent Silent Installation Help*



Cloud Manager Orchestration Agent Installation Notes

Cloud Manager Orchestration Agent: Unattended Installation Help

This file provides details on some installation related tasks and operations for the Cloud Manager© Orchestration Agent and the Cloud Manager Orchestration Server.

Often it is necessary to perform an unattended install. This is particularly true for the Orchestration Agent, which you might need to installed on many machines using some sort of scripting or automation. For example, to install a Windows version of the agent that always connects to a server called 'zos1,' you could use:

```
zosagent_windows_3_0_0_with_jre.exe -q -Dzos.agent.server=zos1
```

The following table lists the command line options you can use for Windows* (non-RPM) installations of the Agent.

Installation Options	Description
-q	Executes the installer in the unattended installation mode.
-manual	The default JRE search sequence is not performed, nor are the bundled JREs used. The installer acts as if no JRE at all has been found. It displays a dialog that lets you choose a JRE or download one if a JRE has been bundled dynamically. If you locate a JRE, it is used for the installed application.
-overwrite	This option is valid only if -q is set. In the unattended installation mode, the installer does not overwrite files where the overwrite policy requires it to ask the user. If -overwrite is set, all such files are overwritten.
-dir <directory>	This option is valid only if -q is set. It sets a different installation directory for the unattended installation mode. The next parameter must be the desired installation directory.
-D<property>=<value>	Properties may be passed in to the particular installer to override default startup options.

Agent Install Property	Description
zos.agent.server	The Server to connect to, empty for automatic discovery.
zos.agent.loglevel	Initial log level (quiet/normal/verbose). Overriden by server when connected.
zos.agent.debug	Generate a debug log (true/false).
zos.agent.password	The (hashed) password that the agent should use to authenticate to the Server.
zos.agent.name	The agent name to use (defaults to hostname)
zos.agent.numagents	The number of agents to run (normally 1).
zos.agent.suffixnum	If more that one agent is run, this specifies the number of digits in the (numeric) name suffix. If not set, alphabetic name extensions are used.
zos.agent.suffixsep	The separator string to be used before the suffix when 'numagents' is greater than 1. The form is '{name}{suffixsep}{extension}' (default is '.')
zos.agent.port	The communication port to use with the Server (default is 8100).
zos.agent.randomload	Randomize load average rather than actually measuring (true/false).
zos.agent.attempts	The number of attempts the agent should make to connect to the server before giving up ('-1' means try forever).
zos.agent.retrytime	The time in seconds to wait between retry attempts.
zos.agent.ip	Used to override the discovered agent IP address. This is useful if multiple network connections are available.
zos.agent.dir	The full (absolute) path to the directory used as t agent root directory. Used as scratch space and where log files are written (default to 'node.default') under the installation directory.
zos.agent.logfile	The name of the agent log file relative to the 'agent.dir' directory.
zos.agent.exec	Specify the path to the (optional) agent exec wrapper binary.
zos.agent.type	Override the agent type detection for physical machines or virtual machines (VM). Legal values are 'physical' (default) or 'vm'.
zos.agent.tls	Sets the mode for secure socket negotiation. Legal values are 'server-default' (default, server decides), 'on' (forced encryption), or 'off' (no encryption, although server may reject connection).
zos.agent.tlsport	Override the secure connection (TLS) port (defaults to 8101).
zos.agent.certificate	Force the agent to use the supplied server certificate (pem file) rather than download that offered by the Server.

Please refer to agent documentation for further details

A.1.2 Silent Installation and Configuration of the Orchestration Agent RPM

Use the following process to configure the Orchestration Agent RPM (downloaded from the product ISO) on multiple servers:

1. Perform the product installation and manual configuration of the agent on a “seed” machine. The processes to do this are described in (referenceto Agent Install).
2. On the “seed” machine, copy the file found at `/etc/opt/novell/novell_zenworks_orch_install.conf` to a location where you can modify it locally.
3. Edit the local copy of `novell_zenworks_orch_install.conf`, updating the fields that require a password (for security purposes, when a configuration program runs, the passwords in the `.conf` file are deleted).
4. Edit any other fields as necessary for the configuration of the Orchestration Agent.
5. Distribute the modified file to the machines where you want to perform a silent configuration.
6. At a machine where you distributed the `.conf` file, open YaST and perform the Add-on Installation of the RPMs as described in Section 2.2.3, “Manually Installing the Agent Packages on SLES Machines,” on page 17. Make sure that you do not configure the agent manually.
7. From the bash prompt on the machine where you are configuring the agent, run the following command:

   ```
   /opt/novell/zenworks/orch/bin/config -s -C $CONF_FILE
   ```

   where *CONF_FILE* is the modified configuration file from Step 5.

The silent configuration runs, then the agent is displayed in the Orchestration Console as registered with the server node.

A.2 Using an Orchestration Job to Install the Orchestration Agent on a VM Host

The following jobe code sample shows how you can use a job to install the Orchestration Agent on a VM host.

```
"""
Search for a VM Grid objects using Constraints and run a VM operation on them.
"""
class test(Job):

   def job_started_event(self):

      # collect all VM Instances whose resource ID
      # starts with the string "apache"

      a = AndConstraint()

      e1 = EqConstraint()
      e1.setFact("resource.type")
      e1.setValue("VM")
      a.add(e1)

      e2 = EqConstraint()
      e2.setValue("apache*")
      e2.setMatchMode(EqConstraint.MATCH_MODE_REGEXP)
      e2.setFact("resource.id")
      a.add(e2)

      vms = getMatrix().getGridObjects(TYPE_RESOURCE,a,None)
      for vm in vms:
         vm.installAgent()
```

A.3 Automatically Installing the Agent on a VM

To automatically install the Orchestration Agent on a VM that you created in the client, right-click a VM that has been shut down, then select *Install Agent*. This launches a job that installs the Orchestration Agent on the VM, regardless of its platform. The agent's service is started the next time you provision the VM.

B Manually Registering a Resource in the Orchestration Console

If you want a higher level of security between the agent and the server, you can manually create a resource account in the Orchestration Console before the Orchestration Agent is installed. This section walks through both stages of the procedure.

- Section B.1, "Using the Orchestration Console to Create a Resource Account," on page 95
- Section B.2, "Installing an Orchestration Agent to Match the New Resource," on page 96

B.1 Using the Orchestration Console to Create a Resource Account

Use the following steps to create a resource object in the Orchestration Console.

1 Make sure that the *Auto Register Agents* check box on the grid object's *Authentication* page is not selected (see Step 2 on page 38).

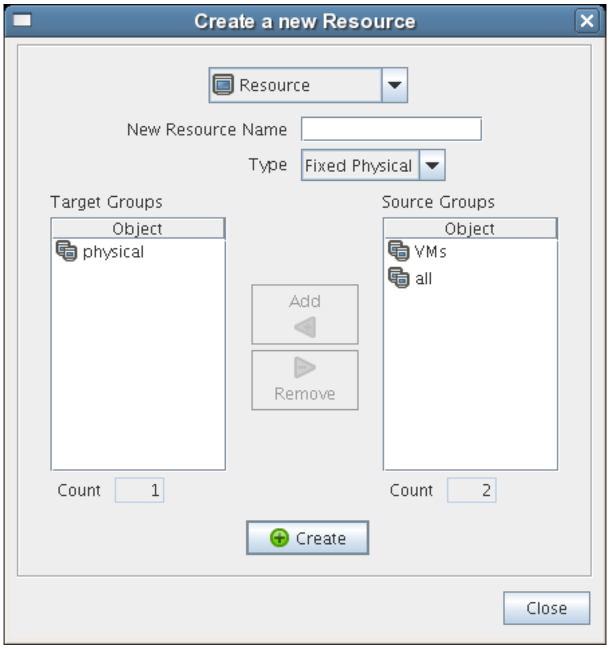
2 (Optional) Create a new resource from the Explorer panel in the Orchestration Console:

2a In the Explorer panel in the Orchestration Console, right-click *Resources*, then click *New Resource* to display the Create a new Resource dialog box.

2b Specify the name of the new resource you want to create in the *New Resource Name* field, then click *OK*.

3 (Optional) Create a new resource from the Main Menu in the Orchestration Console.

3a In the Orchestration Console, click *Actions* > click *Create Resource* to display the an expanded version of the Create a new Resource dialog box.



Resource

New Resource Name

Type: Fixed Physical

Target Groups	Source Groups
Object	Object
physical	VMs all
Count 1	Count 2

This dialog box includes a method for designating the resource as a fixed physical type or a virtual machine type. It also includes a method for including the resource in various resource groups. In this walkthrough, we will install an Orchestration Agent on a fixed physical resource and include it in the *physical* resource group.

The Virtual Machine resource type is not available if you installed the High Performance Computing license only for Orchestrate.

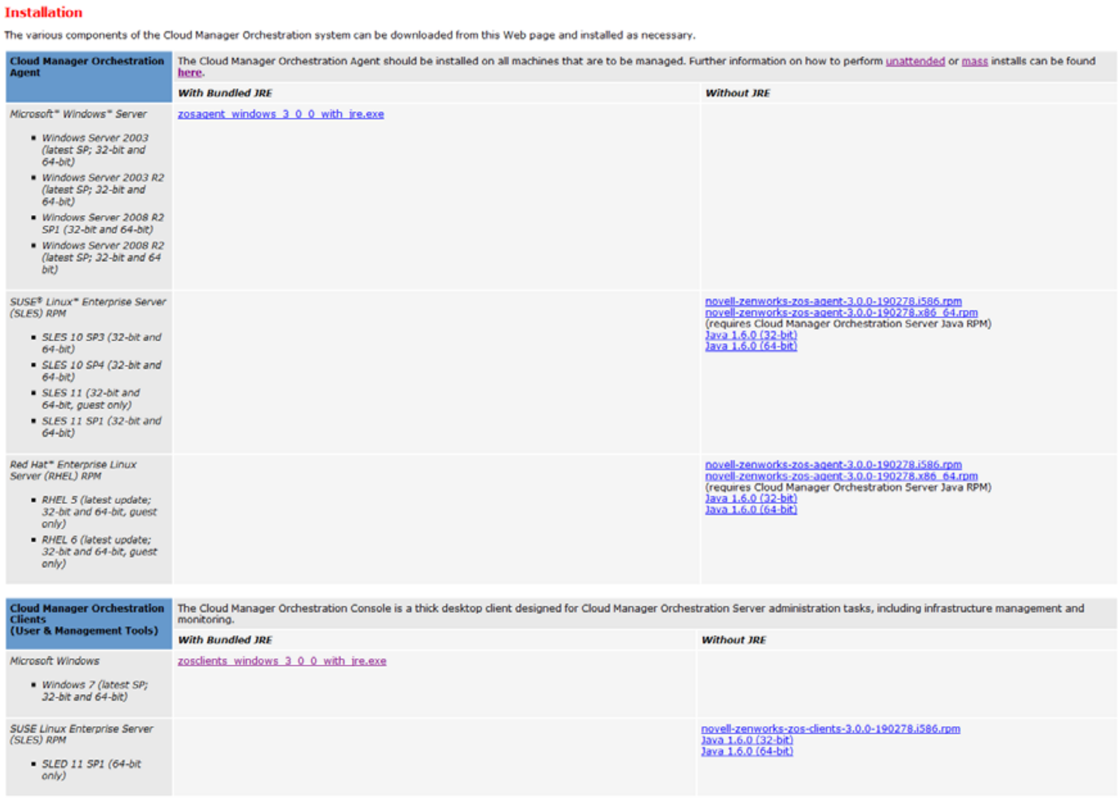
3b Make sure *Fixed Physical* is selected in the *Type* drop-down box, specify the new resource name in the *New Resource Name* field, click *Create*, then click *Close*.

The resource account is created, but is offline, as indicated by its object icon in the Explorer panel or in the Information view of each resource group to which it belongs. The resource is not online until an Orchestration Agent matching the resource is installed.

B.2 Installing an Orchestration Agent to Match the New Resource

This section demonstrates installing an Orchestration Agent to be used as a resource in your Orchestration grid. The information in this part of the walkthrough assumes that a resource account has already been created for the Orchestration Agent being installed.

1. From the managed device desktop, launch a browser to access the Web page for Orchestrate, as described in Section 2.2.1, “Obtaining the Agent Installer and Supporting Files from the Administrator Information Page,” on page 16.
2. Scroll to the *Installation* section of the page:



Installation

The various components of the Cloud Manager Orchestration system can be downloaded from this Web page and installed as necessary.

Cloud Manager Orchestration Agent	The Cloud Manager Orchestration Agent should be installed on all machines that are to be managed. Further information on how to perform unattended or mass installs can be found here.	
	With Bundled JRE	***Without JRE***
Microsoft™ Windows™ Server ▪ *Windows Server 2003 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2003 R2 (latest SP; 32-bit and 64-bit)* ▪ *Windows Server 2008 R2 SP1 (32-bit and 64-bit)* ▪ *Windows Server 2008 R2 (latest SP; 32-bit and 64 bit)*	zosagent_windows_3_0_0_with_jre.exe	
SUSE® Linux™ Enterprise Server (SLES) RPM ▪ *SLES 10 SP3 (32-bit and 64-bit)* ▪ *SLES 10 SP4 (32-bit and 64-bit)* ▪ *SLES 11 (32-bit and 64-bit, guest only)* ▪ *SLES 11 SP1 (32-bit and 64-bit)*		novell-zenworks-zos-agent-3.0.0-190278.i586.rpm novell-zenworks-zos-agent-3.0.0-190278.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)
Red Hat™ Enterprise Linux Server (RHEL) RPM ▪ *RHEL 5 (latest update; 32-bit and 64-bit, guest only)* ▪ *RHEL 6 (latest update; 32-bit and 64-bit, guest only)*		novell-zenworks-zos-agent-3.0.0-190278.i586.rpm novell-zenworks-zos-agent-3.0.0-190278.x86_64.rpm (requires Cloud Manager Orchestration Server Java RPM) Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

Cloud Manager Orchestration Clients (User & Management Tools)	The Cloud Manager Orchestration Console is a thick desktop client designed for Cloud Manager Orchestration Server administration tasks, including infrastructure management and monitoring.	
	With Bundled JRE	***Without JRE***
Microsoft Windows ▪ *Windows 7 (latest SP; 32-bit and 64-bit)*	zosclients_windows_3_0_0_with_jre.exe	
SUSE Linux Enterprise Server (SLES) RPM ▪ *SLED 11 SP1 (64-bit only)*		novell-zenworks-zos-clients-3.0.0-190278.i586.rpm Java 1.6.0 (32-bit) Java 1.6.0 (64-bit)

3 In the agent section of the Administrator Information page, find the installer link for the operating system of the device where you want to install the agent. For this walkthrough, we will install the Windows agent on a Windows operating system.

4 Click the installer link to download the `zosagent_windows_3_0_0_with_jre.exe` version of the agent to the computing node where you plan to install it.

5 From the machine where you will install the agent (in this walkthrough, a Windows 2008 64-bit machine), open the desktop and navigate to the location where you saved the Orchestration Agent file, then double-click the `zosagent_windows_3_0_0_with_jre.exe` icon to launch the Orchestration Agent Setup Wizard.

6 Follow the prompts in the wizard until the *Identify Orchestration Server* page displays, then ensure that you correctly enter the *Platespin_Orchestrate_Server_name* in the *Orchestration Server* field.

IMPORTANT: Make sure that the name you give the agent during the installation matches the name of the resource account you created in "Using the Orchestration Console to Create a Resource Account" on page 95.

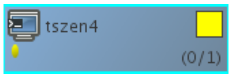
You might find it easier to click *Discover* so that the installer searches for and finds the Orchestration Server on the network.

7 Accept the remaining defaults on the wizard pages to complete the installation of the Agent.

8 When the installation is complete, click *Finish* to exit the wizard.

9 In the Orchestration Console, open the Resources Monitor to observe the resource object you created change from offline to online. When the object is no longer dimmed, the agent has logged in as a resource and is registered.

When the resource is online, the Resources Monitor displays a labeled box representing the registered agent. This box includes information about the agent, including the number of available slots it has and a status color indicating its state of readiness for Orchestrate jobs.



The status color window can be white (inactive), green (available for use), or blue (in use). If the color changes from green to blue, a job is running on this resource. To find out what kind of job is running, you can click on the *Jobs* monitor button on the toolbar.

C Uninstalling Orchestration Component Patterns from a SLES Server

This section includes information about uninstalling NetIQ Cloud Manager from your data center.

There is no supported wizard or self-contained uninstall tool to remove the Cloud Manager Orchestration Server from your Linux machines, nor is the uninstall feature in YaST and YaST2 is not supported, However, if you no longer want to use the server on a given machine, you can use a Linux package management tool to perform the uninstall. There is a variety of tools you can use to perform the uninstall:

- Use the rug command line tool on SUSE Linux Enterprise Server (SLES) 10 machines to remove the server packages.

```
rug remove -t pattern <pattern_name>
```

- Use the zypper command line tool to remove the server packages on SLES 11 machines.

  ```
  zypper remove <RPM_Package>
  ```

- Use the YaST setup and configuration tool on either SLES 10 or SLES 11 machines to select and remove the software packages.
- Use the `rpm -qa` command to look for instaled RPMs and the `rpm -e` command to manually remove one or more of them.

To remove the patterns:

1. Shut down all Cloud Manager Orchestration components running anywhere on the grid, including the Orchestration Agent, the Orchestration Server, the Cloud Manager Monitoring Server, and the Cloud Manager Monitoring Agent.
2. Use a package management tool to uninstall the Orchestration Server RPMs:
   - `novell-zenworks-monitor-gmond`
   - `novell-zenworks-zos-agent`
   - `novell-zenworks-zos-server-data-clients`
   - `novell-zenworks-monitor-web`
   - `novell-zenworks-zos-server-data-jre`
   - `novell-zenworks-orch-config-gui`
   - `novell-zenworks-monitor-gmetad`
   - `novell-zenworks-orch-config`
   - `novell-zenworks-zos-clients`
   - `novell-zenworks-zos-server-data-agent`
   - `novell-zenworks-vmwarehouse-base`

- `novell-zenworks-zos-java`
- `novell-zenworks-zos-server`
- `novell-pso-ws`

3 Verify deletion of all of the following directories used by the Orchestration Server:

- `/opt/novell/zenworks/server`
- `/var/opt/novell/zenworks/server`
- `/etc/opt/novell/zenworks/monitor`
- `/opt/novell/zenworks/agent`
- `/var/opt/novell/zenworks/agent`
- `/root/.novell/zos`
- `/root/.novell/zoc`
- `/etc/apache2/conf.d/zos.conf`
- `/etc/apache2/conf.d/ganglia-auth.conf`
- `/opt/novell/pso-ws`
- `/etc/opt/novell/pso-ws`
- `/var/opt/novell/pso-ws`

D Enabling VNC Access to vSphere 5 VM Guest Consoles

You can allow access through the firewall in a vSphere 5 environment, provided that the ESXi 5 Server and the vCenter Server are properly configured according to VMware documentation. The vSphere Client must also be installed and configured properly according to VMware documentation.

You can use one of two methods to open firewall ports for VNC access:

- Section D.1, "Enabling VNC Access By Opening Multiple Firewall Ports," on page 101
- Section D.2, "Enabling VNC Access by Creating a Special Configuration File," on page 102

D.1 Enabling VNC Access By Opening Multiple Firewall Ports

Use the following steps to enable the 59*xx* firewall ports for VNC access to vSphere 5 VM guest consoles:

1. In your vSphere environment, log in to the vSphere Client, then select *Home* > *Inventory* > *Hosts and Clusters*.
2. In the Hosts/Clusters tree view, select the ESXi host name that represents the server you want to open for VNC access.
3. Select the *Configuration* tab, locate and open the *Software* list box, then select *Security Profile*.
4. In the Firewall section, select the *Properties* link to display the Firewall Properties dialog box.
5. In the dialog box, scroll to and select *GDB Serve*r, then click *OK*.

   Your ESXi server now allows VNC access to Guest VM consoles through its firewall.

   NOTE: If you are using vSphere 4.*x* or earlier, select *VNC Server* in the list box for this step.
6. Repeat these steps for each ESXi host system.

The *GDB Server* setting covers the needed 59*xx* port range in its own port range, so when you enable firewall access for GDB Server, VNC services also become open. Extra open ports do not present a serious security problem, because a user rarely runs manual services that listen on those ports.

If you are concerned about these extra open ports, you can use the method for opening firewall ports explained in Section D.2, "Enabling VNC Access by Creating a Special Configuration File," on page 102.

D.2 Enabling VNC Access by Creating a Special Configuration File

If leaving the extra ports open is a security concern, you can manually add the VNC Server entry to the ESXi 5 firewall configuration and persist that entry across reboots of the server.

IMPORTANT: The preferred method to enable VNC Access to an ESXi 5 server is to use an existing, preconfigured GDB Server firewall entry, as described in Section D.1, "Enabling VNC Access By Opening Multiple Firewall Ports," on page 101.

If you use the method described in this section to enable VNC access, we strongly recommend that you have competent experience with command line Linux/Unix system administration. It is possible to make mistakes while performing these steps that might render your ESXi Server unbootable.

1 In your vSphere environment, log in to the vSphere Client, then select *Home* > *Inventory* > *Hosts and Clusters*.

2 In the Hosts/Clusters tree view, select the ESXi host name that represents the server you want to open for VNC access.

3 Select the *Configuration* tab, locate and open the *Software* list box, then select *Security Profile*.

4 In the Firewall section, select the *Properties* link to display the Firewall Properties dialog box.

5 In the dialog box, scroll to and select *SSH Serve*r, then click *OK*.

6 From a Linux console, ssh to the IP address of your ESXi host. Log in as `root` using that host's root password.

7 Using a Linux editor (such as vi), add the following shell script lines to the end of the `/etc/rc.local` file.

```
cat <<EOF > /etc/vmware/firewall/vncServer.xml
<ConfigRoot>
  <service>
    <id>vncServer</id>
    <rule id='0000'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>
        <begin>5900</begin>
        <end>5999</end>
      </port>
    </rule>
    <enabled>true</enabled>
    <required>false</required>
  </service>
</ConfigRoot>
EOF
esxcli network firewall refresh
```

IMPORTANT: Enter the code *exactly* as shown in the sample above. Use spaces to indicate indents in the code, *do not use* tab characters.

8 Save the `/etc/rc.local` file.

9 While still logged in, run the following command:

```
/sbin/auto-backup.sh
```

10 Log out from the SSH session.

11 From either the ESXi host's console or from the VMWare Client, reboot the ESXi host.

You should now see *VNC Server* as an available service in the Firewall Properties pane. The service should be enabled.

This process creates the `/etc/vmware/firewall/vncServer.xml` config file with the necessary settings to open the firewall ports.

Simply creating and editing this file does not work when the ESXi Server is rebooted because the root file system in ESXi 5 is a volatile RAM disk that is loaded from a master copy on each boot. Any changes made to this RAM disk are lost upon reboot.

A workaround to this rule relies on the fact that the ESXi Server uses the `auto-backup.sh` script to persist a select set of files every 10 minutes (or when changes are made by with the VMware Client or the VI-SDK facilities) from this file system to the master persistent copy. The `/etc/rc.local` file is one of these select files, so adding the shell script to the end of the file can add the needed firewall entry each time the ESXi server boots.