Administration Guide

Novell®
ZENworks® Linux Management

7.3 IR2

February 12, 2010

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

8 ZENworks Administrator Accounts   81

9 ZENworks Object Store and Data Store Maintenance   85

Part III   Device Registration   99

10 Registration Overview   101

11 Registering Devices   103

12 Managing Registration Keys and Rules   107

36 Setting Up Remote Management

Part IX Event Monitoring

37 Event Monitoring Overview

38 Working with Event Logs

39 Message Logger

40 Configuring Message Logger Settings

Part X Reports   531

41 Reports Overview   533

42 Generating ZENworks Reports   535

Part XI Appendixes   545

A Command Line Utilities   547

B Bundle and Policy Schedules   601

C Naming Conventions in the ZENworks Control Center   605

D Imaging Utilities and Components   607

About This Guide

This *ZENworks 7.3 Linux Management Administration Guide* includes conceptual and task-based information to help you configure and maintain your ZENworks® system. The guide is organized as follows:

- Part I, "Understanding ZENworks Linux Management," on page 21
- Part II, "ZENworks System Management," on page 39
- Part III, "Device Registration," on page 99
- Part IV, "Policy Management," on page 123
- Part V, "Package and Content Management," on page 207
- Part VI, "Preboot Services," on page 323
- Part VII, "Hardware and Software Inventory," on page 479
- Part VIII, "Remote Management," on page 493
- Part IX, "Event Monitoring," on page 507
- Part X, "Reports," on page 531
- Part XI, "Appendixes," on page 545

Audience

This guide is intended for ZENworks administrators.

Feedback

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, or go to Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent, updated version of the *ZENworks 7.3 Linux Management Administration Guide*, visit the Novell® ZENworks 7.3 Linux Management Edition documentation Web site (http://www.novell.com/documentation/zlm73).

Additional Documentation

ZENworks 7.3 Linux Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product:

- *Novell ZENworks 7.3 Linux Management Installation Guide*
- *Novell ZENworks 7.3 Linux Management Troubleshooting Guide*

In addition, the other capabilities included in the ZENworks 7 suite have extensive documentation for your use. For a full list of this documentation, see the Novell ZENworks 7 Linux Management documentation Web site (http://www.novell.com/documentation/zlm7_dell).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol ($^{®}$, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Understanding ZENworks Linux Management

Novell® ZENworks® Linux Management is the first fully integrated Linux systems management solution for Linux servers and workstations. ZENworks Linux Management also lets you manage Dell PowerEdge servers by using ZENworks Linux Management capabilities combined with the Dell OpenManage* toolkit capabilities. Whether you use SUSE® Linux Enterprise Server or Red Hat* Enterprise Linux on your PowerEdge servers, you can deploy and maintain hardware, operating systems, and applications from a single administrative console—the ZENworks Control Center.

The following sections provide information about Novell ZENworks Linux Management:

A Quick Tutorial on Basic ZENworks Linux Management Features

1

Novell® ZENworks® Linux Management is designed to let you efficiently manage a large number of Linux devices (servers and workstations) with as little configuration effort as possible.

To help you get started managing with ZENworks, this tutorial provides a brief overview of the major tasks you can perform. The first three sections help you set up a management structure based on best practices, and register devices in your system. You should review these three sections first, in the order presented:

- Section 1.1, "Organizing Devices: Folders and Groups," on page 23
- Section 1.2, "Creating Registration Keys and Rules," on page 25
- Section 1.3, "Setting Up ZENworks Administrator Accounts," on page 26

The remaining sections provide concepts you should be familiar with to successfully manage your devices. You can work on these sections in any order you'd like.

- Section 1.4, "Delivering Software Packages," on page 27
- Section 1.5, "Delivering Content Using File Bundles," on page 28
- Section 1.6, "Defining and Locking Down Device Configuration Settings," on page 29
- Section 1.7, "Using Preboot Services," on page 30
- Section 1.8, "Collecting Software and Hardware Inventory," on page 30
- Section 1.9, "Managing Remote Devices," on page 30
- Section 1.10, "Monitoring Events," on page 31
- Section 1.11, "Generating Reports," on page 32

1.1 Organizing Devices: Folders and Groups

Using the ZENworks Control Center, you can manage devices by configuring settings and assignments directly on the device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, ZENworks lets you organize devices into folders and groups.

You can create folders and groups at any time. However, the best practice is to create the folders and groups you need before you register devices in your ZENworks Management Zone. This is because you can set up registration keys and rules that automatically add devices to the appropriate folders and groups when they register (see Section 1.2, "Creating Registration Keys and Rules," on page 25).

The following sections explain folders and groups and how to create them:

- Section 1.1.1, "Folders," on page 24

1.1.1 Folders

Your ZENworks Management Zone includes two default folders for devices: Servers and Workstations. You can create additional folders within each of these folders to further organize devices.

Folders let you control which ZENworks system configuration settings are applied to which devices, including how often a device refreshes its information from the ZENworks Object Store, what information a device includes in its log files, and whether or not a device can be managed remotely.

You can define the configuration settings at the ZENworks Management Zone, on folders, or on individual devices. Because configuration settings can be defined on folders, you can place similar devices in the same folder and then define the configuration settings on the folder. All devices in the folder inherit the folder configuration settings, which override any settings made at the Management Zone level.

For example, assume that you have 30 SUSE® Linux Enterprise Servers in your environment and 10 Red Hat Enterprise Linux servers. You want to apply different system configuration settings to the two types of servers, so you create two folders (`/Servers/SUSE` and `/Servers/RedHat`) and place the appropriate servers in each folder. Because you have more SUSE servers than Red Hat servers, you configure the settings at the Management Zone level to accommodate the SUSE servers. Then, you configure the settings on the `/Servers/RedHat` folder to accommodate the Red Hat servers and override the settings on the Management Zone.

To create a folder:

1 In the ZENworks Control Center, click the *Devices* tab.
2 If you want to create a folder for servers, click the *Servers* folder.

or

If you want to create a folder for workstations, click the *Workstations* folder.
3 Click *New > Folder* to display the New Folder dialog box.
4 Type the name of the new folder, then click OK.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

1.1.2 Groups

A group is a collection of devices that share similar requirements. The devices might require the same software packages, the same operating system or application configuration settings, or the same inventory collection schedule.

For example, of the 30 SUSE and 10 Red Hat servers mentioned in the Folders section, 10 SUSE servers and 5 Red Hat servers might be dedicated to the Accounting department. As such, they all require the same accounting software. Because groups can be assigned software packages, you could create an Accounting group, add the 15 servers to the group, and then assign the appropriate accounting software packages to the group.

The advantage to making an assignment to a group is that all devices contained in that group receive the assignment, yet you only need to make the assignment one time. In addition, a device can belong to any number of unique groups, and the assignments and associations from multiple groups are additive. For example, if you assign a device to group A and B, it inherits the software packages assigned to both groups.

To create a group:

1 In the ZENworks Control Center, click the *Devices* tab.

2 If you want to create a group for servers, click the *Servers* folder.

or

If you want to create a group for workstations, click the *Workstations* folder.

3 Click *New > Server Group* (or *New > Workstation Group* for workstations) to launch the Create New Group Wizard.

4 Follow the prompts to create the group and add devices to it. For information about what you need to supply at each step of the wizard, click the ? icon.

1.1.3 Folders vs. Groups

As a general rule, you should manage system configuration settings through folders, and manage assignments (software packages, policies, etc.) through groups. This allows you to efficiently manage devices with similar configuration settings by placing them in the same folder and defining the configuration settings on the folder. However, all devices in the folder might not have the same software package or policy requirements. Therefore, you can organize the devices into groups and assign the appropriate bundles and policies to each group.

The most successful management strategy uses both folders and groups to create a hierarchy and organization that is easy to manage. A good folder organization enables you to import devices into a folder so they automatically inherit the correct system configuration settings. A good group organization makes it easy to assign bundles and policies to devices.

1.2 Creating Registration Keys and Rules

You can manually add devices to folders and groups, but this can be a burdensome task if you have a large number of devices or if you are consistently registering new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups when they register. To accomplish this, you can use registration keys, registration rules, or both.

Both registration keys and registration rules let you assign a name, folder, and group memberships to a device. However, there are differences between keys and rules that you should be aware of before choosing whether you want to use one or both methods for registration.

◆ **Registration Keys:** A registration key is an alphanumeric string that you manually define or randomly generate. During installation of the ZENworks Agent on a device, the registration key must be input manually or through a response file (see "Automating Installation of the ZENworks Agent" in the *Novell ZENworks 7.3 Linux Management Installation Guide*). When the device connects to a ZENworks Server for the first time, the device is given a name according to the defined naming scheme and then added to the folder and groups defined within the key.

You can create one or more registration keys to ensure that servers and workstations are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's devices are added to the `/Workstations/Sales` folder but are divided into three different groups (SalesTeam1, SalesTeam2, SalesTeam3) depending on their team assignments. You could create three different registration keys and configure each one to add the Sales workstations to the `/Workstations/Sales` folder and the appropriate team group. As long as each device uses the correct registration key, it is added to the appropriate folder and group.

◆ **Registration Rules:** If you don't want to enter a registration key during installation, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

ZENworks includes a default registration rule for servers and another one for workstations. If a device registers without a key, the default registration rules are applied to determine the folder and group assignments. The two default rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder. The device hostname is used for its name. You cannot delete these two default rules, but you can modify the naming scheme and the folder and groups to which the servers and workstations are added.

The two default rules are designed to ensure that no server or workstation registration fails. You can define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in Section 1.1.3, "Folders vs. Groups," on page 25, you've established folders for devices with similar configuration settings and groups for devices with similar assignments, newly registered devices automatically receive the appropriate configuration settings and assignments.

To create registration keys or rules:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 To create a new registration key, in the Registration Keys section, click *New > Registration* to start the Create New Registration Key Wizard.

or

To create a new registration rule, in the Default Registration Rules section, click *New* to start the Create New Default Rule Wizard.

3 Follow the prompts to create the key or rule. For information about what you need to supply at each step of the wizard, click the ? icon.

For more detailed information about registering devices, see Part III, "Device Registration," on page 99.

1.3 Setting Up ZENworks Administrator Accounts

During installation, a default Administrator account is created. This account provides rights to administer all of your ZENworks system.

You can create additional administrator accounts that provide full access to your ZENworks system. You can also create accounts that limit administrative rights to specific folders (device folders, policy folders, bundle folders, and report folders).

To limit administrator rights, you assign an account rights at the folder level. The root folders are `/Bundles`, `/Devices`, `/Policies`, and `/Reports`. Rights assigned at a root folder are effective in all subfolders (for example, `/Bundles/Workstations`) unless specifically overridden at the subfolder level.

Depending on the administrative functions you want an administrator to be able to perform, you can give an account one of the following levels of rights:

- **All:** Provides create, delete, and modify rights to all objects within the folder.
- **Modify:** Provides rights to edit existing objects only.
- **View:** Provides rights to view object information.

For example, if you want an administrator to be able to view bundles that are located in the `/Bundles` folder and create, delete, or modify bundles in the `/Bundles/Workstations` folder, you would assign the administrator View rights to the `/Bundles` folder and All rights to the `/Bundles/Workstation` folder.

To create an administrator account:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 In the Administrators list, click *New* to display the Add New Administrator dialog box.

3 Provide a username and password for the account, then click *OK* to add the account to the Administrators list.

The administrator can change the password the first time he or she logs in by clicking the key icon located next to the Logout link in the upper right corner of the ZENworks Control Center.

The newly created administrator account is granted View rights to all objects in the Management Zone. To grant additional rights, or to limit the administrator's rights to specific folders only, you need to modify the rights.

4 In the *Administrators* list, click the administrator account to display the account details.

5 Modify the assigned rights. For information about the options on the page, click *Help* or see Chapter 8, "ZENworks Administrator Accounts," on page 81.

6 When you are finished modifying the rights, click *Apply* to save the changes.

1.4 Delivering Software Packages

Software packages are delivered to devices through the use of RPM bundles and catalogs.

An RPM bundle is a grouping of one or more software packages. Bundles contain one or more files that are installed to particular locations on a device, plus information about the bundle, such as version, description, what applications must also be present for it to be installed, and more. A catalog is a group of bundles.

The fundamental difference between RPM bundles and catalogs is that the software in bundles is automatically installed, but users can choose whether or not to install the software included in catalogs. Catalogs are displayed in the ZENworks Linux Management Updater Client, which is part of the ZENworks Agent. For more information, see Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54.

You can define both the deployment schedule and the installation schedule for a bundle. The deployment schedule determines when the bundle's software packages are copied to the device. The installation schedule determines when the packages are installed on the device.

You can also create bundle groups. A bundle group is simply a group of bundles, similar to a catalog. However, installation of bundles in groups is automatic, just like installation of individual bundles.

The following sections contain additional information:

- Section 1.4.1, "Bundles," on page 28
- Section 1.4.2, "Catalogs," on page 28

1.4.1 Bundles

To create a bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundle* list, click *New > Bundle* to display the Create New Bundle Wizard.

3 Select *RPM Package Bundle* (the default option), then click *Next*.

4 Follow the prompts to create the bundle and assign it to devices. For information about what you need to supply at each step of the wizard, click the ? icon.

When assigning the bundle to devices, you can lessen your management overhead by assigning the bundle to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information about using bundles and bundle groups to deliver software to devices, see Chapter 20, "Using RPM and File Bundles," on page 217.

1.4.2 Catalogs

To create a catalog:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundle* list, click *New > Catalog* to display the Create New Catalog Wizard.

3 Follow the prompts to create the catalog, add bundles to it, and assign it to devices. For information about what you need to supply at each step of the wizard, click the ? icon.

When assigning the catalog to devices, you can lessen your management overhead by assigning the catalog to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information about delivering software to devices, see Chapter 22, "Using Catalogs," on page 271.

1.5 Delivering Content Using File Bundles

A File bundle lets you create a bundle and distribute compressed files of the type `tar.gz` and `tar.bz2`. For example, you can include configuration files or data files in file bundles.

To create a File bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundle* list, click *New > Bundle* to display the Create New Bundle Wizard.

3 Select *File bundle*, then click *Next*.

4 Follow the prompts to create the File bundle and assign it to devices. For information about what you need to supply at each step of the wizard, click the [?] icon.

When assigning the bundle to devices, you can lessen your management overhead by assigning the bundle to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information about using bundles and bundle groups to deliver software to devices, see Chapter 20, "Using RPM and File Bundles," on page 217.

1.6 Defining and Locking Down Device Configuration Settings

Through the use of policies, you can control and lock down the configuration settings for the following applications:

- Epiphany Web browser
- Evolution™ e-mail client
- Mozilla Firefox Web browser
- GNOME*
- Novell Linux Desktop
- SUSE Linux Enterprise Desktop

Additionally, you can create policies that run applications on a device, or perform modifications to a text-based configuration file using regular expressions.

You can apply individual policies to devices. You can also add policies to policy groups and apply the policy groups to devices.

Some policies are singular, meaning that only one instance of the policy can apply to the device. Other policies are plural, meaning that multiple instances can apply. Because a device inherits policy assignments from any groups or folders in which it is a member, conflicting assignments can occur. In this case, ZENworks determines the effective policies by first applying any device-assigned policies, then any group-assigned policies, and then any folder-assigned policies.

You can define the schedule for policies. The schedule determines when a policy is applied to a device.

To create a policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New > Policy* to display the Create New Policy Wizard.

3 Follow the prompts to create the policy and assign it to devices. For information about what you need to supply at each step of the wizard, click the [?] icon.

When assigning the policy to devices, you can lessen your management overhead by assigning the policy to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information about using policies and policy groups to control and lock down device settings, see Part IV, "Policy Management," on page 123.

1.7 Using Preboot Services

Preboot Services allows you to automatically or manually do any of the following to a device when it boots up:

- Configure the BIOS, BMC, RAID, and DRAC settings for Dell PowerEdge servers using a Dell Configuration bundle.
- Run scripted installations on the device, such as AutoYaST and kickstart
- Run ZENworks scripts on the device
- Make an image of the device's hard drives and other storage devices
- Restore an image to the device
- Apply an existing image to multiple devices

To accomplish these tasks automatically through the ZENworks Control Center, you need to have PXE (Preboot Execution Environment) enabled on your devices, and have prebootable tasks configured and assigned to the devices. Then, the devices can automatically implement these tasks when they boot. For instructions, see Part VI, "Preboot Services," on page 323.

1.8 Collecting Software and Hardware Inventory

Hardware and software inventory is automatically collected from each device. The hardware inventory includes details such as operating system, RAM, BIOS version, network adaptors, CD-ROM manufacturer, and a host of additional information. The software inventory includes a complete list of all installed packages, as well as all ZENworks-install bundles.

To view a device's hardware and software inventory:

1 In the ZENworks Control Center, click the *Devices* tab.
2 Click the *Servers* or *Workstations* folder to open it.
3 Click a device to display the device's Summary page.
4 Click the *Inventory* tab.

You can also roll up device inventory to a ZENworks 7.3 inventory database. For more information about collecting software and hardware inventory, see Part VII, "Hardware and Software Inventory," on page 479.

1.9 Managing Remote Devices

Sometimes you need to physically perform a task on a remote workstation or server. To do so, ZENworks lets you remotely manage a device through the ZENworks Control Center. When remotely managing a device, there are three modes of operation: Remote Control, Remote View, and Remote Login.

- **Remote Control:** Lets you take control of the device's desktop and perform tasks as if you were physically located at the device.
- **Remote View:** Lets you observe the device's desktop and activity.
- **Remote Login:** Lets you log in to the device, opening a new graphical session without disturbing the user on the device. The user cannot view your Remote Login session.

To manage a remote device:

1 In the ZENworks Control Center, click the *Devices* tab.

2 Click the *Servers* or *Workstations* folder to open it.

3 Click a device to display the device's Summary page.

4 In the Workstation Tasks list or Servers Tasks list (located in the upper left corner of the ZENworks Control Center), click *Remote Control Workstation* or *Remote Control Server* to open the Remote Management dialog box.

5 Select the remote management operation you want to perform: *Remote Control*, *Remote View*, or *Remote Login*, then click *OK*.

The remote session appears. If you receive an error message stating that additional plug-ins are required, see "Administration Workstation Requirements" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

For more information about managing remote devices, see "Remote Management" on page 493.

1.10 Monitoring Events

The ZENworks system generates messages each time a management task is performed. For example, when the ZENworks Agent enforces a policy on a device, it generates an event message. Or, when the ZENworks Server is unable to register a new device, it generates an event message. Depending on the severity level (normal, warning, or critical) of the event and the item type (device, bundle, policy, etc.) for which the event was generated, the event can be displayed in various locations in the ZENworks Control Center.

The following sections provide a brief overview of event monitoring and message logging:

- Section 1.10.1, "Hot List," on page 31
- Section 1.10.2, "Event Log," on page 31
- Section 1.10.3, "System Event Log," on page 32
- Section 1.10.4, "Message Logs," on page 32

For more information about message logs, see Part IX, "Event Monitoring," on page 507.

1.10.1 Hot List

The Hot List displays all events that generated an error (critical or warning). An error event remains in the list until you acknowledge it.

To access the Hot List:

1 In the ZENworks Control Center, click the *Home* tab.

1.10.2 Event Log

Each device, policy, and bundle has an Event Log that displays all of the event messages generated for the item, regardless of severity level (normal, warning, or critical).

The Event Log for a device displays all events that applied to the device. For example, if a bundle or policy is applied to the device, the Event Log displays a message for the event.

The Event Log for a bundle or policy displays all events that applied to the bundle or policy. For example, if a bundle is individually applied to four devices, four messages are displayed in the Event Log, one for each device.

To access an Event Log:

1 In the ZENworks Control Center, click the *Devices* tab, *Bundles* tab, or *Policies* tab, depending on whether you want to view events for a device, bundle, or policy.

2 Click the desired device, bundle, or policy to display its Summary page.

The Event Log is located near the bottom of the Summary page.

1.10.3 System Event Log

Each ZENworks Server has a System Event Log that displays all of the event messages generated for tasks performed by the server, regardless of the event's severity level (normal, warning, or critical). For example, it displays messages for all bundles that the server has applied to devices that it manages.

To access a System Event Log:

1 In the ZENworks Control Center, click the *Devices* tab, then click a ZENworks Server to display its Summary page.

The System Event Log is located near the bottom of the Summary page.

1.10.4 Message Logs

The events that are displayed in the ZENworks Control Center can also be logged to files on disk. The ZENworks Agent can log event messages (the ones that appear in a device's Event Log) to a file on the device's local disk; message logs for all managed devices can also be rolled up to a central log file on the ZENworks Server.

The ZENworks Server can log messages (the ones that appear in the server's System Event Log) to a file on the server's local disk.

For more information about message logs, see Part IX, "Event Monitoring," on page 507.

1.11 Generating Reports

You can generate reports to display bundle and device information, such as the bundle delivery information for each device or the devices registered in the last 24 hours. The ZENworks Control Center provides several predefined reports and lets you create new reports. You can export the reports to XML, CVS, or HTML formats.

ZENworks Linux Managements lets you generate reports specific to your Dell PowerEdge servers.

To generate a report:

1 In the ZENworks Control Center, click the *Reports* tab.

The Reports list includes three default folders: *Bundle Reports*, *Dell Reports*, and *Device Reports*. Each of these folders contains a set of predefined reports you can run. You can also run all of the reports in a folder by selecting the folder.

2 Select the *Device Reports* folder by clicking the box in front of it.

3 Click *Generate* to generate the six device reports.

You can print each of the reports. You can also export them to XML, CSV, and HTML formatted files.

For more information about reports, see Part X, "Reports," on page 531.

2 Using ZENworks Linux Management with Dell PowerEdge Servers

By combining Novell® ZENworks® Linux Management capabilities with the Dell OpenManage toolkit capabilities, you can configure and manage your Dell PowerEdge servers from out of the box through the entire server life cycle. Whether you use SUSE® Linux Enterprise Server or Red Hat Enterprise Linux on your PowerEdge servers, you can deploy and maintain hardware, operating systems, and applications from a single administrative console—the ZENworks Control Center.

ZENworks Linux Management provides the following features to help you deploy and manage Dell PowerEdge servers in your ZENworks system:

2.1 Configuring PowerEdge Servers using Dell Configuration Bundles

Dell Configuration bundles let you configure the BIOS, BMC, RAID, and DRAC settings on Dell PowerEdge servers and create a Dell utility partition. You can also select to run another Preboot Services bundle after these configurations are complete. Dell Configuration bundles let you configure a bare-metal PowerEdge server and quickly and easily put the server into production.

To create a Dell Configuration bundle:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New > Policy* to display the Create New Policy Wizard.

3 Select *Preboot bundle*, then click *Next*.

4 Select *Dell Configuration bundle*, then click *Next*.

5 Follow the prompts to create the policy and assign it to devices. For information about what you need to supply at each step of the wizard, click the ? icon.

When assigning the policy to devices, you can lessen your management overhead by assigning the policy to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information about using a Dell Configuration policy to configure Dell PowerEdge servers, see Section 30.5, "Using Dell Configuration Bundles," on page 454.

2.2 Obtaining, Configuring, and Updating PowerEdge Servers Using Dell Update Package Bundles

Dell Update Package bundles let you update and configure hardware and system settings (including BIOS, DRAC, RAID, BMC, and FRMW configurations) on Dell PowerEdge servers. After you obtain Dell Update Packages from Dell by using the mirroring capabilities of ZENworks Linux Management, you can easily assign the Dell Update Package bundles that are automatically created to PowerEdge servers in your ZENworks system. It is easy for you to determine if an updated Dell Update Package is available for PowerEdge servers in your system and deliver the update. ZENworks Linux Management helps you manage and update your PowerEdge servers though the entire server lifecycle.

The following sections contain additional information:

2.2.1 Obtaining Dell Update Packages from Dell

You can mirror Dell Update Packages from the Dell FTP site to your ZENworks server or you can mirror the CDs you receive from Dell Support.

Dell Update Packages let you update and configure hardware and system settings (including BIOS, DRAC, RAID, BMC, and FRMW configurations) on Dell PowerEdge servers.

To mirror Dell Update Packages from the Dell FTP site or from a CD, you create and configure an XML configuration file and then use the zlmmirror command line utility. The first time you mirror Dell Update Packages, all available packages are mirrored; subsequent mirror sessions obtain upgraded packages only. After the mirroring operation is complete, the Dell Update Packages are automatically bundled and display in the ZENworks Control Center on the Bundles page. You then assign the Dell Update Package bundles to devices just as you would with other bundles.

For more detailed information and step-by-step instructions, see Section 25.5, "Mirroring Dell Update Packages to Your ZENworks Server," on page 309

2.2.2 Assigning Dell Update Package Bundles to Configure and Update PowerEdge Servers

After the mirroring operation is complete, the Dell Update Packages are automatically bundled and display in the ZENworks Control Center on the Bundles page. To install them on PowerEdge servers in your ZENworks system, you must assign them to devices using the Assign Bundle Wizard in the ZENworks Control Center.

To assign a Dell Update Package bundle:

1 In the ZENworks Control Center, click the *Bundles* tab, then click the underlined link next to the folder containing the Dell Update Packages that was created during the mirroring process.

2 Select the desired Dell Update Package bundle by clicking the box next to its name, click *Action*, then click *Assign Bundle* to launch the Assign Bundle Wizard.

3 Follow the prompts to create the Dell Update Package bundle and assign it to devices. For information about what you need to supply at each step of the wizard, click the ? icon.

When assigning the bundle to devices, you can lessen your management overhead by assigning the policy to groups of devices rather than to individual devices. For more information about device groups, see Section 1.1, "Organizing Devices: Folders and Groups," on page 23.

For more detailed information, see Section 23.2, "Assigning Dell Update Package Bundles," on page 283.

2.2.3 Determining If Newer Dell Package Updates Are Available for PowerEdge Servers

After you run a mirror session and obtain updated Dell Update Packages, it is easy to determine if a newer Dell Update Package is available for installation on Dell PowerEdge servers in your ZENworks system.

To determine if there are updated Dell Update Package bundles available for the servers in your system:

1 In the ZENworks Control Center, click the *Devices* tab, then click *Servers*.

A link in the Dell Updates column indicates whether there is a Dell Update Package bundle available in the ZENworks package repository for each Dell PowerEdge server in the list. An update is available in the following situations:

- ◆ If a Dell Update Package exists in the ZENworks package repository but it is not assigned to that specific server model.
- ◆ If a specific Dell Update Package is already assigned to the device, but an updated package has been mirrored and is available in the ZENworks package repository.

2 Click the link to view the name of the Dell Update Package bundle appropriate for the device.

3 If the appropriate Dell Update Package bundle is not yet assigned to the device, continue with Section 23.2, "Assigning Dell Update Package Bundles," on page 283.

or

If the appropriate Dell Update Package bundle is already assigned to the device, continue with Section 23.4, "Deploying an Updated Version of a Dell Update Package Bundle," on page 287.

For more information, see Section 23.3, "Determining If Newer Dell Package Updates Are Available for PowerEdge Servers," on page 287.

2.2.4 Deploying a Newer Dell Update Package

If a specific Dell Update Package is already assigned to the device, but an updated package has been mirrored and is available in the ZENworks package repository, you can deploy the updated version of the package.

1 In the ZENworks Control Center, click the *Bundles* tab, click the underlined link next to the folder containing the Dell Update Packages that was created during the mirroring process.

2 Click the underlined link in the Name column to display the bundle's *Summary* page.

3 Click the Details page.

4 Use the Version drop-down list to select the desired version number, then click Deploy.

For more information, see Section 23.4, "Deploying an Updated Version of a Dell Update Package Bundle," on page 287.

2.3 Using Advanced Dell Inventory Information

Advanced Dell inventory information lets you display inventory information specific to Dell PowerEdge servers. This advanced inventory information helps you determine when PowerEdge configuration settings need to be updated.

For more information, see Chapter 33, "Reviewing the Device Inventory," on page 483.

2.4 Using Advanced Dell Inventory Reports

Advanced Dell reports let you run reports specific to Dell PowerEdge servers to find devices that do not have valid Dell Update Packages installed or to show devices with Dell applications installed (per device or per device model).

For more information, see Section 42.2.1, "Using Templates to Create Dell Reports," on page 539.

ZENworks System Management

II
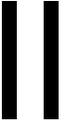
The following sections provide information about general Novell® ZENworks® Linux Management features and procedures:

ZENworks Control Center

3

You use the Novell® ZENworks® Control Center to configure system settings and management tasks in your ZENworks Management Zone. The following sections provide information about the ZENworks Control Center:

- Section 3.1, "Where the ZENworks Control Center Is Installed," on page 41
- Section 3.2, "Accessing the ZENworks Control Center," on page 41
- Section 3.3, "Accessing the ZENworks Control Center through Novell iManager," on page 42
- Section 3.4, "Changing the Timeout Value for the ZENworks Control Center," on page 42
- Section 3.5, "Changing the Debug Settings of ZENworks Control Center," on page 43

ZENworks Linux Management also includes the zlman command line utility to help you manage your ZENworks system. The zlman utility lets you perform the same tasks you can perform in the ZENworks Control Center, with the exception of imaging and preboot tasks. For more information, see Section 4.1, "zlman," on page 45.

3.1 Where the ZENworks Control Center Is Installed

The ZENworks Control Center is installed on all ZENworks Servers in the Management Zone.

You can perform all management tasks on the Primary Server and most management tasks on the Secondary Servers. The one management exception on Secondary Servers is the manipulation (adding, deleting, modifying) of packages in a bundle. This task is not supported because the Primary Server is the source server for packages, meaning that packages are replicated from the Primary Server to Secondary Servers on a regularly scheduled basis. Manipulating a package on a Secondary Server rather than on the Primary Server would result in the modified package being replaced (or removed) the next time the Secondary Server's packages were updated from the Primary Server. For more information about replication of packages, see Chapter 24, "Replicating Content in the ZENworks Management Zone," on page 291.

3.2 Accessing the ZENworks Control Center

1 Using a Web browser that meets the requirements listed in "Administration Workstation Requirements" in the *Novell ZENworks 7.3 Linux Management Installation Guide*, enter the following URL:

    https://*ZENworks_Server_Address*

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server.

The ZENworks Control Center requires an https:// connection; requests to http:// are redirected to https://.

2 When prompted for login credentials, use the Administrator user with the password you provided during the installation.

3.3 Accessing the ZENworks Control Center through Novell iManager

ZENworks Linux Management includes a Novell plug-in module (`.npm`) that you can use to access the ZENworks Control Center from Novell iManager, which is a management console used by a number of other Novell products.

To install the ZENworks Control Center plug-in for iManager:

1 Copy the plug-in (`zlm7link.npm`) from the *Novell ZENworks 7.3 Linux Management* CD to a location on your iManager server.

The `zlm7link.npm` file is located in the `/ImanagerPlugin` directory.

2 Install and configure the plug-in module:

- ◆ If you are using Novell iManager 2.6, follow the instructions in the Novell iManager 2.6 documentation (http://www.novell.com/documentation/imanager26/).
- ◆ If you are using Novell iManager 2.7 or later, see TID 7003078 at Novell Support (http://www.novell.com/support).

3 If Tomcat did not restart during the installation and configuration process, restart Tomcat.

4 Log into iManager.

5 Click the *ZENworks* icon at the top of the page.

6 Enter the ZENworks Control Center URL:

`https://ZENworks_Server_Address`

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server.

7 Click the *ZENworks* icon to launch the ZENworks Control Center.

3.4 Changing the Timeout Value for the ZENworks Control Center

By default, the ZENworks Control Center has a 30-minute timeout value. If you leave the ZENworks Control Center idle on your computer for more than 30 minutes, you are prompted to log in again before continuing. You can increase or decrease the timeout value, or you can specify that the ZENworks Control Center never times out.

To change the timeout value:

1 Open the `/var/opt/novell/zenworks/www/tomcat/base/webapps/zenworks/WEB-INF/config.xml` file in a text editor.

2 Increase or decrease the timeout value, as needed.

or

Specify -1 to specify that the ZENworks Control Center never times out.

3 Save the `config.xml` file.

4 Restart the service by executing the following command:

`/etc/init.d/novell-zenserver restart`

3.5 Changing the Debug Settings of ZENworks Control Center

To change the debug settings of ZENworks Control Center:

1 Open the `/var/opt/novell/zenworks/www/tomcat/base/webapps/zenworks/WEB-INF/config.xml` file in a text editor.

2 Make sure that the value of `debug.enabled` is set to `True`. (By default, the option is set to `True`.)

   The error messages logged by using WebLogger.debug() are written to the standard output.

3 (Optional) Set the value of `debug.tags` is set to any of the following values:

   rpcToServer
   controlTree
   snapshotTimes
   pageLoadTime
   requestParams
   viewStateManager
   RemoteManagement
   WebFramework
   mirrorStatus

   The error messages logged to WebLogger.debugForTag() are written to the standard output.

4 Save the `config.xml` file.

5 Restart the service by executing the following command:

   `/etc/init.d/novell-zenserver restart`

Command Line Administration Utilities

<div style="text-align: right">4</div>

Novell® ZENworks® Linux Management includes several command line utilities to help you manage your ZENworks system. The primary purpose of the command line utilities is to provide access to the ZENworks management functionality in a scriptable environment.

The following command line utilities are available:

4.1 zlman

The zlman utility lets you perform the same tasks you can perform in the ZENworks Control Center, with the exception of imaging and preboot tasks. It is installed on ZENworks Servers in the following location:

```
/opt/novell/zenworks/bin
```

For more information about zlman, view the zlman man page (man zlman) on the ZENworks Server or see zlman (1) (page 562).

4.2 zlm-debug

The zlm-debug utility lets you gather information to help you troubleshoot and solve problems you encounter using ZENworks Linux Management. By default, zlm-debug gathers cache, server, client, configuration, hardware, and package data as well as log files. The information is packaged into a tarball file and placed in the location you specify. It is installed on ZENworks Server and managed devices in the following location:

```
/opt/novell/zenworks/bin
```

By default, zlm-debug creates a tarball, `zlm-debug-yearmonthdate_of_file_creation.tgz` in the /tmp directory.

For more information about zlm-debug, view the zlm-debug man page (man zlm-debug) on the ZENworks Server or see zlm-debug (1) (page 552).

4.3 zlmmirror

The zlmmirror utility lets you mirror RPM and Dell Update Packages packages from ZENworks 6.*x* and 7 servers, Dell FTP servers, YaST Online Update (YOU) servers, Red Hat Network, and Red Carpet® Enterprise servers. It is installed on ZENworks Servers in the following location:

```
/opt/novell/zenworks/bin
```

For more information about zlmmirror, view the zlmmirror man page (man zlmmirror) on the ZENworks Server, see zlmmirror (1) (page 554), or see Chapter 25, "Mirroring Software," on page 293.

4.4 rug

The rug utility lets you perform software and user management through the ZENworks Agent on a managed device. It is installed on managed devices in the following location:

```
/opt/novell/zenworks/bin
```

For SUSE LINUX Enterprise Server 10 (SLES 10) and SUSE LINUX Enterprise Desktop 10 (SLED 10) devices, the rug utility is located in the following directory:

```
/usr/bin
```

For more information about rug, view the rug man page (man rug) on a managed device or see rug (1) (page 586).

4.5 zmd

The zmd utility lets you control how the ZENworks Agent runs on a managed device. It is installed on managed devices in the following location:

```
/opt/novell/zenworks/sbin
```

For SUSE LINUX Enterprise Server 10 (SLES 10) and SUSE LINUX Enterprise Desktop 10 (SLED 10) devices, the ZENworks Agent is located in the following directory:

```
/usr/sbin
```

For more information about zmd, view the zmd man page (man zmd) on a managed device or see zmd (8) (page 548).

4.6 zrmservice

The zrmservice utility lets you control how the ZENworks Remote Management Agent (a component of the ZENworks Agent) runs on a managed device. It is installed on managed devices in the following location:

```
/opt/novell/zenworks/sbin
```

For more information about zrmservice, view the zrmservice man page (man zrmservice) on a managed device or see zrmservice (1) (page 551).

ZENworks Server

<div style="text-align: right">5</div>

The Novell® ZENworks® Server is the backbone of the ZENworks system. It communicates with the ZENworks Agent on managed devices to deliver software, enforce policies, collect inventory, and perform other management tasks. The following sections provide information about the ZENworks Server:

5.1 ZENworks Services

The ZENworks Server includes the following services:

Table 5-1 *ZENworks Services*

Service	Service Name	Description
eDirectory™	ndsd	Used for the ZENworks Object Store.
PostgreSQL Database	postgresql	Used for the ZENworks Data Store; only needed if the Data Store resides on the ZENworks Server.
ZENworks Server	novell-zenserver	Used for communicating with the ZENworks Agent.
ZENworks Loader	novell-zenloader	Used for loading modules not directly associated with the ZENworks Server. This includes the Content Replication, Inventory Rollup, and QueueRunner modules.
ZENworks Server Management	novell-zented	Used for replicating RPM packages and Dell Update Packages from the Primary Server to Secondary Servers.
ZENworks Imaging Service	novell-pbserv	Used to provide imaging services to a device. This includes sending and receiving image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so forth.
ZENworks Preboot Policy Daemon	novell-zmgprebootpolicy	Used by PXE-enabled devices to check if there are any Preboot bundles that are assigned to the device.

Service	Service Name	Description
Proxy DHCP Daemon	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell TFTP server. It also responds to PXE devices to indicate which bootstrap program (`nvlnbp.sys`) to use.
TFTP Daemon (TFTP Server)	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks. It also provides a central repository for these imaging files, such as the Linux kernel and initrd. A PXE-enabled device uses this server to download the bootstrap program (`nvlnbp.sys`).
ZENworks Management Daemon (ZENworks Agent)	novell-zmd	Used to enable the server as a managed device.
ZENworks Imaging Agent	novell-zislnx	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.

The services reside in the `/etc/init.d` directory on the ZENworks Server. Refer to the following sections for instructions to help you control the ZENworks services:

5.1.1 Checking the Status of a ZENworks Service

To check the current status of a service, use the following command:

```
/etc/init.d/servicename status
```

Replace *servicename* with the name of the service as listed in Table 5-1 on page 47.

To check the current status of all services, use the following command:

```
/opt/novell/zenworks/bin/zlm-config --status
```

5.1.2 Starting a ZENworks Service

To start a service, use the following command:

```
/etc/init.d/servicename start
```

Replace *servicename* with the name of the service as listed in Table 5-1 on page 47.

To start all services, use the following command:

```
/opt/novell/zenworks/bin/zlm-config --start
```

To ensure that all services start in the correct order, we recommend that you use the `zlm-config --start` option to start all services rather than starting them one at a time.

5.1.3 Stopping a ZENworks Service

To stop a service, use the following command:

```
/etc/init.d/servicename stop
```

Replace *servicename* with the name of the service as listed in Table 5-1 on page 47.

To stop all services, use the following command:

```
/opt/novell/zenworks/bin/zlm-config --stop
```

5.1.4 Restarting a ZENworks Service

To restart a service that is already running, use the following command:

```
/etc/init.d/servicename restart
```

Replace *servicename* with the name of the service as listed in Table 5-1 on page 47.

To restart all services, use the following command:

```
/opt/novell/zenworks/bin/zlm-config --restart
```

To ensure that all services start in the correct order, we recommend that you use the `zlm-config --restart` option to restart all services rather than restarting only one service.

5.2 RPM Package Repository

The ZENworks Server contains all of the RPM packages and Dell Update Packages that are included in bundles defined within your Management Zone.

The following sections contain more information:

5.2.1 Package Repository Location

The package repository is the `/var/opt/novell/zenworks/pkg-repo` directory on the ZENworks Server. When you add an RPM package to a bundle, the package is automatically uploaded to the package repository. When you mirror Dell Update Packages, the packages are automatically bundled and uploaded to the package repository.

5.2.2 Package Replication

To ensure that all ZENworks Servers have the same RPM packages and Dell Update Package bundles to distribute, the ZENworks Primary Server can replicate all packages to any ZENworks Secondary Servers in the Management Zone. To enable replication, you need to establish a replication schedule (see).

During replication of packages to a Secondary Server, only new packages and updates to existing packages are sent.

5.2.3 Package Administration

Because of the way that packages are replicated from the Primary Server to Secondary Servers, you must run the ZENworks Control Center or zlman utility from the Primary Server to add a package to a bundle. Doing so causes the package to be added to the Primary Server's package repository and then be replicated to all Secondary Servers.

If you add a package to a Secondary Server, the package does not exist on the Primary Server and is therefore removed the next time the Primary Server replicates its packages to the Secondary Server.

The same limitation applies to all package management tasks, such as modifying and deleting a package from a bundle. These tasks must be performed on the Primary Server.

5.3 Uninstalling a ZENworks Server

ZENworks includes a uninstall program (zlm-uninstall) to remove the ZENworks services, Object Store, and other files from a server. If for some reason the uninstall program cannot remove the ZENworks server software, you can manually uninstall the software. The following sections provide instructions for uninstalling the software with the uninstall program or manually.

If your ZENworks Linux Management system has Secondary Servers, you must uninstall the Secondary Servers before uninstalling the primary ZENworks server. Otherwise, during uninstallation of the Secondary Servers, you receive an error message concerning eDirectory that is not applicable because eDirectory was already removed during uninstallation of the Primary ZENworks server.

The following sections contain more information:

5.3.1 Uninstalling a Primary ZENworks Server Using zlm-uninstall

1 Make sure you know the password for the ZENworks Administrator account.

2 Log in to the ZENworks Server as `root`.

3 Run the following command:

```
/opt/novell/zenworks/bin/zlm-uninstall
```

4 Follow the prompts.

5.3.2 Uninstalling a Secondary ZENworks Server By Using zlm-config

1 Make sure you know the password for the ZENworks Administrator account.

2 Log in to the Primary ZENworks Server as `root`.

3 Run the following command:

```
/opt/novell/zenworks/bin/zlm-config --remove-secondary-
server=secondary_server
```

where *secondary_server* is the name of the Secondary Server as displayed in the devices list in ZENworks Control Center.

For example, if your server name is ZEN216, the command is:

```
/opt/novell/zenworks/bin/zlm-config --remove-secondary-server=zen216
```

5.3.3 Manually Uninstalling a Primary or Secondary ZENworks Server

1 Stop the services on the ZENworks Server. If necessary, see .

2 Remove the following directories:

```
/opt/novell/zenworks/share/keystore
/opt/novell/zenworks/datamodel/share/ldap-certs
/etc/opt/novell/zenworks/serverid
/etc/opt/novell/zenworks/serversecret
```

3 Edit `/etc/crontab` to remove the lines that contain ZENworks.

4 (Conditional) If you are removing a Secondary Server, remove the Secondary Server object from the Object Store and Data Store. To do so:

   4a Create a script file like the following one to create a CLASSPATH variable that includes all of the paths to the ZENworks classes:

```
#!/bin/sh
CLASSPATH=''
for i in `ls /opt/novell/zenworks/java/lib/*.jar` ;
do CLASSPATH="$i:$CLASSPATH" ;
done ;
for i in `ls /opt/novell/extend/Common/WSSKD/lib/*.jar` ;
do CLASSPATH=$i:$CLASSPATH" ;
done ;
echo $CLASSPATH
```

   4b Use the following command to remove the ZENworks Secondary Server object:

```
/opt/novell/zenworks/lib/java/bin/java -classpath $CLASSPATH
com.novell.zenworks.datamodel.extensions.installer.LDAPInstaller
uninstall admin_password
```

Replace *admin_password* with the ZENworks Administrator account password.

5 (Conditional) If you are removing the Primary Server and are using a local PostgreSQL database for the ZENworks Data Store, remove the database. To do so, use the following commands:

```
/etc/init.d/postgresql start, su - postgres , dropdb zenworks , dropuser
zenadmin , /etc/init.d/postgresql stop
```

6 Remove the ZENworks Object Store. To do so, use the following commands:

```
ndsconfig rm -F -a admin.system -w admin_passwordrm -rf /var/nds/dibrm /
etc/nds.conf
```

Replace *admin_password* with the ZENworks Administrator account password.

7 Remove the ZENworks RPM packages and the Dell Update Packages, if necessary. To do so:

7a Use the following command to list the package names:

```
rpm -qa | grep novell-zenworks
```

7b Remove each of the packages individually using the following command:

```
rpm -e | package_name
```

or

Use the following simple script to remove multiple packages:

```
for i in `rpm -qa | grep novell-zenworks` ; do rpm -e $i ; done
```

Because of package dependencies, you might need to run this script multiple times to remove all packages. You can verify that all packages have been removed by running the command in Step 7a.

8 Remove the following directories:

```
rm -rf /opt/novell/zenworks/
rm -rf /etc/opt/novell/zenworks/
rm -rf /var/opt/novell/zenworks/
```

5.4 Freeing Disk Space on a ZENworks Server

You can clean up the ZENworks server disk space by either deleting or backing up the old log files. For detailed information on how to back up the log files, see Section 37.6, "Backing Up the Log Files," on page 511.

You can also delete empty directories that might not be removed during the deletion of a package or bundle. The directories are located at /var/opt/novell/zenworks/pkg-repo.

ZENworks Agent

6

The Novell® ZENworks® Agent is installed on each managed device within your ZENworks Management Zone. The agent communicates with the ZENworks Server to deliver software, enforce policies, and perform other management tasks. The following sections provide information about the ZENworks Agent:

- Section 6.1, "ZENworks Agent (zmd)," on page 53
- Section 6.2, "File System Access," on page 54
- Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54
- Section 6.4, "Uninstalling the ZENworks Agent," on page 66

6.1 ZENworks Agent (zmd)

The ZENworks Agent is named zmd. It is sometimes referred to as the ZENworks Management Daemon (zmd).

The ZENworks Agent performs software management functions on the ZENworks managed device, including updating, installing, and removing software and performing basic queries of the device's package management database. Typically, these management tasks are initiated through the ZENworks Control Center or the `rug` utility, which means you should not need to interact directly with the ZENworks Agent.

The ZENworks Agent is installed to the following directory:

```
/opt/novell/zenworks/sbin
```

For SUSE LINUX Enterprise Server 10 (SLES 10) and SUSE LINUX Enterprise Desktop 10 (SLED 10) devices, the ZENworks Agent is located in the following directory:

```
/usr/sbin
```

6.1.1 ZENworks Agent (zmd) Cache Settings

As the ZENworks Agent (zmd) performs its duties, it maintains a cache that stores the content of bundles that are downloaded for installation on that managed device. You can control the age of contents in the cache and its size by using cache settings. Cache cleanup is enforced on both client startup and refresh.

If the process of downloading the bundle is interrupted on the managed device, the zmd starts the download of individual packages from where it was left off.

The cleaning of cached information is always enabled. You can configure the following settings using the `rug set` command in the `rug` utility to manage the cache. For more information about the rug utility, see Section 4.4, "rug," on page 46.

Table 6-1 *ZENworks Management Daemon Cache Settings*

Setting	Description
max-cache-age	Defines the number of days the contents of the cache are retained, after which the contents are deleted. The default is 30 days. If this setting specifies 0 days, the cache content never expires.
	The cache cleanup is enforced on client startup and refresh. The contents of the cache are sorted by date (oldest to newest) and deleted by applying the *max-cache-age* setting, starting with the oldest content.
	To change the *max-cache-age* setting from the default of 30 days to 60 days, for example, you enter the following command from the managed device:
	`rug set max-cache-age 60`
cache-max-size-in-mb	This setting is only enforced at cleanup time; not during bundle download. The default is 300 MB. If this is set to 0, there is no limit to the size of the cache; however, the max-cache-age setting still applies.
	If the cache size exceeds the maximum size specified with this setting, the cache contents are sorted by date and the oldest contents are deleted until the cache size is within the specified size limit. If this size limit is exceed while downloading bundles, the bundle contents are downloaded; however, the next time the device restarts or refreshes, the cache is cleaned until its size is within the specified size limit. The cache cleanup process will not delete files downloaded within the last 24 hours to get within the specified limit.
	To change the *cache-max-size-in-mb* setting from the default of 300 MB to 500 MB, for example, you enter the following command from the managed device:
	`rug set cache-max-size-in-mb 500`

6.2 File System Access

The ZENworks Agent runs as `root`. This provides it with the file system access required to perform its management functions on the device.

On managed devices, do not mount the following directories over NFS: `/etc`, `/opt`, `/usr`, `/home`, `/var`, and `/root`. The ZENworks Agent (zmd) is not designed to work with these directories mounted over NFS, so this configuration is not supported.

6.3 Using the Software Updater, Installer, and Remover from Users' Managed Devices

The ZENworks Linux Management Software Updater, Software Installer, and Software Remover applets are components of the desktop that work through the ZENworks Agent.

In ZENworks Linux Management, these three easy-to-use desktop applets provide users with the ability to update existing software, install new software, remove existing software from their managed devices, and view and edit system preferences. These three desktop applets replace the user interface clients used in previous versions of ZENworks Linux Management. Software Updater,

Installer, and Remover provide users with a simple way to manage software, and the process is integrated into the managed device's desktop. If a rich user interface is required, you should use the `rug` command line interface to accomplish these same tasks. For more information, see Section 4.4, "rug," on page 46.

In previous versions of ZENworks Linux Management, these three applets were combined in one user interface. In ZENworks Linux Management 6.*x*, the client interface was called Red Carpet®. In ZENworks 7 Linux Management, the client interface was called the ZENworks Linux Management Update Client. Software Updater, Installer, and Remover replace Red Carpet and the ZENworks Linux Management Update Client.

The following sections contain information about each applet:

6.3.1 Updating Software

With the Software Updater, you can easily apply updates to your software with just a few clicks. At startup, the Software Updater automatically checks for updates to your system from the sources specified in the Software Updater configuration.

The following sections contain additional information:

Launching the Software Updater

1 Launch the Software Updater by navigating to `/opt/novell/zenworks/bin` and running `zen-updater` with root privileges. To run it as a daemon, run `zen-updater &`.

The Software Updater icon appears in the notification area (GNOME) or the system tray (KDE) of your panel as an icon depicting a globe, which changes to an orange circle with an exclamation point in it when updates are available.

The first time you exit the Software Updater, you will be asked if you want it to load on startup. If you choose *Yes*, you can access the Software Updater from the notification area or system tray rather than by running `zen-updater` from the command line each time you want to launch the applet.

The rug command-line utility also lets you perform software and user management through the ZENworks Agent on a managed device. For background information on the underlying rug command and its configuration options, see Section 4.4, "rug," on page 46.

Configuring Package Sources

Before you can use the use the Software Updater, you need to configure it to check package sources for updates. Ask your system administrator for package sources that are available for your product and for connection details.

NOTE: The Software Updater and the Software Installer use the same configurations. If you add a service using the Software Updater configuration screen, that service will appear in the Software Installer configuration and vice versa.

To add new services:

1 Right-click the *Software Updater* icon, then click *Configure*.

   If the Software Updater icon is not in the system tray, you need to launch the program. See .

2 Click *Add Service*.
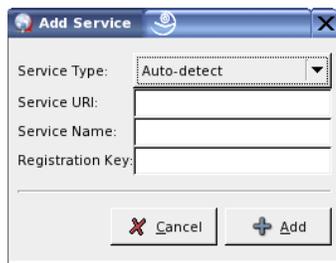
3 Select the type of update repository from the drop-down list. The Software Updater supports the following service types: YUM, ZYPP, NU, RCE, ZENworks, user-mounted sources (Mount), Auto-detect, and Novell Customer Center Registration.

4 Add the connection details for the source type you selected (server URI and registration key), then click *Add*. The service URI is the URL of the service. Registration keys are optional and are made available by the administrator of the service. Only ZENworks and RCE services have registration keys.

   The source is listed in the *Services* tab and is ready to be used and checked for available update packages.

To remove a service:

1 Right-click the *Software Updater* icon, then click *Configure*.

   If the Software Updater icon is not in the system tray, you need to launch the program. See .
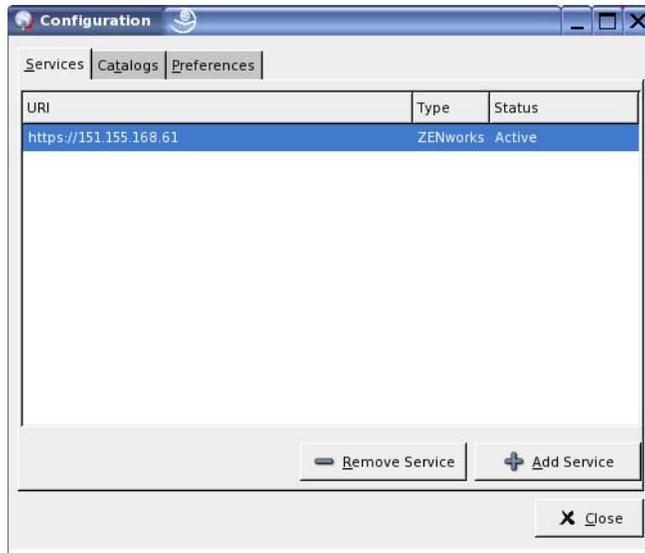
2 Select the services you want to delete, then click *Remove Service*.

Selecting Update Catalogs

Once you have configured one or more services, you can select a set of catalogs from those sources to be checked. There may be, for example, a catalog containing all the software that came with the original release of the product and another one containing all the update packages released since.

To select additional update catalogs:

1 Right-click *Software Updater*, then click *Configure*.

If the Software Updater icon is not in the system tray, you need to launch the program. See .

2 Click the *Catalogs* tab.
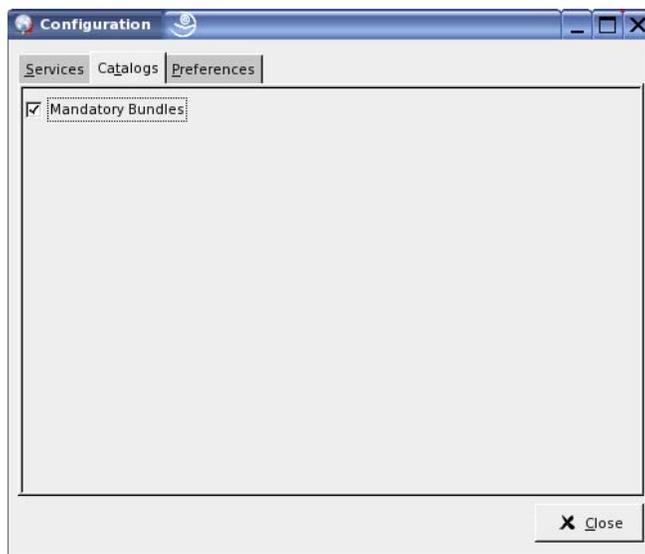
3 Select the catalogs you want or deselect those you don't need, then click *Close*.

Selecting and Applying Updates

When updates are available, the panel icon changes to an orange circle with an exclamation mark in it. When you mouse over the icon, a message pops up indicating that updates are available.

To review and apply updates:

1 Click the *Software Updater* icon.

If the Software Updater icon is not in the system tray, you need to launch the program. See "Launching the Software Updater" on page 55.
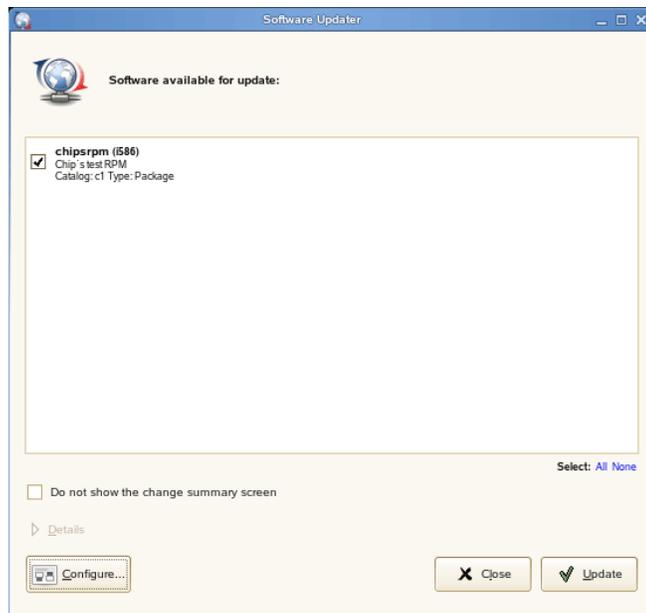
2 Select the updates you want to apply.

Click *Details* for more information about the selected update.

NOTE: To poll the services for updates, right-click the *Software Updater* icon, and then click *Refresh*.

---

3 (Optional) If you do not want to view the change summary information, select *Do not show the change summary screen*. By default, this option is not selected.

4 Click *Update*.

If you chose to view the change summary information in Step 3, the software updater icon blinks when the change summary screen is displayed.

6.3.2 Installing Software

Using ZENworks Linux Management, your administrator can create catalogs containing optional software and assign them to users' devices. Because software packages contained in catalogs are usually considered optional, users can choose whether or not to install the software. If an administrator has assigned catalogs to users' devices, the catalogs display in the Software Installer.

  ◆ "Configuring Package Sources" on page 59

Configuring Package Sources

Before you can use the Software Installer, you need to add package sources from which you can install software.

NOTE: The Software Updater and the Software Installer use the same configurations. If you add a service using the Software Updater configuration screen, that service will appear in the Software Installer configuration and vice versa.

To add a package source:

1 Launch the Software Installer by navigating to `/opt/novell/zenworks/bin` and running `zen-installer` with `root` privileges.

2 Click *Configure*.
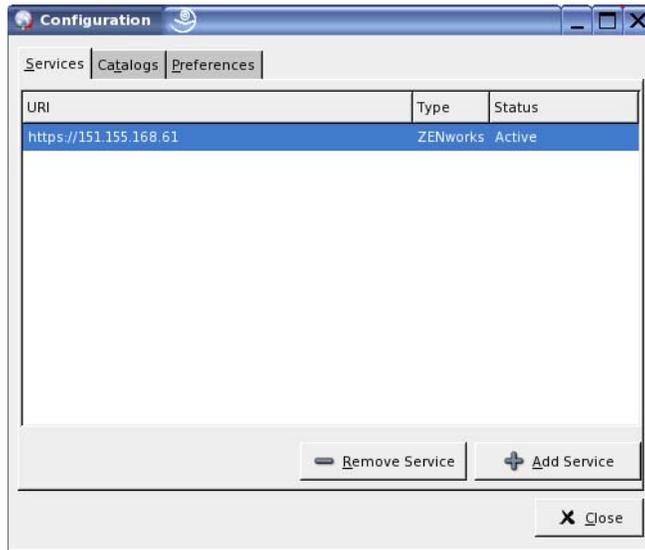
3 Click *Add Service*.
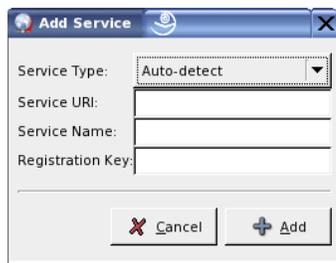
4 Select the type of the service repository from the drop-down list. The Software Updater supports the following service types: YUM, ZYPP, NU, RCE, ZENworks, and user-mounted sources (Mount), Auto-detect, and Novell Customer Center Registration.

5 Add the connection details for the source type you selected (server URI and registration key), then click *Add*. The service URI is the URL of the service. Registration keys are optional and are made available by the administrator of the service. Only ZENworks and RCE services have registration keys.

The source is listed in the *Services* tab and is ready to be used and checked for available packages.

Selecting Installation Catalogs

You can configure the Software Installer to accept various catalogs:

1 Launch the Software Installer by navigating to `/opt/novell/zenworks/bin` and running `zen-installer` with root privileges.

2 Click *Configure*.

3 Click the *Catalogs* tab.
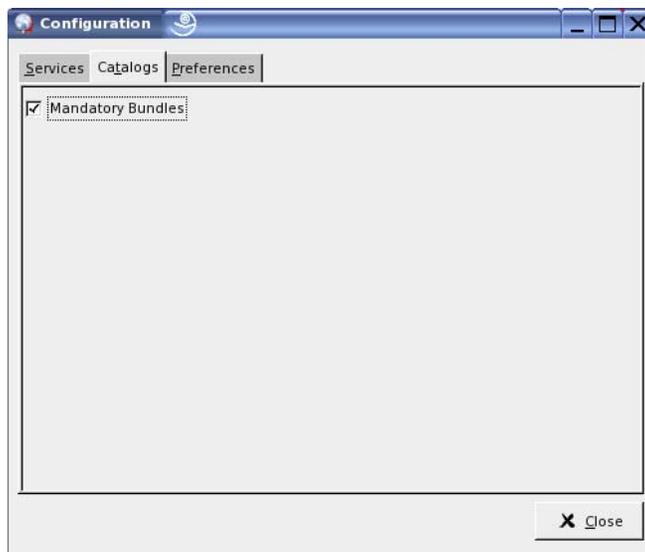
4 Select the catalogs you want or deselect those you don't need, then click *Close*.

Installing Software by Using the Software Installer

To install software:

1 Launch the Software Installer by navigating to `/opt/novell/zenworks/bin` and running `zen-installer` with `root` privileges.
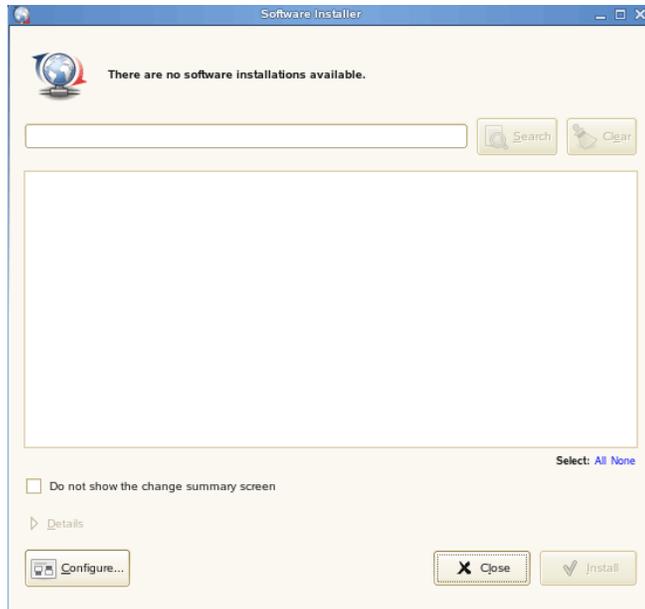
2 Select the software that you want to install or search for software by typing a search term in the search field, then click *Search*. (Click *Clear* to clear the search field.) Click *Details* for information about the selected software. You can select all available software by clicking *All*.

3 (Optional) If you do not want to view the change summary information, select *Do not show the change summary screen*. By default, this option is not selected.

4 Click *Install*.

NOTE: Even though the user has been assigned rights by the administrator for installing the software, the installation of bundle fails.

6.3.3 Removing Software

The Software Remover lets you remove software on a managed device. The utility is in the `/opt/novell/zenworks/bin` directory.

1 Launch Software Remover by navigating to `/opt/novell/zenworks/bin` and running `zen-remover` with root privileges.
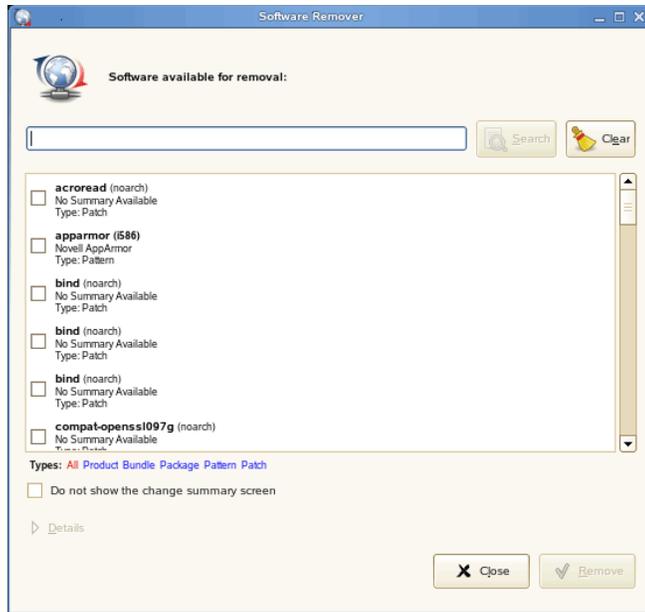
2 Select the software you want to remove. To filter the list, click on the type of software: *All, Product, Bundle, Pattern,* or *Package*. You can click *Details* for more information about the selected software.

3 (Optional) If you do not want to view the change summary information, select *Do not show the change summary screen*. By default, this option is not selected.

4 Click *Remove*.

6.3.4 Viewing System Preferences

1 Right-click the *Software Updater* icon, then click *Configure*.

If the Software Updater icon is not in the system tray, you need to launch the program. See

2 Click the *Preferences* tab.

This window shows the system preferences.

NOTE: You can also display this list from the command line using `rug get.` For more information, see rug (1) (page 586).

6.3.5 Editing System Preferences

1 Right-click the *Software Updater* icon, then click *Configure*.

If the Software Updater icon is not in the system tray, you need to launch the program. See "Launching the Software Updater" on page 55.

2 Click the *Preferences* tab.
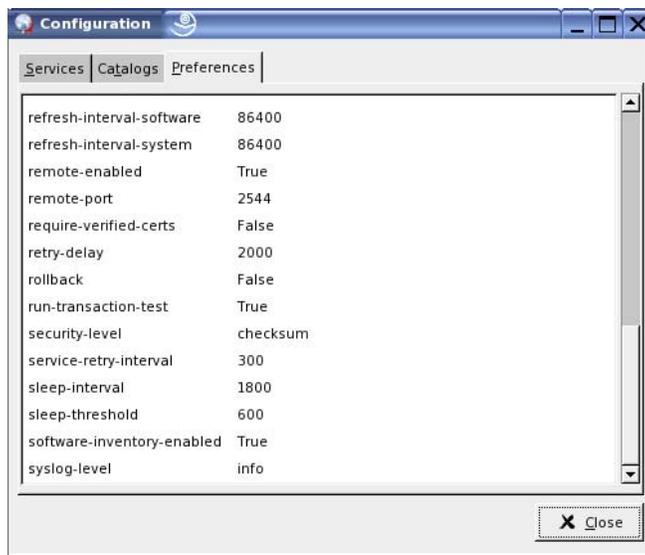
3 (Optional) Select *Start the software updater on login* to automatically start the Software Updater.

4 (Optional) Select *Show the version details* to list all available package updates.

By default, the package list will not show the version details nor will it show if multiple versions of the same package are available. Instead, it will show the "best" package available, or the package with the best architecture and version and with the least number of install/delete requests required.

5 In the preferences list, click the row whose value you want to change, then click the value.

6 Edit preferences as desired.

- ◆ *bind-ip*. For systems using more than one IP address, selects the address at which rcd will bind. Leave empty to bind to all addresses.

- ◆ *blackout-interval*. Time interval for which the device is to be locked. Specify the start time and end time in the HH:MM format, with hours in 24-hour format.

- ◆ *cache-cleanup-enabled*. If True, automatically cleans up the cache. The default is True.

- ◆ *cache-directory*. The directory where cached data are stored. The default is /var/opt/ novell/zenworks/cache/zmd/web.

- ◆ *cache-max-size-hard-limit*. If True, never allow the cache to grow past the maximum size. The default is False.

- ◆ *cache-max-size-in-mb*. Sets the cache size. The default is 300 mb.

- ◆ *delay*. How long before sending delayed actions, in seconds. The default is 900 seconds.

- ◆ *device-locked*. If True, locks the device and zmd blocks install, removal, refresh, and register operations for packages and bundles.

- ◆ *device-shutdown-delay*. Sets the delay for a device shutdown. The default is 2 seconds.

- ◆ *hardware-inventory-enabled*. If True, hardware inventory information will be collected and sent to the server. The default is True.

- ◆ *http-timeout*. Number of seconds until HTTP requests timeout. The default is 180 seconds.

- ◆ *hwinfo-options*. Options to pass to the `hwinfo` command. By default, it is set to null on SLES 9 and NLD devices. For SLES 10 and SLED 10 devices, the default setting for the hwinfo preference is `--nowpa`. If the default setting is changed, the `hwinfo` command resets the wireless configuration settings on SLES 10 and SLED 10.

- ◆ *inventory-scanner-options*. Options to pass to the inventory scanner. The default is "- braille."

- ◆ *log-exception-traces*. Log full traces when an exception is encountered. The default is False.

- ◆ *log-level*. Sets the log level. Options are off, fatal, error, warn, info, and debug. The default is Info.

- ◆ *log-max-files-size*. Maximum size (in MB) of all the `zmd-messages.log` files.

- ◆ *log-soap-xml*. Log soap messages (debug log level only). The default is False.

- ◆ *max-cache-age*. The maximum number of days to cache a file. The default is 30 days.

- ◆ *max-database-age*. Maximum number of days to refresh the database.

- ◆ *max-downloads*. Maximum number of concurrent downloads. The default is 5.

- ◆ *max-retries*. Maximum number of download retries. The default is 3.

- ◆ *memory-threshold*. Memory (in MB) at which zmd should restart because of excessive memory usage.

- *no-verified-certs*.Specify the IP addresses of the servers (separated by a comma) for which you do not want to verify the SSL certificates. The servers are excluded only if *require-verified-certs* is True.

- *proxy-password*. Password for the proxy, if any.

- *proxy-url*.The available options are URL, Bypass, or an empty string. By default, it is set to an empty string, and the device uses the system proxy. Set the value to URL to specify the URL of the proxy server, or set the value to Bypass for the device to bypass the system proxy.

  NOTE: If you modify the system proxy, you must set proxy-url to use the system proxy URL if you want the device to use the system proxy. You can set the proxy URL either by using the rug command or through the zmd settings in the ZENworks Control Center. For more information on how to use the rug command, see rug (1). For more information on how to configure the zmd settings, see Section 7.10, "Configuring the ZENworks Management Daemon (zmd) Settings," on page 76.

- *proxy-username*. Username for the proxy, if any.

- *proxy-excludes*. Specify the IP address or the DNS name of the server that you want to exclude from using the proxy settings. You can specify multiple IP addresses or DNS names by separating the same with a comma. You can use the * wildcard character only in the IP address. Ensure that there is no space in the specified IP address or the DNS name.

- *real-time-package-updates*. If True, the software inventory is sent immediately to the server when a package or bundle is changed on the managed device irrespective of the *refresh-interval-software* schedule set on the managed device. The default is True. If False, the software inventory is sent to the server based on the refresh interval specified in the *refresh-interval-software* schedule.

- *refresh-interval*. How long between refreshes, in seconds. The default is 7200 seconds.

- *refresh-interval-hardware*. How long between hardware refreshes. The default is 86400 seconds.

- *refresh-interval-software*. How long between software refreshes. The default is 86400 seconds.

- *refresh-interval-system*. How long before system refreshes. The default is 86400 seconds.

- *remote-enabled*. Allow clients to connect to this daemon remotely. The default is True.

- *remote-port*. Port used for connections of remote clients. The default value is 5505.

- *require-verified-certs*. Verify SSL certificates from server. This should remain False unless your ZENworks Linux Management server has a signed SSL certificate (generated or purchased). The default is False.

- *retry-delay*. The number of milliseconds to delay before retrying a download. The default is 2000 milliseconds.

- *rollback*. Store more detailed transaction history, enabling rollback feature. The default is False.

- *run-transaction-test*. Run a dryrun before attempting to install or remove packages. The default is True.

- *security-level*. Security requirements to enforce. Possible values are signature, checksum, and none. The default is Checksum.

- *service-retry-interval*. The default is 300 seconds.

- ◆ *sleep-interval*. The number of seconds before the next Service Refresh schedule wakes up. The default is 300 seconds.
- ◆ *sleep-threshold*. The default is 600 seconds.
- ◆ *software-inventory-enabled*. If True, software inventory information will be collected and sent to the server. The default is True.
- ◆ *syslog-level*. Sets the log level. Options are off, fatal, error, warn, info, and debug. The default is Info.

NOTE: You can also edit these system preferences from the command line using `rug set`. For more information, see rug (1) (page 586).

If you change the value of the *bind-ip*, *remote-enabled*, or *remote-port*, you must restart zmd for the changes to take effect.

6.4 Uninstalling the ZENworks Agent

ZENworks includes a uninstall program (zlm-uninstall) to remove the ZENworks Agent from a device. If for some reason the uninstall program is unable to remove the ZENworks Agent, you can manually uninstall the agent. The following sections provide instructions to remove the software:

Using zlm-uninstall to Uninstall the ZENworks Agent

1 Make sure you have unregistered the device. See Chapter 13, "Unregistering and Reregistering Devices," on page 121.

2 Log in to the managed device as `root`.

3 Run the following command:

```
/opt/novell/zenworks/bin/zlm-uninstall
```

4 Follow the prompts.

Manually Uninstalling the ZENworks Agent

1 Use the following command to list the ZENworks package names:

```
rpm -qa | grep novell-zenworks
```

2 Remove each of the packages individually using the following command:

rpm -e | *package_name*

or

Use the following simple script to remove multiple packages:

```
for i in `rpm -qa | grep novell-zenworks` ; do rpm -e $i ; done
```

Because of package dependencies, you might need to run this script multiple times to remove all packages. You can verify that all packages have been removed by running the command in Step 1.

3 Remove the following directories:

```
rm -rf /opt/novell/zenworks/
rm -rf /etc/opt/novell/zenworks/
rm -rf /var/opt/novell/zenworks/
```

NOTE: When you uninstall ZENworks Linux Management on SLES 10 and SLED 10 managed devices, the core zmd packages such as zmd, rug, zen-updater, and zen-inventory are not removed because they are also installed as a part of the distribution. Hence, when you reinstall the ZENworks Agent on these devices, the configuration files such as `zmd.conf` that are associated to these packages persist.

Configuring Management Zone Settings

7

The ZENworks® Management Zone is the top level of the ZENworks management hierarchy. The Management Zone provides an autonomous administrative unit of ZENworks Servers and managed devices (workstations and servers). You use the ZENworks Control Center (the Web-based administrative tool) to manage devices. The ZENworks Servers and managed devices work together to apply the management tasks.

You can use the Configuration tab in the ZENworks Control Center to configure your Management Zone.

The following sections contain additional information:

7.1 Configuring System Variables

The System Variables page lets you define variables that can be used to replace paths, names, and so forth as you enter data in various ZENworks Control Center fields. System variables defined on this page can be used on all objects in your ZENworks Management Zone.

System variables can be overridden at the device or folder level. If you add the same system variable to a device or folder, but give it a different value, the new variable value overrides the inherited system variable value. A variable on the device level overrides the same variable on the folder level, which overrides the same variable on the system level.

The following sections provide additional information:

7.1.1 Creating System Variables

To provide a variable at the device level:

1 In ZENworks Control Center, click the *Devices* tab.

2 Navigate to and click the desired device, click the *Settings* tab.

3 Click *System Variables*, then click *Override settings*.

4 To add a system variable, click *Add*, then fill in the *Name* and *Value* fields.

When specifying the variable in an object's field, use the following syntax:

`${VAR_NAME}`

5 Click *OK*.

Click the ? icon for additional help

To provide a variable at the folder level: from the ZENworks Control Center, click the *Devices* tab, click the (*Details*) link next to the desired folder, click the *Settings* tab, then click *System Variables*. Click the ? icon for additional help.

1 In ZENworks Control Center, click the *Devices* tab.

2 Click the (*Details*) link next to the desired folder, click the *Settings* tab, then click *System Variables*, then click *Override settings*.

3 To add a system variable, click *Add*, then fill in the *Name* and *Value* fields.

When specifying the variable in an object's field, use the following syntax:

`${VAR_NAME}`

4 Click *OK*.

Click the ? icon for additional help

To set system variables for your ZENworks system:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *System Variables*.

3 To add a system variable, click *Add*, then fill in the *Name* and *Value* fields.

When specifying the variable in an object's field, use the following syntax:

`${VAR_NAME}`

4 Click *OK*.

7.1.2 Using Variables in ZENworks Policies: A Sample Use Case

In this scenario, you have a SLES 9 and a SLES 10 managed device. Both devices have a common file, `deviceid`. On SLES 9, the file is located at `/etc/opt/novell/zenworks/zmd`, and on SLES 10 it is located at `/etc/zmd`. Assume that you want to place a copy of `deviceid` in the `/tmp`

directory on both devices by using the Remote Execute policy. Instead of creating two Remote Execute policies, one each for the SLES 9 and SLES 10 managed device, you can create one policy by using system variables.

Perform the following tasks in the order listed:

Creating a System Variable for the SLES 9 Managed Device

1 In ZENworks Control Center, click the *Devices* tab.

2 Click *Servers*.

3 From the list of servers, click the SLES 9 managed device, then click the *Settings* tab.

4 Click *System Variables*, then click *Override settings*.

5 In the System Variables panel, click *Add*, then fill in the following details:

- ◆ **Name:** source_path
- ◆ **Value:** /etc/opt/novell/zenworks/zmd

6 Click *OK*.

7 Click *Apply*, then click *OK*.

Creating a System Variable for the SLES 10 Managed Device

1 In ZENworks Control Center, click the *Devices* tab.

2 Click *Servers*.

3 In the list of servers, click the SLES 9 managed device, then click the *Settings* tab.

4 Click *System Variables*, then click *Override settings*.

5 In the System Variables panel, click *Add*, then fill in the following details:

- ◆ **Name:** source_path
- ◆ **Value:** /etc/zmd

6 Click *OK*.

7 Click *Apply*, then click *OK*.

Creating the Remote Execute Policy and Assigning It to the Managed Devices

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *Remote Execute Policy*, then click *Next* to display the Policy Name page.

4 Fill in the Policy Name, Folder, and Description fields. For more information, see Step 4 on page 165 in Section 16.6, "Remote Execute Policy," on page 164.

5 Click *Next*.

6 In the Remote Execute Policy page, configure the following settings:

- **Executable Type:** Select *Binary*.
- **Maximum waiting time:** Select *Wait till the program completes the execution*.
- **Executable file name:** `/bin/cp`.
- **Executable file parameters:** `${source_path}/deviceid /tmp`.

7 Click *Next* to display the Summary page.

8 Review the information.

9 Click *Next* to display the Policy Assignment page, then assign the policy to SLES 9 and SLES 10 devices

10 Click *Next* to display the Policy Schedule page, then select the schedule to apply to the assignments.

11 Click *Next* to display the Policy Groups page. For more information, see Step 12 in Section 16.6, "Remote Execute Policy," on page 164.

12 Click *Next* to display the Finish page.

13 Click *Finish*.

After the policy is applied on the managed devices, a copy of `deviceid` is created in the `/tmp` directory.

7.2 Configuring the Device Refresh Schedule

The Device Refresh Schedule page determines how often devices contact a ZENworks Server to update policies, settings, and inventory scanning. By default, each refresh schedule occurs every two hours.

These settings apply to all devices in your ZENworks Management Zone unless it is changed on a device folder or individual device. To change refresh schedules for an individual device, click the *Devices* tab, locate and click the device's name, click the *Settings* tab, click *Device Refresh Schedule*, then click *Override Settings*. Click the [?] icon for additional help.

The refresh interval is not reset until the device refresh is complete. For example, assume you set a refresh interval of 2 hours. The device's first refresh occurs at 6:00 p.m. and takes 13 seconds to complete. The second refresh will occur at 8:00:13 p.m. (2 hours after the refresh was completed at 6:00:13). If the second refresh takes 15 seconds to complete, the third refresh will occur at 10:00:28 p.m.

To configure the device refresh schedule for all devices in your ZENworks system:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *Device Refresh Schedule*.

3 Specify the *Days*, *Hours*, and *Minutes* between device refreshes in your ZENworks system.

4 Click *OK*.

7.3 Configuring Device Inventory Settings

The Device Inventory page determines the Inventory Roll-up settings.

Configure the settings on this page to roll up the hardware inventory information from a ZENworks 7 Linux Management database to a ZENworks 7 or later Server Management or Desktop Management Inventory server:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *Device Inventory*.

3 Configure the desired settings:

- **DNS name or IP address of the destination server:** Specify the DNS name or the IP address of the ZENworks 7 or later Server Management or Desktop Management Inventory server to which you want to roll up the hardware inventory information.

- **Time interval between roll ups (in hours):** Specify the time interval between two roll-ups.

4 Click *OK*.

7.4 Configuring Local Device Logging

The Local Device Logging page lets you configure the logging of messages to a managed device's local drive.

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *Local Device Logging*.

3 Fill in the fields to specify local file settings. By default, the path of the files varies, depending on the type of device. For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop (SLED 10) devices, the path is `/var/log`. For all other devices, it is `/var/opt/novell/log/zenworks`.

- **Log message to a local file if severity is:** Specify filtering criteria based on severity. By default, this option is selected if you are on ZENworks 7.3 Linux Management. For a new installation of ZENworks 7.3 Linux Management with IR1IR2, this option is deselected by default. If you upgrade to ZENworks 7.3 Linux Management with IR1IR2 from an earlier version of ZENworks Linux Management, this option displays the value that you selected before upgrading.

  - **Error:** Stores messages with an Error severity.
  - **Warning and above:** Stores messages with Error severity.
  - **Information and above:** Stores messages with a severity of Information, Warning, and Error.
  - **Debug and above:** Stores messages with a severity of Debug, Information, Warning, and Error.

- **Limit file size to:** Specify the maximum size of the file where messages are being stored. The message file is backed up after reaching the specified size. The default setting is 10 MB.

- **Number of backup files per day:** Specify the number of backup files to take per day. The maximum number of backup files is 99. The default setting is 1 if you are on ZENworks 7.3 Linux Management. For a new installation of ZENworks 7.3 Linux Management with IR1IR2, the default value is 5. If you upgrade to ZENworks 7.3 Linux Management with IR1IR2 from an earlier version of ZENworks Linux Management, this

option displays the value that you selected before upgrading. For more information, see "Event Monitoring Troubleshooting Strategies" in the *Novell ZENworks 7.3 Linux Management Troubleshooting Guide*.

4 Fill in the fields to store messages in the device system log file. The path to system log file is `/var/log/messages`.

- **Send message to local system log if severity is:** Specify filtering criteria based on severity.

  - **Error:** Stores messages with Error severity.

  - **Warning and above:** Stores messages with Error severity.

  - **Information and above:** Stores messages with a severity of Information, Warning, and Error.

5 Click *OK*.

These settings apply to all devices in your ZENworks Management Zone unless it is changed on a device folder or individual device. To change refresh schedules for an individual device, click the *Devices* tab, locate and click the device's name, click the *Settings* tab, click *Local Device Logging*, then click *Override Settings*. Click the ? icon for additional help

7.5 Configuring Preboot Services

The Preboot Services page lets you configure the following ZENworks Management Zone default settings for devices that use Preboot Services:

- Preboot menu options
- Image storage security
- Non-registered device network settings
- Non-registered device preboot work assignment
- Server referral list
- Intel Active Management Technology (AMT)

For detailed information, see Section 29.4, "Configuring Preboot Services Defaults," on page 379.

7.6 Configuring Remote Management

The Remote Management Settings page lets you configure the Remote Management settings for the management zone. This includes enable and disable options for remote management operations as well as configurations for custom ports.

For detailed information, see Section 36.1.1, "Configuring Remote Management Settings at the Zone Level," on page 497

7.7 Configuring Centralized Message Logging

The Centralized Message Logging page lets you configure the following to log the messages on the Primary Server:

- Central Server
- Centralized file log

- E-mail notification
- SNMP traps

For detailed information, see Section 40.1.2, "Configuring Centralized Log Settings," on page 526.

7.8 Configuring the Content Replication Schedule

The Content Replication Schedule page lets you specify how often bundles are replicated from the primary ZENworks Server to all secondary ZENworks Servers in the Management Zone. During replication of a bundle, only new packages and updates to existing packages are sent.

For detailed information, see Section 24.2, "Configuring a Content Replication Schedule," on page 292.

7.9 Viewing Default Target Platforms and Configuring Custom Target Platforms

This Target Platforms page lists the server and workstation platforms that ZENworks Linux Management supports as managed devices. You can also define additional custom platforms by adding an entry to the Custom Target Platforms list.

1. In the ZENworks Control Center, click the *Configuration* tab.

2. Click *Platforms*.

3. (Optional) To view the details of a default target platform, click the name of a platform.

4. (Optional) To add a custom target platform, under Custom Target Platforms, click Add to display the Add Platform dialog box.

Figure 7-1   *Add Platform dialog box.*
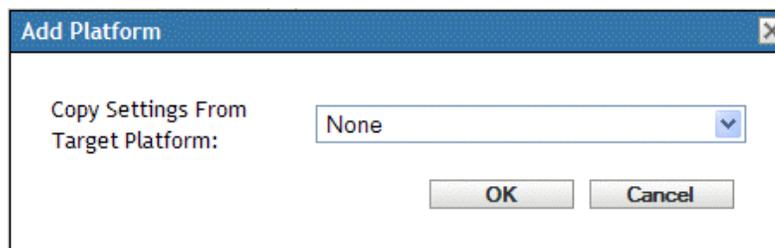
If you have custom distributions that your company has created based on one of the supported platforms, these custom distributions can be recognized by ZENworks Linux Management by adding them as a custom target platform.

5. Select an existing target platform whose settings you want to copy and edit, then click *OK*

The easiest way to create a custom target platform is to copy a default platform's settings that are similar to your custom target and then edit those settings.

6. Fill in the fields:

- **Name:** Specify the name of the platform as you want it displayed in the ZENworks Control Center.

- **Vendor:** Specify the name of the distribution's vendor.

- **Product Name:** Specify the product name of the distribution.
- **Version:** Type the version number.
- **Package Manager:** Specify the package manager for the platform.
- **Architecture:** Specify the architecture.
- **Device Type:** Specify whether the device type for the platform is a workstation or a server.
- **OS Detection String:** Modify the XML strings in the box to point to the file on the device that would contain the release information and the string that the system must match to determine the platform of a device.
- **Enable this Platform:** Select this option to enable this platform so that it will display in menus and other areas in the ZENworks Control Center.

7 Click *OK*.

7.10 Configuring the ZENworks Management Daemon (zmd) Settings

Use the ZENworks Management Daemon Settings page to configure the Zenworks Management Daemon (zmd) settings for your ZENworks Management Zone. These settings apply to all devices in your ZENworks Management Zone unless they are changed on a device folder or individual device. Any changes to the settings on this page are applied to devices upon refresh.

The zmd daemon performs software management functions on the ZENworks managed device, including updating, installing and removing software, and performing basic queries of the device's package management database. Typically, these management tasks are initiated through the ZENworks Control Center or the rug utility, which means you should not need to interact directly with zmd.

The settings that you can configure on this page can also be set using the rug utility. For information about each setting and its corresponding value, see rug (1) (page 586).

To configure a zmd setting:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *ZMD Settings*.

3 Click *Add* to open the Configure Setting dialog box.

Figure 7-2 *Configure Setting dialog box.*
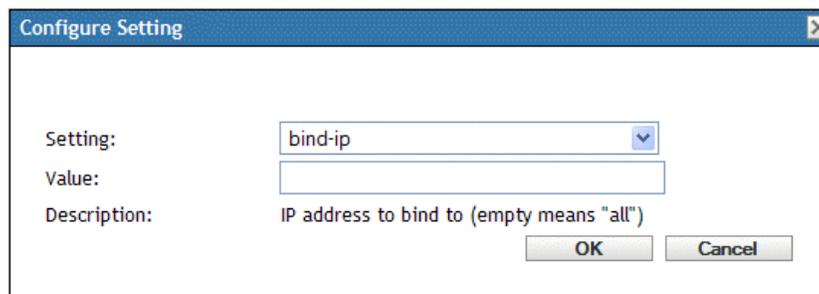
4 Fill in the fields:

- **Setting:** Select a value from the Setting drop-down list.

  The drop-down list contains all available settings in ZENworks Linux Management. If not all modules are installed on a device, settings that control that module will not be used by the zmd daemon. For example, if you do not install the Remote Control module on a device, all settings that configure this module will be ignored.

- **Value:** If the selected setting requires specific values, select the desired value from the drop-down list. If the selected setting does not require specific values, type the value in the Value box.

  After you click *OK*, if ⚠ displays next to the Value box, the setting you typed is either too small/large or you typed an invalid setting.

- **Description:** Displays the description of the selected setting.

The zmd settings can be overridden at the device or folder level. If you add the same zmd setting to a device or folder, but give it a different value, the new setting value overrides the inherited zmd setting value. A setting on the device level overrides the same setting on the folder level, which overrides the same setting on the system level.

To provide a setting at the device level, from the ZENworks Control Center, click the *Devices* tab, navigate to and click the desired device, click the *Settings* tab, click *ZMD Settings*, then click *Override Settings*. Click the Help icon for additional help.

To provide a setting at the folder level, from the ZENworks Control Center, click the *Devices* tab, click the *(Details)* link next to the desired folder, click the *Settings* tab, then click *ZMD Settings*, then click *Override Settings*. Click the Help icon for additional help.

If you add the same setting twice, the first instance of the setting is removed and the new setting is applied to the device when it refreshes.

7.11 Integrating Novell Customer Center with ZENworks Linux Management

Novell Customer Center is an online tool that makes it easier for you to manage your business and technical interactions with Novell. From one location, you can do the following:

- Review the status of supported Novell products, subscriptions, and services
- Obtain support
- Get Linux updates and patches

For more information about Novell Customer Center, see the Novell Customer Center documentation (http://www.novell.com/documentation/ncc/index.html).

ZENworks Linux Management helps you to register all SLES 10 and SLED 10 managed devices into Novell Customer Center at the same time. By integrating Novell Customer Center with the ZENworks Linux Management server, you do not need to individually register each managed device to Novell Customer Center.

To integrate the ZENworks Linux Management Server with Novell Customer Center:

1 Install ZENworks Linux Management Agent on all the managed devices. For more information, see Setting Up Managed Devices in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

2 Register the ZENworks Linux Management Server to Novell Customer Center.

   ◆ **On SLES 10:** Execute `zlm-ncc-reg` `<IP_address_of_the ZENworks_Linux_Management_server>` `<E-Mail_Id_of_Novell_Customer_Center_Account>` `<License_key_for_ZENworks_Linux_Management_or_the_product_ that_entitles_you_to_ZENworks Linux Management>`

   ◆ **On Other Servers:** Execute the `zlm-ncc-reg` command.

   The ZENworks Linux Management Server acts as a Satellite server and registers all the managed devices to Novell Customer Center.

3 Log in to the ZENworks Control Center, then click the *Configuration* tab.

4 In *Management Zone Settings*, click *Novell Customer Center* to display the Novell Customer Center page.
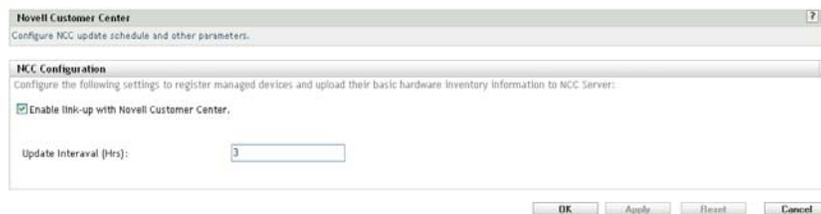
5 Configure the following settings to register the managed devices and upload their basic hardware inventory information to Novell Customer Center:

   ◆ Select *Enable link-up with Novell Customer Center*.

   This enables the server to periodically transmit information about itself and its managed devices to Novell Customer Center.

   ◆ In *Update Interval (Hrs)*, specify how often the server must send information to Novell Customer Center. By default, the interval is 3 hours.

6 Click *Apply*, then click *OK*.

NOTE: To view the information uploaded by the ZENworks Linux Management Satellite server, ensure that the Novell Customer Center account is created before registering the ZENworks Linux Management Server to Novell Customer Center.

7.12 Configuring the ZENworks Server Preferences

ZENworks Server preferences are used to control events triggered from managed device as well as from ZENworks Server. These preferences are configured by default. The following preferences are available for the ZENworks Linux Management Server:

   ◆ **allow-rebuild:** Enables or disables the rebuild action of the managed device during the device registration process. The default value is False.

   ◆ **compute-package-device-updates:** Enables or disables both Package Updates and Device Updates Queue actions triggered on the ZENworks Server. The default value is True.

   ◆ **show-updates-icon:** Enables or disables the Updates icon for devices displayed under the *Devices* tab. The default value is True.

- ◆ **store-file-deps:** Enables or disables filtering of RPM Package dependency metadata. The default value is True.

You can only edit the value of the preferences.

To edit the ZENworks Server preferences:

1 In the ZENworks Control Center, click the *Configuration* tab.
2 Click *ZLM Server Preferences*.

   The ZENworks Server Settings page displays the preferences configured for the server.
3 Click *Edit Preferences* to display the Configure Server Preferences dialog box.
4 Configure the following settings:

   - ◆ In the *Preference* drop-down list, select the preference whose value you want to change.
   - ◆ In the *Value* drop-down list, select the desired value for the selected preference.
5 Click *OK*.

NOTE: The *Apply* and *Reset* buttons are not available for the ZENworks Server Settings page.

7.13 Understanding the StoreFileDeps Preference

StoreFileDeps is a preference on the ZENworks Linux Management server. This preference verifies the Requires and Provides lists of the RPM packages on the server, depending on the value set for the preference. You can set the value of this preference to True or False.

If the value is False, then the ZENworks Linux Management server verifies the Requires list and the Provides list while adding a package to a repository. The server removes from the Provides list those dependencies that are not in use by any other packages. It also adds those dependencies to the Provides list that are in the Requires list of any other RPM package on the repository. By default, the server also removes all the documents, man pages, etc. from the Provides list to reduce the size of the metadata files that move from the server to the client. However, truncating dependencies can create problems while resolving them on the client side. So, before setting the preference value as False, you should import all the packages of different distributions installed on the agents to a catalog on the ZENworks Linux Management server. Only then should you create a bundle or mirror any updates. Importing the packages ensures that all the related packages are available on the repository, and that the necessary dependencies are not filtered out while creating bundles.

If the preference's value is True, the dependencies list is kept as it is on the RPM metadata while creating bundles. This ensures that the server does not add or remove unnecessary dependencies. It also ensures that the dependency resolution does not fail on the client side if the dependent packages are available on the media installation source that is added as a service to the ZENworks Management Daemon. However, this increases the size of the metadata that moves to the client.

7.14 Cleaning Up Inactive Devices

You can remove the inactive or obsolete devices from the ZENworks Servers by configuring the Inactive Device Cleanup schedule in the ZENworks Control Center. However, you cannot remove the inactive devices that are Primary Servers or Secondary Servers.

To configure the Inactive Device Cleanup schedule:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *Inactive Device Cleanup Schedule*.

3 Select *Enable Warning* to set a warning for devices that have been inactive for the specified number of days. The default is 10 days.

4 Select *Enable Move* to move inactive devices to the `InactiveDevices` folder after the specified number of days.

The `InactiveDevices` folder is created automatically. The default is 30 days.

5 Select *Enable Delete* to delete inactive devices from the `InactiveDevices` folder after the specified number of days.

 By default, devices are never deleted from the `Inactive Devices` folder.

6 Select a schedule type from the drop-down list. The default schedule type is *Monthly*. The following schedules are available:

Schedule Type	Description
Monthly	Select the day of the month to run the scheduled event on and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week to run the scheduled event on and set other restrictions that might apply.

7 Click *Apply*.

IMPORTANT: The *Set the "Black Out" time ranges when execution should not occur* option is nonfunctional.

ZENworks Administrator Accounts

8

During installation, a default Administrator account is created. This account provides rights to administer all of your Novell® ZENworks® system.

You can create additional administrator accounts that provide full access to your ZENworks system. You can also create accounts that limit administrative rights to specific device folders, policy folders, bundle folders, and report folders.

You can use the ZENworks Control Center or the zlman command line utility to create and modify administrator accounts. The following procedures explain how to perform these tasks using the ZENworks Control Center. If you prefer the zlman command line utility, see the Administrator Commands section of zlman (1) (page 562).

The following sections provide information to help you create administrator accounts and manage administrator rights:

8.1 Creating an Administrator Account

1 Log in to the ZENworks Control Center using an administrator account that has rights to create other administrator accounts.

   The default account, Administrator, has rights to create additional accounts.

2 In the ZENworks Control Center, click the *Configuration* tab.

   The Administrators section of the Configuration page lists the current accounts.

3 In the *Administrators* list, click *New* to display the Add new Administrator dialog box.

4 Provide a username and password for the account, then click *OK* to add the account to the *Administrators* list.

   The administrator can change the password the first time he or she logs in by clicking the key icon located next to the *Logout* link in the upper-right corner of the ZENworks Control Center.

The newly created administrator account is granted View rights to all objects in the Management Zone. To grant additional rights, or to limit the administrator's rights to specific folders only, you need to modify the rights.

5 To change the administrator's rights, see the next section, Modifying Account Rights.

8.2 Modifying Account Rights

By default, newly created accounts are granted View rights to all objects in the Management Zone. You can modify an administrator's rights so that the administrator can:

- ◆ Change the Management Zone configuration settings.
- ◆ Create or modify other administrator accounts.
- ◆ Create, modify, and delete all objects in the Management Zone or in a specific folder only.
- ◆ Modify all objects in the Management Zone or in a specific folder only.

To modify an administrator's rights:

1 Log in to the ZENworks Control Center using an administrator account that has rights to create and modify other administrator accounts.

The default account, Administrator, has rights to create and modify additional accounts.

2 In the ZENworks Control Center, click the *Configuration* tab.

The Administrators section of the Configuration page lists the current accounts.

3 Click the account you want to modify.

4 Set the General options as desired:

- ◆ **Can create and manage other administrators:** Select this option to enable the administrator to create additional administrator accounts, or to change the settings for existing administrator accounts.
- ◆ **Can modify zone settings:** Select this option to enable the administrator to change the Management Zone settings, registration keys, registration rules, and licensing information included on the Configuration page.

5 Set the bundle, device, policy, and report rights as desired.

You use the Assigned Rights sections to control the administrator's rights to manage bundles, devices, policies, and reports. You can give the administrator All rights (Create, Delete, Modify), Modify rights only, or View rights only.

You assign rights at the folder level. The root folders are `/Bundles`, `/Devices`, `/Policies`, and `/Reports`. Rights assigned at a root folder are effective in all subfolders (for example, `/Bundles/Workstations`) unless specifically overridden at the subfolder level.

For example, if you want the administrator to be able to view bundles that are located in the `/Bundles` folder and create, delete, or modify bundles in the `/Bundles/Workstations` folder, you would assign the administrator View rights to the `/Bundles` folder and All rights to the `/Bundles/Workstation` folder.

The following options are available to add folders and modify the administrator's rights to folders:

- **Add:** By default, the Assigned Rights sections display only the root folders (`/Bundles`, `/Devices`, `/Policies`, and `/Reports`). To assign rights to a folder that is not listed, you need to add the folder to the list. To do so, click *Add* to display the Add Rights Folder dialog box. In the Folders field, click to browse for and select the folder. After you select the folder, select the desire rights assignment (All, Modify, or View), then click *OK*.

- **Edit:** To modify the administrator's rights to a folder that already appears in the list (for example, the `/Bundles` folder), select the folder by clicking the box in front of its name, then click *Edit*. Select the rights assignment you want (All, Modify, or View), then click *OK*.

- **Delete:** To delete a folder from the list, select the folder by clicking the box in front of its name, then click *Delete*. This deletes the administrator's directly assigned rights to the folder. The administrator still inherits the rights assigned to the folder's parent. For example, assume the administrator has View rights in the `/Bundles` folder and All rights in the `/Bundles/Workstations` folder. You delete the `/Bundles/Workstations` folder from the list. The administrator's rights in the `/Bundles/Workstations` folder revert to the rights inherited from the `/Bundles` folders. Therefore, in this example, the administrator goes from having All rights in the `/Bundles/Workstation` folder to having View rights only.

  You cannot delete the root folders (`/Bundles`, `/Devices`, `/Policies`, and `/Reports`).

6 When finished modifying rights, click *Apply* to apply the changes.

ZENworks Object Store and Data Store Maintenance

9

Under normal conditions, the data in the Novell® ZENworks® Object Store and Data Store is always consistent. However, inconsistencies can occur because of database corruption, hardware failures, or even natural disasters. Therefore, we recommend that you periodically back up and restore the Object Store and Data Store.

ZENworks Linux Management provides tools to back up and restore the ZENworks Object Store and the PostgreSQL Data Store If you are using Oracle for the Data Store, we recommend using a tool like RMAN. Basic instructions for using RMAN are included in this section.

IMPORTANT: To restore a ZENworks Linux Management system after the failure of a ZENworks Primary Server, you need backups of the Object Store, Data Store, package repository, and zlmmirror configuration files. For more information, see "Disaster Recovery" in the *Novell ZENworks 7.3 Linux Management Troubleshooting Guide*.

The following sections provide information about the maintenance tasks you can perform.

9.1 Maintaining the ZENworks Object Store

The ZENworks Object Store is Novell eDirectory™ 8.8.3. The Novell eDirectory Service `/etc/init.d/ndsd` should be running to allow the backup and restore operations for ZENworks Object Store.

The following sections provide information for backing up and restoring the Object Store:

9.1.1 Backing Up the ZENworks Object Store

The `zlm_ndsbackup.sh` located in `/opt/novell/zenworks/sbin` allows you to create the ZENworks Object Store backup by using the ndsbackup utility, and the full backup of eDirectory DIB by using the dsbk utility.

You can either back up the Object Store or take a full backup of the eDirectory DIB. We recommend that you back up both of them.

1 Make sure you are logged in as root to the ZENworks Server.

2 Enter the following command to back up the Object Store:

```
# zlm_ndsbackup.sh -U admin.system
```

3 Enter the password to authenticate to the Object Store.

This is the password for the ZENworks Administrator account.

You can also automate the backup process by using the `# zlm_ndsbackup.sh -U admin.system -P ` *`authentication_password_to_the_object_store`* command.

4 Enter the following command to take a full backup of the eDirectory DIB:

```
# zlm_ndsbackup.sh -U admin.system -B
```

IMPORTANT: The Object Store backup and the full backup of eDirectory must run separately, either manually or through a cron job. This is because the backup files need to be created with different time stamps to save them as different files.

The backup program creates a directory in `/var/opt/novell/zenworks/backup/nds/`*`month-yyyy/yyyy-mm-dd`*. The directory name is the date on which the backup is taken. The backup files are saved in this directory. The name of the backup file has the format *timestamp*-backup, and the time stamp indicates the time when the backup was taken. For example:

```
/var/opt/novell/zenworks/backup/nds/August-2005/2005-08-23/10:12:23-backup
```

The log information about the backup operation is saved to `/var/opt/novell/log/zenworks/ndsbackup.log`.

9.1.2 Restoring the ZENworks Object Store

The `zlm_ndsrestore.sh` allows you to restore both the ZENworks Object Store backup and the full backup of the eDirectory DIB.

1 Make sure you are logged in as root to the ZENworks Server.

2 Enter the following command to restore the Object Store:

```
zlm_ndsrestore.sh -U admin.system -F path_to_the_backup_file
```

Make sure that the -F option includes the backup file's complete path.

3 Enter the password to authenticate to the Object Store.

This is the password for the ZENworks Administrator account.

4 Enter the following command to restore the full backup of eDirectory:

```
#  zlm_ndsbackup.sh -U admin.system -F  path_to_the_backup_file  -B
```

5 After the restore operation is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see Section 9.4, "Synchronizing the Object Store and Data Store," on page 98.

The log information about the restore operation is saved to `/var/opt/novell/log/zenworks/ndsrestore.log`.

9.1.3 Deleting the Dangling Objects from ZENworks Object Store

The zlm-edirectory cleanup utility of ZENworks 7.3 Linux Management IR2 helps you to delete dangling objects from ZENworks Object Store.

To run the zlm-edirectory cleanup utility on the ZENworks Server:

1 Close all ZENworks Linux Management operations, if any are running.

2 Create an XML file with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>

<ZLMedirectoryCleanup xmlns="http://www.novell.com/zenworks/
edirectoryCleanup" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <Tree>

    <ZoneName>
      Management_Zone_Name
    </ZoneName>

      <Password>eDirectory_password </Password>

      <Principle>
        Base_DN_of_the_eDirectory (usually, cn=admin,o=system)        </
Principle>

      <RootContext>
        Root_context_to_which_LDAP_connection_is_to_be_established
(usually, o=cell)        </RootContext>

      <IPAddress>IP_address_of_the_ZENworks_Server</IPAddress>

      <Port>
        SSL_port_number_used_by_the_ZENworks_Server (usually, 10636)
</Port>

      <SSL>true</SSL>

      <ImportCertificate> True or False </ImportCertificate>

    </Tree>

</ZLMedirectoryCleanup>
```

The ZENworks server uses the information in the XML file to establish connection with eDirectory.

3 At the server console prompt, go to `/opt/novell/zenworks/sbin` and execute the following command:

`zlm_edirCleanup complete_path_of_the_xml_file`

Where *complete_path_of_the_xml_file* is completed path of the XML file created in Step 2.

4 (Optional) To review the status of the utility, see `/var/opt/novell/log/zenworks/edirCleanup.log`.

9.2 Maintaining the ZENworks Data Store on PostgreSQL

The following sections provide instructions for backing up and restoring the PostgreSQL Data Store:

9.2.1 Displaying the Password for the Default PostgreSQL Database

The password for the default ZENworks PostgreSQL database is stored as plaintext on your ZENworks Primary Server. You can access the database without the password if you are logged on as Root.

If you need the password for maintenance purposes, you can use the following command to display the password (you must be logged in as Root):

```
cat /etc/opt/novell/zenworks/serversecret
```

9.2.2 Understanding Automated Database Maintenance

If you are using a PostgreSQL database, there are some automated maintenance tasks that are performed both daily and monthly.

Daily Maintenance: Once a day, old versions are flagged, allowing the space used by these records to be used for new data; the statistics used by the query engine are updated to achieve the best possible performance. This maintenance runs every day at 2:15 a.m.

Monthly Maintenance: Unlike the daily maintenance, the monthly maintenance actually frees the space used by the old flagged records; this prevents a large disparity between the allocated disk space for the database and the actual space used by the database. Because this is an intensive process, it is scheduled monthly instead of daily. It runs at 3:15 a.m on the first day of each month.

9.2.3 Backing Up the ZENworks Data Store

This section applies only if you are using the PostgreSQL database for your Data Store.

You can use `zlm_dbbackup.sh` to make a backup of the Data Store. This backup utility is located in `/opt/novell/zenworks/sbin`.

The hostname in the `.pgpass` file is used by the `zlm_dbbackup.sh` script to automate the PostgreSQL database backup. Before you begin the backup, make sure the hostname is correct. On the ZENworks Linux Management Primary Server, ensure that the hostname in the `/root/.pgpass` file in the `zlm_dbbackup.sh` script is `localhost`. If the hostname is not `localhost`, edit the `.pgpass` file to change the hostname to `localhost`.

1 Make sure you are logged in as root to a ZENworks Server.

2 On the ZENworks Primary Server with the local data store, enter the following at the command prompt:

```
zlm_dbbackup.sh
```

To take a database backup from the ZENworks Secondary Server, enter the following at the command prompt:

```
zlm_dbbackup.sh -H primary_server_hostname or Primary_Server_IPaddress
```

NOTE: Database backup operation is supported from a Secondary Server only if its PostgreSQL database version is same or higher than that on the Primary Server. For example, you cannot run the backup utility from a SLES 9 Secondary Server if the Primary Server is a SLES 10 server. This is because the SLES 9 server's pg_dump utility, which is used by the backup utility, is incompatible with the PostgreSQL database version running on the Primary Server. You have to run the backup utility on the Primary Server.

A directory with the current date is created at `/var/opt/novell/zenworks/backup/db`. The backup file, named `timestamp-zenworks-backup.tar.gz`, is saved in this directory. For example, if the backup is taken on August 23, 2005 at 11:30 p.m., the following directory and file are created:

```
/var/opt/novell/zenworks/backup/db/2005-08-23/23:30:00-zenworks-backup.tar.gz
```

Log information about the backup operation is saved in the `/var/opt/novell/log/zenworks/dbbackup.log` file.

The utility does not require any user interaction. If desired, you can schedule the database backup operation as a cron job.

9.2.4 Restoring the ZENworks Data Store

This section applies only if you are using the PostgreSQL database for your Data Store.

If necessary, you can restore the ZENworks Data Store from a backup you created. You use `zlm_dbrestore.sh`, located in `/opt/novell/zenworks/sbin`, to restore the Data Store from a backup.

The restore operation drops the existing database and creates a new one.

To restore the ZENworks Data Store:

1 On all ZENworks Servers, stop the ZENworks Server (novell-zenserver) and the ZENworks Loader (novell-zenloader) services by using the following commands:

```
/etc/init.d/novell-zenserver stop
```

```
/etc/init.d/novell-zenloader stop
```

Because all ZENworks Servers access the Data Store, you need to stop these services on all ZENworks Servers on your system. You must also ensure that any external connections to the database are terminated.

2 Make sure you are logged in as root to a ZENworks Server.

3 On the ZENworks Primary Server, enter the following at the command prompt:

```
zlm_dbrestore.sh -F path_to_the_backup_file
```

To restore a database from a Secondary Server, enter the following at the command prompt:

```
zlm_dbrestore.sh -F path_to_the_backup_file -H primary_server_host_name
```

If you have taken a database backup from the Secondary Server, you can restore the database from the Secondary Server only if its PostgreSQL database version is same as that on the Primary Server.

Make sure that the -F option includes the backup file's complete path. For example:

```
zlm_dbrestore.sh -F /var/opt/novell/zenworks/backup/db/2005-08-23/
23:30:00-zenworks-backup.tar.gz
```

4 If prompted, enter Y to stop the ZENworks Server (novell-zenserver).

5 If prompted, enter Y to stop the ZENworks Loader (novell-zenloader).

6 When prompted to supply a password to drop the database, enter the password configured in `/etc/opt/novell/zenworks/hibernate.cfg.xml` that is used for authenticating the PostgreSQL database.

7 When prompted to supply a password to create the new database, enter the password configured in `/etc/opt/novell/zenworks/hibernate.cfg.xml` that is used for authenticating the PostgreSQL database.

The log information about the restore operation is saved in the file `/var/opt/novell/log/zenworks/dbrestore.log`.

8 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see Section 9.4, "Synchronizing the Object Store and Data Store," on page 98.

9 On all ZENworks Servers, start the ZENworks Server (novell-zenserver) and the ZENworks Loader (novell-zenloader) by using the following commands:

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

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

9.2.5 Optimizing the Server Database

To improve the server database performance, use the `zlm-pg-vacuum` script, found in the `/opt/novell/zenworks/bin` directory on the ZENworks Server. When you install a ZENworks Primary Server using a local PostgreSQL database, the installation program creates a script that runs on a daily basis.

The `zlm-pg-vacuum` script runs the `vacuumdb` command, which has a significant impact on database performance. You must log in as `root` before running the `zlm-pg-vacuum` script. For the optimal performance, run the following vacuum scripts:

- **zlm-pg-vacuum or zlm-pg-vacuum --busy-tables:** Depending on the database activity, run the script daily to weekly. Run the script once a week on a lightly loaded server and once a day on a heavily loaded server.

- **zlm-pg-vacuum --full:** Run the script during a period of less activity or during downtime for the database server. Depending on the database activity, run the script weekly or bi-weekly. It performs a full vacuum analyze and exclusively locks tables. It is recommended that you manually run the `zlm-pg-vacuum --full` script once a month by performing the following steps:

  1.Stop all the ZENworks services by executing `zlm-config --stop`.

  2. Execute `zlm-pg-vacuum --full`.

  3. Start all the ZENworks services by executing `zlm-config --start`.

Additionally, you can fine-tune the following parameters depending on your memory requirements and scale:

- In the `/etc/sysctl.conf` file, configure `kernel.shmmax`.
- In the `postgresql.conf` file, configure `shared_buffer`, `sort_mem`, `vacuum_mem`, `wal_buffers`, and `checkpoint_segments`.

For more information on how to fine-tune the parameters, see the PostgreSQL documentation (http://www.postgresql.org/docs/).

Following is a sample scenario that illustrates how you can fine-tune the database parameters. The values indicated in this scenario are sample values; you must fine-tune it according to your requirements. For more information on how to fine-tune the parameters, see the PostgreSQL documentation (http://www.postgresql.org/docs/)

An Example Scenario: In this scenario, assume that the ZENworks server is running on an IBM x346 with two Xeon processors and 4 GB of RAM. The database is running on the same server. 2 GB of RAM is dedicated to the other ZENworks processes, 1 GB of RAM to the operating system and non-ZENworks processes, and the remaining 1 GB of RAM is for PostgreSQL.

To optimize the server database performance:

1 In the `/etc/sysctl.conf` file, set the value of `kernel.shmmax` to `1572864000` so that the process can have 1.5 GB of shared memory.

The shmmax kernel parameter allows PostgreSQL to consume more shared memory. By default, the kernel only allows a process to consume 32 MB of shared memory.

NOTE: This step is not applicable if ZENworks 7.3 Linux Management is running on SLES 10 device because the value of `kernel.shmmax` is 4 GB by default on SLES 10.

2 In the `postgresql.conf` file, configure the following parameters:

- `shared_buffers = 131072`
- `sort_mem = 10240`
- `vacuum_mem = 102400`
- `wal_buffers = 20`
- `checkpoint_segments = 20`

3 Reboot the server for the changes to take effect.

9.2.6 Restarting Novell Zenworks Server Services After Restarting the Database

After restarting the PostgresSQL database on the ZENworks Linux Management Server, the database connections will be restored in approximately 15 minutes. During this time, the ZENworks Control Center and zlman utility might display database-connection errors.

To restore the connections immediately, restart the novell zenworks services by running the following command:

```
/opt/novell/zenworks/bin/zlm-config --restart
```

9.3 Maintaining the ZENworks Data Store on Oracle

The following sections provide instructions for backing up and recovering a ZENworks Data Store using Oracle:

9.3.1 Backup and Recovery Solutions

Oracle provides two methods of backup and recovery:

- Recovery Manager (RMAN)
- User-managed backup and recovery

The RMAN utility is automatically installed with the database. It can back up an Oracle8 database and all later versions of an Oracle* database. RMAN uses server sessions on the database to perform backup and recovery. RMAN has its own syntax and is accessible either through a command-line interface or through the Oracle Enterprise Manager GUI. RMAN also provides APIs to interface with third-party media managers.

The advantage of RMAN is that it obtains and stores metadata about its operations in the control file of the database. An independent recovery catalog can be set up, which is a schema that contains metadata imported from the control file, in a separate recovery catalog database. RMAN performs the necessary record keeping for backups, archived logs, and so forth using the metadata, so restoration and recovery is greatly simplified.

An alternative method of performing recovery is to use operating system commands for backups and SQL*Plus for recovery. This method is called User-managed backup and recovery.

RMAN automates backup and recovery, but the User-managed method requires keeping track of all database files and backups. Therefore, because of its robustness and simplified database administration abilities, RMAN is a highly recommended tool for backup operations. The subsequent sections of this document explain the steps for using RMAN to perform a complete database backup and recovery.

9.3.2 Setting Environment Variables

1 Set the following environment variables to the appropriate values before using RMAN:

+ ORACLE_HOME: The directory where the Oracle software is installed.

  For Oracle 9i R2: Set the variable as `ORACLE_HOME=/opt/oracle/product/9ir2`

  For Oracle 10g R2: Set the variable as `ORACLE_HOME=/opt/oracle/product/10.2/db_1`

+ CLASSPATH: The paths to the libraries installed by Oracle.

  For Oracle 9i R2: Set the variable as `CLASSPATH=$CLASSPATH:/opt/oracle/product/9ir2/JRE:/oracle/opt/oracle/product/9ir2/jlib:/oracle/opt/oracle/product/9ir2/rdbms/jlib:/oracle/opt/oracle/product/9ir2/network/jlib`

  For Oracle 10g R2: Set the variable as `CLASSPATH=$CLASSPATH:/opt/oracle/product/10.2/db_1/JRE:/opt/oracle/product/10.2/db_1/jlib:/opt/oracle/product/10.2/db_1/rdbms/jlib:/opt/oracle/product/10.2/db_1/network/jlib`

+ PATH: The Oracle installation's bin directory.

  For Oracle 9i R2: Set the variable as `PATH=$PATH:/opt/oracle/product/9ir2/bin`

  For Oracle 10g R2: Set the variable as `PATH=$PATH:/opt/oracle/product/10.2/db_1/bin`

You can set the environment variables similarly for Oracle 11g database.

9.3.3 Connecting to the Database

You can use either of the following methods to connect to the Oracle database being used for the Data Store:

+ Start RMAN at the operating system command line without connecting to a database, by issuing the RMAN command without any connection options:

```
$ rman

RMAN> CONNECT TARGET /
```

+ Start the RMAN executable at the operating system command line while connecting to the database:

```
$ rman TARGET /
```

IMPORTANT: If you have installed Oracle 10g or Oracle 11g database on a SLES 10 device, make sure to run the rman executable from the `$ORACLE_HOME/bin/rman` directory.

If the database is already mounted or open, RMAN displays output similar to the following:

```
Recovery Manager: Release 9.2.0.0.0
connected to target database: RMAN (DBID=1237603294)
```

The DBID value displayed is the database identifier for the target database.

If the target database is not started, RMAN shows the following message:

```
connected to target database (not started)
RMAN>   # the RMAN prompt is displayed
```

9.3.4 Starting the Database

1 Start the database using the following command:

```
RMAN> startup mount
```

This command starts an Oracle instance if it is not already started, and mounts the database but does not open it.

If the mount was successful, then the following output is displayed:

```
Oracle instance started
database mounted
```

Otherwise, appropriate error messages are displayed, indicating the causes of failure and suitable solutions.

9.3.5 Backing Up the Database

You can back up the database to the default disk location. The default location is OS-specific. On Linux, the default path where backup files are stored is `$ORACLE_HOME/dbs`.

To make a full backup of the data files, control files, and the current server parameter file to the default device type (which is the disk), use the following backup command at the RMAN prompt:

```
RMAN> BACKUP DATABASE;
```

In the above command, the FORMAT parameter is not specified, so RMAN automatically gives each backup piece a unique name and stores it in the OS-specific default location (`$ORACLE_HOME/dbs` on Linux).

To specify a filename for the backup piece, use the backup command with the FORMAT parameter:

```
 RMAN> BACKUP DATABASE FORMAT'/tmp/%U';
```

%U generates a unique filename.

The RMAN backup command creates a backup set, which is a logical object that contains one or more backup pieces.

The backup command output contains the essential information about the backup, as shown in the following example:

```
Starting backup at JULY 12 2009 19:09:48
using target database controlfile instead of recovery catalogal
located channel: ORA_DISK_1
channel ORA_DISK_1: sid=10 devtype=DISK
channel ORA_DISK_1: starting full datafile backupset
channel ORA_DISK_1: specifying datafile(s) in backupset
including current SPFILE in backupset
including current controlfile in backupset
input datafile fno=00001 name=/oracle/oradata/zenworks/system01.dbf
input datafile fno=00002 name=/oracle/oradata/zenworks/undotbs01.dbf
input datafile fno=00003 name=/oracle/oradata/zenworks/cwmlite01.dbf
input datafile fno=00004 name=/oracle/oradata/zenworks/drsys01.dbf
input datafile fno=00005 name=/oracle/oradata/zenworks/example01.dbf
input datafile fno=00006 name=/oracle/oradata/zenworks /indx01.dbf
input datafile fno=00007 name=/oracle/oradata/zenworks/tools01.dbf
input datafile fno=00008 name=/oracle/oradata/zenworks/users01.dbf
channel ORA_DISK_1: starting piece 1 at  JULY 12 2009  19:09:56
channel ORA_DISK_1: finished piece 1 at  JULY 12 2009 19:10:31
piece handle=/oracle/dbs/lvd6dtk1_1_1 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:39
Finished backup at JULY 12 2009 19:10:33
```

9.3.6 Recovering the Database

You can recover a restored data file by applying archived redo logs and online redo logs; that is, records of changes made to the database after the backup was taken. The following sections provide instructions for two methods you can use to recover the database:

- "Complete Recovery" on page 95
- "Incomplete Recovery" on page 96

Complete Recovery

Complete recovery involves using redo data or incremental backups combined with a backup of a database, tablespace, or data file, to update it to the most current point in time. This is called a complete recovery because Oracle applies all of the redo changes contained in the archived and online logs to the backup. Typically, a complete media recovery is performed after a media failure damages data files or the control file.

1 Use the following sequence of commands to perform a complete recovery of the database.

```
RMAN> connect target /

RMAN> run {

2> startup mount ;

3> restore database ;

4> recover database ;

5> alter database open ;

6> }
```

This results in all data files being restored and then recovered. RMAN applies archive logs as necessary until the recovery is complete.

2 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see Section 9.4, "Synchronizing the Object Store and Data Store," on page 98.

Incomplete Recovery

RMAN can perform recovery of the whole database to a specified non-current time, SCN, or log sequence number. This type of recovery is called incomplete recovery because it does not completely use all of the available redo logs. Incomplete recovery of the whole database is also called database point-in-time recovery (DBPITR).

You should perform an incomplete recovery of the database in the following situations:

◆ Media failure destroys some or all of the online redo logs.

◆ A user error causes data loss, for example, a user inadvertently drops a table.

◆ You cannot perform a complete recovery because an archived redo log is missing.

To perform an incomplete recovery, restore all data files from backups created prior to the time when a recovery is needed, and then open the database with the RESETLOGS option after recovery completes. The RESETLOGS operation creates a new instance of the database—in other words, a database with a new stream of log sequence numbers starting with log sequence 1.

The database must be closed to perform an incomplete recovery.

To perform an incomplete recovery:

1 Set the time format environment variable:

```
$ NLS_DATE_FORMAT="Mon DD YYYY HH24:MI:SS"
```

2 Use the following sequence of commands:

```
$ rman target  /

RMAN> startup mount;

RMAN> run {

2> set until time "to_date('Jul 12 2009 10:24:00', 'MM DD YYYY
HH24:MI:SS')";

3> restore database ;

4> recover database ;

5> }
```

RMAN uses the last backup created before the time mentioned in the set until command to restore the files to their default locations. Then, it uses archived redo logs (if needed) to recover the database.

Two other parameters that can be used with the `set until` command are SCN and log sequence numbers. You obtain SCNs from the alert logs. Find the SCN of an event and recover to a prior SCN. For example:

```
SET UNTIL SCN 1000
```

3 If recovery was successful, open the database and reset the online logs:

```
ALTER DATABASE OPEN RESETLOGS;
```

4 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see Section 9.4, "Synchronizing the Object Store and Data Store," on page 98.

We recommend that you back up the database immediately, preferably with the database mounted (to avoid possible data loss in an open database). Because the database is a new instance, the backups made before the RESETLOGS are not easily usable.

9.3.7 Shutting Down the Database

1 Use the following command to shut down the database:

```
RMAN> SHUTDOWN NORMAL;
```

This command dismounts the database and stops the running Oracle instance.

9.3.8 User-managed Backup and Recovery

1 On all the ZENworks 7.3 Linux Management servers configured with the source database, stop all the ZENworks services by using the following command:

```
zlm-config --stop
```

2 On the source database that has its database instance running, take a logical backup of the ZENworks database objects schema by running the export utilities as follows as an Oracle database user:

```
exp zenadmin/novell@ORCL FILE=NOVELL-ZENWORKS-ORAZLM.DMP LOG=NOVELL-
ZENWORKS-ORAZLM.LOG OWNER=ZENADMIN
```

where ORCL is the default Oracle system identifier, and novell is the default password for the zenadmin user.

This creates the `NOVELL-ZENWORKS-ORAZLM.DMP` backup file and the `ZENWORKS-ORAZLM.LOG` log file on the Oracle Database server.

3 Run the import utility as follows as an Oracle database user on the destination database to import the data and objects:

```
imp zenadmin/novell@ORCL FILE=NOVELL-ZENWORKS-ORAZLM.DMP LOG=NOVELL-
ZENWORKS-ORAZLM.LOG IGNORE=Y FROMUSER=ZENADMIN TOUSER=ZENADMIN
```

where ORCL is the default Oracle system identifier, and novell is the default password for the zenadmin user.

IMPORTANT: Before running the import utility, take a reliable backup of the `/opt/oracle/novell/zenworks/database` directory on the destination database.

Ignore any compilation warnings that might occur during the object creation process.

4 On the destination database, login as `sysdba` user, and stop and start the Oracle instance by using the following commands at the SQL prompt:

```
shutdown immediate
```

```
startup
```

5 On the destination database server, stop and start the listener service by using the following commands at the SQL prompt:

```
lsnrctl stop

lsnrctl start
```

6 On the ZENworks 7.3 Linux Management server, start all the ZENworks services by using the following command:

```
zlm-config --start
```

7 Synchronize the Data Store with the Object Store. For more information on how to synchronize the Data Store with the Object Store, see Section 9.4, "Synchronizing the Object Store and Data Store," on page 98.

9.4 Synchronizing the Object Store and Data Store

If you've restored either the Object Store or the Data Store from backup, you need to make sure the two are synchronized. The dbsync.sh utility lets you synchronize the Data Store with the Object store by removing all devices and bundles that are found in the Data Store but not in the Object Store.

1 Make sure you are logged in as root to the ZENworks Server.

2 Enter the following command on the command prompt:

```
dbsync.sh [--force]
```

The utility has one option, --force or -f. The synchronization operation compares the list of devices and bundles in the two databases. When you use the --force option, dbsync.sh logs the GUIDs and names of the devices and bundles found in the Data Store but not in the Object Store. When you use the --force option, dbsync.sh deletes all devices and bundles that are found in the Data Store but not in the Object Store.

3 Enter the password to authenticate to the Object Store.

The GUIDs and names of the devices and bundles that are in the Data Store but not in the Object Store are logged in the `/var/opt/novell/log/zenworks/dbsync-message.log` file.

9.5 Cleaning Up the ZENworks Database

To clean up the ZENworks database, enter the following command at the server console prompt:

```
zlm_db_cleanup.sh
```

To troubleshoot any errors encountered while running the database clean-up command, refer to the `/var/opt/novell/log/zenworks/dbcleanup.log`.

Device Registration
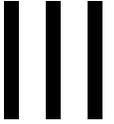
III

The following sections provide information about Novell® ZENworks® Linux Management device registration:

Registration Overview

Novell® ZENworks® Linux Management provides simplified, hands-off management of devices (servers and workstations). Before you can configure application settings through the use of policies, install packages using bundles or catalogs, use preboot services to image devices, collect hardware and software inventory, remotely manage devices, and report on events, you need to install the ZENworks Linux Management Agent on devices and register them against a ZENworks Server.

The ZENworks Management Zone is the top level of the ZENworks management hierarchy. The Management Zone provides an autonomous administrative unit of ZENworks Servers and managed devices (workstations and servers). You use the ZENworks Control Center (the Web-based administrative tool) to manage devices. The ZENworks Servers and managed devices work together to apply the management tasks.

Any device that you want to manage must be registered in the Management Zone. Registering the device adds the device to the ZENworks Object Store and allows you to manage it through the ZENworks Control Center.

For Novell ZENworks to manage a device, you must install the ZENworks Agent software on the device. During installation of the ZENworks Agent software, the device is automatically registered as long as you (or whoever is installing the software) supplies the DNS name or IP address of a ZENworks Server in your Management Zone. You can also register devices at a later time. For more information, see Chapter 11, "Registering Devices," on page 103.

You can also create registration keys or registration rules to register devices in the Management Zone.

Using registration keys lets you define the keys that are used to register devices in the Management Zone. A registration key specifies a set of assignments that are applied to devices that register using that key. The key must be applied during installation of the ZENworks Agent on a device, either manually or by using a script. For more information, see Section 12.1, "Managing Registration Keys," on page 108

If you do not want to use registration keys, you can create registration rules to determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply. For more information, see Section 12.2, "Managing Registration Rules," on page 113.

NOTE: You can register devices against only one ZENworks 7.3 Linux Management Server. However, you can register devices against one ZENworks 7.3 Server and multiple ZENworks 6.6.*x* Linux Management Servers. Registering devices against multiple Servers is useful, for example, during the transitional period while you deploy ZENworks 7.3.

Registering Devices

<div style="text-align: right; font-size: large;">11</div>

The process of registering devices includes installing the ZENworks® Agent on devices and then registering the devices against a ZENworks Server. During installation of the ZENworks Agent software, the device is automatically registered as long as you (or whoever is installing the software) supplies the IP address or DNS name of a ZENworks Server in your Management Zone. You can also register devices at a later time.

NOTE: If you plan to update Dell PowerEdge servers using Dell Update Packages, we recommend that you mirror the packages from the Dell FTP site before installing the ZENworks Agent on the managed PowerEdge servers. You can also mirror the packages after installing the ZENworks Agent on the managed PowerEdge servers but before registering them in the ZENworks Management Zone. Mirroring the Dell Update Packages prior to installing the ZENworks Agent or registering the servers in the Management Zone ensures that all Dell model numbers are loaded into the database, the standard reports are run as the servers register, and the Dell Update Packages exist in the ZENworks package repository. For more information, see Chapter 23, "Using Dell Update Package Bundles," on page 283.

The following sections contain additional information:

11.1 Installing the ZENworks Agent and Registering Devices

You can register devices (servers or workstations) against a ZENworks Server during installation of the ZENworks Agent on devices.

For more information about manually installing and registering the agent or automating installation and registration using a script, see "Setting Up Managed Devices" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

11.2 Registering a Device after Installing the ZENworks Agent

If the person who installed the ZENworks Agent on a device did not specify the Server address (IP address or DNS name) during installation, the device can be registered at a later time by running the following `rug` command from the device:

For SUSE LINUX Enterprise Server 10 (SLES 10) and SUSE LINUX Enterprise Desktop 10 (SLED 10) managed devices:

```
/usr/bin/rug sa https://ZEN_Server_address
```

For SUSE LINUX Enterprise Server 11 (SLES 11) and SUSE LINUX Enterprise Desktop 11 (SLED 11) managed devices:

`/usr/bin/rug sa https://ZEN_Server_address`

For all other managed devices:

`/opt/novell/zenworks/bin/rug sa https://ZEN_Server_address`

Replace *ZEN_Server_address* with the IP address or DNS name of the Primary or Secondary Server.

You can also register a device by using the Software Installer or Updater. For more information, see Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54.

11.3 Automatically Registering the Services at the Initial Startup of zmd

zmd can automatically register the services configured in the `initial-configuration` file. The file is located in `/etc/zmd/` on SLES 10 or SLES 11 and SLED 10 or SLED 11 managed devices, and in `/etc/opt/novell/zenworks/zmd/` on other managed devices.

The `initial-configuration` file contains the URL for the supported services that zmd registers at initial startup. zmd uses the information in the in the `initial-configuration` file to mount all the services the first time it starts. These services are not loaded during the subsequent startups because zmd records the already mounted services in `@localstatedir@/lib/zmd/services`. If you want zmd to mount the services listed in `initial-configuration` every time it starts, you must delete the services file before starting zmd.

To have zmd automatically register devices, you must manually create the `initial-configuration` file with the following contents:

```
[URL of the service]
type = service_type
key = service_name
```

In the file, you can also specify the `registration_code` for services that need a key for registration.

If you want to use special characters such as $! & ; ' " in the key value, you must enclose the value within single quotes.

A sample `initial-configuration` file is as follows:

```
[https://10.0.0.0]
type=zenworks
[https://update.novell.com/data]
type=rce
[http://www2.ati.com/suse]
type=YUM
```

```
key=yum_service
```

Managing Registration Keys and Rules

12

You can manually add devices to folders and groups, but this can be a burdensome task if you have a large number of devices or are consistently registering new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups when they register. To accomplish this, you can use registration keys, registration rules, or both.

Both registration keys and registration rules let you assign a name, folder, and group memberships to a device. However, there are differences between keys and rules that you should be aware of before choosing whether you want to use one or both methods for registration.

- **Registration Keys:** A registration key is an alphanumeric string that you manually define or randomly generate. During installation of the ZENworks® Agent on a device, the registration key must be input manually or through a response file. When the device connects to a ZENworks Server for the first time, the device is given a name according to the defined naming scheme and then added to the folder and groups defined within the key.

  You can create one or more registration keys to ensure that servers and workstations are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's devices are added to the `/Workstations/Sales` folder but are divided into three different groups (SalesTeam1, SalesTeam2, and SalesTeam3) depending on their team assignments. You could create three different registration keys and configure each one to add the Sales workstations to the `/Workstations/Sales` folder and the appropriate team group. As long as each device uses the correct registration key, the device is added to the appropriate folder and group.

  Registration key names are not case sensitive. For example, registration keys named "MyKey" and "mykey" cannot exist in the same folder. If you try to create a registration key named "Mykey" in a folder that already contains a registration key named "mykey," you receive the error message "Unable to complete your request for the following reason: Unable to create the New Registration Key, see Tomcat logs for details."

- **Registration Rules:** If you don't want to enter a registration key during installation, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

  ZENworks includes a default registration rule for servers and another one for workstations. If a device registers without a key, the default registration rules are applied to determine the folder and group assignments. The two default rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder. The device hostname is used for its name. You cannot delete these two default rules, but you can modify the naming scheme and the folder and groups to which the servers and workstations are added.

  The two default rules are designed to ensure that no server or workstation registration fails. You can define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in , you've established folders for devices with similar configuration settings and groups for devices with similar assignments, newly registered devices automatically receive the appropriate configuration settings and assignments.

The following sections contain additional information:

12.1 Managing Registration Keys

You can define the keys that are used to register devices in the Management Zone. A registration key specifies a set of assignments that are applied to devices that register using that key. The key must be applied during installation of the ZENworks Agent on a device, either manually or by using a script.

If you do not want to use registration keys, you can create registration rules to determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply. For more information, see Section 12.2, "Managing Registration Rules," on page 113.

You can use the ZENworks Control Center or the zlman command line utility to create and modify registrations. The following procedures explain how to perform these tasks using the ZENworks Control Center. If you prefer the zlman command line utility, see the Registration Commands section of zlman (1) (page 562).

The following sections contain additional information:

12.1.1 Creating Keys to Register Devices

1 In the ZENworks Control Center, click the *Configuration* tab.

2 In the Registration Keys section, click *New*, then click *Registration* to launch the Create New Registration Key Wizard.

3 Fill in the fields:

Name (used as the registration key code): Provide a name for the registration key. When devices register during installation or later using the `rug sa` command, this is the name the device provides to be assigned this registration. Any device that presents this name is given the assignments associated with this registration.

Choose something simple for reduced security, or click *Generate* to create a complex registration string that is difficult to guess. Use the *Generate* option along with a registration key limit for increased security.

The following characters cannot be used when creating a registration: # * (+ \ ; ' " < > / ,

Folder: Specify the folder for this registration key. This is for organizational purposes only. Devices do not need to know where a registration key is located in order to use it, they simply need to know the key name.

Description: Provide a description for the key. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

Number of times this key can be used: Choose whether to allow the key to be used an unlimited number of times or specify a number of times that the key can be used.

For security purposes, this option lets you limit the number of devices that can register using this key.

4 Click *Next* to display the Naming and Containment Rules page.

Create New Registration Key	sdf2	?
⚙ Step 2: Naming and Containment Rules		

Supply the template used to create the machine name, and the folder the machine should be placed in when imported.

Name given to imported machines:

${HostName}

Folder where imported machines should be placed:

/Devices/Workstations

<< Back   Next >>   Cancel

5 Fill in the fields to specify a naming scheme and the folder where the devices will be added:

Name given to imported machines: Provide a naming scheme for registering devices. To create a naming scheme, select one or more of the following machine variables:

CPU

DNS

GUID

Hostname (default)

OS

Avoid spaces in your naming scheme; these spaces must be escaped when using the command line utilities. For example, use ${HostName}-${OS} rather than ${HostName} ${OS}.

Folder where imported machines should be placed: Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

6 Click *Next* to display the Group Membership page.
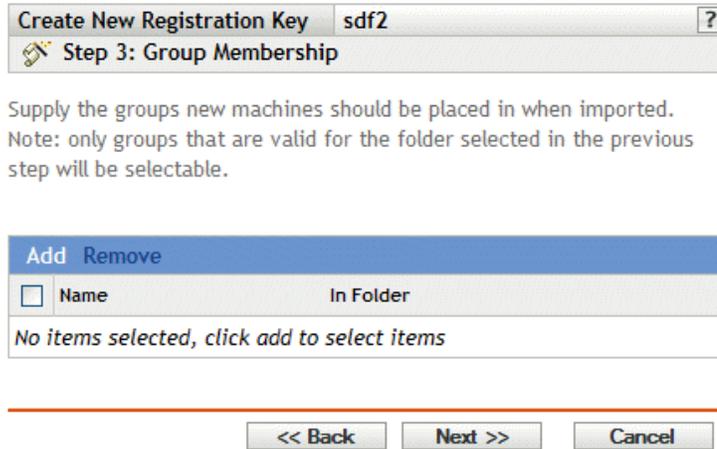
Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both group A and group B, the device receives all assignments from both groups.

Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the /Devices/ Workstations folder, you can only choose workstation groups.

7 Click *Next* to display the Summary page.

8 Review the information on the Summary page, making any changes to the settings by using the *Back* button as necessary. Click *Finish* to create the registration key according to the settings on the Summary page.

12.1.2 Editing Existing Registration Keys

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click the underlined link for the registration key that you want to edit.

> **NOTE:** If you edit an existing registration key, be aware that the changes you make apply only to newly registered devices. If the device is already registered, the original settings remain. For example, if you change the naming and folder containment settings, those devices already registered retain the previous naming convention and remain in the original folder they were placed in. You could, however, unregister the devices and then reregister them to ensure that the new naming convention and folder containment settings are applied to the previously registered devices. For more information, see .

2a (Optional) In the *General* section, make the desired changes:

Description: Edit the description for the key. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

Number of times this key can be used: Choose whether to allow the key to be used an unlimited number of times or specify a number of times that the key can be used.

For security purposes, this option lets you limit the number of devices that can register using this key.

2b (Optional) In the *Values Applied to Imported Machines* section, make the desired changes:

Name given to imported machines: Select one or more machine variables to provide a naming scheme for registering devices.

Avoid spaces in your naming scheme, because these spaces must be escaped when using the command line utilities. For example, use ${HostName}-${OS} rather than ${HostName} ${OS}.

Folder where imported machines should be placed: Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

Group membership: Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the /Devices/Workstations folder, you can only choose workstation groups. To remove a group, select the box next to the group's name, then click *Remove*.

NOTE: If you change group membership for a device and then reregister it, the previous group membership is left intact and the new group membership is added. For example, device A is a member of group 1. You then edit the key to change membership to group 2. When the device is reregistered, the device is a member of both groups.

3 Click *Apply*.

12.1.3 Renaming, Copying, or Moving Registration Keys

1 In the ZENworks Control Center, click the *Configuration* tab.

2 In the Registration Keys section, click *Advanced*.

3 Select a registration key by selecting the box next to its name, click *Edit*, then click an option:

- **Rename:** Click *Rename*, type a new name for the registration key, then click *OK*.
- **Copy:** Click *Copy*, type a new name for the registration key, then click *OK*.

  The copy option is useful to create a new registration key that is similar to an existing key. You can copy a key and then edit the new key's settings.

- **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

  The folder for registration keys is for organizational purposes only. Devices do not need to know where a registration key is located in order to use it, they simply need to know the key name.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* and *Copy* options are not available from the *Edit* menu.

12.1.4 Deleting Registration Keys

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Select the key by clicking the check box next to the key, then click *Delete*.

12.2 Managing Registration Rules

Registration rules let you determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply.

By default, the list includes a default registration rule for servers and another one for workstations. These two rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder. The device hostname is used for its name. You cannot delete these two default rules, but you can modify the naming scheme and the groups to which the servers and workstation are added.

The two server and workstation default rules are designed to ensure that no server or workstation registration fails. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If you establish folders for devices with similar configuration settings and groups for devices with similar bundle and policy assignments, newly registered devices automatically receive the configuration settings and assignments appropriate to them.

If you do not want to use registration rules, you can create registration keys. Using registration keys lets you define the keys that are used to register devices in the Management Zone. For more information, see Section 12.1, "Managing Registration Keys," on page 108.

The following sections contain additional information:

- Section 12.2.1, "Creating Rules to Register Devices," on page 113
- Section 12.2.2, "Editing Existing Registration Rules," on page 117
- Section 12.2.3, "Renaming or Copying Registration Rules," on page 118
- Section 12.2.4, "Reordering Registration Rules," on page 119
- Section 12.2.5, "Deleting Registration Rules," on page 119

12.2.1 Creating Rules to Register Devices

1 In the ZENworks Control Center, click the *Configuration* tab.

2 In the Default Registration Rules section, click *New* to launch the Create New Default Rule Wizard.

3 Fill in the fields:

Name: Provide a name for the registration rule.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Description: Provide a description if desired. The description is displayed on the rule's Details page. If you are creating several registration rules, you might want to use the description to detail each rule.

4 Click *Next* to display the Import Filters page.

5 Click *Add Filter* to specify the criteria used to determine which devices should use this Default Registration Rule.

    5a Select an option from the drop-down list in the left field, select *Equal to*, *Contains*, *Starts with*, or *Ends with* from the drop-down list in the center field, then type a value in the right field.

The options you can use are listed below, along with possible values. The format for all values, with the exception of Device Type, is free form string.

Criteria	Possible Value
CPU	Intel Pentium M processor 1600MHz
DNS	abc.xyz.com
Device Type	Server or Workstation
GUID	5bf63fb9b1ed4cd880e1a428a1fcf737
Hostname	zenserver
IPAddress	123.456.78.99
OS	The format for this value is not free form; the values for the supported OS platforms are: dell-dup-os nld-9-i586 nld-9-x86_64 rhel-3as-i386 rhel-3as-x86_64 rhel-3es-i386 rhel-3es-x86_64 rhel-3ws-i386 rhel-3ws-x86_64 rhel-4as-i386 rhel-4as-ia32e rhel-4as-x86_64 rhel-4es-i386 rhel-4es-x86_64 rhel-4ws-i386 rhel-4ws-x86_64 sled-10-i586 sled-10-x86_64 sles-10-i586 sles-10-ia64 sles-10-ppc sles-10-s390 sles-10-x86_64 sles-8-i386 sles-9-i586 sles-9-x86_64 suse-93-i586 suse-93-x86_64

5b (Conditional) Click *Add Filter* again to add an additional row of criteria and repeat Step 5a and Step 5b, as many times as necessary.

Be aware that the rows in the filter are separated by And. If you specify multiple rows in the filter, the criteria in all rows must be met for the rule to apply.

6 Click *Next* to display the Naming and Containment Rules page.

Create New Default Rule	?
Step 3: Naming and Containment Rules	

Supply the template used to create the machine name, and the
folder the machine should be placed in when imported.

Name given to imported machines:

${HostName}

Folder where imported machines should be placed:

/Devices/Workstations

<< Back   Next >>   Cancel

7 Fill in the fields:

Name given to imported machines: Provide a naming scheme for registering devices.

Avoid spaces in your naming scheme; these spaces must be escaped when using the command line utilities. For example, use ${HostName}-${OS} rather than ${HostName} ${OS}.

Folder where imported machines should be placed: Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

8 Click *Next* to display the Group Membership page.

Create New Default Rule	?
Step 4: Group Membership	

Supply the groups new machines should be placed in when
imported. Note: only groups that are valid for the folder selected in
the previous step will be selectable.

Add Remove	
☐ Name	In Folder
No items selected, click add to select items	

<< Back   Next >>   Cancel

Adding groups causes devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both group A and group B, the device receives all assignments from both groups.

Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the `/Devices/ Workstations` folder, you can only choose workstation groups.

9 Click *Next* to display the Summary page.

10 Review the information on the Summary page, making any changes to the settings by using the *Back* button as necessary. Click *Finish* to create the registration rule according to the settings on the Summary page.

12.2.2 Editing Existing Registration Rules

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click the underlined link for the registration rule that you want to edit.

NOTE: If you edit an existing registration rule, be aware that the changes you make apply only to newly registered devices. If the device is already registered, the original settings remain. For example, if you change the naming and folder containment settings, those devices already registered retain the previous naming convention and remain in the original folder they were placed in. You could, however, unregister the devices and then reregister them to ensure that the new naming convention and folder containment settings are applied to the previously registered devices. For more information, see Chapter 13, "Unregistering and Reregistering Devices," on page 121.

---

3 (Optional) In the *General* section, make the desired changes:

Description: Edit the description for the rule. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

4 (Optional) In the *Import Filters* section, make the desired changes.

4a Select an option from the drop-down list in the left field, select *Equal to*, *Contains*, *Starts with*, or *Ends with* from the drop-down list in the center field, then type a value in the right field.

The criteria options you can use are listed below, along with possible values. The format for all values, with the exception of Device Type, is free form string.

Criteria	Possible Value
CPU	Intel Pentium M processor 1600MHz
DNS	abc.xyz.com
Device Type	Server or Workstation
GUID	5bf63fb9b1ed4cd880e1a428a1fcf737
Hostname	zenserver
IPAddress	123.456.78.99

Criteria	Possible Value
OS	The format for this value is not free form; the values for the supported OS platforms are: suse-93-i586 suse-93-x86_64 sles-9-i586 sles-9-x86_64 rhel-3as-i386 rhel-3es-i386 rhel-3ws-i386 rhel-4as-i386 rhel-4es-i386 rhel-4ws-i38

4b (Optional) Click *Add Filter* again to add an additional row of criteria and repeat Step 4a and Step 4b, as many times as necessary.

Be aware that the rows in the filter are separated by And. If you specify multiple rows in the filter, the criteria in all rows must be met for the rule to apply.

5 (Optional) In the *Values Applied to Imported Machines* section, make the desired changes:

Name given to imported machines: Select one or more machine variables to provide a naming scheme for registering devices.

Avoid spaces in your naming scheme; these spaces must be escaped when using the command line utilities. For example, use ${HostName}-${OS} rather than ${HostName} ${OS}.

Folder where imported machines should be placed: Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

Group membership: Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the /Devices/Workstations folder, you can only choose workstation groups. To remove a group, select the box next to the group's name, then click *Remove*.

6 Click *Apply*.

12.2.3 Renaming or Copying Registration Rules

1 In the ZENworks Control Center, click the *Configuration* tab.

2 In the *Default Registration Rules* section, click *Advanced*.

3 Select a registration rule by selecting the box next to its name, click *Edit*, then click an option:

  ◆ **Rename:** Click *Rename*, type a new name for the registration rule, then click *OK*.

◆ **Copy:** Click *Copy*, type a new name for the registration rule, then click *OK*.

The copy option is useful to create a new registration rule that is similar to an existing rule. You can copy a key and then edit the new rule's settings.

If more than one check box is selected, the *Rename* and *Copy* options are not available from the *Edit* menu.

12.2.4 Reordering Registration Rules

Rules are applied from the top down, and only the first matching rule is applied to a registering device. You should order the more restrictive rules first, then the more general rules, followed by the two default server and workstation rules (which always remain the last two rules).

To move a rule up or down in the list:

1 Select the rule by selecting the check box next to the rule.

2 Click *Move Up* or *Move Down*.

12.2.5 Deleting Registration Rules

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Select the registration rule by selecting the check box next to the rule, then click *Delete*.

12.3 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, registration keys, registration rules, and more.

To create a folder:

1 In the ZENworks Control Center, click the *Configuration* tab.

2 Click *New*, then click *Folder* to display the New Folder dialog box.

3 Fill in the fields:

- **Name:** Provide a unique name for your folder. This is a required field.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.

- **Description:** Provide a short description of the folder's contents.

4 Click *OK*.

Unregistering and Reregistering Devices

<div align="right">

13

</div>

Under certain circumstances, it might be necessary to unregister devices from or reregister devices against the ZENworks® Server.

The following sections contain additional information:

13.1 Possible Scenarios for Unregistering and Reregistering Devices

The following list illustrates possible scenarios in which you might want to unregister and reregister devices:

- You have secondary ZENworks Servers set up by job function (engineering, marketing, and so forth), an employee transfers to another job function, and you want to change the ZENworks Server that the device is registered against.

- You move a device from one physical location to another and you want to change the device's ZENworks Management Zone or the ZENworks Server that the device is registered against.

- You want to balance server load by changing the ZENworks Server that a device is registered against.

  In these three scenarios, you could unregister the device and then reregister it in another ZENworks Management Zone or against another ZENworks Server. It is not necessary to remove the device object from the ZENworks Control Center because the updated Management Zone or ZENworks Server information is updated in the object's properties.

- You edit a registration key or registration rule to change the naming convention and folder containment settings as explained in Section 12.1.2, "Editing Existing Registration Keys," on page 111 and Section 12.2.2, "Editing Existing Registration Rules," on page 117 and you want all managed devices named and placed in folders according to the new settings.

  In this scenario, only newly registered devices use the new settings. You can unregister devices, remove them from the ZENworks Control Center (click the *Devices* tab, navigate to and select devices by selecting the check box next to the their names, then click *Delete*), and then reregister them to ensure that the devices are renamed and placed in the proper folders according to the edited settings.

- You no longer want to manage a device using ZENworks Linux Management.

  When you unregister a device, the device is no longer registered against a ZENworks Server and the device is no longer managed.

IMPORTANT: If you delete a device object in the ZENworks Control Center but do not unregister the device, when the device is refreshed according to its schedule or if the user runs the `rug refresh` command, the device reregisters and a corresponding device object is re-created in the ZENworks Control Center. If you no longer want to manage the device using ZENworks Linux Management, ensure that you unregister the device, as explained below.

When you unregister a device, the ZENworks Agent software remains on the device. You can leave the ZENworks Agent on the device in case you want to reregister it, or you can uninstall the ZENworks Agent. For more information, see Section 6.4, "Uninstalling the ZENworks Agent," on page 66.

13.2 Unregistering Devices

To unregister a device, run the `rug sd` command from the device.

For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop 10 (SLED10) managed devices:

```
/usr/bin/rug sd service_number
```

For other managed devices:

```
/opt/novell/zenworks/bin/rug sd service_number
```

You can obtain the *service_number* by using the `rug sl` command. For more information on how to use the `rug` command, see rug (1) (page 586).

You can also unregister a device by using the Software Installer or Updater. For more information, see Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54.

13.3 Reregistering Devices

To reregister a device, run the `rug sa` command from the device.

For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop 10 (SLED10) managed devices:

```
/usr/bin/rug sa https://ZEN_Server_address
```

For other managed devices:

```
/opt/novell/zenworks/bin/rug sa https://ZEN_Server_address
```

Replace *ZEN_Server_address* with the IP address or DNS name of the Primary or Secondary Server.

Policy Management

IV

The following sections provide information about Novell® ZENworks® Linux Management Policy Management features and procedures:

- Chapter 14, "Policy Management Overview," on page 125
- Chapter 15, "Understanding Policies," on page 127
- Chapter 16, "Creating Policies," on page 133
- Chapter 17, "Managing Policies," on page 183

Policy Management Overview

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device according to the defined schedule.

The following sections contain additional information:

- Section 14.1, "Understanding Policies," on page 125
- Section 14.2, "Creating Policies," on page 125
- Section 14.3, "Managing Policies," on page 126

14.1 Understanding Policies

Before you start creating policies, you should have a basic understanding of policies, know the basic terminology, and know the different types of policies available in ZENworks Linux Management. For more information, see Chapter 15, "Understanding Policies," on page 127.

14.2 Creating Policies

ZENworks Linux Management Policies give you the ability to define and lock down configuration settings on managed devices (servers and workstations). ZENworks Linux Management provides policies for a number of popular applications, including the Novell Linux Desktop. It also includes a policy to execute script, binary, or Java files and a policy to apply changes to text files.

ZENworks Linux Management lets you create the following policies:

Table 14-1   *ZENworks Linux Management Policies*

Policy	Description
Epiphany Policy	Configures the Epiphany Web browser. For step-by-step instructions to create this policy, see Section 16.1, "Epiphany Policy," on page 133.
Evolution Policy	Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see Section 16.2, "Evolution Policy," on page 139.
Firefox Policy	Configures the Firefox* Web browser. For step-by-step instructions to create this policy, see Section 16.3, "Firefox Policy," on page 145.
Generic GNOME Policy	Configures the GNOME-based applications. For step-by-step instructions to create this policy, see Section 16.4, "Generic GNOME Policy," on page 151.
Novell Linux Desktop Policy	Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see Section 16.5, "Novell Linux Desktop Policy," on page 156.

Policy	Description
Remote Execute Policy	Executes a script, binary, or Java* file. For step-by-step instructions to create this policy, see Section 16.6, "Remote Execute Policy," on page 164.
SUSE Linux Enterprise Desktop Policy	Configures the SUSE Linux Enterprise Desktop settings. For step-by-step instruction to create this policy, see Section 16.7, "SUSE Linux Enterprise Desktop Policy," on page 169.
Text File Policy	Applies changes to a text file. For step-by-step instructions to create this policy, see Section 16.8, "Text File Policy," on page 176.

NOTE: The Epiphany, Evolution, Firefox, Generic GNOME, Novell Linux Desktop, and SUSE Linux Enterprise Desktop policies are referred as GConf-based policies.

14.3 Managing Policies

In addition to creating policies, as described in Chapter 16, "Creating Policies," on page 133, you can create folders to organize policies, create policy groups to ease administration of policies, assign policies to devices, edit existing policies, and more.

For more information, see Chapter 17, "Managing Policies," on page 183.

Understanding Policies

15

Novell® ZENworks® Linux Management policies provide a mechanism of uniformly configuring applications. ZENworks policies let you configure system and application settings and then set them as Lockdown or Default. Lockdown lets you restrict users from changing settings, so the application must use the values that are configured in the policy. Default lets users change settings.

A policy applies to all users on assigned devices. You can use the Lockdown and Default mechanisms to configure applications in such a way that critical and important settings are locked and an appropriate default value is provided for other settings that might be relevant. Also, if you do not want to enforce a particular setting, you can exclude that setting while creating or editing a policy.

You can also use policies to modify configuration files and execute scripts or programs on managed devices.

Policies can be used to create a set of configurations that you can deploy on any number of managed devices, thereby providing the devices with a uniform configuration and eliminating the need to configure each device separately. You can also create policies with different settings and assign them appropriately to give a different configuration to a specific set of devices.

On managed devices, each policy type is enforced by a Policy Handler/Enforcer, which makes all the configuration changes necessary to enforce and unenforce the settings in a given policy. The Policy Handler/Enforcer executes with root privileges.

The following sections provide basic concepts you should understand as you begin using policies:

- Section 15.1, "Types of Policies," on page 127
- Section 15.2, "Assignments," on page 128
- Section 15.3, "Schedules," on page 128
- Section 15.4, "Groups," on page 129
- Section 15.5, "System Requirements," on page 130
- Section 15.6, "Effective Policies," on page 130

15.1 Types of Policies

ZENworks lets you create the following types of policies:

- **Epiphany policy:** Lets you disable certain Epiphany Web browser settings, such as automatic downloading and opening of files, loading contents from unsafe protocols, and accessing the browser's History. The Epiphany policy also lets you configure a default home page, configure cookie settings, and more. For step-by-step instructions to create this policy, see Section 16.1, "Epiphany Policy," on page 133.

- **Evolution policy:** Lets you disable certain Evolution™ e-mail client settings, such as signatures, showing only subscribed folders, and overriding the server-supplied folder namespace. The Evolution policy also lets you configure image settings, junk e-mail settings, Mime types settings, and more. For step-by-step instructions to create this policy, see Section 16.2, "Evolution Policy," on page 139.

- **Firefox policy:** Lets you disable certain Firefox Web browser settings, such as saving passwords and updating themes and extensions. The Firefox policy lets you configure pop-ups, JavaScript* control, and more. For step-by-step instructions to create this policy, see Section 16.3, "Firefox Policy," on page 145.

- **Generic GNOME policy:** Lets you configure GConf-based applications. You can import settings from a device that is registered with the ZENworks Linux Management Server or you can define your own GConf settings. While importing settings from a device, the system imports all settings, including default settings, from that device. You must specify the name of a user on the device from where you are importing the GConf settings. Only those GConf settings are imported that are related to the user you have specified. For step-by-step instructions to create this policy, see Section 16.4, "Generic GNOME Policy," on page 151.

- **Novell Linux Desktop policy:** Lets you configure the Novell Linux Desktop settings. This policy lets you remove certain items from the system menu, program menu, and personal settings. It also lets you configure background image settings, shade settings, proxy settings, and more. For step-by-step instructions to create this policy, see Section 16.5, "Novell Linux Desktop Policy," on page 156.

- **Remote Execute policy:** Executes a script, binary, or Java file. The Remote Execute policy also lets you specify your own script to be executed on managed devices. For step-by-step instructions to create this policy, see Section 16.6, "Remote Execute Policy," on page 164.

- **SUSE Linux Enterprise Desktop policy:** Lets you configure the SUSE Linux Enterprise Desktop settings. This policy lets you remove certain items from the system menu, program menu, and personal settings. It also lets you configure background image settings, shade settings, proxy settings, and more. For step-by-step instructions to create this policy, see Section 16.7, "SUSE Linux Enterprise Desktop Policy," on page 169.

- **Text File policy:** Applies changes to a text file. The Text File policy lets you append or prepend to a file and also lets you apply a search-based change in which a given string in the file can be replaced with another string, be deleted, and so forth. The search string can be specified using a regular expression.

  This policy also allows you to execute a script, binary, or Java program before and after the text-file modification. It can be used for example, to change a configuration file. You might want to stop a service before the file is modified and restart the service after the file modification.

  While creating a policy, only one file and one change can be specified. Editing a policy allows you to add multiple files and specify more than one change to a file. For step-by-step instructions to create this policy, see Section 16.8, "Text File Policy," on page 176.

15.2 Assignments

You can assign a policy directly to a device, or you can assign it to a folder or group in which the device is a member. As a general rule, you should try to assign policies to device groups rather than device folders.

15.3 Schedules

When assigning a policy to a device, you can specify the schedule for applying the policy. Depending on the type of policy being applied, the following schedules are available. Click the link in the left frame for details about each policy and its options, which vary, depending on the schedule. Keep in mind that there are two different refresh schedules: the one you set with the individual

policy and the System Global Refresh Schedule you set under the *Configuration* tab. Otherwise, you might get unexpected results. For example, if you set a policy to refresh every day and don't change the System Global Refresh Schedule, the policy will refresh every two hours by default.

Table 15-1   *Available Schedules*

Schedule Type	Description	Applicable For
Date Specific	Select one or more dates on which to enforce the policy on devices and set other restrictions that might apply. If you schedule an event in the past, the scheduled event will occur when the assigned device refreshes.	Remote Execute and Text File policies
Day of the Week Specific	Select one or more days of the week on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Event	The User Login event triggers the enforcement of the policy.	Epiphany, Evolution, Firefox, Generic GNOME, Novell Linux Desktop, and SUSE Linux Enterprise Desktop policies.
Monthly	Select the day of the month on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Relative to Refresh	Schedule when the policy is enforced, either immediately after the device refreshes or a specified amount of time after the device refreshes. The event runs on the first device refresh only and will not run on subsequent refreshes. You can also specify whether the policy's enforcement is repeated and specify a time period when you do not want the policy enforced to help minimize network traffic during that time. For more information, see Section 17.9, "Refreshing Policies," on page 202.	Remote Execute and Text File policies

15.4 Groups

A policy group is a collection of one or more policies. You can create policy groups and assign them to devices the same way you would assign individual policies.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

15.5 System Requirements

System requirements specify the conditions that must be satisfied on the managed device for the policy to be effective. System requirements are specified for each policy to ensure that the conditions necessary for a proper enforcement of a policy are met.

The appropriate default system requirements are included in a policy when it is created. When you create or edit a policy, you can modify or remove the requirements. No default system requirement is available for the Text File and Remote Execute policies.

You can change the system requirement setting if the settings included in the policy are available on different versions or platforms. If not, all the settings configured in the policy are not effective. For example, if the Distribution >= Novell Linux Desktop 9 requirement is removed from the Firefox policy and the policy is specified to be enforced on all platforms, the settings are not effective because the lockdown option for Firefox is available only for the Novell Linux Desktop.

You should remove the system requirement only if you are sure that it will not cause problems. For example, in a Generic GNOME policy created by importing settings from a device, the system requirement is set to the operating system of the device from which the settings were imported. If you have included settings in the policy that are available on other platforms, you can remove or change the system requirement.

IMPORTANT: Even if the requirements are removed and the application version or operating system is incompatible, the policy is enforced but a warning message is generated. If the appropriate application (Epiphany, Evolution, or Firefox) is not installed, the policy is not enforced and an error message is generated.

15.6 Effective Policies

A device inherits its policy assignments from its parent folders, its group memberships, and itself; when conflicting assignments occur, the assignments on the device override group assignments, which override folder assignments.

You can tell which policies are in effect for a device by viewing the Effective Policies section on the Device Summary page. To view the effective policies, click the *Devices* tab, navigate the folders to find the device, click the device, then click the *Summary* tab.

All the effective policies are listed under the *Effective Policies* section on the Device Summary page. The following table provides a description of each icon that indicates the effectiveness of a policy:

Table 15-2 *Policy Status Icons*

Icon	Description
	The policy is effective and will be enforced on the device.
	The policy might be effective. The policy will be enforced if the system requirements are met. Otherwise, the policy will not be enforced.
	The policy is not effective and will not be enforced.

For the Text File and Remote Execute policies, all policies whose system requirements are met are applied on the device. For all other policies, the first policy amongst the effective policies, whose system requirements are met, is applied on the device

Creating Policies

16

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device as per the defined schedule.

The following sections contain additional information about the available ZENworks Linux Management policies:

16.1 Epiphany Policy

The Epiphany policy is used to configure the Epiphany Web browser.

To configure the Epiphany policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy type* list, click *Epiphany Policy*, then click *Next* to display the Policy Name page.

```
Create New Epiphany Policy                                    ?
  Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *
[                                  ]

Folder: *
[/Policies                        ]  🔍

Description:
[                                  ]
[                                  ]
[                                  ]
[                                  ]
[                                  ]
[                                  ]

Fields marked with a blue asterisk are required.

         << Back      Next >>      Cancel
```

4 Fill in the fields:

- ◆ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- ◆ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- ◆ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Epiphany Lockdown Settings page.
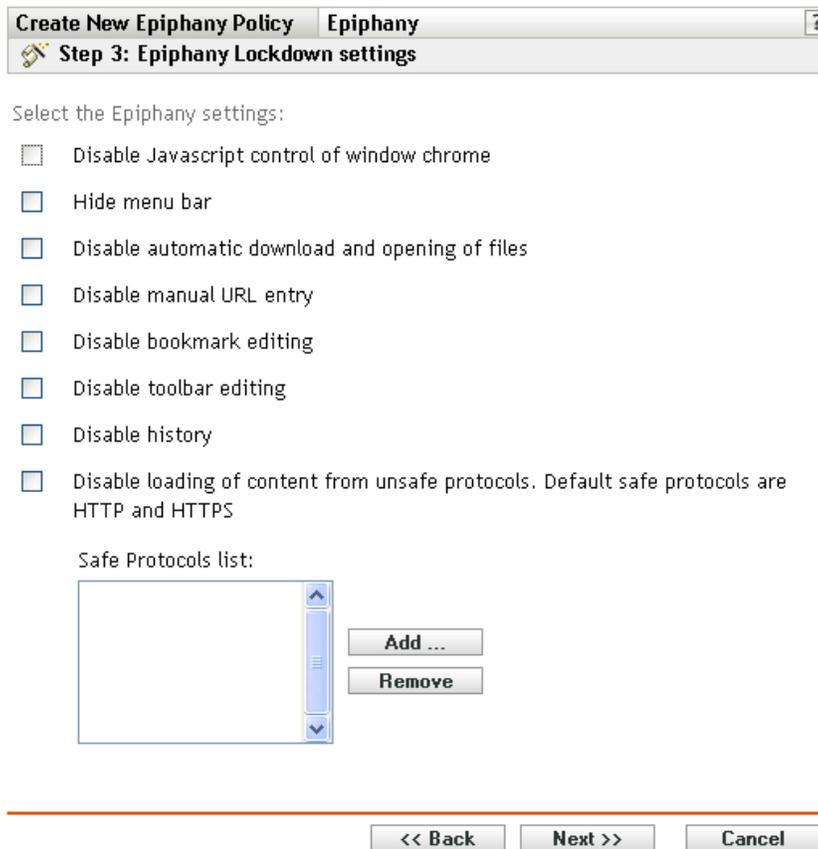
6 Select the desired options (by default, all options are disabled):

Disable JavaScript control of window chrome: Select this option to disable the JavaScript control and modification of the Epiphany Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

Hide menu bar: Select this option to hide the menu bar of the Epiphany Web browser.

Disable automatic download and opening of files: Select this option to prevent users from downloading and opening files automatically.

If you include this setting in the policy, users are always asked if they want to save a file or open it. For example, if users want to download a file, they are prompted to specify the location to save or open the file. If the user clicks *Open*, the file is downloaded and opened with the corresponding application.

Disable manual URL entry: Select this option to prevent users from manually entering URLs in the address bar.

Disable bookmark editing: Select this option to prevent users from editing a bookmark.

Disable toolbar editing: Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

Disable history: Select this option to prevent users from accessing the history, which contains links to pages recently visited.

Disable loading of contents from unsafe protocols. Default safe protocols are HTTP and HTTPS: Select this option to prevent the downloading of data that is transmitted using an unsafe protocol. Unsafe protocols do not encrypt the data sent across a network.

After you check this option, the following buttons are available:

- ◆ **Add:** To add a protocol to the *Safe protocol* list, click *Add*, specify a protocol name, then click *OK*.
- ◆ **Remove:** To remove a protocol from the *Safe protocol* list, select the protocol, then click *Remove*.

7 Click *Next* to display the Epiphany Configuration Settings page.

```
Create New Epiphany Policy    Epiphany                              [?]
 ⚙ Step 4: Epiphany Configuration settings

Select any Epiphany configuration settings you would like to provide.
For each setting you select, provide a value, and optionally, enable the lock to
prevent the value from changing after it is set.

   ☐    Homepage URL              🔒  [                          ]
   ☐    Download folder *         🔒  [                          ]
   ☐    Allow Popups              🔒  [Yes ▾]
   ☐    Allow Java                🔒  [Yes ▾]
   ☐    Allow Javascript          🔒  [Yes ▾]
   ☐    Cookies                   🔒  [Always Accept         ▾]
   ☐    Disk space for temporary files  🔒  [50     ] MB

Fields marked with a blue asterisk are required.
_____

            [ << Back ]   [ Next >> ]   [ Cancel ]
```

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking 🔒. The options that are not enabled are excluded from the policy and are not applied to the device.

Homepage URL: Specify the URL to automatically display when users launch the Epiphany Web browser.

Download folder: Specify the directory where you want users to download data. If the folder you specify does not exist, it is created relative to all users' home directories. If you specify an absolute path, ensure that it is at a location where all users have Read and Write access to files.

Allow popups: Select this option to allow or disallow pop-ups to be displayed in the Epiphany Web browser.

Allow Java: Select this option to allow or disallow Java applications to run on the Epiphany Web browser.

Allow JavaScript: Select this option to allow or disallow JavaScript applications to run on the Epiphany Web browser.

Cookies: Select this option to configure how the Epiphany Web browser handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser, in turn, stores this information in a file. The available options are *Always accept*, *Only from the sites you visit*, and *Never accept*.

Disk space for temporary files: Specify the amount of disk space to allow for storing temporary files for the browser.

9 Click *Next* to display the Default System Requirements for Epiphany Policy page.

Create New Epiphany Policy	Epiphany	?

🖈 **Step 5: Default system requirements for Epiphany policy**

The following condition is added as a default system requirement to this policy.

If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☑ Apply policy on devices with version of Epiphany >= `1.2.5`   *

Fields marked with a blue asterisk are required.

```
      << Back      Next >>      Cancel
```

10 Specify the minimum system requirements that must be satisfied for the Epiphany Web browser policy settings to be effective.

The *Apply policy on devices with version of Epiphany* field displays the minimum version of the Epiphany Web browser required for all policy settings to be effective. Epiphany 1.2.5 is the minimum required version. Policy settings are applied only if the user has the same or later version of the Epiphany Web browser installed. If the user does not have the Epiphany Web browser installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Epiphany Web browser is installed on a managed device or not. If the system finds that the Epiphany Web browser is installed on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Epiphany Web browser is not installed on a managed device, the policy is not enforced and an error message is generated.

11 Click *Next* to display the Summary page.

12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Epiphany policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

 ◆ Specify assignments for this policy

 ◆ Specify the schedule for this policy

 ◆ Specify groups for this policy

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

13b You can also select Folder or Group objects.

13c Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13d Click *OK*.

14 Click *Next* to display the Policy Schedule page.

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

16 Click *Next* to display the Policy Groups page.

```
┌─────────────────────────────────────────────────────────────────────────┐
│ Create New Epiphany Policy │ Epiphany                           │ [?] │
│ ⚙ Step 9: Policy Groups                                                  │
└─────────────────────────────────────────────────────────────────────────┘

Specify the groups for this policy:

┌─────────────────────────────────────────────────────────────────────────┐
│ Add  Remove                                                              │
├─────────────────────────────────────────────────────────────────────────┤
│ ☐  Name                          In Folder                               │
├─────────────────────────────────────────────────────────────────────────┤
│ No items selected, click add to select items                             │
└─────────────────────────────────────────────────────────────────────────┘

              [ << Back ]   [ Next >> ]      [ Cancel ]
```

17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

18 Click *Next* to display the Finish page.

19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.2 Evolution Policy

The Evolution policy is used to configure the Evolution™ e-mail client.

To configure the Evolution policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *Evolution Policy*, then click *Next* to display the Policy Name page.

Create New Evolution Policy　ww　[?]

✦ **Step 2: Policy Name**

Specify the name of the new policy:

Policy Name: *

[   ]

Folder: *

[/Policies   ] 🔍

Description:

[   ]

Fields marked with a blue asterisk are required.

[<< Back]　[Next >>]　[Cancel]

4 Fill in the fields:

- ✦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- ✦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- ✦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Evolution Lockdown Settings page.
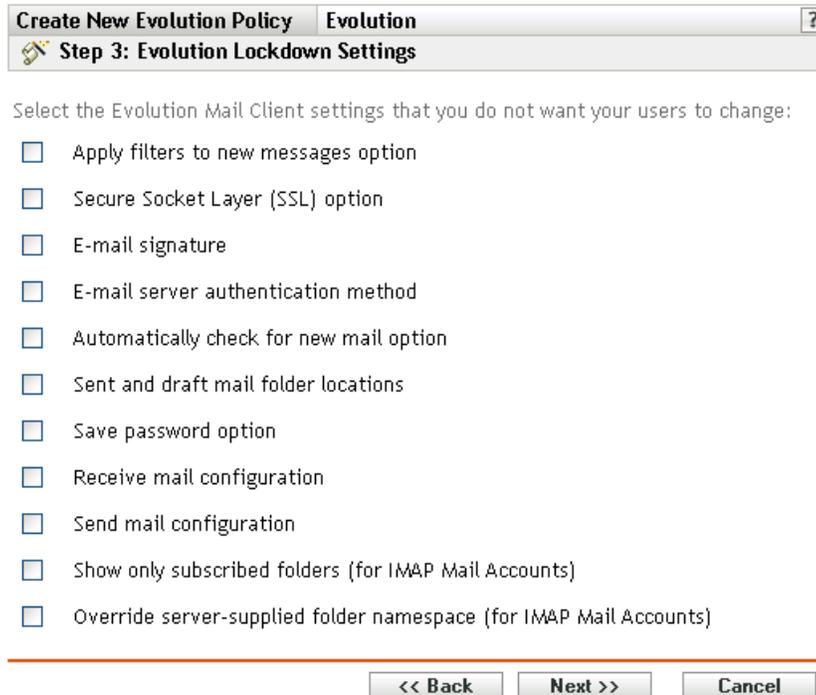
6 Select the desired options (by default, all options are disabled):

The options on this page allow you to prevent users from changing the following Evolution e-mail client settings. Select an option to prevent users from changing that setting in the Evolution e-mail client.

Apply filter to new messages option: Applies the filter to all new messages users receive.

Secure Socket Layer (SSL) option: Specifies whether the Evolution e-mail client should connect to the server using SSL.

SSL is a protocol that provides encrypted communications on the network and enables secure communications between the Evolution client and the server.

E-Mail signature: Specifies whether an e-mail signature should be added to the contents of a message.

E-mail server authentication method: Specifies the kind of authentication to be used when users connect to the mail server.

Automatically check for new mail option: Specifies whether the Evolution client should automatically check for new mail.

Sent and draft mail folder locations: Specifies the folders that users can select to store draft and sent mail.

Save password option: Specifies whether passwords should be saved so that users are not prompted for a password at every login.

Receive mail configuration: Configures the various options for receiving mail. For example, e-mail server and authentication details, checking for new mail, and applying filters.

Send mail configuration: Configures the various options for sending mail, for example, server and authentication details.

Show only subscribed folders (for IMAP mail accounts): Specifies that only the subscribed IMAP folders be shown to users. Internet Message Access Protocol (IMAP) lets users access e-mail messages that are stored on the mail server. Because the mail folders exist on the IMAP server and accessing them is time-consuming, Evolution lets users subscribe to certain IMAP folders.

Override server-supplied folder namespace (for IMAP mail accounts): Lets users change the IMAP name space that contains mail messages for the server.

NOTE: Users cannot create a new Evolution e-mail account if Receive Mail Configuration and Send Mail Configuration settings are included in the policy. These settings should be included in the policy only if the users' e-mail accounts have been created in the Evolution e-mail client.

---

7 Click *Next* to display the Evolution Configuration Settings page.

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking 🔒. The options that are not enabled are excluded from the policy and are not applied to the device.

Default character encoding for display: Lets you choose a character interpretation set for displaying e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

Default character encoding for composed mail: Lets you choose a character interpretation set for composing e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

Empty trash folders on exit: Lets you specify when to empty the Trash folder. The available options are *Never*, *Every time*, *Once per day*, *Once per week*, and *Once per month*.

Check inbox for junk mail: Lets you specify if the incoming mail must be checked for junk mail.

Include remote junk mail tests: Lets you specify if the remote junk filtering option should be used for filtering incoming mail.

For example, the Evolution client stores a message in the Junk Mail folder if it finds the mail address a blacklisted address.

Loading Images: Lets you decide how images embedded in e-mail messages are loaded in the Evolution client.

The following options are available:

- **Never load images off the Internet:** If you select this option, the Evolution e-mail client never loads images. If you select this option users can still view the images in the message by selecting the appropriate menu options in the Evolution e-mail client.

- **Load images if sender is in address book:** If you select this option, images are loaded only if the sender of the e-mail message is in the receiver's address book.

- **Always load images off the Internet:** If you select this option, images are loaded regardless of their source.

Mime types available for viewing attachments: Lets you select the MIME types that Evolution allows to be viewed using available Bonobo controls.

Evolution provides built-in support for opening certain MIME types. Those MIME types that are not supported by Evolution can be viewed by using certain available Bonobo controls. Bonobo controls provide a means to view both the MIME types that are supported and those that are not supported by Evolution.

After you select this option, you can select items from the *Mime types available* list and then use the arrow button to move the selected item to the *Mime types selected* list.

9 Click *Next* to display the Default System Requirements for Evolution Policy page.

10 Specify the minimum system requirements that must be satisfied for the Evolution policy settings to be effective.

The *Apply policy on devices with version of Evolution* field displays the minimum version of the Evolution client required for all policy settings to be effective. Evolution 2.0.1 is the minimum required version. Policy settings are applied only if the user has the same or a later version of the Evolution e-mail client installed. If the user does not have the Evolution e-mail client installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Evolution client is installed on a managed device or not. If the system finds the Evolution client on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Evolution client is not installed on a managed device, the policy is not enforced and an error message is generated.

11 Click *Next* to display the Summary page.

12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Evolution policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ◆ Specify assignments for this policy
- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy

Create New Evolution Policy	Evolution	?
Step 7: Policy Assignments		

Specify the assignments for this policy:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

〈〈 Back   Next 〉〉   Cancel

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

13b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

16 Click *Next* to display the Policy Groups page.

17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

18 Click *Next* to display the Finish page.

19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.3 Firefox Policy

The Firefox policy is used to configure the Mozilla* Firefox Web browser.

The Firefox policy is supported only if the lockdown version of Firefox is available on the Novell Linux Desktop, SLED 10, and SLED 11 devices. The Firefox policy is additionally supported on SLES 10 and SLES 11 devices if you apply ZENworks 7.3 Linux Management Hot Patch 1.

To configure the Firefox policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the Policy Type list, click *Firefox Policy*, then click *Next* to display the Policy Name page.

4 Fill in the fields:

◆ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

◆ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

◆ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Firefox Lockdown Settings page.
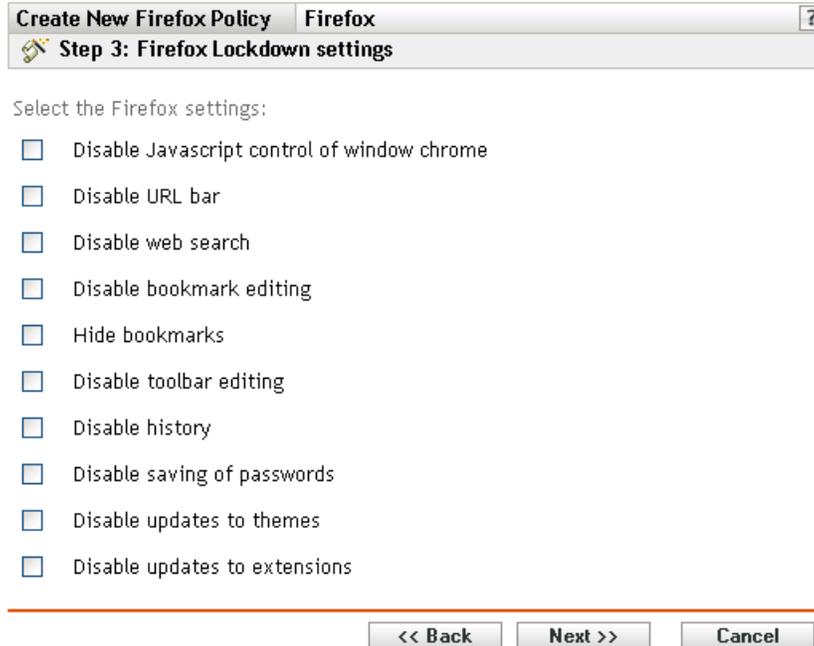
```
Create New Firefox Policy    Firefox                              [?]
⚙ Step 3: Firefox Lockdown settings

Select the Firefox settings:
  ☐  Disable Javascript control of window chrome
  ☐  Disable URL bar
  ☐  Disable web search
  ☐  Disable bookmark editing
  ☐  Hide bookmarks
  ☐  Disable toolbar editing
  ☐  Disable history
  ☐  Disable saving of passwords
  ☐  Disable updates to themes
  ☐  Disable updates to extensions

           [ << Back ]   [ Next >> ]      [ Cancel ]
```

6 Select the desired options (by default, all options are disabled):

Disable Javascript control of window chrome: Select this option to disable the JavaScript control and modification of the Firefox Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

Disable URL bar: Select this option to prevent users from manually entering URLs in the address bar.

Disable web search: Select this option to prevent users from using the Web search bar to search the Web pages. If you select this option, the search bar and *Add Engine* option are disabled.

Disable bookmark editing: Select this option to prevent users from editing a bookmark.

Hide bookmarks: Select this option to hide bookmarks, including all the bookmarks listed in the *Bookmark* menu and bookmarks toolbar. Make sure that you select *Disable Bookmark Editing* if you select the *Hide Bookmarks* option.

Disable toolbar editing: Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

Disable history: Select this option to prevent users from accessing the History, which contains links to pages recently visited.

Disable saving of password: Select this option to prevent Firefox from saving users' passwords. Whenever a user enters a password in Firefox, it prompts the user and asks if the password should be saved. If the user clicks Yes, Firefox saves the password and fills it in automatically whenever the user visits that page again.

Disable updates to themes: Select this option to prevent users from updating a theme file.

The theme file contains the Control, Window Border, and Icons elements, which determine the appearance of user's browser. Themes are skins for Firefox, and they allow you to change the look and feel of the browser and personalize it to your taste. A theme can simply change the colors of Firefox or it can change the entire browser appearance.

Disable updates to extensions: Select this option to prevent users from updating the extensions to add a new functionality to Firefox.

Extensions are add-ons that add new functionality to Firefox. They can add anything from a toolbar button to a completely new feature. Extensions customize the browser to fit the personal needs of each user. For example, an extension can be used to add an IRC client to Firefox or to automatically copy highlighted content to the clipboard.

7 Click *Next* to display the Firefox Configuration Settings page.

Create New Firefox Policy	Firefox	?

Step 4: Firefox Configuration settings

Select any Firefox configuration settings you would like to provide.

For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

- ☐ Homepage URL 🔒 [   ]
- ☐ Allow Popups 🔒 Yes ▾
- ☐ Allow Java 🔒 Yes ▾
- ☐ Allow Javascript 🔒 Yes ▾
- ☐ Allow sites to set cookies 🔒 Yes ▾
  - Keep Cookies   Until they expire ▾
- ☐ Allow loading of images 🔒 Anywhere ▾
- ☐ Disk space for temporary files 🔒 50 MB
- ☐ Download Folder 🔒
  - ◉ Ask the user where to save every file
  - ○ Save all files to this folder   Desktop ▾
  - Folder path [   ] *

Fields marked with a blue asterisk are required.

[<< Back] [Next >>] [Cancel]

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking 🔒. The options that are not enabled are excluded from the policy and are not applied to the device.

Homepage URL: Specify the URL to automatically display when users launch the Firefox Web browser.

Allow popups: Select this option to allow or disallow pop-ups to be displayed in the Firefox Web browser.

Allow Java: Select this option to allow or disallow Java applications to run on the Firefox Web browser.

Allow JavaScript: Select this option to allow or disallow JavaScript applications to run on the Firefox Web browser.

Allow sites to set cookies: Select this option to configure how Firefox handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser stores this information in a file.

You can select a value in the Keep Cookies drop-down list to specify if a Web server should be allowed to set cookies.

If you select Yes, specify how long to store the cookies:

- **Until they expire:** Firefox retains a cookie until it expires.
- **Ask me every time:** Firefox asks the user about the action to be taken with each cookie. Users can select *Allow*, *Allow for this session only*, or *Deny*.
- **Until I close Firefox:** Firefox retains cookies while the browser is open. When the browser is closed, Firefox removes all cookies.

Allow loading of images: Lets you specify the source from where images are loaded.

The following options are available:

- **Anywhere:** If you select this option, images are loaded regardless of their source.
- **From originating website only:** If you select this option, images are loaded only if the source of the images is the current site.
- **Never:** If you select this option, Firefox never loads images.

Disk space for temporary files: Specify the disk space allowed to store temporary files for the browser.

Download folder: Lets you specify the directory where you want users to save downloaded files.

The following options are available:

- **Ask the user where to save every file:** If you select this option, Firefox asks the users where to save files every time files are downloaded.
- **Save all files to this folder:** If you select this option, specify a location to save files.

  The following options are available:

  - **Desktop:** Select Desktop to save downloaded files on the Desktop.
  - **My Downloads:** Select My Downloads to save downloaded files in the My Downloads folder.
  - **Home:** Select Home to save the downloaded files in a folder in the Home directory.
  - **Other:** Select Other to store the downloaded files in a location of your choice. Specify the complete path, including the directory where the downloaded files should be saved.

9 Click *Next* to display the Summary page.

10 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Firefox policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with .

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ◆ Specify assignments for this policy
- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy

Create New Firefox Policy	Firefox	?

Step 7: Policy Assignments

Specify the assignments for this policy:

Add Remove		
☐ **Name**	**In Folder**	
No items selected, click add to select items		

[<< Back] [Next >>] [Cancel]

11 Assign the policy to the devices.

11a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

11b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

11c Click *OK*.

12 Click *Next* to display the Policy Schedule page.

Create New Firefox Policy	Firefox	?

Step 7: Policy Schedule

Select the schedule to apply to the policy assignments.

Schedule Type:
[Event ▼]

Select the event that this schedule should be triggered on:

☑ User Login

[<< Back] [Next >>] [Cancel]

13 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

14 Click *Next* to display the Policy Groups page.

Create New Firefox Policy	Firefox	?
Step 9: Policy Groups		

Specify the groups for this policy:

Add **Remove**	
☐ **Name**	**In Folder**
No items selected, click add to select items	

<< Back   Next >>   Cancel

15 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

16 Click *Next* to display the Finish page.

17 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.4 Generic GNOME Policy

The Generic GNOME policy is used to configure GConf- based applications on a device.

To configure the GNOME policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *Generic GNOME Policy*, then click *Next* to display the Policy Name page.

4 Fill in the fields:

- ◆ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- ◆ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- ◆ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Source page.

6 Select the desired option, then click *Next*.

Import the settings from a device: Use this option to import the existing GConf settings from any device that is registered with the ZENworks Linux Management Server. The system obtains all settings, including default settings, from that device. You can enforce these settings on a desired managed device or group of devices at a later time.

Before you import settings to your device, make sure the GConf settings are correct on the device you are importing from.

If you choose this option, continue with .

Define a setting on your own: Create a directory and corresponding key settings such as key names, types, and values. At a later time, you can enforce these settings on a managed device or on a group of devices.

Make sure that you specify the correct key names and types.

If you choose this option, continue with .

7 (Conditional) If you chose the *Import the settings from a device* option in , choose the device from which you want to import the GConf settings.

7a Select one of the following options:

Selected machine: Browse to and select a device from which you want to import GConf settings, then click *OK*.

Only managed devices that are registered with the ZENworks Linux Management Server are displayed.

DNS name / IP address: Specify the DNS name or IP address of a managed device from which you are importing GConf settings. Ensure that the device is registered with the ZENworks Linux Management Server.

7b Specify the username of the managed device from which you are importing the GConf settings.

Only those GConf settings are imported that are related to the specified user. Ensure that the specified user has a valid account on the managed device from which you are importing the settings.

7c Click *Next* to import the top-level directories. The four top-level directories that are imported are Apps, Desktop, System, and GNOME.

7d Select one or more directory whose settings you want to import, then click *Next*.

7e (Optional) Add or delete the keys and their respective values from the imported GConf settings, then click *Next* and skip to .

For detailed information about defining your own GConf settings, click the [?] button on the Built Gconf Tree page.

8 (Conditional) If you chose the *Define a setting on your own* in , define your own Gconf settings by adding and deleting keys on the Gconf Tree, then click *Next*.

For detailed information about defining your own Gconf settings, click the [?] button on the Built Gconf Tree page.

9 Click *Next* to display the default system requirements for Generic GNOME Policy page.
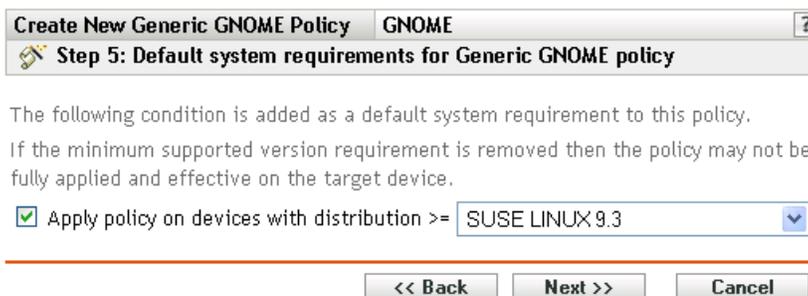
10 Specify the minimum system requirements for Generic GNOME policy settings to be effective.

The value you specify in the *Apply policy on devices with distribution* field indicates the distribution and minimum version that is required for the policy settings to be effective. The policy is applied if the device has the same version or a later version of the distribution.

If you chose the *Import from a device* option in , the default value is the operating system of a device from which you have imported GConf settings. If you have not included this setting in the policy, and if the operating system of a managed device (where the

policy is to be applied) is different than the operating system of the device from which the settings have been imported, a warning message is generated. However, the policy settings are enforced.

If you chose the *Define a setting on your own* option in Step 6 on page 153, and you want to include the default system requirement in the policy, you must specify the distribution and version of the operating system. If you do not include this setting in the policy, the system does not check for minimum operating system requirements and immediately enforces the policy.

Refer to the contents of the `/etc/SuSE-release` or `/etc/redhat-release` file to obtain the correct string for your platform.

11 Click *Next* to display the Summary page.

12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Generic GNOME policy is created but it does not have devices assigned or a schedule. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ◆ Specify assignments for this policy
- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy

Create New Generic GNOME Policy	GNOME	?
🔧 **Step 7: Policy Assignments**		

Specify the assignments for this policy:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

         << Back   Next >>   Cancel

13 Assign the policy to the devices.

 13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

  You can also select Folder or Group objects.

 13b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

  Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

 13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

16 Click *Next* to display the Policy Groups page.

17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

18 Click *Next* to display the Finish page.

19 Review the information on the *Finish* page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.5 Novell Linux Desktop Policy

The Novell Linux Desktop policy is used to configure the GNOME Novell Linux Desktop settings on a device.

To configure the Novell Linux Desktop policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *Novell Linux Desktop Policy*, then click *Next* to display the Policy Name page.

4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Novell Linux Desktop Lockdown Settings page.

Create New Novell Linux Desktop Policy   NLD   `?`

Step 3: Novell Linux Desktop Lockdown Settings

Selecting an item from the list below will disable or remove the associated feature on the users desktop. The user will be unable to access menu items or controls associated with the feature.

☐ Disable panel configuration

☐ Disable launcher creation

☐ Remove computer icon from desktop

☐ Remove trash icon from desktop

☐ Remove user's home icon from desktop

[<< Back]   [Next >>]   [Cancel]

6 Select the desired options (by default, all options are disabled):

Selecting an item from the list disables or removes the associated feature on the user's desktop. The user cannot access menu items or controls associated with the feature.

Disable panel configuration: Lets you prevent users from configuring a panel. If you select this option, users cannot add and remove the icons on the panel.

Disable launcher creation: Lets you prevent users from creating application launchers.

Remove computer icon from desktop: Lets you remove the computer icon from users' desktops.

Remove trash icon from desktop: Lets you remove the trash icon from users' desktops.

Remove user's home icon from desktop: Lets you remove the Home icon from users' desktops.

7 Click *Next* to display the Novell Linux Desktop Menu Lockdown page.

8 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

Remove from System menu: Lets you remove items from the *System* menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' *System* menus.

Remove from Program Menu: Lets you remove items from the *Program* menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' *Program* menus.

9 Click *Next* to display the Novell Linux Desktop Personal Settings and Applets Lockdown page.

10 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

Remove from personal settings: Lets you remove items from the Personal Settings of Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' Personal Settings.

Remove applets: Lets you prevent the applets from being displayed on users' Novell Linux Desktop. Select an applet from the *Applets* list and move it to the box on the right side. Selected applets are not displayed on users' Novell Linux Desktop.

11 Click *Next* to display the Novell Linux Desktop Configuration Settings page.

Create New Novell Linux Desktop Policy | **NLD** | ?

Step 6: Novell Linux Desktop Configuration Settings

Click the checkboxes to select settings which will be enforced on the desktop.

For each setting you select, provide a value, and optionally, lock the setting to prevent the value from changing after it is set.

☐ Background image file name *
(eg. /opt/gnome/share/images/roses.jpeg)

☐ Background position
Centered

☐ Background shade
Solid

☐ Theme file name *
(eg. /opt/gnome/share/themes/metacity/index.theme)

☐ Proxy Settings

○ Direct internet connection

◉ Manual proxy configuration

HTTP Proxy *   Port * 8080   **Authentication**
HTTP Secure Proxy   Port * 0
FTP Proxy   Port * 0
Socks Proxy   Port * 0

○ Automatic proxy configuration

Autoconfiguration URL

Fields marked with a blue asterisk are required.

<< Back   **Next >>**   **Cancel**

12 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking 🔒. The options that are not enabled are excluded from the policy and are not applied to the device.

Background image filename: Lets you specify the filename and complete location of a background image. This image file is displayed as a background on users' desktops. The file should exist on the managed device at the specified location.

Background position: Lets you specify background image display options. *Center* displays an image in the center of the screen, *Fill Screen* stretches the image to cover the entire screen, *Scaled* enlarges the image until the image meets the screen edges, and *Tiled* repeats the image over the screen. Select *No Background* to prevent the image from being displayed on the desktop.

Background shade: Lets you choose an available shade to decorate the background. Select *Solid* to have the background image uniform across the desktop. Select *Vertical* to have the image become darker as you go up, and select *Horizontal* to have the image become darker as you go from left to right.

Theme filename: Lets you specify a theme file name and its complete location. The appearance of the windows, icons, buttons, and other graphical user interface controls are changed according to the selected theme.

Proxy settings: Specify a proxy setting:

- **Direct internet connection:** Lets users connect to the Internet without using the proxy server.

- **Manual proxy configuration:** Lets you manually configure the proxy. Specify the *HTTP Proxy* value, *HTTP Secure Proxy* value, *FTP Proxy* value, *Socks Proxy* value, and corresponding port numbers.

  To authenticate the user before proxy configuration, click Authentication. In the HTTP Proxy Authentication dialog box, select *Use Authentication*, specify the username and password, then click *OK*.

- **Automatic proxy configuration:** Lets you automatically configure the proxy from a certain URL by specifying the URL.

13 Click *Next* to display the Default System Requirements for the Novell Linux Desktop Policy page.
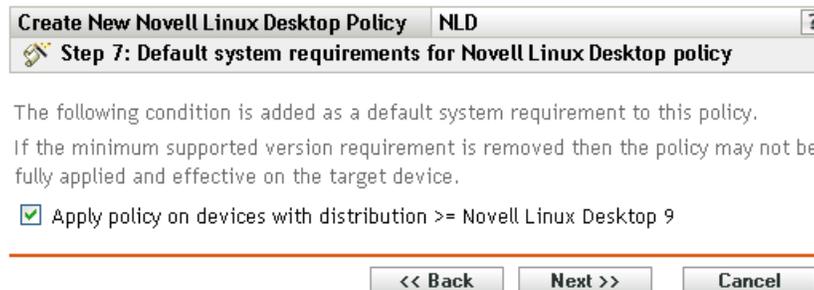
14 Specify the minimum version of Novell Linux Desktop required for all policy settings to be effective. Policy settings are applied only if a device has the same version or a newer version of the Novell Linux Desktop. If a device does not have Novell Linux Desktop 9 or newer, the policy does not apply correctly.

Even if you do not include this setting in the policy, the system checks for Novell Linux Desktop. If it does not find Novell Linux Desktop, an error message is generated and the policy is not applied.

NOTE: To ensure successful enforcement of all configured items, you need Novell Linux Desktop 9 with Support Pack 2 with GNOME.

15 Click *Next* to display the Summary page.

16 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Novell Linux Desktop policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with .

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy

- Specify the schedule for this policy
- Specify groups for this policy

Create New Novell Linux Desktop Policy | NLD | [?]
Step 9: Policy Assignments

Specify the assignments for this policy:

Add **Remove**	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

17 Assign the policy to the devices.

17a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

17b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

17c Click *OK*.

18 Click *Next* to display the Policy Schedule page.

Create New Novell Linux Desktop Policy | NLD | [?]
Step 10: Policy Schedule

Select the schedule to apply to the policy assignments.

Schedule Type:
[Event ▾]

Select the event that this schedule should be triggered on:

☑ User Login

[<< Back] [Next >>] [Cancel]

19 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

20 Click *Next* to display the Policy Groups page.

Create New Novell Linux Desktop Policy	NLD	?
Step 11: Policy Groups		

Specify the groups for this policy:

Add Remove

☐	**Name**	**In Folder**
No items selected, click add to select items		

[<< Back] [Next >>]   [Cancel]
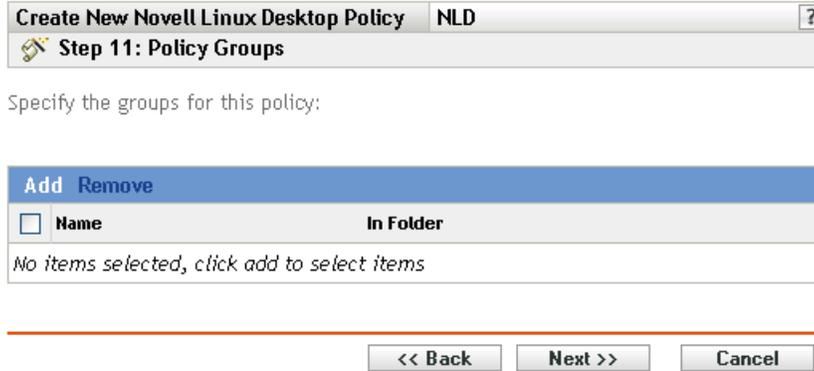
21 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the *Selected* list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

22 Click *Next* to display the Finish page.

23 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.6 Remote Execute Policy

The Remote Execute policy is used to execute any Script, Binary, or Java file.

To configure the Remote Execute policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the Policy Type list, click *Remote Execute Policy*, then click *Next* to display the Policy Name page.

Create New Remote Execute Policy   [?]

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

[   ]

Folder: *

[/Policies   ] 🔍

Description:

[   ]
[   ]
[   ]
[   ]
[   ]
[   ]

Fields marked with a blue asterisk are required.

[<< Back] [Next >>] [Cancel]

4 Fill in the fields:

- ◆ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- ◆ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- ◆ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next*.

6 Select the desired options:

Executable type: Select an executable type to run on a managed device (script, binary, or Java). Depending on the executable type you select, different options are available, as described below.

Maximum waiting time: Indicate the waiting time after starting the script, binary, or Java program. The following table explains the available options:

Option	Description
Do not wait	The Remote Execute enforcer does not wait for the program to be completed.
Wait till the program completes the execution	The Remote Execute enforcer waits for the program to be completed.
Wait for <n> sec	Indicates how many seconds the Remote Execute enforcer should wait after starting the program.

NOTE: The launched program is not terminated by the enforcer if you select the *Do not wait* or *Wait for <n> sec* options.

(Conditional) If you chose *Script* in the *Executable Type* field in Step 6 on page 166, the following options are available:

Script to run: Select an option from the drop-down list:

◆ **Specify a file:** Fill in the fields:

Script filename: Specify the complete absolute path, including the filename, of the script you want to run on a managed device.

Script parameters: Specify any parameters to be passed to the specified script file. If you want to specify Shell operators such as redirection operators in *Script parameter*, then you must select *Script* in the Executable Type field and *Define your own script* in the *Script to run* field.

Script engine: Specify the name and location of the script engine that runs the script. For example, `/usr/bin/perl`.

Script engine parameters: Specify any parameters to be passed to the specified script engine.

◆ **Define your own script:** Type your script in the box.

(Conditional) If you chose *Binary* in the *Executable Type* field in Step 6 on page 166, the following options are available:

Executable file name: Specify the complete absolute path, including the filename, of the binary program you want to run on a managed device.

Executable file parameters: Specify any parameters to be passed to the specified binary program.

NOTE: You cannot perform shell operations, such as redirection using the executable type Binary. You can use *Executable file parameters* to pass only those parameters that are required by the executable specified in the *Executable file name* field. If you want to use shell operations, define your own script.

(Conditional) If you chose *Java* in the *Executable Type* field in Step 6 on page 166, the following options are available:

Java program name: Specify the Java program you want to run on a managed device.

Program parameters: Specify any parameters to be passed to the specified Java program.

Java Runtime Executable (JRE): Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

JRE parameters: Specify the parameters to be passed to the Java Runtime Executable (JRE).

NOTE: The Own Defined Script specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

---

7 Click *Next* to display the Summary page.

8 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Remote Execute policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

◆ Specify assignments for this policy

- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy

Create New Remote Execute Policy	Remote_Execute	?

✏ **Step 5: Policy Assignments**

Specify the assignments for this policy:

Add **Remove**	
☐ **Name**	**In Folder**
No items selected, click add to select items	

<< Back   Next >>   Cancel

9 Assign the policy to the devices.

   9a Click *Add* to browse for and select the appropriate Server or Workstation objects.

      You can also select Folder or Group objects.

   9b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

      Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

   9c Click *OK*.

10 Click *Next* to display the Policy Schedule page, then select the schedule to apply to the assignments.

   The settings you configure on this page determine when the policy is applied to devices.

   See for information about the available schedules.

NOTE: If you select *Day of the Week Specific* as the schedule type and *Start Immediately at Start Time, and then Repeat until End Time Every*, and if the Start Time and End Time spans midnight, the Remote Execute policy is executed only at the Start Time and fails to repeat execution.

---

11 Click *Next* to display the Policy Groups page.
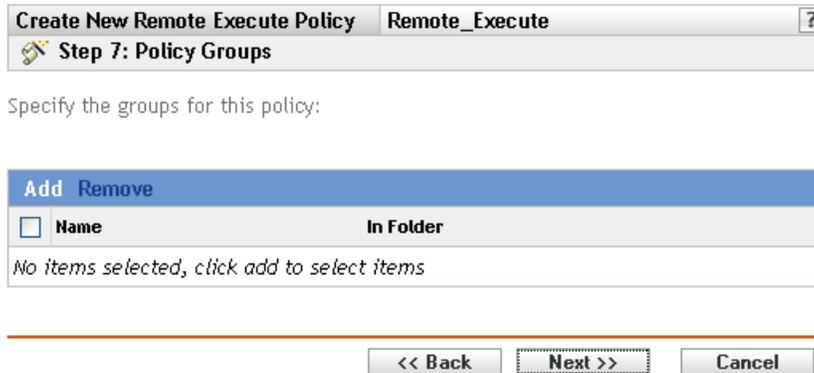
12 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the *Selected* list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

13 Click *Next* to display the Finish page.

14 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured per settings on the Finish page.

16.7 SUSE Linux Enterprise Desktop Policy

The SUSE Linux Enterprise Desktop policy is used to configure the SUSE Linux Enterprise Desktop settings on a device.

To configure the SUSE Linux Enterprise Desktop policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *SUSE Linux Enterprise Desktop Policy*, then click *Next* to display the Policy Name page.

4 Fill in the fields:

   ◆ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

   For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

   ◆ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

   ◆ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the SUSE Linux Enterprise Desktop Main Menu Settings page.
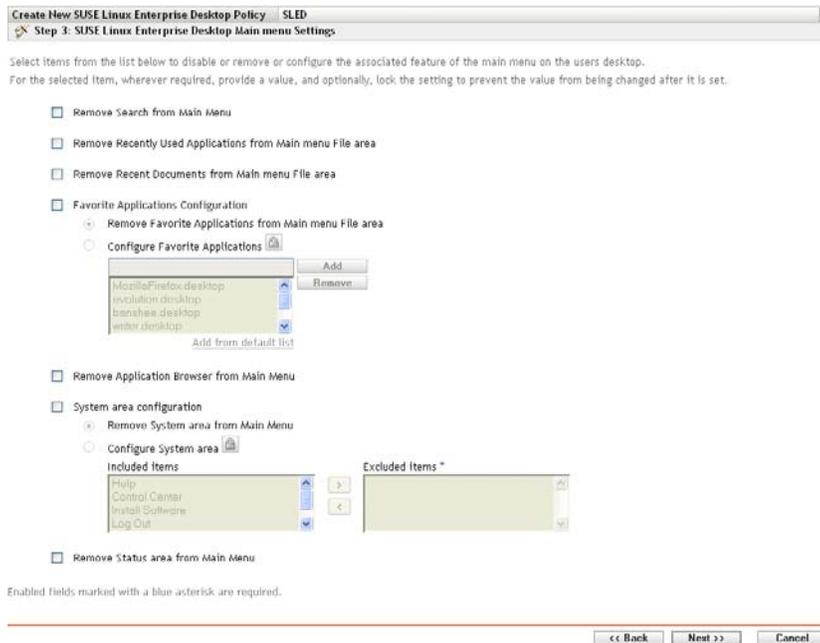
6 Select the desired options (by default, all options are disabled).

Selecting an item from the list disables or removes the associated feature on the user's desktop. The user cannot access menu items or controls associated with the feature.

Remove Search from Main Menu: Lets you remove Search from the main menu of the user's SUSE Linux Enterprise Desktop.

Remove Recently Used Applications from the Main Menu File Area: Lets you remove the recently used applications from the main menu file area of the user's SUSE Linux Enterprise Desktop.

Remove Recent Documents from Main Menu File Area: Lets you remove the recent documents from the main menu file area of the user's SUSE Linux Enterprise Desktop.

Favorite Applications Configuration: Lets you configure the following settings:

- ◆ **Remove Favorite Applications from Main Menu File Area:** Lets your remove favorite applications from the main menu file area of the user's SUSE Linux Enterprise Desktop.

- ◆ **Configure Favorite Applications:** Lets you to add or remove items from the Favorite Applications list. Selecting this option locks its setting. To unlock it, click 🔒.

  To add an application to the list, specify the application name and click Add. You can also add from the default list.

  To remove an application from the list, select the application you want to delete, and click Remove.

Remove Application Browser from Main Menu: Lets you remove the application browser from the main menu of the user's SUSE Linux Enterprise Desktop.

System Area Configuration: Lets you configure the following settings:

- ◆ **Remove System Area from Main Menu:** Lets you remove the system area from the main menu of the user's SUSE Linux Enterprise Desktop.

◆ **Configure System Area:** Lets you to configure items in the system area of the main menu of SUSE Linux Enterprise Desktop. In the Included Items list, select an item you want to remove from the user's System menu, and move it to the Excluded Items list.

Remove Status Area from the Main Menu: Removes the status area from the main menu of the user's SUSE Linux Enterprise Desktop.

7 Click *Next* to display the SUSE Linux Enterprise Desktop General Lockdown and Control Center Action List Settings page.
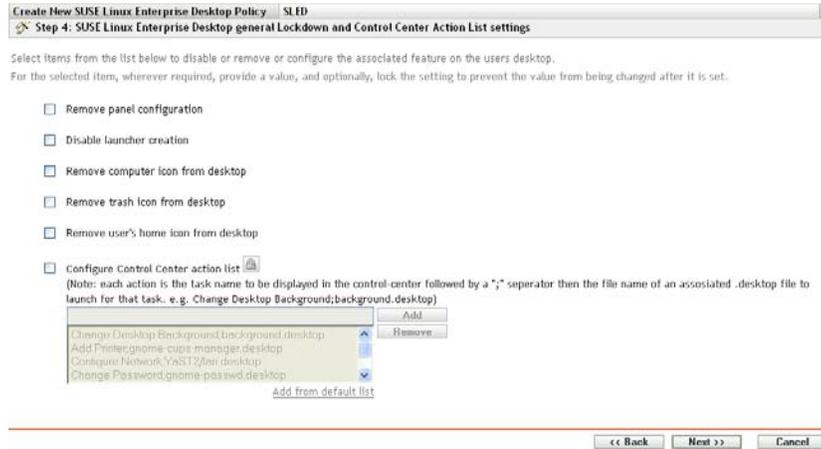
8 Select the desired options (by default, all options are disabled).

Selecting an item from the list disables or removes the associated feature on the user's desktop. The user cannot access menu items or controls associated with the feature.

Remove Panel Configuration: Lets you prevent users from configuring a panel. If you select this option, users cannot add and remove the icons on the panel.

Disable Launcher Creation: Lets you prevent users from creating application launchers.

Remove Computer Icon from Desktop: Lets you remove the computer icon from users' desktops.

Remove Trash Icon from Desktop: Lets you remove the trash icon from users' desktops.

Remove User's Home Icon from Desktop: Lets you remove the Home icon from users' desktops.

Configure Control Center Action List: Lets you to add or remove items from the Control Center action list. Selecting this option locks its setting. To unlock it, click ![lock].

To add an item to the list, specify the application name and click Add. You can also add from the default list.

To remove an item from the list, select the application you want to delete, and click Remove.

9 Click *Next* to display the SUSE Linux Enterprise Desktop Proxy Settings page.

10 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking 🔒. The options that are not enabled are excluded from the policy and are not applied to the device.

Background Image Filename: Lets you specify the filename and complete location of a background image. This image file is displayed as a background on users' desktops. The file should exist on the managed device at the specified location.

Background Position: Lets you specify background image display options. *Center* displays an image in the center of the screen, *Fill Screen* stretches the image to cover the entire screen, *Scaled* enlarges the image until the image meets the screen edges, and *Tiled* repeats the image over the screen. Select *No Background* to prevent the image from being displayed on the desktop.

Background Shade: Lets you choose an available shade to decorate the background. Select *Solid* to have the background image uniform across the desktop. Select *Vertical* to have the image become darker as you go up, and select *Horizontal* to have the image become darker as you go from left to right.

Theme Filename: Lets you specify a theme file name and its complete location. The appearance of the windows, icons, buttons, and other graphical user interface controls are changed according to the selected theme.

Proxy Settings: Specify a proxy setting:

- **Direct Internet Connection:** Lets users connect to the Internet without using the proxy server.

- **Manual Proxy Configuration:** Lets you manually configure the proxy. Specify the *HTTP Proxy* value, *HTTP Secure Proxy* value, *FTP Proxy* value, *Socks Proxy* value, and corresponding port numbers.

  To authenticate the user before proxy configuration, click Authentication. In the HTTP Proxy Authentication dialog box, select *Use Authentication*, specify the username and password, then click *OK*.

◆ **Automatic Proxy Configuration:** Lets you automatically configure the proxy from a certain URL by specifying the URL.

11 Click *Next* to display the Default System Requirements for the SUSE Linux Enterprise Desktop Policy page.

```
Create New SUSE Linux Enterprise Desktop Policy   SLED                                    [?]
    Step 6: Default system requirements for SUSE Linux Enterprise Desktop policy

The following condition is added as a default system requirement to this policy.
If the minimum supported version requirement is removed, the policy may not be fully applied and effective on the target device.

☑ Apply policy on devices with distribution = SUSE Linux Enterprise Desktop 10

                                                      << Back      Next >>      Cancel
```

12 Specify the minimum version of SLED Linux Enterprise Desktop required for all policy settings to be effective. Policy settings are applied only if a device has the same version or a newer version of the SLED Linux Enterprise Desktop. If a device does not have SLED Linux Enterprise Desktop 10 or newer, the policy does not apply correctly.

Even if you do not include this setting in the policy, the system checks for SLED Linux Enterprise Desktop. If it does not find SLED Linux Enterprise Desktop, an error message is generated and the policy is not applied.

13 Click *Next* to display the Summary page.

14 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the SUSE Linux Enterprise Desktop policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

  ◆ Specify assignments for this policy
  ◆ Specify the schedule for this policy
  ◆ Specify groups for this policy

```
Create New SUSE Linux Enterprise Desktop Policy    SLED                    [?]
    Step 9: Policy Assignments

Specify the assignments for this policy.

┌─────────────────────────────────────────────────────────────────────┐
│ Add  Remove                                                           │
├──┬──────────────────────────┬───────────────────────────────────────┤
│☐ │ Name                     │ In Folder                             │
├──┴──────────────────────────┴───────────────────────────────────────┤
│ No items selected, click add to select items                         │
└─────────────────────────────────────────────────────────────────────┘

                              << Back      Next >>      Cancel
```
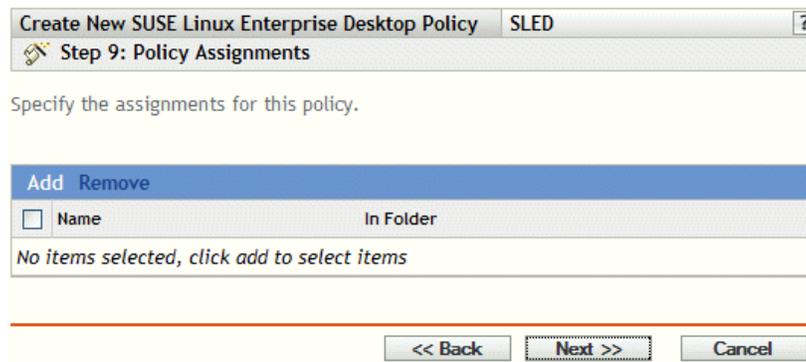
15 Assign the policy to the devices.

15a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

15b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

15c Click *OK*.

16 Click *Next* to display the Policy Schedule page.

| Create New SUSE Linux Enterprise Desktop Policy | SLED | ? |
| Step 9: Policy Schedule | | |

Select the schedule to apply to the policy assignments.

Schedule Type:
Event ▾

Select the event that this schedule should be triggered on:

☑ User Login

<< Back   Next >>   Cancel

17 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules and their options.

18 Click *Next* to display the Policy Groups page.

| Create New SUSE Linux Enterprise Desktop Policy | SLED | ? |
| Step 11: Policy Groups | | |

Specify the groups for this policy.

Add Remove

☐	Name	In Folder
No items selected, click add to select items		

<< Back   Next >>   Cancel

19 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the *Selected* list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

20 Click *Next* to display the Finish page.

21 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

16.8 Text File Policy

The Text File policy is used to make changes to any text file on a device.

To configure the Text File policy:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the Policy Type list, click *Text File Policy*, then click *Next* to display the Policy Name page.

```
Create New Text File Policy                              [?]
  Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *
[                                    ]

Folder: *
[/Policies                  ] [🔍]

Description:
[                                    ]
[                                    ]
[                                    ]
[                                    ]
[                                    ]

Fields marked with a blue asterisk are required.

              [ << Back ]  [ Next >> ]  [ Cancel ]
```

4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.

- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the General page.
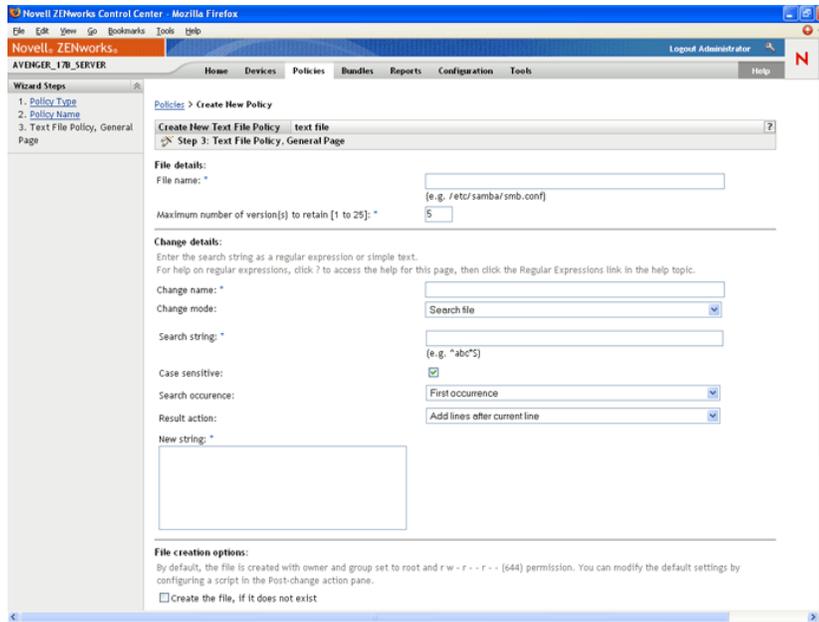
6 Select the desired options:

Filename: Specify the name and the complete path of a file you want to change.

Maximum number of versions to retain: Specify the maximum number of backups to be maintained for a file that has been changed. If the maximum limit of backups is reached, the oldest backup of a file is deleted. The backup is created in the same location as the specified file.

Change name: Specify the name of the change you want to perform in the file. If you want to make more than one change in the same file, go to the Settings page.

Change mode: Select an option from the drop-down list:

- **Search file:** Lets you search for the given text in the entire file. Fill in the fields:

  - **Search string:** Specify the text you want to search for in a given file. The search string can be simple text or a regular expression. For detailed information on regular expressions, click the [?] button.

    Case sensitive: Select this option to distinguish between uppercase and lowercase characters. When *Case sensitive* is selected, the system finds only those instances in which the capitalization matches the text you have specified in the search string.

    Search occurrence: Indicates the occurrence of the search text you have given. The available options are *First Occurrence*, *Last Occurrence*, and *Find All Occurrences*. For example, if you select *First Occurrence*, the system finds the first occurrence of the search string and performs the specified action on it.

    Result action: Select the operation from the drop-down list that you want perform on the specified search text.

- **Append lines to file:** Lets you append the given lines of text to the file

- **Prepend lines to file:** Lets you prepend the given lines of text to the file.

New string: Specify the text to be used for carrying out the specified action in the file. For example, you can select to replace a search string with a new string.

Create the file, if it does not exist: Allows you to create the specified file, if it does not exist. The file is created with the specified contents.

Contents of the file: Allows you to add contents to the specified file. This option is available only if you select the *Create the file, if it does not exist* option. The file is created with owner and group set to root and r w - r - - r - - (644) permission. If any directory specified in the absolute file path does not exist, then it is created with owner and group set to root and r w x r - x r- x (755) permission. You can modify the ownership and permissions by configuring a script in the Post Change Action pane. (The Post Change Action pane is located in the Script page. To access the Script page, click *Next* in the General Page user interface.)

Apply the change details: Applies the settings configured in the Change Details pane. By default, this option is selected when you select the *Create the file, if it does not exist* option.

7 Click *Next* to display the Script Page.

8 Fill in the fields:

Pre-change action: Specify the actions to perform before modifying the text files:

- ◆ **Executable type:** Select the executable type from the drop-down list that you want to run before modifying the file. The available options are *None*, *Binary*, *Java*, and *Script*.

  (Conditional) If you chose *Script* in the *Executable type* field, the following options are available:

  Script to run: Select an option from the drop-down list (*Specify a File* or *Define Your Own Script*):

  - ◆ **Specify a file:** Fill in the fields:

Script filename: Specify the complete path, including the filename, of the script you want to run on a managed device.

Script parameters: Specify any parameters to be passed to the specified script file.

Script engine: Specify the name and location of the script engine that runs the script. For example, `/usr/bin/perl`.

Script engine parameters: Specify any parameters to be passed to the specified script engine.

   ◆ **Define your own script:** Type your script in the box.

(Conditional) If you chose Binary in the *Executable type* field, the following options are available:

Executable file name: Specify the complete path, including the filename, of the binary program you want to run on a managed device.

Executable file parameters: Specify any parameters to be passed to the specified binary program.

(Conditional) If you chose *Java* in the *Executable type* field, the following options are available:

Java program name: Specify the Java program you want to run on a managed device.

Program parameters: Specify any parameters to be passed to the specified Java program.

Java Runtime Executable (JRE): Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

JRE parameters: Specify the parameters to be passed to the Java Runtime Executable (JRE).

NOTE: The *Own Defined Script* specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

Action when the execution fails: Select an action you want the system to perform when an execution fails. You can continue modifying the file by selecting *Continue modifying the text file* or you can stop the modifications in the file by selecting *Do not modify the text file*.

NOTE: The backup of the text file is taken after the pre-change action completes the execution and before the text file modification starts.

Post-change action: Specify the actions to perform after the actual changes are done in the file.

   ◆ **Executable type:** Select the executable type you want to run after modifying the file. Select Binary, Java, Script, or None from the drop-down list. Depending on which type you select, the available options vary. For more information about the specific options, see the descriptions in the Pre-Change Action section directly above.

9 Click *Next* to display the Summary page.

10 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Text File policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Text File Policy	Text_File	?
✎ Step 6: Policy Assignments		

Specify the assignments for this policy:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

11 Assign the policy to the devices.

11a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

11b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

11c Click *OK*.

12 Click *Next* to display the Policy Schedule page, then select the schedule to apply to the assignments.

The settings you configure on this page determine when the policy is applied to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules.

13 Click *Next* to display the Policy Groups page.

Create New Text File Policy	Text_File	[?]
⚒ Step 8: Policy Groups		

Specify the groups for this policy:

Add Remove

☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

14 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the *Selected* list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see Section 17.3, "Creating Policy Groups," on page 185.

15 Click *Next* to display the Finish page.

16 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

Managing Policies

17

Novell® ZENworks® Linux Management Policies give you the ability to define and lock down configuration settings of various applications on managed devices. ZENworks Linux Management provides policies for a number of popular applications, plus powerful tools to create customized policies for other applications. In addition to creating policies, as described in Chapter 16, "Creating Policies," on page 133, you can create groups and folders to assign policies to, edit existing policies, and more.

The following sections contain additional information:

- Section 17.1, "Creating Policies," on page 183
- Section 17.2, "Creating Folders," on page 184
- Section 17.3, "Creating Policy Groups," on page 185
- Section 17.4, "Assigning Policies," on page 188
- Section 17.5, "Removing Policy Assignments," on page 189
- Section 17.6, "Adding Policies to Existing Groups," on page 190
- Section 17.7, "Editing Policies," on page 190
- Section 17.8, "Editing System Requirements," on page 200
- Section 17.9, "Refreshing Policies," on page 202
- Section 17.10, "Verifying Policy Enforcement," on page 202
- Section 17.11, "Renaming, Copying, or Moving Policies," on page 203
- Section 17.12, "Deleting Policies, Policy Groups, and Folders," on page 204
- Section 17.13, "Unenforcing Policies," on page 205

17.1 Creating Policies

Step-by-step instructions to create policies are contained in Chapter 16, "Creating Policies," on page 133.

ZENworks lets you create seven types of policies:

- **Epiphany policy:** Configures the Epiphany Web browser. For step-by-step instructions to create this policy, see Section 16.1, "Epiphany Policy," on page 133.
- **Evolution policy:** Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see Section 16.2, "Evolution Policy," on page 139.
- **Firefox policy:** Configures the Firefox Web browser. For step-by-step instructions to create this policy, see Section 16.3, "Firefox Policy," on page 145.
- **Generic GNOME policy:** Configures GConf applications. For step-by-step instructions to create this policy, see Section 16.4, "Generic GNOME Policy," on page 151.
- **Novell Linux Desktop policy:** Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see Section 16.5, "Novell Linux Desktop Policy," on page 156.

- **Remote Execute policy:** Executes a script, binary, or Java file. For step-by-step instructions to create this policy, see Section 16.6, "Remote Execute Policy," on page 164.
- **Text File policy:** Applies changes to a text file. For step-by-step instructions to create this policy, see Section 16.8, "Text File Policy," on page 176.

17.2 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Policy, and Policy Group objects.

To create a folder:

1 In the ZENworks Control Center, click the *Policies* tab.

2 Click *New*, then click *Folder* to display the New Folder dialog box.

3 Fill in the fields:

- **Name:** Provide a unique name for your folder. This is a required field.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.

- **Description:** Provide a short description of the folder's contents.

4 Click *OK*.

17.3 Creating Policy Groups

A policy group lets you organize policies to ease administration and to provide easier assigning and scheduling of the policies in the policy group.

To create a policy group:

1 In the ZENworks Control Center, click the *Policies* tab.

2 Click *New*, then click *Policy Group* to display the Basic Information page.

3 Fill in the fields:

- **Group name:** (Required) Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface (the administrative tool for ZENworks Linux Management) and in the user interface.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** (Required) Type the name or browse to the folder that contains this policy group.

- **Description:** Provide a short description of the policy group's contents. This description displays in the ZENworks Control Center.

4 Click *Next* to display the Summary page.

Review the information on the Summary page, making any changes to the policy-group settings by using the *Back* button as necessary.

Depending on your needs, you can create the policy group now or you can specify members, assignments, and schedules for this policy group.

5 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the policy group is created but it does not have members, devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the policy group by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Add Group Members page to perform the following tasks:

- ◆ Specify members for this policy group
- ◆ Specify assignments for this policy group
- ◆ Specify the schedule to apply the policy-group assignments

Create New Group	Policies	?
🖎 **Step 3: Add Group Members**		

Specify the members for this group:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

6 Specify the policies to include in this policy group.

6a Click *Add* to browse for and select the appropriate policy objects.

6b Click the underlined link in the *Name* column to select the desired policies and display their names in the *Selected* list box.

6c Click *OK*.

7 Click *Next* to display the Add Assignments page.

Create New Group	Policies	?
🖎 **Step 4: Add Assignments**		

Specify the assignments for this group:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

8 Assign the policy group to the desired devices.

8a Click *Add* to browse for and select the appropriate device objects.

You can also select Folder or Group objects.

8b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

8c Click *OK*.

9 Click *Next* to display the Schedule page.

10 Select the schedule to apply to the assignments.

The settings you configure on this page determine when the policies in the policy group are assigned to devices.

See Section 15.3, "Schedules," on page 128 for information about the available schedules.

11 Click *Next* to display the Summary page, then review the information, making any changes to the settings by using the Back button as necessary.

12 Click *Finish*.

17.4 Assigning Policies

When you assign policies, you specify device assignments and assignment schedules for an existing policy.

When you created policies, midway through the Create Policy Wizard, you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the policy was created without assigning devices to it, specifying assignment schedules, or specifying groups for the policy. Before the policy can be applied to assigned devices, you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the policy-creation process.

1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by checking the box next to its name, click *Action*, then click *Assign Policy* to display the Policy Assignments page.

2 Assign the policy to the desired devices.

2a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

2b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

2c Click *OK*.

3 Click *Next* to display the Schedule page.

Assign Policy	?
Step 2: Schedule	

Specify the schedule to use for the assignments.

Schedule Type:
No Schedule ▾

[<< Back] [Next >>] [Cancel]

4 Select the schedule to apply to the assignments.

The settings you configure on this page determine when the policy is applied to devices.

Depending on the type of policy you are assigning, the available schedules vary. See Section 15.3, "Schedules," on page 128 for information about the available schedules.

5 Click *Next* to display the Finish page.

6 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to assign the policy as configured according to the settings on the Finish page.

In addition to the preceding steps to assign policies, the following are other options to assign a policy to devices:

◆ By selecting a policy and then using the Assignments section of the policy's Summary page.

◆ By selecting a device, device group, or folder and then selecting *Assign Policy* in the Action menu.

◆ By using the Effective Policy section on the device's Summary page.

17.5 Removing Policy Assignments

You can remove the policy assignments by selecting a policy and then removing the device from the Assignments section on the Policy Summary page. You can also do this by clicking the appropriate device on the Devices page and disassociating a policy by using the Effective Policies section.

After a policy is disassociated from a device, it is unenforced on the device. For more details on unenforcement of a policy, see Section 17.13, "Unenforcing Policies," on page 205.

You do not need to delete a policy to disassociate it from a device.

17.6 Adding Policies to Existing Groups

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create.

1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by selecting the box next to its name, click *Action*, then click *Add to Group* to display the Targets page.

Add To Group		?
Step 1: Targets		

Select the groups that will contain the items.

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

<< Back   Next >>   Cancel
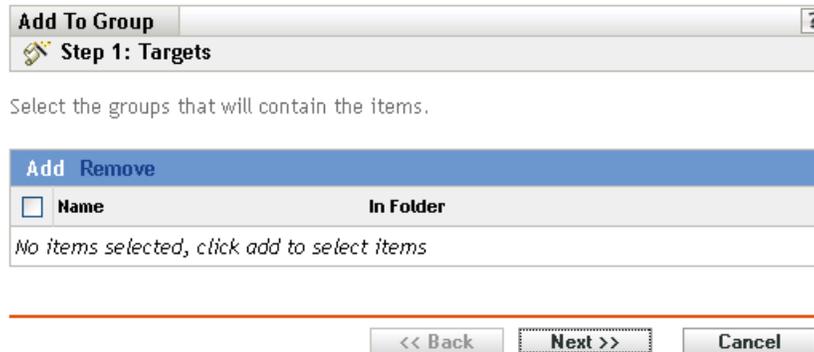
2 Click *Add* to open the Select Groups dialog box, click the desired objects to add them to the Selected list, then click *OK* to display the selected groups in the list on the Targets page.

3 Click *Next* to display the Finish page.

4 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the policy to the group.

17.7 Editing Policies

You can edit an existing policy to change its description, add or remove assignments, add or remove the policy from existing policy groups, change configuration settings, and more.

Following sections describes how you can edit different types of policies:

- Section 17.7.1, "Editing Epiphany, Evolution, Firefox, and NLD Policies," on page 190
- Section 17.7.2, "Editing Generic GNOME Policies," on page 193
- Section 17.7.3, "Editing Remote Execute Policies," on page 195
- Section 17.7.4, "Editing Text File Policies," on page 197
- Section 17.7.5, "Viewing Policy Enforcement Status," on page 200

17.7.1 Editing Epiphany, Evolution, Firefox, and NLD Policies

You can edit, include, or remove lockdown settings, configuration settings, and system requirements of the application policies. Epiphany, Evolution, Firefox, Novell Linux Desktop, and SUSE Linux Enterprise Desktop policies are the application policies.

1 In the ZENworks Control Center, click the *Policies* tab.

2 Click the policy's name to display the Summary page, then make the desired configuration changes.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type (Novell Linux Desktop Policy, Firefox Policy, and so forth).

Revision: Displays the policy's revision number. To change the revision number, click Increment Revision.

Number of errors not acknowledged: Displays the number of errors not acknowledged.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose.

Click *Edit* to change the description, if necessary.

2b Review the information in the *Assignments* section, then make the desired configuration changes.

The *Assignments* section lists the devices, device groups, and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see Section 17.4, "Assigning Policies," on page 188.

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

2c Review the information in the *Event Log* section, then make the desired changes.

The *Event Log* section lists all unacknowledged errors and warnings.

The *Status* column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the *Event* column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the *Date* column to indicate that the item has been acknowledged).

2d Review the information in the *Upcoming Events* section.

The *Upcoming Events* section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

2e Review the information in the *Groups* section, then make the desired configuration changes.

The *Groups* section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the *Select* column to select the desired group and display its name in the *Selected* list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

3 Click the *Details* tab, then make the desired configuration changes. For more information about the available options, see the section about the appropriate policy in Chapter 16, "Creating Policies," on page 133.

3a To edit the system requirements of a policy, see Section 17.8, "Editing System Requirements," on page 200.

3b Click *Apply* to save any changes you have made.

4 After a policy is modified, the *Revision* field of the policy, which is available under the *General* section of the Summary page, must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

17.7.2 Editing Generic GNOME Policies

1 In the ZENworks Control Center, click the *Policies* tab.

2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to Step 3 on page 194.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

2a Review the information in the *General* section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type as Generic GNOME policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment Revision*.

Number of errors not acknowledged: Displays the number of errors that are not acknowledged.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

2b Review the information in the *Assignments* section, then make the desired configuration changes.

The *Assignments* section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page, which includes a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see .

Remove: Select the device by clicking the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

2c Review the information in the *Event Log* section, then make the desired changes.

The *Event Log* section lists all unacknowledged errors and warnings.

The *Status* column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the *Event* column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the *Date* column to indicate that the item has been acknowledged).

2d Review the information in the *Upcoming Events* section.

The *Upcoming Events* section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

2e Review the information in the Groups section, then make the desired configuration changes.

The *Groups* section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page, which includes a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

3 Click the *Details* tab, then make the desired configuration changes.

3a You can add a new key or directory by selecting the directory under which you want to add the new key or directory. You can use the *New* menu to add a new key or directory.

If you want to configure more application keys using the same policy, the *Import From a Device* option is more appropriate. You can configure the device, test it, and then import the settings to update the policy.

You can import from the same device that was used to create the original policy or you can import from any other device. When you import settings, you have additional options, such as the following:

Add the new imported settings that are not present in the policy: Adds only those GConf settings that are not part of existing policy settings. This is selected by default. Use this option to update the policy by including more directories and keys.

Override the settings that are already present in the policy with the imported settings: Overrides the existing settings with the imported policy settings. Use this option to use the newly imported settings instead of the ones configured in the policy.

Remove settings from the policy that are not present among the imported settings:

Removes those policy settings that are not present in the imported settings. Use this feature to discard any additional settings that might be present in the original policy and that you do not want as a part of the updated policy.

3b Edit the minimum system requirements according to your preferences. To edit the system requirements of the Generic GNOME policy, see Section 17.8, "Editing System Requirements," on page 200.

3c Click *Apply* to save any changes you have made.

4 After a policy is modified, the *Revision* field of the policy (under the *General* section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

17.7.3 Editing Remote Execute Policies

1 In the ZENworks Control Center, click the *Policies* tab.
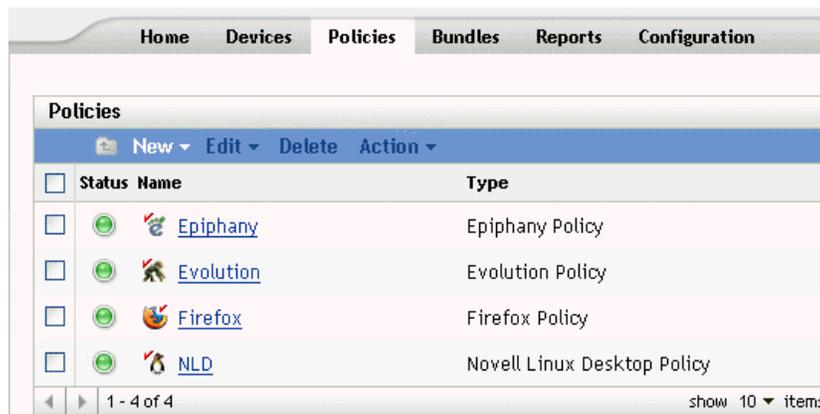
2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to Step 3 on page 197.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

2a Review the information in the *General* section, then make the desired configuration changes (you can edit only the *Revision* and *Description* options in this section).

Policy type: Displays the policy type as Remote Execute policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment Revision*.

Number of errors not acknowledged: Displays the number of unacknowledged errors.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

2b Review the information in the *Assignments* section, then make the desired configuration changes.

The *Assignments* section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page, which includes a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see Section 17.4, "Assigning Policies," on page 188.

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

2c Review the information in the *Event Log* section, then make the desired changes.

The *Event Log* section lists all unacknowledged errors and warnings.

The *Status* column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the *Event* column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the *Date* column to indicate that the item has been acknowledged).

2d Review the information in the *Upcoming Events* section.

The *Upcoming Events* section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

2e Review the information in the *Groups* section, then make the desired configuration changes.

The *Groups* section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page, which includes a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove*.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the *Select* column to select the desired group and display its name in the *Selected* list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

3 Click the *Details* tab, then make the desired configuration changes. For more information about the available options, see Section 16.6, "Remote Execute Policy," on page 164.

You can add system requirements to a policy. For more information, see Section 17.8, "Editing System Requirements," on page 200.

3a Click *Apply* to save any changes you have made.

4 After a policy is modified the *Revision* field of the policy (available under the *General* section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

17.7.4 Editing Text File Policies

1 In the ZENworks Control Center, click the *Policies* tab.

| Home | Devices | **Policies** | Bundles | Reports | Configuration |

Policies

New ▾   Edit ▾   Delete   Action ▾

☐	Status	Name	Type
☐	●	🦔 Epiphany	Epiphany Policy
☐	●	🐾 Evolution	Evolution Policy
☐	●	🦊 Firefox	Firefox Policy
☐	●	🔺 NLD	Novell Linux Desktop Policy

◀ ▶ 1 - 4 of 4   show 10 ▾ items

2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to Step 3 on page 199.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

2a Review the information in the *General* section, then make the desired configuration changes (you can edit only the *Revision* and *Description* options in this section).

Policy type: Displays the policy type as Text File policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment revision*.

Number of errors not acknowledged: Displays the number of unacknowledged errors.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

2b Review the information in the *Assignments* section, then make the desired configuration changes.

The *Assignments* section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page, which includes a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see Section 17.4, "Assigning Policies," on page 188.

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

2c Review the information in the *Event Log* section, then make the desired changes.

The *Event Log* section lists all unacknowledged errors and warnings.

The *Status* column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the *Event* column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced,* select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

2d Review the information in the *Upcoming Events* section.

The *Upcoming Events* section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

2e Review the information in the *Groups* section, then make the desired configuration changes.

The *Groups* section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the *Name* column, then clicking *Remove* to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the *Select* column to select the desired group and display its name in the *Selected* list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

3 Click the Details page. This page lets you perform the following actions:

Editing Item	Description
Edit the existing change to be made	Lets you update the modifications to be made.
Add a new change to the same file	Lets you make multiple changes to the same file.
Add a new file to be changed and the corresponding changes	Lets you modify multiple files using the same policy.
Rename the change	Lets you keep the changed name consistent with the changes made.
Edit the file to be modified	Lets you edit the filename to apply the changes to another file or update the filename.
Delete files and changes	Lets you delete the files and changes.
Reorder files and changes	A file is modified in the order of the changes shown in the ZENworks Control Center. You can use this option to order the sequence of changes. Because the second modification is done on the updated file after the first modification is complete, and so on, ordering changes lets you perform logical operations. Ordering of files lets you modify files in a logical order.

Editing Item	Description
Edit the pre- and post-change actions	Lets you add, edit, or remove the pre- and post-change actions for the policy. You can also edit the action to be taken when a pre-change action fails.

You can add system requirements to a policy. For more information, see Section 17.8, "Editing System Requirements," on page 200.

3a Click *Apply* to save any changes you have made.

4 After a policy is modified, the *Revision* field of the policy (available under the *General* section of the Summary page) must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

17.7.5 Viewing Policy Enforcement Status

You can view the status of a policy by looking at the icon located next to each policy. The following table describes each color code and its description:

Color Code	Policy Status
Green	Normal. The policy has been successfully enforced on all associated devices.
Yellow	Warning. A device has encountered a warning when trying to apply this policy.
Red Cross	Critical. A device has encountered an error when trying to apply this policy.

To view more information about a warning or error, click the policy to review the event log.

17.8 Editing System Requirements

The purpose of the system requirements is to limit some policies to run on devices that have the necessary requirements to enforce the policy. When more than one GConf-based policy of the same type is assigned, the first policy that meets the requirements is enforced on managed devices. All effective Remote Execute and Text File policies are enforced on managed devices.

You can specify the system requirements by defining certain conditions, called filters. You can set up simple system requirements that contain only one filter, or you can set up complex system requirements containing multiple filters or groups of filters. If you set up system requirements using more than one filter, you must also specify the logical relationship between the filters.

To set up a filter:

1 In the ZENworks Control Center, click the *Policies* tab.

2 Select a policy for which you want to edit the system requirements.

3 Click the *Details* tab.

4 In the *Combine Filters Using* field, select AND or OR.

This setting lets you specify the logical relationship between filter sets and filters. Select And to satisfy all the sets of filters and select Or to satisfy any one of the filter sets. By default, the filters are defined in one filter set. Within a filter set, select OR to satisfy any one of the filter conditions and select AND to satisfy all the filter conditions.

5 (Optional) Click *Add filter*. The new filter is added and it is applied based on the logical relationship you have defined in Step 4 on page 200.

6 (Optional) Click *Add filter set* to add a new filter set. This filter is also applied based on the logical relationship you have defined in Step 4 on page 200.

7 Select a value from the first drop-down list.

The operator list and other text boxes are displayed based on the value you have selected in the first drop-down list.

8 Specify a value in the text box. The following table describes values you can select in the first drop-down list and corresponding examples you can specify:

Criteria	Field 1	Field 2	Field 3
Date of File	Filename with complete path	Logical condition	Date
Distribution	Logical condition	Distribution name with version number	-
Environment	Environment Variable	Logical condition	Value
Find File	Filename with full path	Logical condition	-
Find RPM	RPM name Make sure that the RPM name you specify is case-sensitive.	Logical condition	-
Free Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Kernel	Logical condition	Linux kerne_version. For example, Linux 2.6.5-7.111	-
Processor	Logical condition		-
Size of file	Filename with complete path	Logical condition	Size in bytes
Total Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Used Disk Space	File System. For example, /dev/hda1	Logical condition	Value in KB

Criteria	Field 1	Field 2	Field 3
Version of RPM	RPM name Make sure that the RPM name you specify is case-sensitive.	Logical condition	Version (2.0.1)

9 Select an operator from the drop-down list.

The operator drop-down list is displayed based on the value you have selected in the first drop-down list. For example, if you select *Version of RPM*, the available operators are *Equal to*, *Not Equal to*, *Less Than*, *Greater than, > Greater than or equal to*, and *Less than or equal to*. If you select *Size of file*, the available operators are *Less than*, *Greater than*, *Greater than or equal to*, and *Less than or equal to*. If you select *Date of file*, the available options are *On, > After*, *On or after*, *Before*, and *On or before*. If you select *Date of file*, you can also select a specific date.

10 Click *Apply*.

17.9 Refreshing Policies

If you assign a new policy to a device or update a policy, you can ensure that the policy is updated on managed devices by refreshing the policies. Each device periodically refreshes its settings. It is not necessary to manually refresh each device after updating a policy. To ensure that the updated policy is immediately pulled down, you can manually refresh the device using the following methods:

- In the ZENworks Control Center, click the *Devices* tab, select the appropriate device, click *Actions*, then click *Refresh Device*.
- On a managed device, start a console session and execute the `rug refresh` command.

  On SUSE Linux Enterprise Server 10 (SLES 10) or SUSE Linux Enterprise Desktop (SLED 10) managed devices:

  `/usr/bin/rug refresh`

  On other managed devices:

  `/opt/novell/zenworks/bin/rug refresh`

Performing either action results in the managed device refreshing its policies and other settings. A newly assigned or updated policy is delivered to the device and is applied according to its schedule.

17.10 Verifying Policy Enforcement

ZENworks Linux Management lets you verify the enforcement of a policy after it has been assigned to a device or updated and the device has been refreshed (either manually or automatically by ZENworks). After a policy has been enforced, a message is logged indicating the success or failure of the policy enforcement. These messages can be seen in the Event log of the device on which the policy was applied or can be seen in the Event log of the policy that was applied.

To verify the enforcement of the GConf-based policies, you need to re-login to the assigned device. You can then start the application and verify that the policy has been enforced correctly.

If a desktop or user interface session is in progress on a managed device with GConf-based policies assigned to it, and an updated policy is enforced on that device by a console login or an `su` command, all updated settings may not be immediately applicable on the desktop session. The updated settings are reflected only when the user logs in via the user interface session again.

In the Novell Linux Desktop policy, some of the configuration settings are file-permission-based, and hence for a `root` user, these settings such as items in the Program menu and System menu will be accessible even if it is locked.

For the Remote Execute and Text File policies, the enforcement occurs according to the schedule. To verify the enforcement, check the managed device to ensure that the specified changes or actions have taken place.

You can also verify the enforcement status or check for errors by looking at the zmd log on the managed device (`/var/opt/novell/log/zenworks/zmd-messages.log` for all managed devices except SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop 10 (SLED 10) devices. The path for SLES 10 and SLED 10 devices is `/var/log/zmd-messages.log`).

17.11 Renaming, Copying, or Moving Policies

Use the *Edit* drop-down list on the Policies page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the object. For example, if you select a Policy object, you can rename, copy, and move the policy. If you select a Policy Group object, you can rename or move the Policy Group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the *Edit* menu.

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the Policies list, select the box next to the policy's name, click *Edit*, then click an option.

- ◆ **Rename:** Click *Rename*, type a new name for the policy, then click *OK*.
- ◆ **Copy:** Click *Copy*, type a new name for the copy, then click *OK*.

  The copy option is useful to create a new policy that is similar to an existing policy. You can copy a policy and then edit the new policy's settings.

Only policy settings are copied; policy groups and assignments are not copied.

◆ **Move:** Click *Move*, select a destination folder for the selected objects, then click *OK*.

If you rename or move a policy, its assignments are still in place. ZENworks Linux Management does not reapply the policy to devices because of the name or location change.

17.12 Deleting Policies, Policy Groups, and Folders

Before you delete policies, policy groups, and folders from the ZENworks Control Center, review the following information to ensure that you obtain the desired results.

Deleting Policies: Depending on your needs, you can delete a policy from your ZENworks Linux Management system or remove a policy's assignments from devices.

If you delete a policy from your ZENworks Linux Management system, the policy does not display on the Policies or Devices pages in the ZENworks Control Center. When a policy is deleted, it is unassigned and unenforced from the device with which it was assigned. For more information, see Section 17.13, "Unenforcing Policies," on page 205.

Deleting Policy Groups: The results of deleting a policy group is similar to that of deleting a policy.

If you delete a policy group from your ZENworks Linux Management system, the policy group does not display on the Policies page in the ZENworks Control Center and the policy group's assignments are removed. However, the individual policies contained in the group are not removed from the ZENworks Control Center and still display on the Policies page.

When a policy group is deleted, its member policies are not deleted, but the associations are removed. The policies of a policy group are unenforced from the devices to which the policy group was associated. For more information, see Section 17.13, "Unenforcing Policies," on page 205.

Deleting Folders: If you delete a folder that contains policies from your ZENworks Linux Management system, both the folder and its policies are removed from the ZENworks Control Center. The policies contained in the folder are unenforced from the device to which they were assigned. For more information, see Section 17.13, "Unenforcing Policies," on page 205.

To delete a policy, policy group, or folder:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the box next to the desired item's name, then click *Delete*.

If the item you are deleting is a folder, you are prompted whether or not to delete the folder and its contents.

When a policy folder is deleted, each of its policies and subfolders are also deleted.

17.13 Unenforcing Policies

Policies are unenforced when either a policy is deleted or it is unassigned from a device. On the next refresh, the policy data is removed from the managed device. For GConf-based policies, when a user logs in after a refresh, the configuration changes made by the policy are undone. Unenforcement is not supported for the Remote Execute and Text File policies.

Package and Content Management

V

The following sections provide information about Novell® ZENworks® Linux Management Package and Content Management features and procedures:

Package and Content
Management Overview

18

Novell® ZENworks® Linux Management lets you install packages or files using either a bundle or a catalog. Content included in a bundle that is directly assigned is considered mandatory; the software or files are installed on all assigned devices. A catalog is a collection of RPM bundles or Dell Update Package bundles; content included in a catalog is usually considered optional.

ZENworks Linux Management also provides content replication to replicate content (packages, Dell Update Packages, bundles, and catalogs) from one server to other servers in your system.

The content replication feature in ZENworks Linux Management lets you replicate content from the Primary ZENworks server to Secondary Servers in a single ZENworks Management Zone.

The mirroring feature (zlmmirror, a command line utility) lets you replicate content between Management Zones or from remote servers. You use mirroring to obtain Dell Update Packages (DUPs) from the Dell FTP site or from a CD obtained from Dell, RCE services, and YOU patches.

You can use the ZENworks Control Center or the zlman command line utility to create and modify packages, bundles, and catalogs. The procedures in this section explain how to perform these tasks using the ZENworks Control Center. If you prefer the zlman command line utility, see zlman (1) (page 562).

The following sections contain additional information:

- Section 18.1, "Understanding RPM and File Bundles," on page 211
- Section 18.2, "Understanding Catalogs," on page 211
- Section 18.3, "Understanding Dell Update Package Bundles," on page 212
- Section 18.4, "Understanding the zlman Utility," on page 212
- Section 18.5, "Replicating Content in the ZENworks Management Zone," on page 212
- Section 18.6, "Mirroring Software," on page 212

To distribute and install RPMs on managed devices, you need to ensure that all dependent packages are also imported to the ZENworks Linux Management server. For example, to distribute updates to the SLES 10 devices mirrored from updates.novell.com, you need to ensure that all the packages from the SLES 10 media are imported to the ZLM server. You need to assign the bundles or catalogs containing the dependent RPMs to the managed devices.

You can upload packages in bulk into the ZENworks server using a script. A sample script is as follows. You can customize it according to your requirements.

```
#!/bin/bash

#

# Run this program from a directory filled with RPMS to load them into a bundle
in ZLM.

#
```

```
# All rpms, except src and nosrc rpms, in the directory and all of its
subdirectories will be loaded into the bundle and architecture indicated
below.

#

# Don't forget to enter your admin password below and update the bundlename and
architecture below.

#

if [ $# -lt 3 ]

then

 echo "Usage :: zlmload.sh <bundle_name> <arch> <admin_password>"

 echo "Example :: zlmload.sh SLES-9-Distro sles-9-i586 novell"

exit

fi


# Create the bundle to load into

zlman -V -U administrator -P$3 bc $1


# loop through these directories and load all of the rpms

STARTDIR=`pwd`

STARTTIME=`date`

time \

for dir in `find . |grep .rpm |grep -v src.rpm|grep -v nosrc.rpm|awk -F / '{NF-
-; OFS="/"; print $0}'| sort | uniq`; do

  cd $STARTDIR

  cd $dir

  echo "Loading RPM's from `pwd`"

  zlman -V -U administrator -P$3 bap $1 $2 *.rpm;

done

ENDTIME=`date`


echo "Load started at $STARTTIME"

echo "and ended at $ENDTIME"
```

18.1 Understanding RPM and File Bundles

An RPM bundle is a grouping of one or more software packages. Bundles contain one or more files that are installed to particular locations on a device, plus information about the bundle, such as version, description, what applications must also be present for it to be installed, and more.

ZENworks Linux Management uses Red Hat Package Manager (RPM). RPM is a powerful package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages on different devices.

ZENworks Linux Management supports the RPM format.

Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all devices assigned to the bundle (the bundle is directly assigned to devices, device groups, or device folders).

A file bundle lets you create a bundle containing one or more files of any type and distribute them to assigned devices. For example, you can include configuration files or data files in file bundles. A file bundle is useful to distribute any files that are not part of an RPM package.

When you create a bundle using the Create New Bundle Wizard, you are given the choice of creating an RPM package bundle, a preboot bundle, or a file bundle. A preboot bundle performs operations before the operating system boots. If you are familiar with ZENworks Desktop Management, preboot bundles are similar to imaging operations. For more information, see Part VI, "Preboot Services," on page 323.

You can also create bundle groups to collect several bundles to ease administration and to provide easier assigning and scheduling of the bundles in the bundle group.

For more information and step-by-step instructions, see Chapter 20, "Using RPM and File Bundles," on page 217.

18.2 Understanding Catalogs

A catalog is a collection of bundles; bundles included in a catalog are usually considered optional. You can use catalogs to deploy and install optional or dependent packages to assigned devices. If you deploy optional packages to devices by using a catalog, users can choose whether to deploy and install the software packages included in the bundles inside the catalog. Users use the ZENworks Linux Management Software Installer, Software Updater, and Software Remover applets to manage the software on managed devices. For more information, see Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54.

You can also use bundles in a catalog to provide dependent packages for a primary package contained in a bundle or in another catalog. For example, suppose you want to include Java Runtime in a catalog and, optionally, hide the catalog from the user interface. If a package contained in a bundle or in another catalog needs Java Runtime (it is listed as a dependency for the primary package), the package containing Java Runtime becomes mandatory and is deployed and installed on all devices that the primary package is deployed and installed on.

For more information and step-by-step instructions, see Chapter 22, "Using Catalogs," on page 271.

18.3 Understanding Dell Update Package Bundles

ZENworks Linux Management lets you mirror Dell Update Packages (DUPs) from the Dell FTP site or from a CD obtained from Dell support to your ZENworks server. Dell Update Packages let you update and configure hardware and system settings (including BIOS, DRAC, RAID, BMC, and FRMW configurations) on Dell PowerEdge servers.

For more information and step-by-step instructions, see Chapter 23, "Using Dell Update Package Bundles," on page 283.

18.4 Understanding the zlman Utility

The zlman utility is the command-line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use zlman.

The zlman utility lets you create and modify bundles, including adding packages to bundles and creating patch bundles. You can also use zlman to create and modify catalogs, including adding bundles to catalogs.

For more information, see zlman (1) (page 562).

18.5 Replicating Content in the ZENworks Management Zone

ZENworks Linux Management uses a hierarchical organization to simplify device management. At the top level, a ZENworks Management Zone provides an autonomous unit of ZENworks Servers and managed devices (workstations and servers). The ZENworks Servers manage the devices.

Each ZENworks Management Zone has one Primary Server, and optionally, one or more Secondary Servers to help distribute workload.

All RPM packages and Dell Update Packages must reside on the Primary Server. ZENworks Linux Management uses content replication to replicate packages to each Secondary Server in your Management Zone.

For more information, see Chapter 24, "Replicating Content in the ZENworks Management Zone," on page 291.

18.6 Mirroring Software

ZENworks Linux Management lets you connect to a remote server and copy software catalogs, bundles, or packages from the remote server to your server using a few simple commands.

Depending on your needs, you might have more than one ZENworks Management Zone in your system. To replicate content across Management Zones, you must use zlmmirror.

You also use mirroring to obtain Dell Update Packages from the Dell FTP site or from a CD obtained from Dell support.

For more information, see Chapter 25, "Mirroring Software," on page 293.

Understanding RPM Packages

<div style="text-align: right">19</div>

The RPM Package Manager is a system used to manage software packages. You can use this package format to distribute the software packages either in the precompiled binary form or the source code form. The RPM packages are usually targeted at particular distributions such as SLES 9 or SLED 9. An RPM package file is identified with a `.rpm` extension.

For example, the package format for the file `novell-zenworks-install-7.2-2-0.0.0.i386` is `novell-zenworks-install-7.2-2-0.0.0.i386.rpm`.

Review the following section to understand how to install the RPM packages:

19.1 Installing the RPM Packages

You can install an RPM package either from an RPM file located on the local file system, or from remote locations and repositories such as Yellow Dog Updater, Modified (YUM) and ZENworks® / YaST Packages Patches Patterns Products (ZYPP). The ZENworks Management Daemon automatically downloads packages from the repositories.

19.2 Understanding the RPM Repositories

An RPM repository, also known as a repo, is a storage location from which you can retrieve the software packages and install them on your device. You can also maintain these repositories on Internet servers.

For example, many Linux distributions use Advanced Packaging Tool or YUM to download and install the RPM packages from the repositories.

The following sections explain the different types of repositories and the distributions they are used in:

19.2.1 ZYPP Repository

The SLES 10 and SLED 10 media are ZYPP repositories.

19.2.2 YaST Online Update (YOU) Repository

The package updates from this repository are provided in terms of patches only. This repository updates the following distributions:

- SLES 9
- NLD
- OES 1

This repository is available at YaST Online Update (https://you.novell.com/update). This server requires authentication with your Novell account name and password.

19.2.3 RCE Repository

The RCE repository contains metadata files that contain the packages and patches along with their information. The ZENworks Linux Management 6.6 server hosts this repository. This repository updates the following distributions:

- NLD
- SLES 10 and SLED 10
- OES 1 (Linux)
- ZENworks Linux Management 7x, 6.x

This repository is available at Red Carpet Enterprise (https://update.novell.com/data). This server requires authentication with your Novell account name and password.

19.2.4 NU Repository

The NU repository is basically a collection of YUM repositories. The NU repository stores the actual RPM packages and patches. It also contains several metadata files that contain all the required information about the packages and patches. This repository updates the following distributions:

- OES 2
- SLES 10 and SLED 10
- SLE 10 SP1 (SLES 10 SP1 and SLED 10 SP1) or later

The NU repository is available at Novell update (https://nu.novell.com/repo). This server requires authentication with your Novell account name and password.

19.3 Understanding the Dependencies of RPM Packages

Each RPM package shares a list of binaries and libraries. These binaries and libraries might be required by other RPM packages during installation; if so, this creates a dependency. The RPM system cannot determine the packages that resolve such dependencies. So the ZENworks Management Daemon automatically searches for the packages in the repositories, and downloads them to resolve the dependencies.

For example, if you request to install package A that depends on package B, and package B depends on package C, the ZENworks Management Daemon automatically finds the dependent packages B and C from the available repositories or catalogs and installs them along with the requested package A.

19.4 Loading Base Packages

You should load the base packages from all the distributions of the managed devices into the catalogs on the ZENworks Linux Management server. This ensures that the base packages are optionally available to the agents and are used only to resolve package dependencies.

To load the packages from the distributions into the catalogs on the ZENworks Linux Management server, you must perform the following tasks in the order listed:

1 Create a package bundle in the ZENWorks Control Center. Alternatively, you can also use the `zlman bundle-create` command.

2 Mount the distribution media or iso and browse to and select the directories that contain packages you want to add to the bundle.

3 Add the directories to the package bundle by using the `zlman bundle-add-package <bundle name > <target> *.rpm` command.

> **IMPORTANT:** You must not assign this bundle directly to the managed devices. Doing so installs all the packages in the bundle on the agent.

4 Create a catalog and assign the bundle to it.

5 Assign the catalog to the required managed devices.

19.5 Patching the Client Systems

If you are using the SLES 10 ZENworks Linux Management agents, you can receive updates by registering with the Novell Customer Center. You can then apply these updates to your system by using the `rug/zen-updater` command. However, this process is not recommended in a ZENworks Linux Management setup because of the excessive usage of bandwidth by the SLES 10 agents to download the updates.

The best way to obtain updates is to periodically use zlmmirror to mirror the updates to the ZENworks Linux Management server, and then assign the mirrored bundle to the managed devices, which saves the Internet bandwidth. The zlmmirror has the advantage of mirroring updates from NU, YOU, YUM, RCE, and RHN repositories to which the ZENworks Linux Management agents cannot register directly. See the zlmmirror man pages for details.

Using RPM and File Bundles

20

Using Novell® ZENworks® Linux Management, you can install software using either a bundle or a catalog.

A bundle contains one or more files that are installed to particular locations on a device. A catalog is a collection of RPM bundles, Dell Update Package bundles, or bundle groups; bundles included in a catalog are usually considered optional. For more information about catalogs, see Chapter 22, "Using Catalogs," on page 271.

Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to devices, the device group, or the device folder).

The zlman utility is the command line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use zlman. For more information, see zlman (1) (page 562).

The following sections contain additional information:

- Section 20.1, "Understanding Bundles," on page 217
- Section 20.2, "Creating RPM Bundles," on page 218
- Section 20.3, "Creating File Bundles," on page 229
- Section 20.4, "Assigning Bundles," on page 238
- Section 20.5, "Editing Bundles," on page 241
- Section 20.6, "Adding Bundles to Catalogs," on page 245
- Section 20.7, "Creating Folders," on page 245
- Section 20.8, "Creating Bundle Groups," on page 247
- Section 20.9, "Adding Bundles to Existing Groups," on page 251
- Section 20.10, "Uninstalling Bundles from Devices," on page 252
- Section 20.11, "Deleting Bundles, Bundle Groups, and Folders," on page 255
- Section 20.12, "Renaming, Copying, or Moving Bundles," on page 256
- Section 20.13, "Deploying a Different Version of a Bundle," on page 257
- Section 20.14, "Using a Remote Execute Policy to Remove Bundles and Packages from Devices," on page 258
- Section 20.15, "Generating Bundle Reports," on page 261
- Section 20.16, "Best Practices for Adding Packages to Bundles," on page 262

20.1 Understanding Bundles

ZENworks Linux Management lets you create the following types of bundles:

- Section 20.1.1, "RPM Bundles," on page 218

Dell Update Package bundles are discussed in Chapter 23, "Using Dell Update Package Bundles," on page 283.

20.1.1 RPM Bundles

An RPM bundle is a grouping of one or more software packages. ZENworks Linux Management ships all software in this format. Bundles contain one or more files that are installed to particular locations on a system, plus information about the bundle, such as version, description, what applications must also be present for it to be installed, and more.

ZENworks Linux Management supports the RPM format.

For step-by-step instructions, see Section 20.2, "Creating RPM Bundles," on page 218.

20.1.2 Preboot Bundles

A preboot bundle performs operations before the operating system boots. If you are familiar with ZENworks Desktop Management, preboot bundles are similar to imaging operations.

For more information about preboot bundles, see Part VI, "Preboot Services," on page 323.

20.1.3 File Bundles

A file bundle lets you create a bundle containing one or more files of any type and distribute them to assigned devices. For example, you can include configuration files or data files in file bundles. A file bundle is useful to distribute any files that are not part of an RPM package.

For step-by-step instructions, see Section 20.3, "Creating File Bundles," on page 229.

20.2 Creating RPM Bundles

You can use the ZENworks Control Center or the zlman command line utility to create bundles. The following procedure explains how to create a bundle using the ZENworks Control Center. If you prefer the zlman command line utility, see the Bundle Commands section of zlman (1) (page 562).

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundle* list, click *New*, then click *Bundle* to display the Select Bundle Type page.
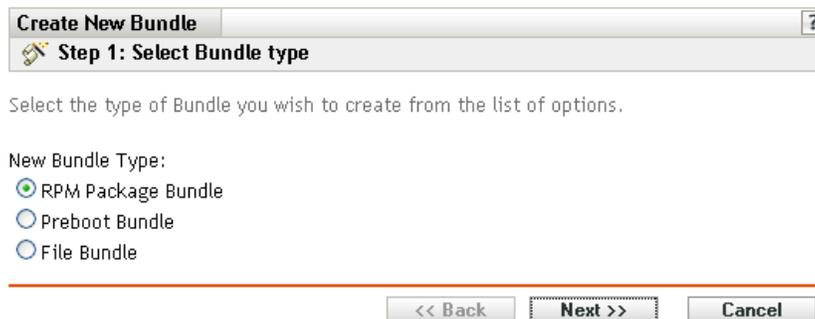
3 Select *RPM package bundle* (the default option), then click *Next* to display the Name and Description page.

For information about the other bundle types, see Part VI, "Preboot Services," on page 323, Chapter 23, "Using Dell Update Package Bundles," on page 283, and Section 20.3, "Creating File Bundles," on page 229.

4 Fill in the fields:

- **Name:** (Required) Provide a unique name for the RPM bundle. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Display name:** Provide a name that displays for users in the ZENworks Linux Management Update Client (installed on managed devices during the ZENworks Agent installation) when they update software. The display name can be the same name that you provided in the *Name* field; however, you can choose to make the name more intuitive for users.

- **Folder:** Type the name or browse to the folder that this bundle will be created in. Folders display in the ZENworks Control Center. The default folder is /Bundles.

- **Ensure this Bundle Stays Installed on all Assigned Devices (Ensure Persistence):**

  (Selected by default.) If this option is selected, the packages inside the RPM bundle are initially installed according to the bundle's schedule and the packages are reinstalled on assigned devices if they are removed in the future. If this option is not selected, the packages are installed initially according to schedule, but the packages are not checked to

see if they have been removed from assigned devices and the packages are never reinstalled. This option applies to RPM bundles only; it does not apply to preboot, file, or Dell Update Package (DUP) bundles.

- **Description:** Provide a short description of the bundle's contents. This description displays in the ZENworks Control Center and in the ZENworks Linux Management Updater applet, which is the user interface for updating software.

5 Click *Next* to display the Packages page.

Use the Packages page to upload RPM packages to the bundle or to import RPM packages contained in the ZENworks Linux Management package repository. The packages that you upload to a bundle must already exist on the local device on which you are running the ZENworks Control Center. During the bundle-creation process, packages are copied to the ZENworks Server and placed in the package repository (`/var/opt/novell/zenworks/pkg-repo`).

Create New Bundle	Bundle_1					
🗞 Step 3: Packages						

Add the RPMs that will be included in this Bundle.

Packages						
Add ▾ Remove Action ▾						
☐ Name ▲	Version	Summary	Operating System	Architecture	Install Type	Freshen
No items available.						
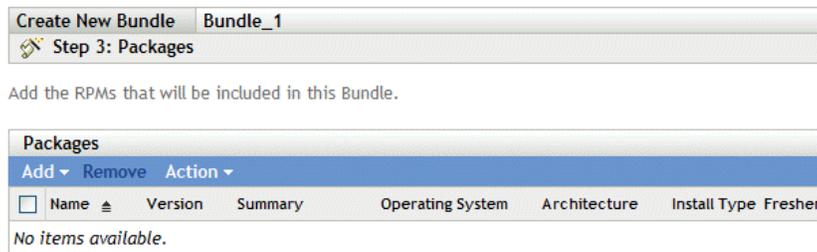
6 Add the RPM packages to include in the bundle using the *Upload RPM* and the *Import from Repository* options.

You can use either the *Upload RMP* option or the *Import from Repository* option, or you can use both options, depending on your needs.

After you upload or import packages into the list, you can view the details of a selected package by clicking the underlined link in the *Name* column. You can remove a selected package from the list by using the *Remove* option.

6a (Optional) Click *Add > Upload RPM* to open the RPM File Upload dialog box, then fill in the fields:
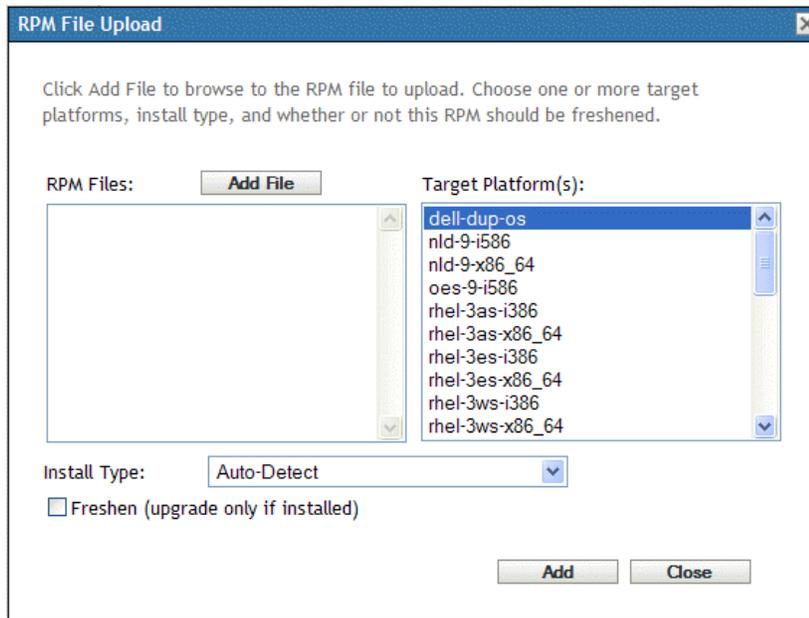
Add file: Click *Add File* to open the RPM File Upload dialog box. Browse to and select the RPM packages that you want to add to the bundle. The RPM packages must be located on the local device on which you are running the ZENworks Control Center. Click *OK* to upload the packages to the ZENworks Linux Management server. The package repository is the `/var/opt/novell/zenworks/pkg-repo` directory on the ZENworks Server.

Target platforms: Select one or more platforms from the *Target Platforms* list. You can press `Shift+click` or `Ctrl+click` to select multiple platforms.

The target platform is the platform of the devices that the package will be installed on. ZENworks Linux Management does not auto-detect the target platform by examining the RPM packages because RPM packages are not limited to working on only one platform; RPM packages can be created to work on multiple platforms. For this reason, the administrator must select the platform of the target devices.

NOTE: Bundles can be installed on any platform; bundles are not platform-specific. The packages contained in bundles are platform-specific and can be installed only on devices supporting the specified platform.

You can, however, create a bundle containing several packages that apply to various Linux platforms. When the bundle is assigned to a group of devices or to a folder that contains devices running on different platforms, each managed device gets the appropriate packages installed.

For example, you could create a bundle containing two packages: PackageA and PackageB. PackageA applies to suse-93-i586, rhel-3es-i386, and sles-9-i586. PackageB applies to rhel-3es-i386 only. If you assign the bundle to a folder containing three devices, with each device running one of these platforms, the bundle will be installed on all three devices; however, PackageA will be installed on all three devices and PackageB will be installed only on the device running rhel-3es-i386.

For this reason, the ZENworks Control Center might indicate that a bundle is effective for a device even if one or several packages contained in the bundle was not installed.

If you want a bundle to be platform-specific, you must use a script and have the script verify the target platform before deploying and installing the bundle.

Install type: Use the Install type drop-down list to choose from the following installation options:

- ◆ **Auto-detect:** Automatically detects whether the bundle is already installed on assigned devices and either installs the bundle or updates an existing bundle, if necessary. Basically, the *Auto-detect* option determines whether the *Update* or the *Install* option functionality (explained below) is best, and then performs that operation. Any kernel packages are installed using the *Install* option functionality; other packages are installed using the *Update* option functionality. This is the default option and should be used in most situations.

- ◆ **Update:** Updates the packages on assigned devices if the packages in the bundle are newer than what is installed on the devices. If the packages are not installed on the assigned devices, ZENworks Linux Management installs them. With the *Update* option, you don't need to worry whether a package is already installed because the package is either updated (if needed) or installed on the device. Parallel installation of a package is not possible with the *Update* option.

- ◆ **Install:** Installs the bundle on all assigned devices. If previous versions of the packages exist on the devices, ZENworks Linux Management does not update the existing packages. As a result, packages can be installed multiple times (parallel installations), which might cause overlap issues. This option is rarely used; you should use the default option, *Auto-detect*, under most circumstances. You should use this option almost exclusively to install kernel packages.

Freshen (upgrade only if installed): Use this option to transact a package only if a previous version of the package is already installed on the device. You can use the *Freshen* option in conjunction with the *Auto-detect*, *Update*, or *Install* options.

6b (Optional) Click *Add > Import from repository* to open the Package Import dialog box, then select the packages to import. You can use the Search options on the right side of the Package Import dialog box to locate packages.
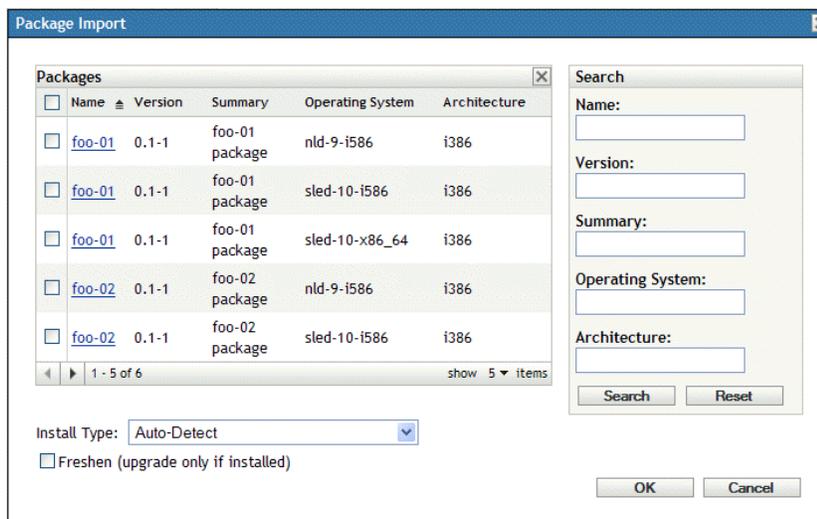
6c Select an install type from the drop-down list:

- **Auto-detect:** Automatically detects whether the bundle is already installed on assigned devices and either installs the bundle or updates an existing bundle, if necessary. Basically, the *Auto-detect* option determines whether the *Update* or the *Install* option functionality (explained below) is best, and then performs that operation. Any kernel packages are installed using the *Install* option functionality; other packages are installed using the *Update* option functionality. This is the default option and should be used in most situations.

- **Update:** Updates the packages on assigned devices if the packages in the bundle are newer than what is installed on the devices. If the packages are not installed on the assigned devices, ZENworks Linux Management installs them. With the *Update* option, you don't need to worry whether a package is already installed because the package is either updated (if needed) or installed on the device. Parallel installation of a package is not possible with the *Update* option.

- **Install:** Installs the bundle on all assigned devices. If previous versions of the packages exist on the devices, ZENworks Linux Management does not update the existing packages. As a result, packages can be installed multiple times (parallel installations), which might cause overlap issues. This option is rarely used; you should use the default option, *Auto-detect*, under most circumstances. You should use this option almost exclusively to install kernel packages.

6d (Optional) Select the *Freshen* option.

The *Freshen* option transacts a package only if a previous version of the package is already installed on the device. You can use the *Freshen* option in conjunction with the *Auto-Detect, > Update*, or *Install* options.

7 Click *Next* to display the Scriptable Actions page.

The Scriptable Actions page lets you configure the script engine that you want to use and the scripts you want to execute.

As part of the process of distributing a bundle, ZENworks Linux Management can launch scriptable actions that will be executed before and after the bundle is distributed, installed, and uninstalled. For example, you can get data files from a Web server before installing an application that uses them, run applications, and so forth.

NOTE: You can configure multiple scripts for each bundle. Repeat the configuration process as many times as desired, choosing different options from the *Scriptable Action* and *Executable Type* drop-down lists, explained below.

8 Click *New* to display the New Scriptable Action dialog box.

New Scriptable Action

Scriptable Action:	Pre-Distribution
Executable type:	Script
Maximum waiting time:	○ Do not wait ◉ Wait till the program completes the execution ○ Wait for ____ sec
Script to run:	Specify a file
Script file name: *	____ (e.g. /usr/local/xyz.pl)
Script parameters:	____ (e.g. abc efg)
Script engine: *	____ (e.g. /usr/local/bin/perl)
Script engine parameters:	____ (e.g. -c abc -s efg)

OK   Cancel

9 Fill in the fields:

9a Scriptable Action: Select one of the following actions:

- **Pre-distribution/post-distribution:** Lets you perform tasks that must be done before or after a bundle is deployed to assigned devices. Deploying a bundle means that the packages or files inside the bundle are downloaded from the ZENworks server to the assigned devices. The packages and files are not yet available for use.

- **Pre-installation/post-installation:** Lets you perform tasks that must be done before or after a bundle is installed. Installing a bundle means that the software packages and files are installed to assigned devices and available for use.

- **Pre-uninstallation/post-installation:** Lets you perform tasks that must be done before a bundle is uninstalled. Uninstalling a bundle means that the software packages and files are uninstalled on assigned devices and no longer available for use.

9b Executable type: Select one of the following actions:

- **Script:** Specify a shell script that executes on assigned devices.

- **Binary:** Specify an executable program that runs on assigned devices.

- **Java:** Specify a Java executable class that launches on assigned devices.

9c Maximum waiting time: Select one of the following options:

- **Do not wait:** Specify that the ZENworks Management Daemon (ZMD) does not block while the script completes.

- **Wait until the program completes the execution:** Specify that ZMD blocks until the script completes.

- **Wait for _ sec:** Specify that ZMD blocks until the script completes and the specified number of seconds expires.

9d (Conditional) If you chose *Script* in Step 9b, fill in the fields:

- **Script to run:** Choose an option from the drop-down list:

  - **Specify a file:** Lets you specify a file that is already on the device on which you are running the ZENworks Control Center. If you choose this option, fill in the remaining fields in the dialog box, as described below.

  - **Define your own script:** Lets you type a script in the ZENworks Control Center. If you choose this option, a text box displays where you type your script. This script is delivered to the assigned devices as part of the bundle and is executed in the standard device shell environment. With this option, there are no additional options to configure.

- **Script filename:** (Required) Specify the path to the script file on the target device, for example, `/usr/local/xyz.pl`.

- **Script parameters:** Specify any additional parameters you want to place on the command line after the script filename is specified. This results in parameters being passed to your executable script.

- **Script engine:** (Required) Specify the interpreter that launches to run your script, for example, `/usr/local/bin/perl`.

- **Script engine parameters:** Specify any parameters you want included on the command line when the script engine launches.

9e (Conditional) If you chose *Binary* in Step 9b, fill in the fields:

- **Executable filename:** (Required) Specify the path to the executable file. This file must already exist on the device on which you are running the ZENworks Control Center.

- **Executable file parameters:** Specify any additional parameters you want to place on the command line when the executable file launches.

9f (Conditional) If you chose *Java* in Step 9b, fill in the fields:

- **Java program name:** (Required) Type the class path to the class file you want to launch, for example, `com.novell.TestProg`.

- **Program parameters:** Specify any additional parameters to pass to the Java class at execution time.

- **Java Runtime Executable (JRE):** (Required) Specify the path to the JRE* that launches the class, for example, `/usr/local/JRE/bin/java`. The JRE must be already installed on the assigned device.

- **JRE parameters:** Specify any parameters you want to pass to the JRE system, for example, `-cp/usr/lib/tools.jar`.

10 Click *Next* to display the Summary page, then review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary.

Depending on your needs, you can create the bundle now or you can configure additional options for this bundle.

11 Click *Finish* to create the bundle as configured per settings on the Summary page. If you click *Finish*, the bundle is created but it does not have devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the bundle by continuing with Section 20.4, "Assigning Bundles," on page 238.

or

Click *Next* to display the Bundle Assignment page to perform the following tasks:

- Specify assignments for this bundle
- Specify special flags, such as flags to specify to remove conflicting packages or trying a dry run to test a bundle's deployment
- Specify the deployment schedule for this bundle
- Specify the installation schedule for this bundle
- Specify groups for this bundle

Create New Bundle	Bundle_1	?
⚙ Step 6: Bundle Assignments		

Specify the assignments for this bundle:

Add **Remove**	
☐ **Name**	**In Folder**
☐ 📁 Workstations	/Devices

`<< Back`   `Next >>`   `Cancel`

12 Assign the bundle to the devices that you want to distribute the bundle to.

12a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

12b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.

12c Click *OK*.

13 Click *Next* to display the Bundle Options page.

14 (Optional) Specify the desired Special Flag options:

 * **Remove conflicting packages:** Select this option to specify that conflicting packages are uninstalled from devices before installing new packages. By default, this option is selected, so conflicting packages (previous versions of the same package, for example) are uninstalled before the current package is installed. If this option is not selected, packages are not installed if a conflict is detected.

 * **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle can be successfully deployed. If there are any issues that could prevent the RPM bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/log/zenworks`.

   A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

 * **Bundle lock:** Select this option to lock bundles on the managed devices from the server.

   You can also use the command line utility to lock the bundles. The Bundle lock option is only available during the assignment of bundle or bundle groups to the managed devices. For more information, see Section 21.2, "Locking and Unlocking a Bundle on a Managed Device," on page 266

15 Specify the desired Scheduling options:

 * **Deploy and install at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

   The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.

Schedule Type	Description
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

- ◆ **Deploy and install at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

  The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

  The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

  The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

- ◆ **Deploy and install immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle deploy and install immediately when the Wizard completes, providing that the assigned devices are online. The packages inside the bundle deploy to and install on devices that are not online when they refresh.

16 Click *Next* to display the Bundle Groups page.

17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired bundle groups and display their names in the Selected list box.

Using bundle groups eases administration efforts by letting you group several bundles so you can use common assignments, schedules, and so forth, rather than configuring these settings for each bundle you create.

18 Click *Next* to display the Summary page.

19 Review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Summary page.

20 Click *OK*.

20.3 Creating File Bundles

You can use the ZENworks Control Center or the zlman command line utility to create file bundles. The following procedure explains how to create a file bundle using the ZENworks Control Center. If you prefer the zlman command line utility, see the Bundle Commands section of zlman (1) (page 562).

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the Bundle list, click *New*, then click *Bundle* to display the Select Bundle Type page.
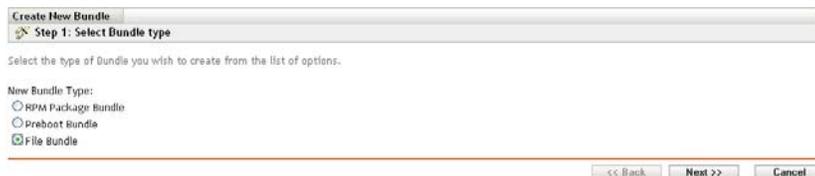
3 Select *File bundle*, then click *Next to display the Name and Description page.*

For more information about the other two bundle types, see Section 20.2, "Creating RPM Bundles," on page 218 and Part VI, "Preboot Services," on page 323.

4 Fill in the fields:

- **Name:** (Required) Provide a unique name for the file bundle. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Display name:** Provide a name that displays for users when they update software. The display name can be the same name that you provided in the *Name* field; however, you can choose to make the name more intuitive for users.

- **Folder:** Type the name or browse to the folder that this bundle will be created in. Folders display in the ZENworks Control Center. The default folder is /Bundles.

- **Description:** Provide a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Updater applet, which is the user interface for updating software.

5 Click *Next* to display the Files page to add the files to include in this bundle.

6 Add the files to include in the bundle using the *Upload* and the *Import from bundle* options.

The files that you upload to a bundle must already exist on the local device on which you are running the ZENworks Control Center. You can use either the *Upload* option or the *Import from bundle* option, or you can use both options, depending on your needs.

After you upload or import files into the list, you can remove a selected package from the list by using the *Remove* option.

6a (Optional) Click *Add > Upload* to open the File Upload dialog box, then fill in the fields:
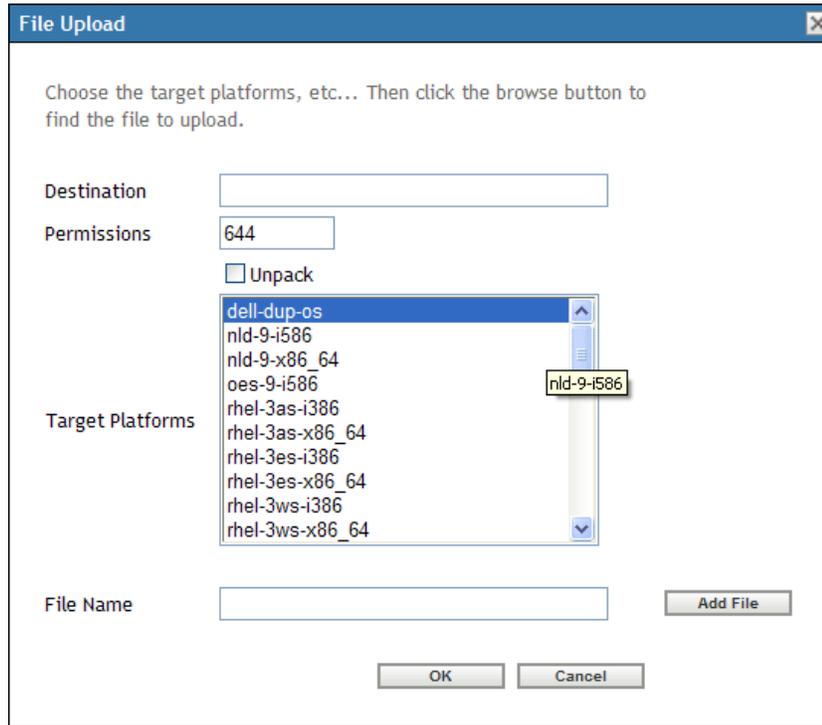
Destination: Specify the full path of the destination where the files will be deployed on the assigned devices.

Permissions: Specify the UNIX file permissions to be applied to the files after deployment. A reasonable standard for file permissions is 644. This option is not applicable for compressed files.

Unpack: Select *Unpack* to indicate that the files are compressed and should be decompressed and extracted on the assigned devices. If you select *Unpack*, the *Permissions* option is not applicable. The supported compression formats are `tar.gz` and `tar.bz2`.

Target platforms: Select one or more platforms from the *Target Platforms* list. You can press `Shift+click` or `Ctrl+click` to select multiple platforms.

File to upload: Browse to and select the files that you want to add to the bundle. The files must be located on the local device on which you are running the ZENworks Control Center. Click *OK* to upload the files to the ZENworks Linux Management server.

If an existing file bundle is upgraded, and during upgrade if you remove one or more files from the bundle, the newer version of the bundle is deployed on the managed device but the files removed from the file bundle is not removed from the managed device. To remove files deployed through a file bundle, disassociate the file bundle from the managed device.

6b (Optional) Click *Add > Import from bundle* to open the File Import dialog box, fill in the fields, then click *OK*.
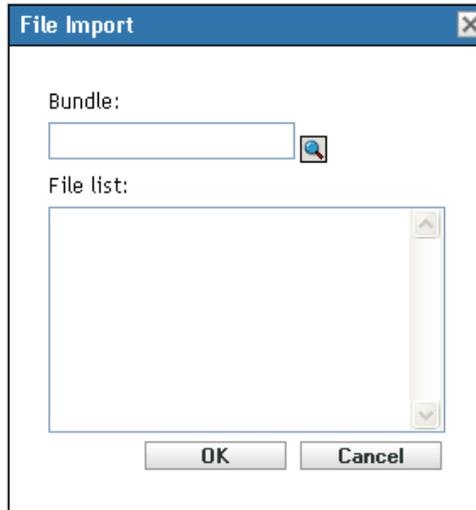
The ZENworks Server contains all of the files that are included in bundles defined within your Management Zone. The package repository is the `/var/opt/novell/zenworks/pkg-repo` directory on the ZENworks Server. When you add a file or RPM package to a bundle, the file or package is automatically uploaded to the package repository.

Bundle: Browse to and select the bundle you want to import packages from.

File list: Select the files to import.

7 Click *Next* to display the Scriptable Actions page.

The Scriptable Actions page lets you configure the script engine that you want to use and the scripts you want to execute.

As part of the process of distributing a bundle, ZENworks Linux Management can launch scriptable actions that will be executed before and after the bundle is distributed, installed, and uninstalled. For example, you can get data files from a Web server before installing an application that uses them, run applications, and so forth.

NOTE: You can configure multiple scripts for each bundle. Repeat the configuration process as many times as desired, choosing different options from the Scriptable Action and Executable Type drop-down lists, explained below.

8 Click New to display the New Scriptable Action dialog box.

9 Fill in the fields:

9a **Scriptable Action:** Select one of the following actions:

* **Pre-distribution/post-distribution:** Lets you perform tasks that must be done before or after a bundle is deployed to assigned devices. Deploying a bundle means that the packages or files inside the bundle are downloaded from the ZENworks server to the assigned devices. The packages and files are not yet available for use.

* **Pre-installation/post-installation:** Lets you perform tasks that must be done before or after a bundle is installed. Installing a bundle means that the software packages and files are installed to assigned devices and available for use.

* **Pre-uninstallation/post-installation:** Lets you perform tasks that must be done before a bundle is uninstalled. Uninstalling a bundle means that the software packages and files are uninstalled on assigned devices and no longer available for use.

9b **Executable type:** Select one of the following actions:

* **Script:** Specify a shell script that executes on assigned devices.

* **Binary:** Specify an executable program that runs on assigned devices.

* **Java:** Specify a Java executable class that launches on assigned devices.

9c **Maximum waiting time:** Select one of the following options:

* **Do not wait:** Specify that the ZENworks Management Daemon (ZMD) does not block while the script completes.

- ◆ **Wait until the program completes the execution:** Specify that ZMD blocks until the script completes.
- ◆ **Wait for _ sec:** Specify that ZMD blocks until the script completes and the specified number of seconds expires.

9d (Conditional) If you chose *Script* in Step 9b, fill in the fields:

- ◆ **Script to run:** Choose an option from the drop-down list:
  - ◆ **Specify a file:** Lets you specify a file that is already on the device on which you are running the ZENworks Control Center. If you choose this option, fill in the remaining fields on the dialog box, as described below.
  - ◆ **Define your own script:** Lets you type a script in the ZENworks Control Center. If you choose this option, a text box displays where you type your script. This script is delivered to the assigned devices as part of the bundle and is executed in the standard device shell environment. With this option, there are no additional options to configure.
- ◆ **Script filename:** (Required) Specify the path to the script file on the target device, for example, `/usr/local/xyz.pl`.
- ◆ **Script parameters:** Specify any additional parameters you want to place on the command line after the script filename is specified. This results in parameters being passed to your executable script.
- ◆ **Script engine:** (Required) Specify the interpreter that launches to run your script, for example, `/usr/local/bin/perl`.
- ◆ **Script engine parameters:** Specify any parameters you want included on the command line when the script engine launches.

9e (Conditional) If you chose *Binary* in Step 9b, fill in the fields:

- ◆ **Executable filename:** (Required) Specify the path to the executable file. This file must already exist on the device on which you are running the ZENworks Control Center.
- ◆ **Executable file parameters:** Specify any additional parameters you want to place on the command line when the executable file launches.

9f (Conditional) If you chose *Java* in Step 9b, fill in the fields:

- ◆ **Java program name:** (Required) Type the class path to the class file you want to launch, for example, `com.novell.TestProg`.
- ◆ **Program parameters:** Specify any additional parameters to pass to the Java class at execution time.
- ◆ **Java Runtime Executable (JRE):** (Required) Specify the path to the JRE that launches the class, for example, `/usr/local/JRE/bin/java`. The JRE must be already installed on the assigned device.
- ◆ **JRE parameters:** Specify any parameters you want to pass to the JRE system, for example, `-cp/usr/lib/tools.jar`.

10 Click *Next* to display the Summary page, then review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary.

Depending on your needs, you can create the bundle now or you can configure additional options for this bundle.

11 Click *Finish* to create the bundle as configured per settings on the Summary page. If you click *Finish*, the bundle is created but it does not have devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the bundle by continuing with Section 20.4, "Assigning Bundles," on page 238.

or

Click *Next* to display the Bundle Assignment page to perform the following tasks:

- ◆ Specify assignments for this bundle
- ◆ Specify special flags, such as flags to specify to remove conflicting packages or trying a dry run to test a bundle's deployment
- ◆ Specify the deployment schedule for this bundle
- ◆ Specify the installation schedule for this bundle
- ◆ Specify groups for this bundle

Create New Bundle	Bundle_1		?
	Step 6: Bundle Assignments		

Specify the assignments for this bundle:

Add Remove	
☐ **Name**	**In Folder**
☐ 📁 Workstations	/Devices

[<< Back] [Next >>] [Cancel]

12 Assign the bundle to the devices that you want to distribute the bundle to.

12a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

12b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.

12c Click *OK*.

13 Click *Next* to display the Bundle Options page.

Create New Bundle   test11   [?]

Step 7: Bundle Options

Set special flags for Bundles(only), which affects how the bundle will be handled. Configure the deployment, and installation
schedules if Bundle or update schedules if Catalog.

Special Flags
☑ Remove conflicting packages
☐ Attempt a dry run
☐ Bundle lock

Scheduling
◉ Deploy and install at a scheduled time:
   Schedule:
   [Relative to Refresh]   🕐
◯ Deploy and install at separate scheduled times:
   Deployment Schedule:
   [Relative to Refresh]   🕐

   Installation Schedule:
   [Relative to Refresh]   🕐
◯ Deploy and install immediately (when this wizard completes)

   [<< Back]   [Next >>]   [Cancel]

14 (Optional) Select the *Bundle lock* special flag to lock bundles on the managed devices from the server.

You can also use the command line utility to lock the bundles. For more information, see Section 21.2, "Locking and Unlocking a Bundle on a Managed Device," on page 266

The *Remove conflicting packages* and *Attempt a dry run* special flags are not applicable for File Bundles.

15 Specify the desired Scheduling options:

   ◆ **Deploy and install at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

   The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

   ◆ **Deploy and install at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

   The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

◆ **Deploy and install immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

16 Click *Next* to display the Bundle Groups page.

Create New Bundle   Bundle_1   [?]
Step 8: Bundle Groups

Specify the groups for this bundle:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

〈〈 Back   Next 〉〉   Cancel

17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired bundle groups and display their names in the Selected list box.

Using bundle groups eases administration efforts by letting you group several bundles so you can use common assignments, schedules, and so forth, rather than configuring these settings for each bundle you create.

18 Click *Next* to display the Summary page.

19 Review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Summary page.

20 Click *OK*.

20.4 Assigning Bundles

When you create RPM bundles, file bundles, or bundle groups, you have the choice of assigning the object as part of the creation process, or you can create the object without assigning it.

If you created the object without assigning it, the object was created without assigning devices to it, specifying deployment and installation schedules, setting special flags, and so forth. Before the object can be deployed and installed on assigned devices, you must complete the following steps. If you assigned the object during its creation, you have already performed the following procedure.

1 In the ZENworks Control Center, click the *Bundles* tab, select the desired bundle or bundle group in the *Bundles* list by clicking the box next to its name, click *Action*, then click *Assign Bundle* to display the Devices to be Assigned page.

```
Assign Bundle                                              [?]
    Step 1: Devices to be Assigned

Select the devices to be assigned to the previously selected bundles.

  Add  Remove
  ☐   Name                        In Folder
No items selected, click add to select items


                       << Back      Next >>      Cancel
```

2 Assign the bundle or bundle group to the devices that you want to distribute the bundle or bundle group to.

  2a Click *Add* to browse for and select the appropriate Server or Workstation objects.

  You can also select Folder or Group objects.

  2b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

  Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.

  2c Click *OK*.

3 Click *Next* to display the Bundle Options page.

4 (Optional) Specify the desired Special Flag options:

- ◆ **Remove conflicting packages:** Select this option to specify that conflicting packages and files are uninstalled from devices before installing new packages and files. By default, this option is selected, so conflicting packages and files (previous versions of the same package, for example) are uninstalled before the current package or file is installed. If this option is not selected, packages and files are not installed if a conflict is detected. This option is not applicable for File bundles.

- ◆ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle or files can be successfully deployed. If there are any issues that could prevent the RPM bundle or file bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/log/zenworks`. This option is not applicable for File bundles.

  A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

- ◆ **Bundle lock:** Select this option to lock bundles on the managed devices from the server.

  You can also use the command line utility to lock the bundles. For more information, see Section 21.2, "Locking and Unlocking a Bundle on a Managed Device," on page 266

5 Specify the desired Scheduling options:

- ◆ **Deploy and install at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

  The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.

Schedule Type	Description
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

◆ **Deploy and install at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

◆ **Deploy and install immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

6 Click *Next* to display the Finish page.

7 Review the information on the Finish page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Summary page.

8 Click *OK*.

20.5 Editing Bundles

You can edit an existing bundle to change its description, add or remove assignments, add or remove the bundle from existing catalogs or bundle groups, add or remove packages from the bundle, deploy a different version of the bundle, and more.

You can use the ZENworks Control Center or the zlman command line utility to edit bundles. The following procedure explains how to edit a bundle by using the ZENworks Control Center. If you prefer the zlman command line utility, see the Bundle Commands section of zlman (1) (page 562).

To edit a bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.
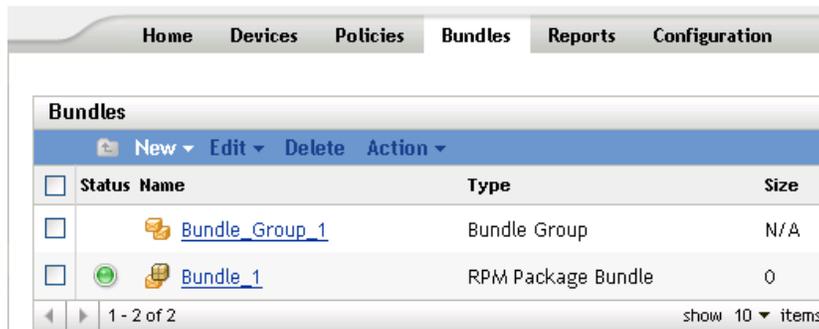
2 Click the bundle's name to display the Summary page, then make the desired configuration changes as explained below.

Use the Summary page to view detailed information about the selected bundle. This page provides general information about the bundle, lists the individual devices that are assigned to the bundle, displays an event log, shows upcoming events, and lists the catalogs or groups that the bundle belongs to.

You can also use this page to edit the bundle group's description, add or remove assignments for the bundle, and change other configuration settings, as described below.

2a Review the information in the *General* section, then make the desired configuration changes (you can edit only the *Description* in this section).

Size: Displays the number of packages that make up the bundle.

Version: Displays the bundle's version number. You can have multiple versions of the same bundle. If you click the *Details* tab on this page and make any configuration changes, the version number increments.

Number of errors not acknowledged: An error is anything that causes the deployment or installation of the bundle to fail. The number displayed indicates the number of unacknowledged errors, which display in the *Event Log* section below.

Number of warnings not acknowledged: A warning is anything that does not cause the deployment or installation of the bundle to fail, but indicates minor problems with the packages or bundle. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the bundle. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the bundle was created. The description provides a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the user interface.

Click *Edit* to change the bundle group's description, if necessary.

2b Review the information in the *Assignments* section, then make the desired configuration changes.

The *Assignments* section lists the devices that are assigned to the selected bundle. You can click the device name to view information about each device that is directly assigned to the bundle, including its schedule and other options.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page, which includes a list of the devices that are assigned to the selected bundle, the folder that contains each device, each device's deployment and installation schedule, and whether the *Allow remove* , *Dry run* and *Bundle Lock* options are enabled. You can use the Edit Assignments page to edit certain settings, such as the deployment and installation schedules as well as the *Allow remove*, *Dry run* options and *Bundle Lock*.

Add: Click *Add* to launch the Assign Bundle Wizard to select the devices to be assigned to the selected bundle. For more information, see Section 20.4, "Assigning Bundles," on page 238.

Remove: Select the device by clicking the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this bundle.

Action > Deploy and Install Now: Click *Action > Deploy and Install Now* to immediately deploy and install the bundle on the selected device (without regard to its schedule or waiting for a device refresh). To access the *Action* menu, you must select a device or device folder by clicking the check box next to its name.

2c Review the information in the *Event Log* section, then make the desired changes.

The *Event Log* section lists all unacknowledged errors and warnings.

The *Status* column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the *Event* column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the *Date* column to indicate that the item has been acknowledged).

2d Review the information in the *Upcoming Events* section.

The *Upcoming Events* section lists events scheduled for the selected bundle. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month. Click *Refresh* to see upcoming events for the selected bundle.

2e Review the information in the *Catalogs/Groups* sections, then make the desired configuration changes.

The *Catalogs/Groups* sections list the catalogs and groups that contain the selected bundle.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Catalogs/Groups page to display a list of the catalogs and groups that contain the selected bundle. You can click *Add* to open the Select Groups dialog box to add the selected bundle to existing catalogs or groups. You can also remove a bundle or group by clicking the check box next to the *Name* column, then clicking *Remove* to remove the bundle from that catalog or group.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the *Select* column to select the desired catalog or group and display its name in the *Selected* list box.

Remove: Select the device by clicking the check box next to the appropriate catalog or bundle name, then click *Remove* to remove the selected bundle from the catalog or group.

3 Click the *Details* tab, then make the desired configuration changes.

Use the Details page to view detailed information about the selected bundle, such as the bundle's version number, name and display name, folder, description, a list of the individual RPM packages that make up the bundle, and the distribution/installation/uninstallation scripts that the bundle will use.

You can also use the options on this page to deploy a different version of the selected bundle to assigned devices, delete a particular version of the bundle, add or remove packages from the bundle, and change the script engine and scripts that you want to use for the bundle.

3a Review the information in the *RPM Package Bundle Settings* section, then make the desired configuration changes.

Version: Displays the selected bundle's version number. You can have multiple versions of the same bundle. If you make any configuration changes on this page (changing the display name or description, adding a package to or removing a package from the bundle, or adding or modifying a script), the version number increments. You can use the *Version* drop-down list to view the details of each version of the selected bundle. Text below the *Version* box informs you which version of the bundle is deployed on assigned devices.

Deploy: Lets you deploy a different version of the currently deployed bundle. Use the *Version* drop-down list to select the desired version number, then click *Deploy*.

Only one version of a bundle can be deployed at any given time. For example, suppose a bundle has multiple versions: 1, 2, and 3. If version 1 is currently deployed, all associated devices have version 1 of the bundle deployed. If you then make version 3 the deployed version, all devices with version 1 deployed and still associated to that bundle will be automatically upgraded to version 3.

Delete: Lets you delete a version of the currently deployed bundle. Use the *Version* drop-down list to select the desired version number, then click *Delete*.

Copy: Lets you copy a version of the selected bundle. Use the *Version* drop-down list to select the desired version number, then click *Copy*. You can then alter the settings of the copied version to create a new version of the bundle.

If you create a copy of the YOU patch bundle, the copied version is converted to the RPM package bundle type. Before deploying the RPM package bundle to the device, you must remove the patch RPMs from the bundle. However, you cannot install the copied version of the YOU patch bundle if it contains only scripts.

Display name: Displays the name that displays for users when they update software. The display name, which can be more intuitive for users, was provided when the bundle was created. You can edit the display name.

Description: Displays a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Update Client, which is the user interface. You can edit the description.

Enforce Persistence: (Selected by default.) If this option is selected, the packages inside the RPM bundle are initially installed according to the bundle's schedule and the packages are reinstalled on assigned devices if they are removed in the future. If this option is not selected, the packages are installed initially according to schedule, but the packages are not checked to see if they have been removed from assigned devices and the packages are never reinstalled. This option applies to RPM bundles only; it does not apply to preboot, file, or Dell Update Package (DUP) bundles.

3b Review the information in the *Packages* section, then make the desired configuration changes.

The *Packages* section displays the RPM packages contained in the selected bundle. Use the *Packages* section to upload RPM packages to the bundle, to import RPM packages contained in the ZENworks Linux Management package repository, or to remove packages from a bundle. The packages that you upload to a bundle must already exist on the local device on which you are running the ZENworks Control Center, or you can import packages from the package repository.

You can use the following options:

Upload RPM: Click *Add > Upload RPM* to open the RPM File Upload dialog box. For more information, see .

Import from repository: Click *Add > Import from repository* to open the Package Import dialog box. For more information, see .

Remove: Click *Remove* to remove the selected packages from the bundle, as needed. The packages removed from the deployed version of the bundle are uninstalled from the managed devices only when a new version of the bundle is deployed.

To remove the patch RPMs from the YOU patch bundle, you must first create a copy of the YOU patch bundle, then remove the patches from the copied version of the bundle.

To create a copy of the YOU patch bundle:

1. Click the *Copy* button located at the top of the page.

2. In the Copy dialog box, specify a name for the copy version.

3. Click *OK*.

You cannot install the copied version of the YOU patch bundle if it contains only scripts.

Set Freshen: Click *Action > Set Freshen* to transact a package only if a previous version of the package is already installed on the device. You can use the Freshen option in conjunction with the Auto-Detect, Update, or Install options available in *Edit*.

Unset Freshen: Click *Action > Unset Freshen* to turn off Freshen; the package is transacted regardless if the package is already installed on the device or not.

Edit: Click *Action > Edit* to display the RPM File Upload dialog box where you can change the selected package's install type and *Freshen* option.

Install type: Click *Action > Edit > Install Type* to use the Install type drop-down list to choose from the following installation options:

- **Auto-detect:** Automatically detects whether the bundle is already installed on assigned devices and either installs the bundle or updates an existing bundle, if necessary. Basically, the *Auto-detect* option determines whether the *Update* or the

Install option functionality (explained below) is best, and then performs that operation. Any kernel packages are installed using the *Install* option functionality; other packages are installed using the *Update* option functionality. This is the default option and should be used in most situations.

◆ **Update:** Updates the packages on assigned devices if the packages in the bundle are newer than what is installed on the devices. If the packages are not installed on the assigned devices, ZENworks Linux Management installs them. With the *Update* option, you don't need to worry whether a package is already installed because the package is either updated (if needed) or installed on the device. Parallel installation of a package is not possible with the *Update* option.

◆ **Install:** Installs the bundle on all assigned devices. If previous versions of the packages exist on the devices, ZENworks Linux Management does not update the existing packages. As a result, packages can be installed multiple times (parallel installations), which might cause overlap issues. This option is rarely used; you should use the default option, *Auto-detect*, under most circumstances. You should use this option almost exclusively to install kernel packages.

Freshen (upgrade only if installed): Use this option to transact a package only if a previous version of the package is already installed on the device. You can use the *Freshen* option in conjunction with the *Auto-detect*, *Update*, or *Install* options.

NOTE: To view details about each package, click the desired package in the *Name* column.

3c Review the information in the *Scriptable Actions* section, then make the desired configuration changes.

As part of the process of distributing a bundle, ZENworks Linux Management can launch scriptable actions that will be executed before and after the bundle is distributed, installed, and uninstalled. For example, you can get data files from a Web server before installing an application that uses them, run applications, and so forth.

Each action displays the script engine that was specified when the bundle was created. To create a new action, click *New* to display the Scriptable Action dialog box. For detailed instructions, see Step 9 on page 224.

4 Click *Apply* to save any changes you have made.

20.6 Adding Bundles to Catalogs

Instructions to add bundles to existing catalogs are included in the Using Catalogs section. For more information, see Section 22.4, "Adding Bundles to Catalogs," on page 279.

20.7 Creating Folders

You can use the ZENworks Control Center or the zlman command line utility to create folders. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see zlman (1) (page 562).

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Bundle, Bundle Group, and Catalog objects.

To create a folder:
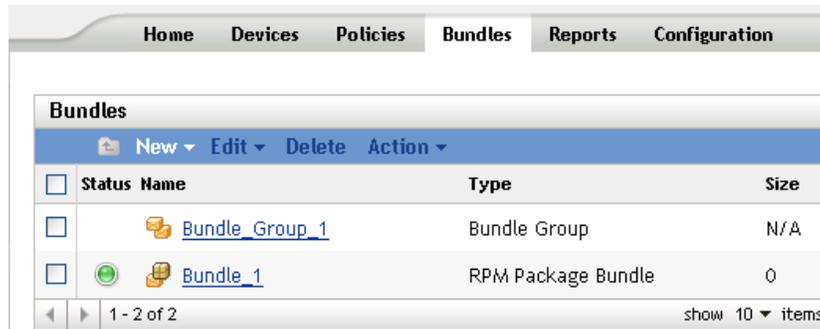
1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New*, then click *Folder* to display the New Folder dialog box.
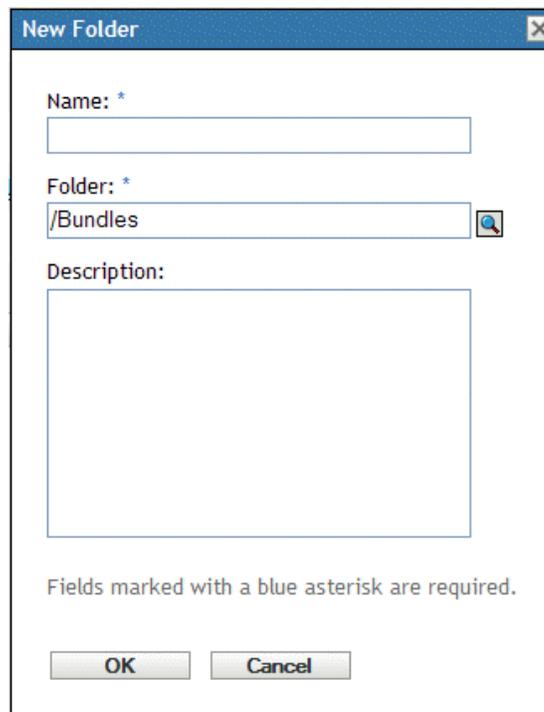
3 Fill in the fields:

- **Name:** Provide a unique name for your folder. This is a required field.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.

- **Description:** Provide a short description of the folder's contents.

4 Click *OK*.

20.8 Creating Bundle Groups

A bundle group lets you group bundles to ease administration and to provide easier assigning and scheduling of the bundles in the bundle group.

You can use the ZENworks Control Center or the zlman command line utility to create bundle groups. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Bundle Commands section of zlman (1) (page 562).

To create a bundle group:

1 In the ZENworks Control Center, click the *Bundles* tab.
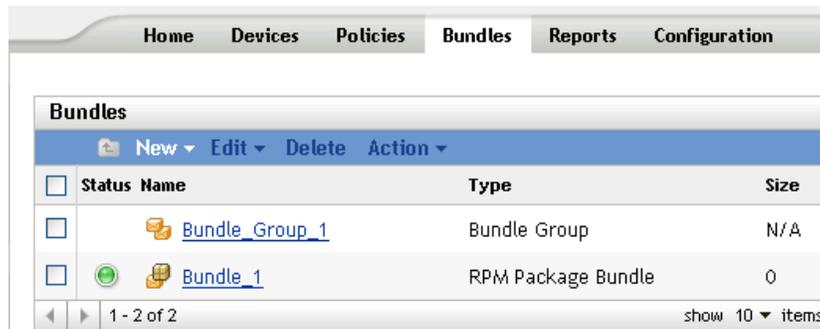
2 Click *New*, then click *Bundle Group* to display the Basic Information page.
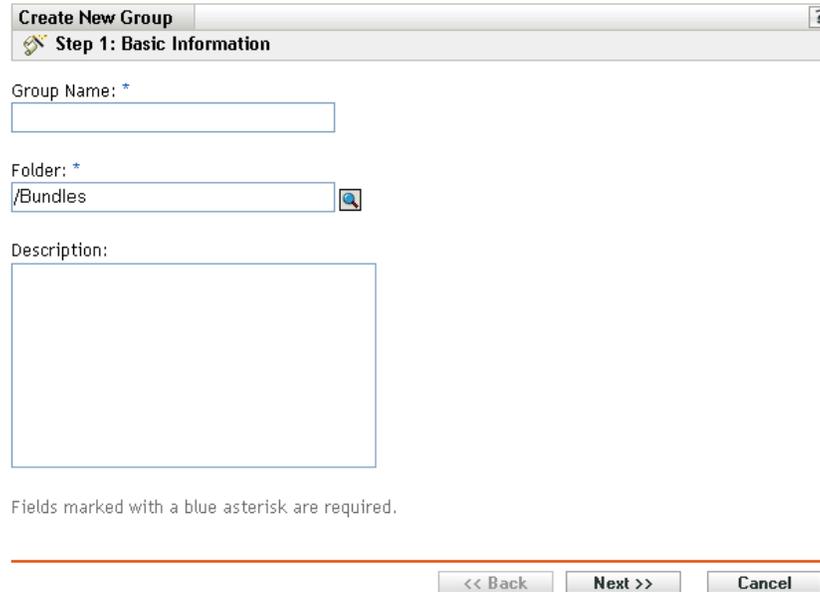
3 Fill in the fields:

- ◆ **Group name:** (Required) Provide a unique name for your bundle group. This name is displayed in the ZENworks Control Center interface (the administrative tool for ZENworks Linux Management) and in the user interface.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** (Required) Type the name or browse to the folder that contains this bundle group.

- **Description:** Provide a short description of the bundle group's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Update Client, which is the user interface for updating software.

4 Click *Next* to display the Summary page.

Review the information on the Summary page. Click the *Back* button to make any changes to the bundle-group settings.

Depending on your needs, you can create the bundle group now or you can specify members, assignments, and schedules for this bundle group and configure other options.

5 Click *Finish* to create the bundle group as configured per settings on the Summary page. If you click *Finish*, the bundle group is created but it does not have members, devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the bundle group by continuing with Section 20.4, "Assigning Bundles," on page 238.

or

Click *Next* to display the Add Group Members page to perform the following tasks:

- Specify members for this bundle group

- Specify assignments for this bundle group

- Set special flags, such as flags to remove conflicting packages and attempt a dry run of the package installation

- Specify the schedule to install or deploy the bundles

Create New Group	Group_1		?

 Step 3: Add Group Members

Specify the members for this group:

Add **Remove**	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

6 Specify the bundles to include in this bundle group.

6a Click *Add* to browse for and select the appropriate bundle objects.

6b Click the underlined link in the *Name* column to select the desired bundles and display their names in the *Selected* list box.

6c Click *OK*.

7 Click *Next* to display the Add Assignments page.
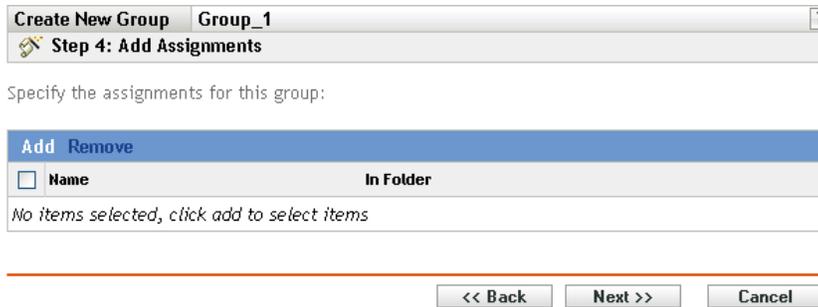
8 Assign the bundle group to the devices that you want to distribute the bundle group to.

8a Click *Add* to browse for and select the appropriate device objects.

You can also select Folder or Group objects.

8b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.

8c Click *OK*.

9 Click *Next* to display the Bundle Options page.

10 (Optional) Specify the desired Special Flag options:

 * **Remove conflicting packages:** Select this option to specify that conflicting packages and files are uninstalled from devices before installing new packages and files. By default, this option is selected, so conflicting packages and files (previous versions of the same package, for example) are uninstalled before the current package or file is installed. If this option is not selected, packages and files are not installed if a conflict is detected.

◆ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle or files can be successfully deployed. If there are any issues that could prevent the RPM bundle or file bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/log/zenworks`.

A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

◆ **Bundle lock:** Select this option to lock bundles on the managed devices from the server.

You can also use the command line utility to lock the bundles. For more information, see Section 21.2, "Locking and Unlocking a Bundle on a Managed Device," on page 266

11 Specify the desired Scheduling options:

◆ **Deploy and install at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

◆ **Deploy and install at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

- ◆ **Deploy and install immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

12 Click *Next* to display the Summary page.

13 Review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Summary page.

14 Click *OK*.

20.9 Adding Bundles to Existing Groups

Using bundle groups eases administration efforts by letting you group several bundles so you can use common assignments, schedules, and so forth, rather than configuring these settings for each bundle you create.

You can use the ZENworks Control Center or the zlman command line utility to add bundles to existing groups. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Bundle Commands section of zlman (1) (page 562).

1 In the ZENworks Control Center, click the *Bundles* tab, select the desired bundle in the Bundles list by clicking the box next to its name, click *Action*, then click *Add to Group* to display the Targets page.
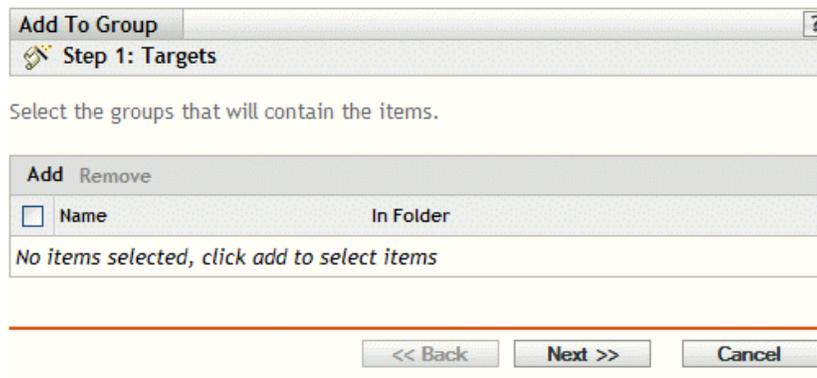
2 Click *Add* to open the Select Groups dialog box, click the desired groups to add them to the Selected list, then click *OK* to display the selected groups in the list on the Targets page.

3 Click *Next* to display the Finish page.

4 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the bundle to the group.

20.10 Uninstalling Bundles from Devices

Use the Uninstall Bundle Wizard to schedule when software contained in a bundle is uninstalled from devices that are no longer assigned to the bundle.

If you remove a bundle's assignments, the previously assigned devices are no longer assigned to the bundle; however, the software in the bundle remains on those devices. Likewise, if you delete a bundle by clicking the *Bundles* tab, checking the box next to a bundle's name, and then clicking *Delete*, the software is not removed from assigned devices.

The Uninstall Bundle Wizard lets you choose whether or not to uninstall the software on those previously assigned devices. If you specify that you want to remove the software, you can specify a schedule to uninstall the software.

NOTE: You can use the Uninstall Bundle Wizard to uninstall only RPM and File bundles. You can remove the assignments from preboot, Dell Update Package (DUP), and patch bundles, but they cannot be uninstalled by using the Uninstall Bundle Wizard.

You can remove bundles from devices using either the *Bundles* tab or the *Devices* tab in the ZENworks Control Center. If you want to remove the software contained in a bundle from one or more devices, you should use the *Bundles* tab. If you want to remove one or more bundles from a specific device, you should use the *Devices* tab.

The following sections contain more information:

- Section 20.10.1, "Using the Bundles Page to Remove Bundles from Devices," on page 252
- Section 20.10.2, "Using the Devices Page to Remove Bundles from Devices," on page 254

20.10.1 Using the Bundles Page to Remove Bundles from Devices

To remove the software contained in a bundle from one or more devices, you should launch the Uninstall Bundle Wizard from the Bundles page.

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundles* list, click the underlined link for the desired bundle to display its Summary page.

3 In the *Assignments* section, select the box next to the device's name from which you want to remove the bundle, then click *Remove* to launch the Uninstall Bundle Wizard.
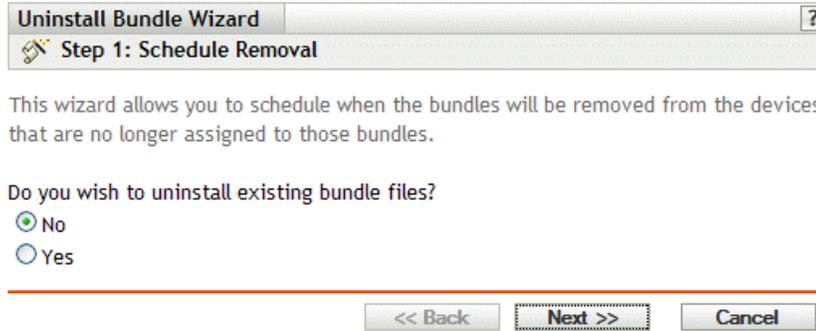
4 Specify a removal option:

- ◆ **No:** Although the device is removed from the *Assignments* section and the bundle is no longer assigned to the device, the software remains installed on the previously assigned device.

- ◆ **Yes:** The software is uninstalled from previously assigned devices according to the schedule you specify in the next step of this wizard.

5 (Conditional) If you chose Yes in Step 4, click *Next* to display the Schedule page.

6 Select a schedule type from the drop-down list.

The settings you configure on this page determine when the assignments are removed from previously assigned devices.

The following schedules are available. Click the link in the left column for more information about each schedule type.

Schedule Type	Description
Date Specific	Select one or more dates on which to remove assignments and set other restrictions that might apply.
Relative to Refresh	Schedule when the assignments are removed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the assignment removal is repeated and specify a time period when you do not want the assignments removed to help minimize network traffic during that time.

7 Click *Next* to display the Finish page, make any changes by using the *Back* button as necessary, then click *Finish* to complete the assignment removal.

20.10.2 Using the Devices Page to Remove Bundles from Devices

1 In the ZENworks Control Center, click the *Devices* tab, then click the *Servers* link to display a list of servers or server groups in your ZENworks Linux Management system.

or

In the ZENworks Control Center, click the *Devices* tab, then click the *Workstations* link to display a list of workstations and workstation groups in your ZENworks Linux Management system.

2 Click the underlined link for the server, server group, workstation, or workstation group that you want to remove a bundle from.

If you clicked a server or workstation group, skip to Step 4.

3 In the *Effective Bundles* section on the Summary page, click *Advanced* to display all bundles assigned to this device.

4 Select the box next to the desired bundle, then click *Remove* to launch the Uninstall Bundle Wizard.

Uninstall Bundle Wizard   [?]

🔹 **Step 1: Schedule Removal**

This wizard allows you to schedule when the bundles will be removed from the devices that are no longer assigned to those bundles.

Do you wish to uninstall existing bundle files?
- ⦿ No
- ○ Yes

[<< Back]   [Next >>]   [Cancel]

---
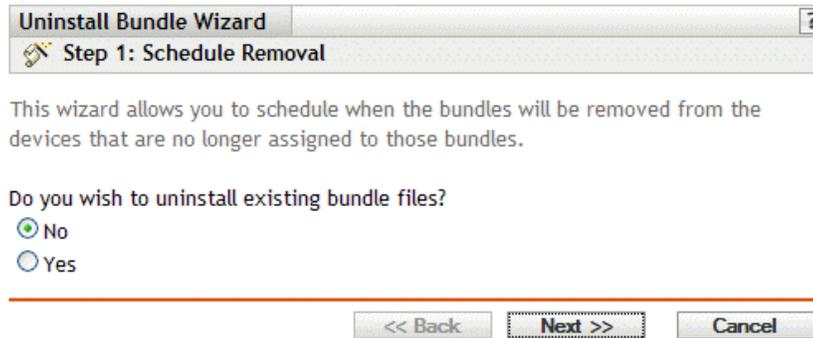
5 Specify a removal option:

- **No:** Although the device is removed from the Assignments section and the bundle is no longer assigned to the device, the software remains installed on previously assigned devices.

- **Yes:** The software is uninstalled from previously assigned devices according to the schedule you specify in the next step of this wizard.

6 Click *Next* to display the Schedule page.

7 Select a schedule type from the drop-down list.

The settings you configure on this page determine when the assignments are removed from previously assigned devices.

The following schedules are available. Click the link in the left column for more information about each schedule type.

Schedule Type	Description
Date Specific	Select one or more dates on which to remove assignments and set other restrictions that might apply.
Relative to Refresh	Schedule when the assignments are removed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the assignment removal is repeated and specify a time period when you do not want the assignments removed to help minimize network traffic during that time.

8 Click *Next* to display the Finish page, make any changes by using the *Back* button as necessary, then click *Finish* to complete the assignment removal.

20.11 Deleting Bundles, Bundle Groups, and Folders

Before you delete bundles, bundle groups, and folders from the ZENworks Control Center, review the following information before performing the procedure in this section to ensure that you obtain the desired results.

You can use the ZENworks Control Center or the zlman command line utility to perform certain tasks in ZENworks Linux Management. The following procedures explain how to perform these tasks using the ZENworks Control Center. If you prefer the zlman command line utility, see the Registration Commands section of zlman (1) (page 562).

Deleting Bundles: Depending on your needs, you can delete a bundle from your ZENworks Linux Management system, remove a bundle's assignments from devices, or use the Uninstall Bundle Wizard to remove the software from assigned devices.

If you delete a bundle from your ZENworks Linux Management system, the bundle does not display on the Bundles or Devices pages in the ZENworks Control Center; however, the software contained in that bundle remains on the previously assigned devices.

If you remove a bundle's assignments, the previously assigned devices are no longer assigned to the bundle; however, the software in the bundle remains on those devices.

Deleting Bundle Groups: The results of deleting a bundle group is similar to that of deleting a bundle.

If you delete a bundle group from your ZENworks Linux Management system, the bundle group does not display on the Bundles page in the ZENworks Control Center and the bundle group's assignments are removed. However, the individual bundles contained in the group are not removed from the ZENworks Control Center and still display on the Bundles page. As with bundles, when you delete a bundle group from the ZENworks Control Center, the software contained in that bundle group remains on the previously assigned devices.

Deleting Folders: If you delete a folder that contains bundles from your ZENworks Linux Management system, both the folder and its bundles are removed from the ZENworks Control Center. However, the software contained in those bundles remain on the previously assigned devices.

Using the Uninstall Bundle Wizard: If you use the Uninstall Bundle Wizard, you can choose whether or not to uninstall the software on previously assigned devices. If you specify that you want to remove the software, you can specify a schedule to uninstall the software. For more information, see Section 20.10, "Uninstalling Bundles from Devices," on page 252.

To delete a bundle, bundle group, or folder:

1 In the ZENworks Control Center, click the *Bundles* tab.
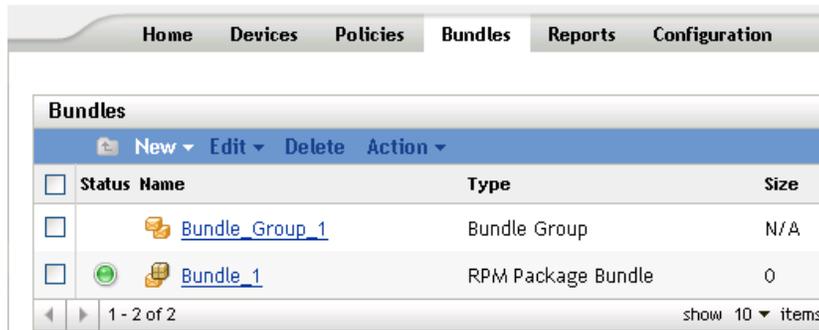
2 In the *Bundles* list, select the box next to the desired item's name, then click *Delete*.

If the item you are deleting is a folder, you are prompted whether or not to delete the folder and its contents.

20.12 Renaming, Copying, or Moving Bundles

Use the *Edit* drop-down list on the Bundles page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a Bundle object, you can rename, copy, and move the bundle. If you select a Bundle Group object, you can rename or move the Bundle Group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the *Edit* menu.

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundles* list, select the box next to the bundle's name, click *Edit*, then click an option.

- ◆ **Rename:** Click *Rename*, type a new name for the bundle, then click *OK*.

IMPORTANT: Do not rename patch bundles.

- ◆ **Copy:** Click *Copy*, type a new name for the copy, then click *OK*.

  The copy option is useful to create a new bundle that is similar to an existing bundle. You can copy a bundle and then edit the new bundle's settings.

  If you create a copy of the YOU patch bundle, the copied version is converted to the RPM package bundle type. Before deploying the RPM package bundle to the device, you must remove the patch RPMs from the bundle. However, you cannot install the copied version of the YOU patch bundle if it contains only scripts.

- ◆ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

If you rename or move a bundle, its assignments are still in place and ZENworks Linux Management does not redistribute the catalog to devices because of the name or location change.

20.13 Deploying a Different Version of a Bundle

You can have multiple versions of the same bundle, although only one version of a bundle can be deployed at any given time. If you make any configuration changes to an existing bundle (changing the display name or description, adding a package to or removing a package from the bundle, or adding or modifying a script), the version number increments.

Only one version of a bundle can be deployed at any given time. For example, suppose a bundle has multiple versions: 1, 2, and 3. If version 1 is currently deployed, all associated devices have version 1 of the bundle deployed. If you then make version 3 the deployed version, all devices with version 1 deployed and still associated to that bundle will be automatically upgraded to version 3.

For more information about editing bundles, which might cause version numbers to increment, see Section 20.5, "Editing Bundles," on page 241. Note that only changes made on the Details page cause the version number to increment, as described in Step 3 on page 243.

The following section contains additional information:

- ◆ Section 20.13.1, "Bundle Version Deployment Behavior (ZENworks Control Center vs. the zlman Utility)," on page 257

20.13.1 Bundle Version Deployment Behavior (ZENworks Control Center vs. the zlman Utility)

You can modify an existing bundle using either the ZENworks Control Center or the `zlman` utility, which causes the bundle's version number to increment. Depending on the method you use to modify a bundle, the deployment behavior of the new version varies.

If you use the ZENworks Control Center to modify a bundle, the version number increments but the new version of the bundle is not automatically deployed; you must manually deploy the new version, as described in Step 3a on page 243.

If you use the `zlman` utility to modify a bundle, the version number increments and the new version of the bundle is automatically deployed; you do not have to manually deploy the edited bundle.

20.14 Using a Remote Execute Policy to Remove Bundles and Packages from Devices

If you remove a bundle's assignments, the previously assigned devices are no longer assigned to the bundle; however, the software in the bundle remains on those devices. Likewise, if you delete a bundle by clicking the *Bundles* tab, selecting the box next to a bundle's name, then clicking *Delete*, the software is not removed from assigned devices.

To remove the bundles and software packages from devices, you can use the Uninstall Bundle Wizard, as explained in Section 20.10, "Uninstalling Bundles from Devices," on page 252 or you can configure a Remote Execute policy to run a script and then assign the policy to devices. You can remove a bundle, a package, or a list of packages.

You cannot remove a catalog by using a Remote Execute policy, but you can remove the bundles and packages contained in a catalog.

To configure a Remote Execute policy to remove bundles and packages from devices:

1 In the ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click *New*, then click *Policy* to display the Create New Policy page.

3 In the *Policy Type* list, click *Remote Execute Policy*, then click *Next* to display the Policy Name page.

4 Fill in the fields:

- **Name:** (Required) Provide a unique name for the policy. The name you provide is displayed in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** (Required) Type the name or browse to the folder that this bundle will be created in. Folders display in the ZENworks Control Center.

- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next*.

6 Select *Script* from the *Executable type* drop-down list.

7 Specify the waiting time after starting the script.

8 Select *Specify your own script* from the *Script to run* drop-down list.

9 Type your script in the script box.

   The following table provides example scripts that you can use, depend on your needs:

Sample Script	Description
`rug bundle-remove bundle1`	Removes bundle1 from all devices that you assign the policy to.
`rug rm package1`	Removes package1 from all devices that you assign the policy to.
`rug rm package1 package2 package3`	Removes package1, package2, and package3 from all devices that you assign the policy to. Separate the package name with spaces.

NOTE: If you use rug rm *package_name* to remove a package that is contained in an installed bundle that contains other packages, only the specified package is removed from assigned devices. The other packages in the bundle are not removed.

If a bundle has multiple packages, when one or more package is removed, the bundle is still marked as installed in the ZENworks Control Center. Depending on the bundle's schedule, the server may re-install the package.

10 Click *Next* to display the Summary page.

11 Click *Finish* to create the policy as configured per settings on the Summary page. If you click *Finish*, the Remote Execute policy is created but it does not have devices assigned or a schedule. At some point in the future, you need to configure additional options for the policy by continuing with Section 17.4, "Assigning Policies," on page 188.

or

Click *Next* to display the Policy Assignments page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Remote Execute Policy	Remote_Execute	?
Step 5: Policy Assignments		

Specify the assignments for this policy:

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

<< Back   Next >>   Cancel

12 Assign the policy to the devices.

12a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

12b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a policy to a Folder or Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

12c Click *OK*.

13 Click *Next* to display the Policy Schedule page, select the schedule to apply to the assignments from the drop-down list, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is assigned to devices.

The following schedules are available. Click the link in the left column for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to assign the policy to devices and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week on which to assign the policy to devices and set other restrictions that might apply.
Monthly	Select the day of the month on which to assign the policy to devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the policy is assigned, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the policy's assignment is repeated and specify a time period when you do not want the policy assigned to help minimize network traffic during that time.

14 Click *Next* to display the Policy Groups page.

15 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the *Name* column to select the desired policy groups and display their names in the *Selected* list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create.

16 Click *Next* to display the Finish page.

17 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured per settings on the Finish page.

20.15 Generating Bundle Reports

Reports let you create custom views for your ZENworks environment. Reports can contain details from a large volume of inventory, packaging, and other device information. You can create new reports, edit existing reports, delete reports, or generate one or multiple reports simultaneously. You can also create folders that let you organize and store reports based on your own criteria.

The following bundle reports are provided with ZENworks Linux Management:

- **Bundle Reports:** This folder contains the following reports:
  - Bundle Delivery Failures
  - Bundle Delivery in the Past 24 Hours
  - Bundle Delivery Information Per Device
  - Last Bundle Delivery Per Device
- **Dell Reports:** This folder contains the following reports:
  - Devices Not Having Valid Dell Update Package Bundles <Template>
  - Devices Not Having Valid RPM Package Bundles <Template>
  - Installed Dell Applications Per All Devices
  - Installed Dell Applications Per PowerEdge Model
- **Device Reports:** This folder contains the following reports:
  - Device Errors in the Past 24 Hours
  - Device Errors in the Past Week
  - Devices Disk Usage
  - Devices Inactive for the Past 90 Days
  - Devices Registered in the Past 24 Hours
  - Devices Registered in the Past Week

For more information, see Part X, "Reports," on page 531.

20.16 Best Practices for Adding Packages to Bundles

- To add multiple packages to a bundle, use `zlman`.

  For more information on zlman, see zlman (1) (page 562).
- To create several bundles with multiple packages, create one bundle at a time and add multiple packages to it, instead of running the commands at the same time. For example, if you want to create three bundles with 100 packages each, run the `zlman` commands in sequence, instead of executing them from three shells simultaneously.
- To assign a large number of bundles to managed devices at one time, create a bundle group in ZENworks Control Center and assign it to the managed devices. For example, if you want to assign YOU patches to a server, create a bundle group with all of the YOU patches, and assign the bundle group to the server instead of assigning the YOU patches individually to the server. Assigning patches individually would take a long time and might not be completed if done from ZENworks Control Center.

  For more information on bundle groups, see Section 20.8, "Creating Bundle Groups," on page 247.
- To quickly deploy large package sets, adjust the level of security provided by the connection between the managed device and the ZENworks Server. To change the security level:
  1. On the ZENworks Server, open the `/etc/opt/novell/zenworks/tomcat/base/server.xml` file.

2. In the Connector section for port 443, change the value of ciphers to 128 bits as shown below:

```
ciphers="SSL_RSA_WITH_RC4_128_SHA"
```

This reduces the workload of the managed device and increases the speed of the streaming of the packages to it.

IMPORTANT: Setting this attribute instructs the server to offer RC4 encryption at 128b as the only available cipher suite. The client will comply as part of the SSL negotiation. However, changing the encryption to RC4 reduces the security of the system, compared to the default encryption such as AES, and makes it susceptible to being broken into.

---

3. Restart the ZENworks Server.

Understanding the Package and Content Management Features Available on a Managed Device

21

The following sections provide detailed information about the Package and Content Management features available on a managed device:

21.1 Locking and Unlocking a Package on a Managed Device

You can lock a package on the managed device to prevent it being deleted, or to prevent it from being upgraded to a newer version.

To lock a package:

1. List all the packages installed on the managed device by entering the `rug pa` command. From the list, select the package you want to lock.

2. Lock the package by entering the `rug la` *package_name* [*<relation> <version>*] command.

   The *package_name* can include wildcard characters. The following table explains the valid relational operators that can be used with the package in the command:

Relational Operator	Functionality
=	Locks only the specific package version.
<	Locks all versions of the package older than the specified version excluding the specified version.
>	Locks all versions of the package later than the specified version excluding the specified version.
<=	Locks all versions of the package older than the specified version as well as the specified version.
>=	Locks all versions of the package later than the specified version as well as the specified version.

If you want to install a specific version of the package, ZENworks first checks if the package version has been locked, then installs the package version only if it is not locked. For example, lets assume that all the later versions of the package, "X 1.7" have been locked by using the `rug la X >1.7` command. If you try to install X 1.9 package by using the `rug in X (1.9)` command, the installation fails.

3 Ensure that the package is locked by entering the `rug ll` command. This displays all the locked packages.

To unlock a package:

1 List all the packages that are locked on the managed device by entering the `rug ll` command. This displays the package name and its lock index.

2 Select the package you want to unlock.

3 Unlock the package by entering the `rug ld` *lock_index* command.

4 Ensure that the package is unlocked by entering the `rug ll` command. This displays only the locked packages.

21.2 Locking and Unlocking a Bundle on a Managed Device

You can lock a bundle on the managed device to prevent it from being deleted, or to prevent it from being upgraded to a newer version.

You can lock or unlock a bundle either from the ZENworks Control Center or from the command line utility.

21.2.1 Locking or Unlocking a Bundle by Using the ZENworks Control Center

You can also lock bundles in ZENworks Control Center while performing the following actions:

- Creating RPM Bundles
- Creating File Bundles
- Assigning Bundles
- Creating Bundle Groups
- Creating Catalogs
- Assigning Catalogs
- Assigning Dell Update Package Bundles

21.2.2 Locking a Bundle by Using the Command Line Utility

1 List all the bundles installed on the managed device by entering the `rug bl` command. From the list, select the bundle you want to lock.

2 Lock the bundle by entering the `rug bla` *bundle_name* command.

bundle_name can include wildcard characters.

3 Ensure that the bundle is locked by entering the `rug bll` command. This displays all the locked bundles except those that are locked on the server by the administrator.

NOTE: If a locked bundle has packages, you can remove the packages from the managed device even though the bundle is locked by using `rpm -e |` *package_name* or `rug rm` *package_name*. To prevent the removal of packages, you must individually lock the packages. For more information on how to lock a package, see Section 21.1, "Locking and Unlocking a Package on a Managed Device," on page 265.

21.2.3 Unlocking a Bundle by Using the Command Line Utility

1 List all the bundles that are locked on the managed device by entering the `rug bll` command. This displays the bundle name and its lock index.

2 Select the bundle you want to unlock.

3 Unlock the bundle by entering the `rug bld` *lock_index* command.

4 Ensure that the bundle is unlocked by entering the `rug bll` command. This displays only the locked bundles.

21.3 Reverting to a Previously Installed Software Configuration State

You can use the `rug ro` *date_time* command or create a checkpoint by using `rug cpa` *checkpoint_name* command to revert to a previously installed software configuration state.

An Example Use Case: In this use case, you enable the rollback preference, install a package, and then roll back to the previously installed configuration state. The package is automatically uninstalled.

1 Enable the Rollback preference by executing the `rug set rollback true` command.

The Rollback preference is set to False by default.

2 Subscribe to a catalog by executing the `rug sub catalog_name` command.

3 List all packages contained in the catalog by executing the `rug pa catalog_name` command.

4 Make a note of the date and time when you enable the Rollback preference by executing the date command.

or

Create a checkpoint by using the `rug cpa` *checkpoint_name* command.

5 Install a package by executing the `rug in package_name` command.

6 Ensure that the package is installed by executing the `rug pa catalog_name` command.

The status of the package should be "i".

7 Roll back to the previously installed configuration state by executing the `rug ro date_time` command.

or

If you have created a checkpoint in Step 4, then execute the `rug ro checkpoint_name` command.

For example: `rug ro "02/20/2009 15:55:56 PM"`

The date and time you specify must be from the time you enable the Rollback preference to the current time. If you do not specify the date, the current date is used.

Specify the date in the mm/dd/yyyy format. For example, 02/28/2007. For more information on the date format, see the rug man page or rug (1) (page 586).

The package installed in Step 5 is uninstalled.

8 To ensure that the package is uninstalled, execute the `rug pa catalog_name` command and verify that the status of the package is blank.

21.4 Installing the Best Package

ZENworks® Linux Management helps the SUSE® Linux Enterprise 10 users to determine the package version best suited for their device by providing the rug in utility and the zen-installer utility. This ensures that there is minimal risk for the incompatibilities with the latest version of the kernel, ATI and XGL enablement, etc., and several key packages.

The following sections provide more information:

- Section 21.4.1, "Using the rug in Utility to Install the Best Package," on page 268
- Section 21.4.2, "Using the zen-installer Utility to Install the Best Package," on page 268

21.4.1 Using the rug in Utility to Install the Best Package

If you want zmd to install the package version best suited for the managed device and not the package with the latest version:

1 On the managed device, enter the `rug in package_name` command.

If you want to install a specific version of the package, and do not want zmd to choose the best package:

1 On the managed device, execute the `rug in package_name-package_version` command.

21.4.2 Using the zen-installer Utility to Install the Best Package

If you want zmd to install the package version best suited for the managed device and not the package with the latest version:

1 On the managed device, enter the `zen-installer` command.

The Software Installer window is displayed.

2 Click *Configure*, then click the *Preferences* tab.

3 Ensure that the *Show Version Details* option is deselected. The option is deselected by default.

4 Click *Close*.

The Software Installer window displays the packages available for installation.

5 Select the package to be installed, then click Install.

zmd installs the package version best suited for the managed device.

If you want to install a specific version of the package, and do not want zmd to choose the best package:

1 On the managed device, enter the `zen-installer` command.

The Software Installer window is displayed.

2 Click *Configure*, then click the *Preferences* tab.

3 Select *Show Version Details*.

4 Click *Close*.

The Software Installer window displays the packages and versions available for installation.

5 Select the package to be installed, then click Install.

Using Catalogs

<div align="right">22</div>

Using Novell® ZENworks® Linux Management, you can install packages using either a catalog or a bundle. A catalog is a collection of RPM bundles or Dell Update Package bundles; bundles included in a catalog are usually considered optional. Packages included in a bundle that is directly assigned is considered mandatory; the packages are installed on all assigned devices (the bundle is directly assigned to devices, the device group, or the device folder). For more information about bundles, see Chapter 20, "Using RPM and File Bundles," on page 217 or Chapter 23, "Using Dell Update Package Bundles," on page 283.

The zlman utility is the command-line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use zlman. For more information, see zlman (1) (page 562).

The following sections contain additional information:

- Section 22.1, "Understanding Catalogs," on page 271
- Section 22.2, "Creating Catalogs," on page 271
- Section 22.3, "Assigning Catalogs," on page 276
- Section 22.4, "Adding Bundles to Catalogs," on page 279
- Section 22.5, "Renaming or Moving Catalogs," on page 279
- Section 22.6, "Deleting Catalogs," on page 280
- Section 22.7, "Creating Folders," on page 281

22.1 Understanding Catalogs

A catalog is a collection of bundles; bundles included in a catalog are usually considered optional. You can use catalogs to deploy and install optional or dependent packages to assigned devices. If you deploy optional packages to devices using a catalog, users can choose whether to deploy and install the software packages included in the bundles inside the catalog. Users use the ZENworks Linux Management Installer, Updater, or Remover programs to manage the software on managed devices. For more information, see Section 6.3, "Using the Software Updater, Installer, and Remover from Users' Managed Devices," on page 54.

You can also use bundles in a catalog to provide dependent packages for a primary package contained in a bundle or in another catalog. For example, suppose you want to include Java Runtime in a catalog and, optionally, hide the catalog from the user interface. If a package contained in a bundle or in another catalog needs Java Runtime (it is listed as a dependency for the primary package), the package containing Java Runtime becomes mandatory and is deployed and installed on all devices that the primary package is deployed and installed on.

22.2 Creating Catalogs

You can use the ZENworks Control Center or the zlman command line utility to create catalogs. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Catalog Commands section of zlman (1) (page 562).

1 In the ZENworks Control Center, click the *Bundles* tab.

2 In the *Bundle* list, click *New*, then click *Catalog* to display the Catalog Name page.

```
Create New Catalog                                              [?]
  Step 1: Catalog Name

Specify the name, description, and display name for the new catalog:

Catalog Name: *
[                              ]

Display Name: *
[                              ]

Folder: *
[/Bundles                     ] [Q]

Description:
[                              ]
[                              ]
[                              ]
[                              ]
[                              ]
[                              ]

Fields marked with a blue asterisk are required.

                        [<< Back]  [Next >>]    [Cancel]
```

3 Fill in the fields:

- **Catalog name:** (Required) Provide a unique name for your catalog. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Display name:** (Required) Provide a name that displays for users when they install, update, or remove software. The display name can be the same name that you provided in the *Name* box; however, you can choose to make the name more intuitive for users. In the next step in this wizard, Catalog Attributes, you can specify to hide this catalog from users.

- **Folder:** (Required) Type or browse to the folder that contains this catalog in the ZENworks Control Center interface.

- **Description:** Provide a short description of the catalog's contents. This description displays in the ZENworks Control Center interface and in the user interface. In the next step in this wizard, Catalog Attributes, you can specify to hide this catalog in the user interface.

4 Click *Next* to display the Catalog Attributes page.
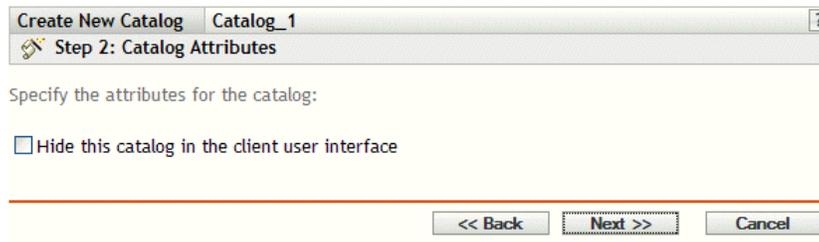
5 (Optional) Select the *Hide this catalog in the client user interface* option to hide the catalog from users; the catalog displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management, but is hidden from users.

This option is useful if you have a bundle or catalog containing a primary package that has dependent packages that must already be installed on devices. You can hide the catalog containing these dependent packages from users. When the primary package in a bundle or catalog is deployed and installed, all dependent packages in the hidden catalog are also deployed and installed.

For example, suppose you have an anti-virus application that you want to deploy and install using a catalog. You could make this catalog visible to users. Suppose that you also need to install updated definition files on devices before the primary package in the bundle or catalog can be installed. You could hide the catalog containing the definition files from users. When the primary package in the bundle or in the visible catalog is deployed and installed, the dependent packages in the hidden catalog are also deployed and installed.

IMPORTANT: If you hide an optional catalog (none of the packages contains dependent packages) from the user interface, the catalog is never deployed and installed. For this reason, you should only hide catalogs that contain dependent packages. When the primary package contained in a bundle or catalog is deployed and installed, the dependent packages contained in the hidden catalog are also deployed and installed.

6 Click *Next* to display the Summary page, then review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary.

Depending on your needs, you can create the catalog now or you can configure additional settings for this catalog.

7 Click *Finish* to create the Catalog as configured per settings on the Summary page. If you click *Finish*, the catalog is created but it does not contain bundles, have any assignments, a schedule, and so forth. At some time in the future, you need to perform the steps under Section 22.3, "Assigning Catalogs," on page 276.

or

Click *Next* to display the Select Bundles page to perform the following tasks:

- Specify bundles and bundle groups to place in this catalog
- Specify the assignments for this catalog
- Specify special flags, such as flags to specify to remove conflicting packages or trying a dry run to test a bundle's deployment
- Specify the update and deployment schedules for this bundle

```
Create New Catalog    Catalog_1                                              [?]
    Step 4: Select Bundles

Specify the bundles and bundle groups to place in this catalog:

  Add  Remove
  [ ]  Name                          In Folder
  No items selected, click add to select items


                              << Back      Next >>       Cancel
```
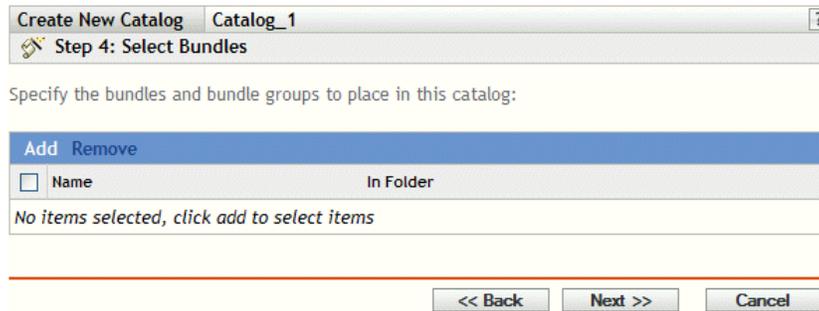
8 Specify bundles and bundle groups for this catalog.

8a Click *Add* to display the Select Bundles dialog box, then browse for and select the bundles and bundle groups you want to assign to this catalog.

Click the underlined link in the *Name* column to select the bundles or bundle groups and to display their names in the *Selected* list box.

8b Click *OK*.

9 Click *Next* to display the Catalog Assignments page.

```
Create New Catalog    Catalog_1                                              [?]
    Step 5: Catalog Assignments

Specify the assignments for this catalog:

  Add  Remove
  [ ]  Name                          In Folder
  No items selected, click add to select items


                              << Back      Next >>       Cancel
```
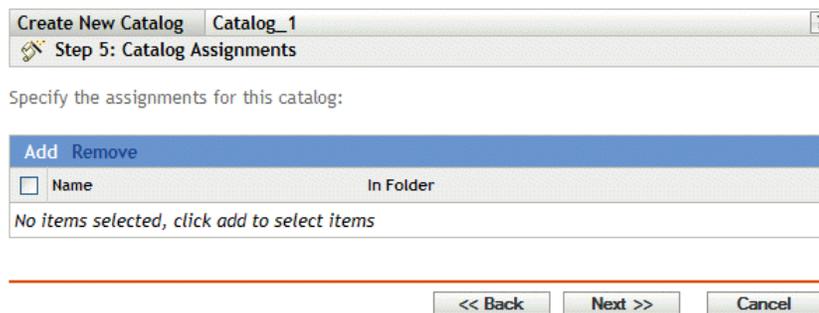
10 Assign this catalog to the devices that you want to distribute the catalog to.

10a Click *Add* to display the Select Assignments dialog box.

10b Click the blue arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

You can also select Folder or Group objects.

Assigning a catalog to a Folder or Group object is the preferred method of associating the catalog. Assigning the catalog to a large number of objects (for example, more than 250) might cause increased server utilization.

10c Click *OK*.

11 Click *Next* to display the Bundles Options page.

Bundles > Create New Catalog

Create New Catalog	catalog 1		?

Step 6: Bundle Options

Set special flags for Bundles(only), which affects how the bundle will be handled. Configure the deployment, and installation schedules if Bundle or update schedules if Catalog.

Scheduling

⦿ Deploy and update at a scheduled time:

Schedule:

Relative to Refresh

◯ Deploy and update at separate scheduled times:

Deployment Schedule:

Relative to Refresh

Update Schedule:

Relative to Refresh

◯ Deploy and update immediately (when this wizard completes)

[<< Back] [Next >>] [Cancel]

12 Specify the desired Scheduling options:

- ◆ **Deploy and update at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

  The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

- ◆ **Deploy and update at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

  The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.

Schedule Type	Description
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

◆ **Deploy and update immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

13 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to create the item as configured per settings on the Finish page.

14 Click *OK*.

22.3 Assigning Catalogs

When you assign catalogs, you specify device assignments, special flags, and deployment or update schedules for an existing catalog.

In Step 7 under Section 22.2, "Creating Catalogs," on page 271, you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the catalog was created without assigning devices to it, setting special flags, or specifying deployment or update schedules for the catalog. Before the catalog can be deployed or updated on assigned devices, you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the catalog-creation process.

1 In the ZENworks Control Center, click the *Bundles* tab, select the desired catalog in the *Bundles* list by clicking the box next to its name, click *Action*, then click *Assign Catalog* to display the Devices To Be Assigned page.
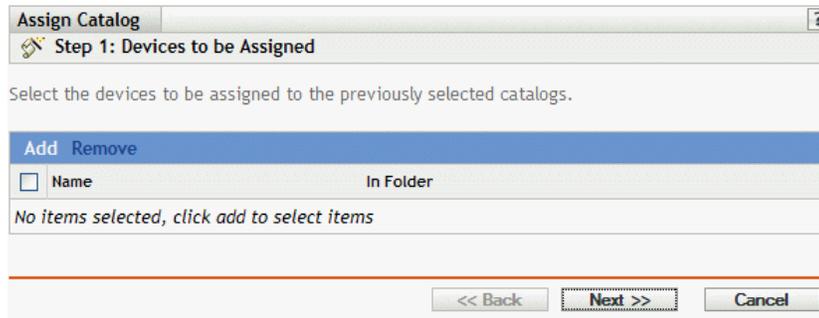
2 Assign the catalog to the devices that you want to distribute the catalog to.

    2a Click *Add* to browse for and select the appropriate device objects.

       You can also select Folder or Group objects.

    2b Click the down-arrow next to *Servers* or *Workstations* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

       Assigning a catalog to a Folder or Group object is the preferred method of assigning the catalog. Assigning the catalog to a large number of objects (for example, more than 250) might cause increased server utilization.

    2c Click *OK*.

3 Click *Next* to display the Bundle Options page.

4 Specify the desired Scheduling options:

    ◆ **Deploy and update at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

       The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

◆ **Deploy and update at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

◆ **Deploy and update immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

5 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to assign the catalog as configured per settings on the Finish page.

6 Click *OK*.

22.4 Adding Bundles to Catalogs

You can use the ZENworks Control Center or the zlman command line utility to add bundles to catalogs. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Catalog Commands section of zlman (1) (page 562).

1 In the ZENworks Control Center, click the *Bundles* tab.
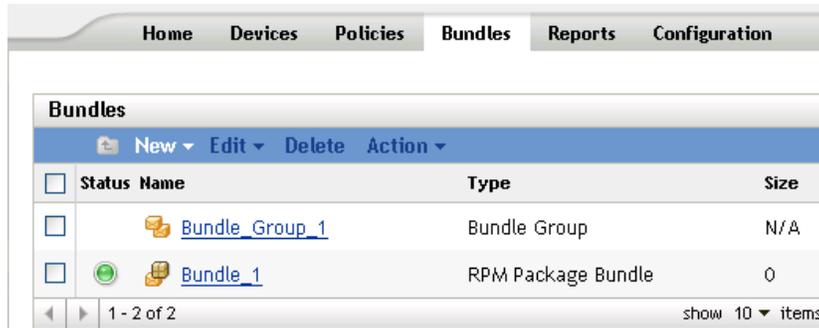
2 In the *Bundles* list, select the box next to the bundle's name, click *Action*, then click *Add to Catalog* to display the Targets page.
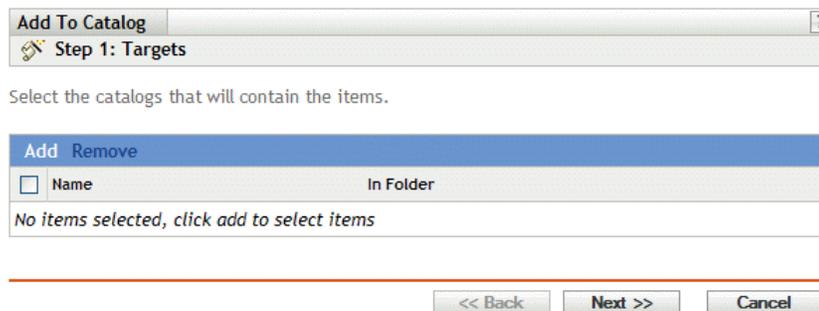
3 Select the catalog to contain the selected bundles.

  3a Click *Add* to open the Select Catalogs dialog box, then click the desired catalogs to add them to the *Selected* list.

  3b Click *OK* to display the selected catalogs in the list on the Targets page.

4 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the bundle to the catalog.

22.5 Renaming or Moving Catalogs

You can use the ZENworks Control Center or the zlman command line utility to rename or move catalogs. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Catalog Commands section of zlman (1) (page 562).

Use the *Edit* drop-down list on the Bundles page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a catalog object, you can rename and move the catalog, but you cannot copy it. If you select a bundle object, you can rename, copy, or move the object. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the Edit menu.

1 From the ZENworks Control Center, click the *Bundles* tab.

	Home	Devices	Policies	**Bundles**	Reports	Configuration

Bundles

📁 New ▾ Edit ▾ Delete Action ▾

	Status	Name	Type	Size
☐		🗂 Bundle_Group_1	Bundle Group	N/A
☐	🟢	📦 Bundle_1	RPM Package Bundle	0

◀ ▶ 1 - 2 of 2   show 10 ▾ items

2 In the *Bundles* list, select the box next to the catalog's name, click *Edit*, then click an option.

  ◆ **Rename:** Click *Rename*, type a new name for the catalog, then click *OK*.

  ◆ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

    If you rename or move a catalog, its assignments are still in place and ZENworks Linux Management does not redistribute the catalog to devices because of the name or location change.

22.6 Deleting Catalogs

If you delete a catalog from your ZENworks Linux Management system, the catalog does not display on the Bundles or Devices pages in the ZENworks Control Center; however, the software in the catalog that is installed remains on the previously assigned devices.

If you remove a catalog's assignments, the previously assigned devices are no longer assigned to the catalog; however, the software in the catalog remains on those devices.

To remove the software contained in catalogs from devices, see Section 20.14, "Using a Remote Execute Policy to Remove Bundles and Packages from Devices," on page 258.

You can use the ZENworks Control Center or the zlman command line utility to delete catalogs. The following procedure explains how to perform this task using the ZENworks Control Center. If you prefer the zlman command line utility, see the Catalog Commands section of zlman (1) (page 562).

To delete a catalog from the ZENworks Control Center:

1 In the ZENworks Control Center, click the *Bundles* tab.
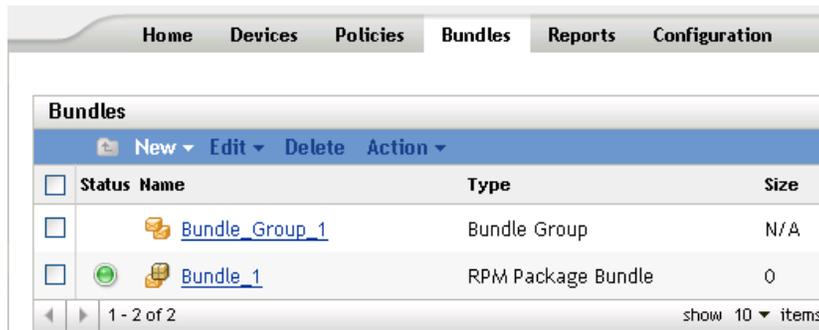
2 In the *Bundles* list, check the box next to the catalog's name, then click *Delete* to remove the catalog from the ZENworks Control Center.

3 Click *OK* on the warning window that displays.

22.7 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Bundle, Bundle Group, Catalog, Device, and Device Group objects.

To create a folder:
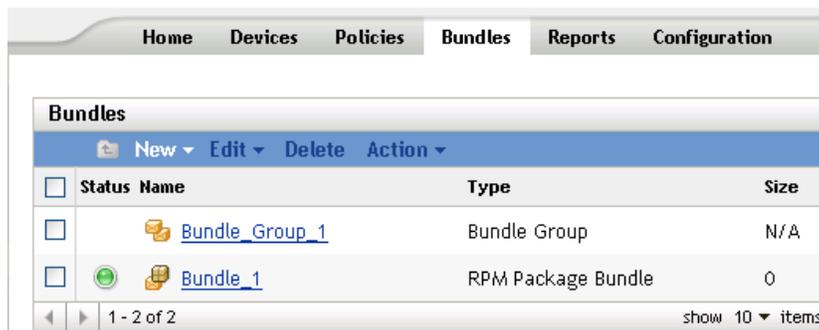
1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New*, then click *Folder* to display the New Folder dialog box.

3 Fill in the fields:

- **Name:** Provide a unique name for your folder. This is a required field.

  For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

- **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.

- **Description:** Provide a short description of the folder's contents.

4 Click *OK*.

Using Dell Update Package Bundles

<div align="right">

23

</div>

Novell® ZENworks® Linux Management lets you mirror Dell Update Packages (DUPs) from the Dell FTP site or from a CD to your ZENworks server. Dell Update Packages let you update and configure hardware and system settings (including BIOS, DRAC, RAID, BMC, and FRMW configurations) on Dell PowerEdge servers.

IMPORTANT: Before you can use Dell Update Packages on your Dell servers, you must complete the steps in "Enabling Dell PowerEdge Support" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

The following sections contain additional information:

23.1 Obtaining Dell Update Packages

You mirror Dell Update Packages from the Dell FTP site to your ZENworks server. You can also mirror Dell Update Packages from a CD obtained from Dell support.

For complete instructions, see Section 25.5, "Mirroring Dell Update Packages to Your ZENworks Server," on page 309.

23.2 Assigning Dell Update Package Bundles

After the mirroring operation is complete, the Dell Update Packages are automatically bundled and displayed in the ZENworks Control Center on the Bundles page. To install them on PowerEdge servers in your ZENworks system, you must assign them to devices using the Assign Bundle Wizard in the ZENworks Control Center.

NOTE: If you assign the Dell Update Packages to devices using bundles, the packages are always installed. For this reason, it is possible to downrev your firmware using Dell Update Packages distributed via bundles.

If you assign the Dell Update Packages to devices using catalogs, the packages are installed only in an upgrade situation. It is not possible to downrev firmware using Dell Update Packages distributed via catalogs. For more information about catalogs, see Chapter 22, "Using Catalogs," on page 271.

To assign Dell Update Package bundles:

1 In the ZENworks Control Center, click the *Bundles* tab, then click the underlined link next to the folder that was created during the mirroring process to contain the Dell Update Packages.

If the particular Dell Update Package does not display in the *Bundles* list, click the right-arrow at the bottom of the list to display the next set of Dell Update Package bundles. By default, ten items display in the list. You can also click the down-arrow on the *show x items* option to display more items in the list.

2 Select the desired Dell Update Package bundle by checking the box next to its name, click Action, then click Assign Bundle to display the Devices to be Assigned page.

Assign Bundle	?
✨ **Step 1: Devices to be Assigned**	

Select the devices to be assigned to the previously selected bundles.

Add Remove	
☐ **Name**	**In Folder**
No items selected, click add to select items	

[<< Back] [Next >>] [Cancel]

3 Assign the bundle or bundle group to the devices that you want to distribute the bundle or bundle group to.

3a Click *Add* to browse for and select the appropriate Server objects.

You can also select Folder or Group objects.

3b Click the down-arrow next to *Servers* to expand the list, then click the underlined link in the *Name* column to select the desired objects and display their names in the *Selected* list box.

Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.

3c Click *OK*.

4 Click *Next* to display the Bundle Options page.

Create New Bundle   Bundle_1   [?]

Step 7: Bundle Options

Set special flags which affect how this bundle will be handled, and configure the deployment and installation or update schedules

Special Flags
- ☑ Remove conflicting packages
- ☐ Attempt a dry run

Scheduling
- ⦿ Deploy and install at a scheduled time:

  Schedule:

  `Relative to Refresh` 🕐

- ○ Deploy and install at separate scheduled times:

  Deployment Schedule:

  `Relative to Refresh` 🕐

  Installation Schedule:

  `Relative to Refresh` 🕐

- ○ Deploy and install immediately (when this wizard completes)

[<< Back]   [Next >>]   [Cancel]

5 (Optional) Specify the desired Special Flag options:

- ◆ **Remove conflicting packages:** Select this option to specify that conflicting packages and files are uninstalled from devices before installing new packages and files. By default, this option is selected, so conflicting packages and files (previous versions of the same package, for example) are uninstalled before the current package or file is installed. If this option is not selected, packages and files are not installed if a conflict is detected.

- ◆ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle or files can be successfully deployed. If there are any issues that could prevent the RPM bundle or file bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/log/zenworks`.

  A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

6 Specify the desired Scheduling options:

- ◆ **Deploy and install at a scheduled time:** Use this option to schedule the deployment and installation of the bundles contained in this bundle group. Click the *Schedule* icon to choose the schedule type.

  The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.

Schedule Type	Description
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

◆ **Deploy and install at separate scheduled times:** Use this option to specify an optional deployment schedule separate from the installation schedule. If you select this option, you can set up a deployment schedule and an installation schedule. If you do not select this option, the packages will be deployed and installed on assigned devices according to the schedule. Click the *Schedule* icon to choose the schedule type.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
Date Specific	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

The *Deploy and install at separate scheduled times* option is not set by default. In most situations, there is no need to deploy and install packages inside bundles at different times. You can, depending on your needs, schedule deployment and installation at different times to conserve network bandwidth or to perform the actions at more convenient times for users.

The deployment schedule determines when the packages and files inside the bundle are downloaded from the server to the assigned devices. The packages and files are not yet installed and available for use. The installation schedule determines when the packages and files are installed on assigned devices so the packages will be available for use.

◆ **Deploy and install immediately (when this wizard completes):** Select this option to specify that the packages inside the bundle group deploy and install immediately when the Create New Group Wizard completes, providing that the assigned devices are online. The packages inside the bundle group deploy to and install on devices that are not online when they refresh.

7 Click *Next* to display the Finish page.

8 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary. Click *Finish* to assign the bundle as configured per settings on the Summary page.

9 Click *OK*.

23.3 Determining If Newer Dell Package Updates Are Available for PowerEdge Servers

After you run a mirror session and obtain updated Dell Update Packages, it is easy to determine if a newer Dell Update Package is available for installation on Dell PowerEdge servers in your ZENworks system.

1 In the ZENworks Control Center, click the *Devices* tab, then click *Servers*.

A ✉ icon in the Updates column indicates whether there is a Dell Update Package bundle available in the ZENworks package repository for each Dell PowerEdge server in the list. An update are available in the following situations:

- If a Dell Update Package exists in the ZENworks package repository but it is not assigned to that specific server model.
- If a specific Dell Update Package is already assigned to the device, but an updated package has been mirrored and is available in the ZENworks package repository.

2 Click the ✉ icon to view the name of the Dell Update Package bundle appropriate for the device.

3 If the appropriate Dell Update Package bundle is not yet assigned to the device, continue with Section 23.2, "Assigning Dell Update Package Bundles," on page 283.

or

If the appropriate Dell Update Package bundle is already assigned to the device, continue with Section 23.4, "Deploying an Updated Version of a Dell Update Package Bundle," on page 287.

23.4 Deploying an Updated Version of a Dell Update Package Bundle

You can have multiple versions of the same Dell Update Package bundle, although only one version of a bundle can be deployed at any given time. If you perform a mirror session and obtain an update for a Dell Update Package, the Dell Update Package bundle's version number increments; however, the mirroring process does not automatically deploy the updated version of the bundle.

Only one version of a bundle can be deployed at any given time. For example, suppose a bundle has multiple versions: 1, 2, and 3. If version 2 is currently deployed, all associated devices have version 2 of the bundle deployed. If you receive an update to this package via mirroring, a link on the *Devices* > *Servers* page in the ZENworks Control Center indicates that an update is available (as described in Section 23.3, "Determining If Newer Dell Package Updates Are Available for PowerEdge Servers," on page 287). To update the bundle on devices, you must make version 3 the deployed version; all devices with version 2 deployed and still associated to that bundle will be automatically upgraded to version 3.

To deploy an updated version of a Dell Update Package bundle:

1 In the ZENworks Control Center, click the *Bundles* tab, then click the underlined link next to the folder that was created during the mirroring process to contain the Dell Update Packages.

If the particular Dell Update Package does not display in the *Bundles* list, click the right-arrow at the bottom of the list to display the next set of Dell Update Package bundles. By default, ten items display in the list. You can also click the down-arrow on the *show x items* option to display more items in the list.

2 Click the underlined link in the *Name* column to display the bundle's Summary page.

3 Click the *Details* tab.
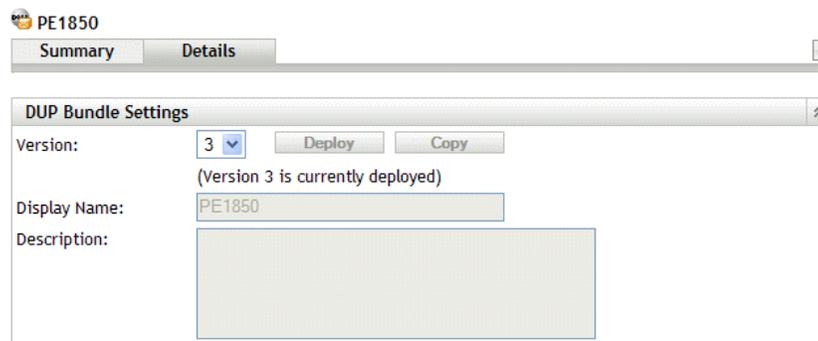
4 Use the Version drop-down list to select the desired version number, then click Deploy.

23.5 Modifying the Contents of a Dell Update Package Bundle

You can copy a Dell Update Package bundle and then modify its contents. You can, however, only remove existing packages or replace an existing package with a newer version of that same package. You cannot add new packages to the bundle.

Be aware that if you modify the contents of a Dell Update Package bundle, it will no longer be a Certified Dell Update Package, which limits the level of technical support you can obtain for any problems you may encounter using that bundle. For this reason, use caution when modifying the contents of a Dell Update Package bundle.

To make a copy of an existing Dell Update Package bundle:

1 In the ZENworks Control Center, click the *Bundles* tab, click the underlined link next to the folder containing the Dell Update Packages that was created during the mirroring process.

If the particular Dell Update Package does not display in the Bundles list, click the right-arrow at the bottom of the list to display the next set of Dell Update Package bundles. By default, ten items display in the list. You can also click the down-arrow on the *show x items* option to display more items in the list.

2 Click the underlined link in the *Name* column to display the bundle's *Summary* page.

3 Click the *Details* tab.

PE1850

| Summary | Details | ? |

DUP Bundle Settings

Version: 3 ▾ [Deploy] [Copy]

(Version 3 is currently deployed)

Display Name: PE1850

Description:
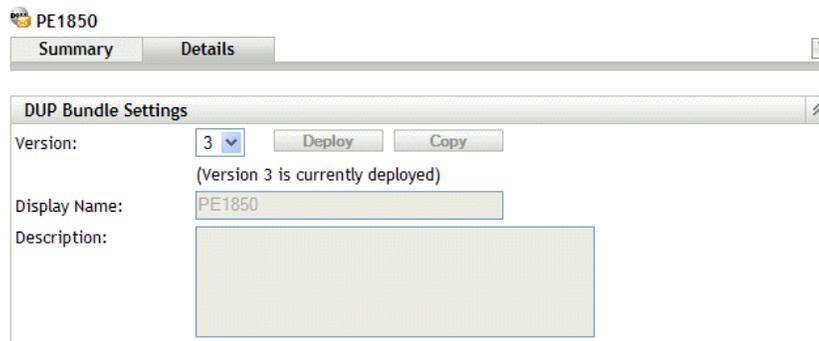
4 Use the Version drop-down list to select the desired version number, then click Copy.

5 Provide a new name for the copy of the bundle, then click *OK*.

To modify the contents of the copy of an existing Dell Update Package bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click the underlined link in the Name column for the copy of the Dell Update Package whose contents you want to modify.

3 Click the *Details* page.

4 (Conditional) To replace an existing package with a newer version of that same package, click *Add*, click *Import from Repository*, select the newer version of the package by clicking the check box next to its name, then click *OK*.

5 (Conditional) To remove an existing package, select the package by clicking the check box next to its name, then click *Remove*.

Replicating Content in the ZENworks Management Zone

24

Novell® ZENworks® Linux Management uses a hierarchical organization to simplify device management. At the top level, a ZENworks Management Zone provides an autonomous unit of ZENworks servers and managed devices (workstations and servers). The ZENworks servers manage the devices.

Each ZENworks Management Zone has one Primary Server, and optionally, one or more Secondary Servers to help distribute the workload.

All RPM packages, Dell Update Packages (DUPs), and files contained in file bundles must reside on the Primary Server. ZENworks Linux Management uses content replication to replicate packages to each Secondary Server in your system.

NOTE: Depending on your needs, you might have more than one ZENworks Management Zone in your system. The content replication procedure in this section helps you replicate content from the Primary Server to Secondary Servers in a particular Management Zone. To replicate content across Management Zones, you must use zlmmirror. For more information, see Chapter 25, "Mirroring Software," on page 293.

24.1 Replicating the Content Immediately

1 In the ZENworks Control Center, click the *Devices* tab.

2 Click the *Servers* folder link in the *Devices* list.

3 Click the link in the *Name* column for your ZENworks Primary Server to display the device's details.

4 In the *Server Tasks* section in the upper left corner, click *Replicate repositories now*.
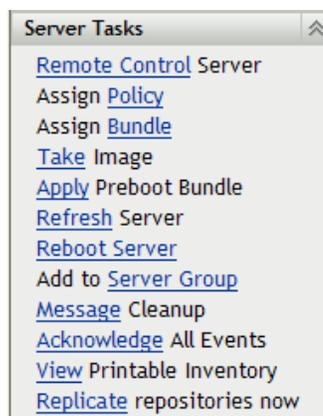
24.2 Configuring a Content Replication Schedule

1 In the ZENworks Control Center, click the *Configuration* tab.
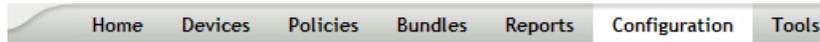
2 Click *Content Replication Schedule* to display the Content Replication Schedule page.

3 Select a schedule type from the drop-down list.

The Content Replication Schedule determines how often bundles are replicated from the Primary ZENworks Server to all Secondary Servers in the Management Zone. During replication of a bundle, only new packages and updates to existing packages are sent.

The following schedules are available:

Schedule Type	Description
Date Specific	Select one or more dates on which to replicate the content to Secondary Servers and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week on which to replicate content to Secondary Servers and set other restrictions that might apply.
Monthly	Select the day of the month on which to replicate content to. Secondary Servers and set other restrictions that might apply

4 Click *Apply*.

Mirroring Software

25

Novell® ZENworks® Linux Management lets you connect to a remote server and copy software catalogs, bundles, or packages (including Dell Updated Packages) from the remote server to your server by using a few simple commands.

Depending on your needs, you might have more than one ZENworks Management Zone in your system. The information in this section helps you mirror content across Management Zones or from remote servers. For information about replicating content from a ZENworks Primary Server to ZENworks Secondary Servers in a particular Management Zone, see Chapter 24, "Replicating Content in the ZENworks Management Zone," on page 291.

You can mirror software by using the zlmmirror command line application. Software can be mirrored to a ZENworks Primary Server from the following remote servers:

- ZENworks Linux Management (from the servers in one ZENworks Management Zone to another Management Zone)
- Dell Update Packages (DUPs)
- YaST® Online Updates
- Red Hat Network
- Red Carpet Enterprise or ZENworks 6.6.*x* Linux Management
- YUM (Yellow dog Updater, Modified)
- NU

NOTE: To mirror from a ZENworks 6.6.*x* Linux Management server to a ZENworks 7.3 Linux Management server, the 6.6.*x* server must also be a YaST Online Update (YOU) server.

Novell, Dell, SUSE®, and Red Hat each maintain servers of their respective types, enabling you to simply mirror the catalogs and bundles you are interested in without needing to maintain or update these repositories.

Mirroring is the preferred method to obtain the majority of the software you distribute to managed devices. If you use a strict firewall where outbound connections are not automatically allowed, connecting to a remote port 80 or a remote port 443 is necessary.

IMPORTANT: Mirroring YaST online updates for a SLES 9 platform with ia64, ppc, or s390 architectures is not supported in ZENworks 7.2 Linux Management or later.

The following sections contain additional information:

- Section 25.1, "zlmmirror," on page 294
- Section 25.2, "xzlmmirror," on page 294
- Section 25.3, "Configuring a Software Mirror," on page 294
- Section 25.4, "Distributing Catalogs from a Public ZENworks Linux Management Server," on page 308
- Section 25.5, "Mirroring Dell Update Packages to Your ZENworks Server," on page 309

25.1 zlmmirror

All of the software components necessary to use zlmmirror are installed during the ZENworks Linux Management installation process.

The zlmmirror executable is located in `/opt/novell/zenworks/bin/`. You can view help for zlmmirror at any time by running the following command:

```
zlmmirror --help
```

You can view the zlmmirror man page (man zlmmirror) on the ZENworks Server or see zlmmirror (1) (page 554).

25.2 xzlmmirror

The xzlmmirror utility is a graphical user interface that lets you create and edit a mirror configuration file, and store it in an XML file that is compatible with the existing zlmmirror utility. You can view catalogs and bundles that are located on a remote repository by using this utility. You can mirror software catalogs, bundles, and packages from external repositories by using these configuration files.

For more information on creating a configuration file by using the xzlmmirror utility, see Section 25.3.2, "Creating a Configuration File by Using the xzlmmirror Utility," on page 300.

The xzlmmirror executable is located in `/opt/novell/zenworks/bin/`.

25.3 Configuring a Software Mirror

Configuring a software mirror consists of the following:

1. Creating a separate XML configuration file for each remote server you want to mirror. You can create the configuration file either by using the command line utility or by using the xzlmmirror utility.

   See Section 25.3.1, "Creating the Configuration Files by using the Command Line Utility," on page 295 and Section 25.3.2, "Creating a Configuration File by Using the xzlmmirror Utility," on page 300

2. Mirroring patch bundles.

   See Section 25.3.3, "Mirroring Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2 from the NU and RCE Type Repositories," on page 306

3. Testing and running the mirroring operation. You can do this either by using zlmmirror or xzlmmirror.

   See Section 25.3.4, "Testing and Performing the Mirroring Operation by Using zlmmirror," on page 307 and Section 25.3.5, "Testing and Performing the Mirroring Operation by Using the xzlmmirror Utility," on page 307

25.3.1 Creating the Configuration Files by using the Command Line Utility

Run the following command to generate an empty configuration file:

```
zlmmirror conf-generate filename.xml
```

This command generates a template configuration file named zlmmirror-config.xml in the current directory.

You can also convert the configuration file from an earlier version of ZENworks Linux Management or Red Carpet, or create configuration files manually. Configuration files are specified using the -c flag:

```
zlmmirror command -c filename.xml
```

If no configuration file is specified, the default configuration file location is /etc/opt/novell/zenworks/zlmmirror.xml.

You can check the configuration file for errors and display the parsed configuration information by using the conf-validate (cv) *filename* command.

After you have a base configuration file created, the following tasks walk you through adding the necessary configuration information:

- "Step 1: Servers" on page 295
- "Step 2: Catalog and Bundle Configuration" on page 298

Step 1: Servers

You must provide details about a remote server containing the software you want to mirror, and a local server, which is your ZENworks Linux Management server receiving the mirrored software.

RemoteServer

```
<RemoteServer>
   <Base>http://red-carpet.ximian.com/</Base>
   <Type>rce</Type>
   <User />
   <Password />
</RemoteServer>
```

Configuration Element	Description
Base	Path to the server you want to mirror, in the following format depending on Type: **ZLM:** `https://`*server* **DELL:** `http://ftp.dell.com` **RCE:** `https://`*server*/*path* **YAST:** `http(s)://server/path` or `ftp://server/path` **RHN:** `http(s)://server/path` **YUM:** `http://server/path` **STATIC:** `/path/on/filesystem` **NU:** `https://nu.novell.com/repo`
Type	Type of server you want to mirror: **ZLM:** ZENworks 7.3 Linux Management **DELL:** Dell Update Package FTP Server **RCE:** Red Carpet® Enterprise™, or ZENworks 6.*x* Linux Management **YAST:** YAST Online Updates **RHN:** Red Hat Network **YUM:** YUM **NU:** `Novell Updates`
User	Name to use when connecting to the remote server. If no user is specified, zlmmirror reads the identity from the following location depending on Type: **ZLM:** `/etc/opt/novell/zenworks/zmd/deviceid` for SLES 9 and OES, `/etc/zmd/deviceid` for SLES 10 and SLED 10 **RCE:** `/etc/ximian/mcookie` **YAST:** `/etc/sysconfig/onlineupdate` When connecting to an RHN server or a Dell server, leave this element empty. **NU:** `/etc/opt/novell/zenworks/zmd/deviceid` for SLES 9 and OES, `/etc/zmd/deviceid` for SLES 10 and SLED 10 For the Novell Updates (NU) server, the device must be registered with NCC to use the deviceid as User.

Configuration Element	Description
Password	Password to use when connecting to the remote server. If no password is specified, zlmmirror reads the password from the following location depending on Type: **ZLM:** `/etc/opt/novell/zenworks/zmd/secret` for SLES 9 and OES, and `/etc/zmd/secret` for SLES 10 and SLED10 **RCE:** `/etc/ximian/partnernet` **YAST:** `/etc/sysconfig/onlineupdate` When connecting to an RHN server or Dell server, leave this element empty. **NU:** `/etc/opt/novell/zenworks/zmd/secret` for SLES 9 and OES, and `/etc/zmd/secret` for SLES 10 and SLED10 For the Novell Updates (NU) server, the device must be registered with NCC to use the device secret as Password.

Proxy	The Proxy configuration element is optional and is used with an Internet Proxy. You can add the Proxy element anywhere in the RemoteServer section.
	
	If the Internet proxy requires authentication, the format looks like the following example:
	
	`<Proxy>http://username:password@server:port</Proxy>`
	
	If the Internet proxy does not require authentication, the format looks like the following example:
	
	`<Proxy>https://server:port</Proxy>`

LocalServer

```
<LocalServer>
   <Base></Base>
   <Type>zlm</Type>
   <User>Administrator</User>
   <Password>password</Password>
</LocalServer>
```

Configuration Element	Description
Base	If the Type element indicates STATIC mirroring, use the Base element to define the destination path where files will be stored (`/path/on/filesystem`, for example). If the Type element indicates ZLM mirroring, leave the Base element empty.

Configuration Element	Description
Type	Type of mirroring you want performed:
	ZLM: Mirrors catalogs and bundles directly to your ZENworks Linux Management server. After mirroring, mirrored catalogs and bundles are displayed in the ZENworks Control Center.
	You cannot perform ZLM mirroring on Secondary Servers.
	STATIC: Mirrors packages to the file system of your ZENworks Linux Management server, but does not add them to ZENworks.
	You can perform only static mirroring on Secondary Servers.
User	Name to use when connecting to your ZENworks Linux Management (local) server. The Administrator user should be specified if you want to use the default administrator account.
Password	Password for the account provided in User. If you are using the Administrator account, this is the password you specified during the server installation. For information about encoding your password, see Section 25.10, "Encoding the ZENworks Server Password," on page 319

Step 2: Catalog and Bundle Configuration

You must provide details about the catalogs and bundles you want mirrored to your server.

Before you mirror the catalogs and bundles to your server, you can view the available catalogs and bundles on the remote server.

To view the available catalogs, run the following command:

```
zlmmirror slc -c filename.xml
```

To view the available bundles, run the following command:

```
zlmmirror slb -c filename.xml
```

CatalogConf

Each catalog you want to mirror must have a separate CatalogConf section:

```
<CatalogConf>
   <Name>Red Carpet 2</Name>
   <LocalName>Red Carpet 2</LocalName>
   <Target>sles-9-i586</Target>
   <Package>lib.*</Package>
</CatalogConf>
```

Configuration Element	Description
Name	Name of the catalog you want to mirror from this remote server.
	This is the only required parameter.

Configuration Element	Description
Local Name	Name of the catalog you want the mirrored software placed in. If no Local Name is specified, the catalog name from the remote server is used. The local name for the catalog should not be same as that reserved for the <catalogname>-patches folder
Folder	Specifies the eDirectory™ folder (for example, /folder1/folder2) where bundles and catalogs are created and updated. If not specified, the catalogs and bundles are created and updated in the /zlmmirror folder.
Target	Restricts the mirroring operation on this catalog to packages and patches that support the specified target platforms. If no target is specified, packages for all platforms are mirrored. This element can be specified multiple times, and can contain either a target name or a regular expression string for wildcard matching of target names. For example, to include targets beginning with sles such as sles-9-i586, use the regular expression *<Target>*sles.**</Target>*.
ExcludeTarget	Same as Target, except packages and patches supporting the specified target platform(s) are excluded. ExcludeTarget is performed after Target, so platforms appearing in a Target and ExcludeTarget are ultimately excluded. For example, to exclude targets that end with i586 such as sles-9-i586, use the regular expression *<ExcludeTarget>*.*i586*</ExcludeTarget>*.
Bundle	Restricts the mirroring operation on this catalog to the specified bundles. If not specified, all bundles are mirrored. This option is valid only for ZENworks Linux Management and YAST source servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for matching bundle names.
LocalBundleName	Renames the bundle name locally. This is applicable only for the RCE, NU, and RHN services in which a catalog has only one bundle on the remote server. If you specify <LocalBundleName>, you must not specify the <Bundle> tag. This tag is not applicable when you mirror OES from the RCE service with more than one bundle per catalog.
ExcludeBundle	Same as Bundle, except packages and patches contained in the specified bundles are excluded. This option is valid only for ZENworks Linux Management and YAST source servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for matching bundle names. ExcludeBundle is performed after Bundle, so bundles appearing in a Bundle and ExcludeBundle are ultimately excluded.
Package	Restricts the mirroring operation on this catalog to the specified packages. If not specified, all packages are mirrored. This option can be specified multiple times, and can contain either a package name or a regular expression string for matching package names. This option is not supported for YOU patches.
ExcludePackage	Same as Package, except specified packages are excluded. This option can be specified multiple times, and can contain either a package name or a regular expression string for matching package names. This option is not supported for YOU patches. ExcludePackage is performed after Package, so packages appearing in a Package and ExcludePackage are ultimately excluded.

Configuration Element	Description
Category	Restricts the mirroring operation on the catalog to the specified categories of patch bundles. If the category is not specified, all patch bundles are mirrored. Valid values are recommended, optional, and security. This tag is applicable only for the NU type servers of SLES 10, SLED 10, and OES 2.
ServicePackGroups	Accepts Boolean values (true or false) only. By default `<ServicePackGroups>` is set to true, and it automatically creates bundle groups. This option is supported for YOU patches only
AutoDeploy	Mirroring the packages to existing bundle creates a newer version of the bundle and deploys it on the server. If AutoDeploy is set to false, then the mirroring operation restricts the deployment of the newer bundle. Accepts only the boolean values (true or false). By default, the option is set to true
CreateMonolithicBundle	Automatically creates monolithic package bundles consisting of only latest package rpms. It creates a separate monolithic bundle for each Service Pack release, and a separate monolithic bundle with the updates after the latest Service Pack release. It accepts Boolean values (true or false) only. By default the option is set to true. This option is supported for YOU patches only.
FilterPatchRPM	Restricts the mirroring operation of the YOU patch bundles to filter all the packages of the `.patch.rpm` type. This option creates an equivalent RPM package bundle in the local server. Accepts only the Boolean values (true or false). By default, the option is set to false. This option is supported only for the YOU patches. If the option is set to true, it filters the scripts of type `.sh` along with the `.patch.rpm` packages while mirroring YaST patches.

NOTE: The use of regular expressions (regexes) has changed in ZENworks 7.3 Linux Management. ZENworks 7.3 Linux Management does not use wildcard character matching. In ZENworks Linux Management 6.6.*x*, you can use a wildcard expression string instead of a regular expression string. In ZENworks 7.3 Linux Management, you should use `<Bundle>patch-.*</Bundle>` to mirror all bundles with the name starting with "patch-". ZENworks Linux Management supports all the Java regular expressions. For more information on the Java regular expressions, see the Java documentation (http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html).

25.3.2 Creating a Configuration File by Using the xzlmmirror Utility

The xzlmmirror utility is a graphical user interface that lets you to create or edit the mirror configuration files, and store it in an XML file that is compatible with the existing zlmmirror utility. The file consists of the configuration information for the remote servers, proxy servers, local servers, and catalogs.

Do the following tasks in the order listed to create a configuration file:

1.
2.

You can also edit the configuration file. For more information, see

Configuring the Servers

1 To start the xzlmmirror utility, enter the following command at the command line:

`xzlmmirror`

The xzlmmirror-Server Settings window is displayed.
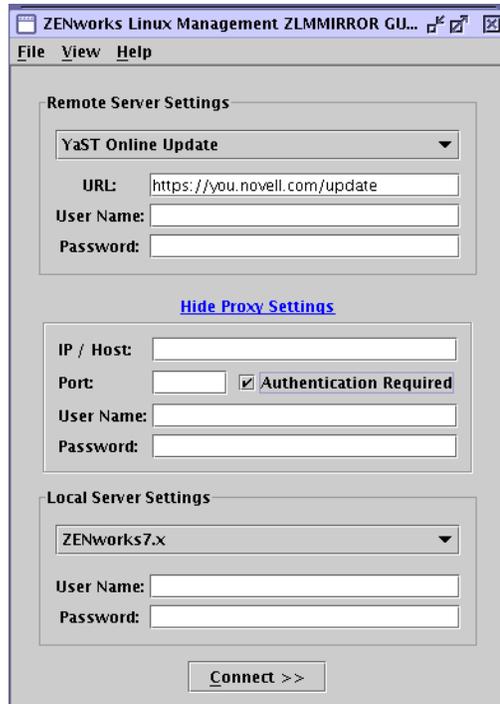
2 Configure the remote server that contains the software you want to mirror:

    2a Select the remote server type that contains the software you want to mirror.

- **ZLM:** ZENworks 7.3 Linux Management
- **DELL:** Dell Update Package FTP Server
- **RCE:** Red Carpet® Enterprise™ or ZENworks 6.*x* Linux Management
- **YAST:** YaST Online Updates
- **RHN:** Red Hat Network
- **YUM:** YUM
- **NU:** Novell Updates

The default URL of the server you want to mirror is displayed automatically in the following format, depending on the server type you have selected:

- **ZLM:** `https://server`
- **DELL:** `http://ftp.dell.com`
- **RCE:** `https://server/path`
- **YAST:** `http(s)://server/path` or `ftp://server/path`
- **RHN:** `http(s)://server/path`
- **YUM:** `http://server/path`

- ◆ **STATIC:** `/path/on/filesystem`
- ◆ **NU:** `https://nu.novell.com/repo`

2b Specify the username and password to connect to the remote server.

3 (Conditional) If you are connecting to the remote server through a proxy server, configure the proxy server settings. If the remote server does not connect through a proxy server, skip to Step 4.

3a Click *Show Proxy Settings*.

3b Specify the IP address or the host name of the proxy server.

3c Specify the port number of the proxy server.

3d To authenticate to the proxy server, select the *Authentication Required* check box, and specify the username and password for the proxy server.

4 Configure the local server that you want to receive the mirrored software. You can mirror the software either directly to your ZENworks Linux Management server, or to the file system of your ZENworks Linux Management server. However, mirroring the software to the file system does not add it to ZENworks.

4a Select the local server that you want to receive the mirrored software.

4b Specify the username and password to connect to the local server.

4c To validate the credentials for the servers, and to connect to the remote server, click *Connect*.

5 To view the log information of the server configurations, go to `/var/opt/novell/log/zenworks/zlmmirror.log` file.

6 Continue with "Configuring the Catalogs" on page 302.

Configuring the Catalogs

The xzlmmirror-Catalog Settings window is automatically displayed after the credentials are validated for the servers that you have specified in the xzlmmirror-Server Settings window. You must provide details about the catalogs and bundles you want mirrored to your server in the xzlmmirror-Catalog Settings window.

Review the following sections:

- ◆ "Adding Catalogs" on page 302
- ◆ "Editing Catalog Settings" on page 305

Adding Catalogs

The Add Catalogs page lets you configure each catalog you want to mirror.
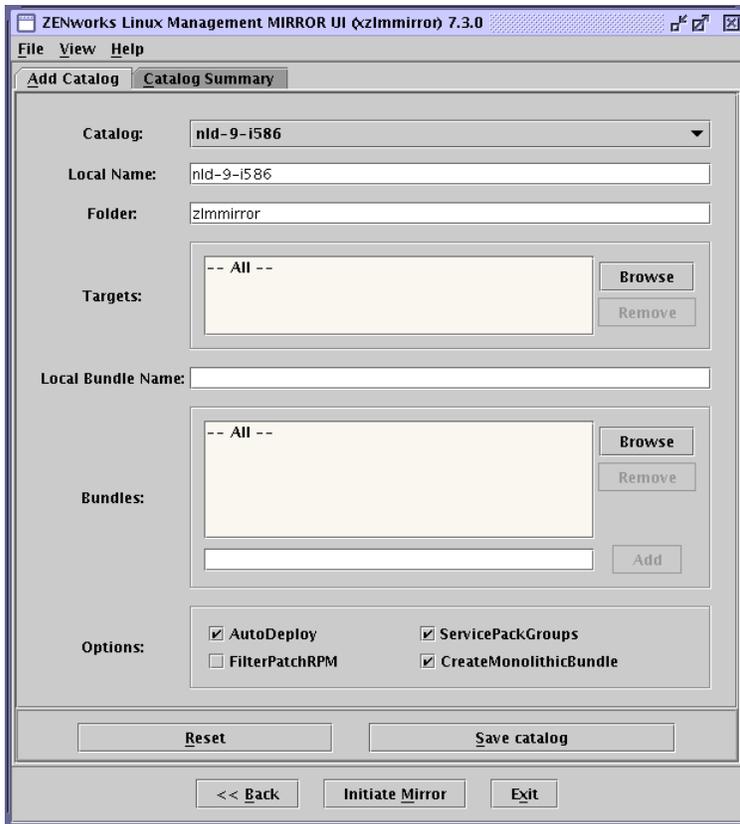
1 In the *Catalog* drop-down list, select the catalog that you want to configure.

2 In the *Local Name* field, specify a name for the selected catalog.

   The local name for the catalog should not be same as that reserved for the <catalogname>-patches folder. If the name is not specified, then the name of the catalog selected in the *Catalog* field is used.

3 In the *Folder* field, specify the eDirectory folder in which the bundles and catalogs are created and updated.

   If no folder is specified, then the catalogs and bundles are created and updated in the `/zlmmirror` folder.

4 In the *Targets* list, click *Browse* to browse for and select the targets you want to mirror. By default, all the targets in the selected catalog are mirrored.

   To remove a target from the list, select the target, then click *Remove*.

5 (Conditional) The *Category* field is displayed only if you have selected the NU type servers of SLES 10, SLED 10, and OES 2 in the xzlmmirror-Server Settings window. Select the categories you want to mirror. The available options are *Security*, *Recommended*, and *Optional*. By default, all the categories are mirrored.

6 In the *Local Bundle Name* field, specify a name for the bundle.

   If you specify the local bundle name, you must not specify the <Bundle> tag. This is applicable only for the RCE, NU, and RHN services in which a catalog has only one bundle on the remote server. The local bundle name is not applicable when you mirror OES from the RCE service with more than one bundle per catalog.

7 In the *Bundles* pane, specify the bundles you want to mirror by using one of the following ways:

- ◆ Click *Browse* to browse for and select the bundles you want to mirror. By default, all the bundles in the selected catalog are mirrored.

- ◆ Specify the bundle name you want to mirror, and click *Add* to add it to the list.

Deselect the check box next to the bundle to exclude it from the list.

To remove a bundle from the list, select the bundle, then click *Remove*.

8 (Conditional) If you are not using the YOU patches, specify the package you want to mirror in the *Packages* pane by using one of the following ways:

- ◆ Click *Browse* to browse for and select the packages you want to mirror. By default, all the packages in the selected catalog are mirrored.

- ◆ Specify the package name you want to mirror, and click *Add* to add it to the list.

To remove a package from the list, select the package, then click *Remove*.

9 To restrict the deployment of a new bundle when mirroring packages to an existing bundle, deselect the *AutoDeploy* check box.

This option is selected by default.

10 Configure the following additional options in the *Options* group if you are using YOU patches:

ServicePackGroups: Automatically creates bundle groups. This option is selected by default.

FilterPatchRPM: Allows the mirroring operation of the YOU patch bundles to filter all the packages of the `.patch.rpm` type. Select this check box to restrict the mirroring operation of the YOU patch bundles to filter all the packages of the `.patch.rpm` type. This option creates an equivalent RPM package bundle in the local server.

CreateMonolithicBundle: Creates monolithic package bundles consisting of only latest package RPMs. It creates a separate monolithic bundle for each Service Pack release, and a separate monolithic bundle with the updates after the latest Service Pack release. This option is selected by default.

11 (Optional) To set the default values for the catalog, click *Reset*.

12 To save the catalog settings in the Catalog Summary page, click *Save Catalog*.

To save the catalog settings to a file, click *File > Save*. You can only save those catalog settings that are listed in the Catalog Summary page to a file.

13 (Optional) To configure a different server, or to reset the server settings that you have already configured, click *Back*.

14 Continue with initiating the mirroring process. For more information, see .

Editing Catalog Settings
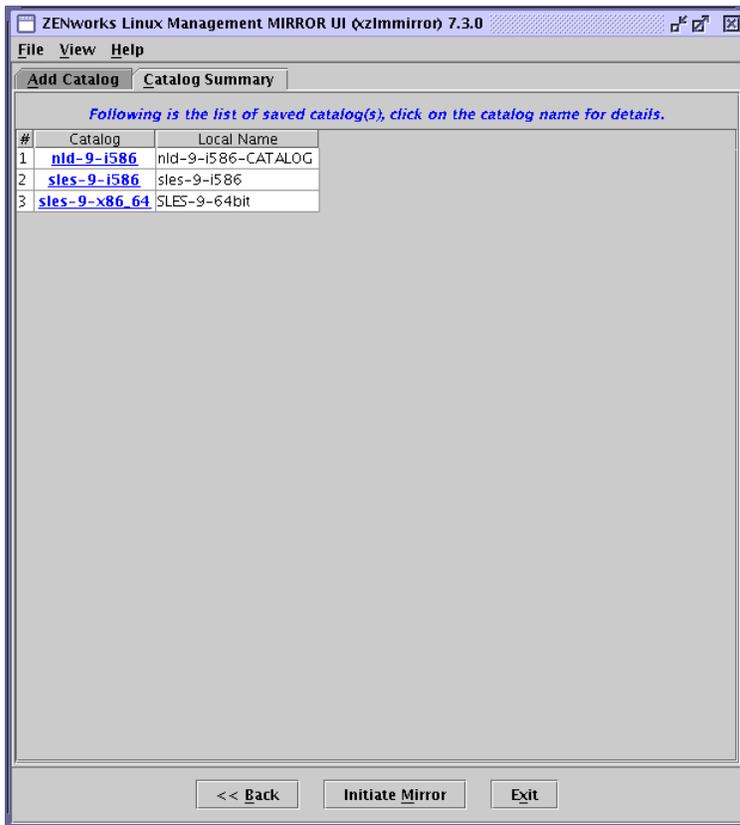
1 Click *Catalog Summary*.

The page displays the catalog names, the local names, and the category of the catalogs that you configured in the Add Catalogs page.

2 To view or edit the settings for a specific catalog, click the catalog.

The Catalog Details dialog box is displayed.

3 Click *Edit* to edit the catalog information displayed in the window.

Editing the Configuration File

1 Launch the xzlmmirror utility by entering the following command at the command line:

    xzlmmirror

2 Click *File > Open*.

3 Browse for and select the configuration file you want to edit.

The xzlmmirror-Server Settings window is displayed, where you can edit the desired settings.

For more information, see Section 25.3.2, "Creating a Configuration File by Using the xzlmmirror Utility," on page 300.

25.3.3 Mirroring Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2 from the NU and RCE Type Repositories

You can mirror patch bundles for SLES 10, SLED 10, SLES 11, SLED 11 and OES 2 from the NU and RCE type repositories such as nu.novell.com and update.novell.com. Review the following sections for more information:

- "Mirroring the Monolithic and Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2" on page 306
- "Mirroring the Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2" on page 306
- "Mirroring the Monolithic Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2" on page 306

Mirroring the Monolithic and Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2

Mirroring updates for SLES 10, SLED 10, SLES 11, SLED 11, and OES 2 platforms from NU Server and RCE Server by using the `zlmmirror m -c conf.xml` command creates patch bundles and a monolithic bundle`<catalogname>-bundle` with all the packages in it.

Mirroring the Patch Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2

To mirror only the patch bundles for SLES 10, SLED 10, SLES 11, SLED 11, and OES 2 platforms from RCE type and NU type remote servers, use the `-p` option in the `zlmmirror m -p -c mirror-conf.xml` command.

NOTE: The download progress is not displayed for individual packages while mirroring SLES 11 and SLED 11 patch bundles from the NU repository.

Mirroring the Monolithic Bundles for SLES 10 / SLED 10 / SLES 11 / SLED 11 / OES 2

To mirror the monolithic bundles without creating the patch bundles, use the `<Bundle>` tag of the mirror configuration file.For example, use `<Bundle>SLED10-Updates-bundle</Bundle>` to mirror the SLED10-Updates catalog.The slb option displays both monolithic and patch bundles. You can download the desired bundle by using the `<Bundle>` tag. To download the specific packages in the monolithic bundle, use the `<Bundle>` tag for the monolithic bundle and `<Package>` tags for the specific packages.For example, a sample `<Catalog>` section to mirror the Mozilla packages of the monolithic bundle is as follows:

```
<Catalog>

  <Name>SLED10-Updates</Name>

  <LocalName>SLED10-Updates</LocalName>

  <Folder></Folder>

  <Target>sled-10-i586</Target>

  <ExcludeTarget></ExcludeTarget>

  <Bundle>SLED10-Updates-bundle</Bundle>
```

```
  <ExcludeBundle></ExcludeBundle>

  <Package>Mozilla*</Package>

  <ExcludePackage></ExcludePackage>
</Catalog>
```

NOTE: The local name for the catalog should not be same as the name reserved for the folder `<catalogname>-patches`. In other words, the `<localName>` tag of the mirror configuration file should not use the same name as the `<catalogname>-patches`.

25.3.4 Testing and Performing the Mirroring Operation by Using zlmmirror

Before starting the mirroring operation, make sure that at least 10 GB of diskspace is available on the device.

After you have created the configuration file for a remote server, run the following command to perform a dry run of the mirroring operation, and optionally add the verbose flag to see detailed messages:

```
zlmmirror mirror -c filename.xml --dryrun --verbose
```

If this operation provides the intended results, run the mirror command without the dry run flag to complete the operation:

```
zlmmirror mirror -c zlmmirror-config.xml
```

If you mirror a bundle that contains multiple packages with multiple install type/freshen flags set, a unique version of the bundle is created for each install type/freshen combination.

For example, suppose you mirror a bundle that contains four packages assigned to one OS target. Of these four packages, one package has the install type flag set to false, the second package has the install flag set to true, the third package has the freshen flag set to false, and the fourth package has the freshen flag set to true. In this situation, four unique versions of the bundle are created.

The number of unique bundles created also depends on the number of OS targets. In the previous example, suppose the four packages, each with a different install type/freshen combination, have two OS targets. In this situation, a unique bundle is created for each install type/freshen combination and another unique bundle is created for each OS target. In this example, eight unique bundles are created.

The number of unique bundle versions created equals the number of unique install type/freshen combinations times the number of unique OS targets.

25.3.5 Testing and Performing the Mirroring Operation by Using the xzlmmirror Utility

Before you begin the mirroring process, you need to create the mirror configuration file. For more information, see Section 25.3.2, "Creating a Configuration File by Using the xzlmmirror Utility," on page 300.

To mirror the software:

1 Click *Initiate Mirror* in the Catalogs Settings window to initiate the mirroring process. The Mirror Options dialog box is displayed.

2 Select the options that you need:

Dry run: Prints the packages to be mirrored or added.

Packagesets: Mirrors only the patch bundles for RCE and NU servers. This excludes the package set bundles.

Force nevra: Overwrites an existing package with a new package with a conflicting NEVRA (name, epoch, version, release, and architecture).

Re-Download: Downloads the contents even if they are already mirrored.

Sync-local: Synchronizes the local server repository with the remote server repository.

Debug: Displays the debug output.

Verbose: Displays the verbose output.

3 Click *OK*. The Configuration Summary dialog box is displayed, where you can view the mirror options and all the mirror configuration settings.

4 Click *Proceed* to begin the mirroring process.

25.4 Distributing Catalogs from a Public ZENworks Linux Management Server

The following sections contain additional information:

◆ Section 25.4.1, "Creating a Public ZENworks Linux Management Server," on page 308
◆ Section 25.4.2, "Accessing a Public ZENworks Linux Management Server," on page 308

25.4.1 Creating a Public ZENworks Linux Management Server

1 Create a default registration rule on the ZENworks Linux Management Server that creates a device in a specified folder.

For more information, see Part III, "Device Registration," on page 99 and Section 17.2, "Creating Folders," on page 184.

2 Assign all catalogs that you want to make public to that folder.

For more information, see Section 22.3, "Assigning Catalogs," on page 276.

25.4.2 Accessing a Public ZENworks Linux Management Server

1 Create a zlmmirror configuration file.

For more information, see Section 25.3.1, "Creating the Configuration Files by using the Command Line Utility," on page 295.

2 Install the ZENworks Linux Management agent on a workstation and register against the public ZENworks Linux Management Server using no registration key (to use the default registration rule).

For more information, see "Installing the ZENworks Agent and Registering the Device" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

3 Copy the contents of the `deviceid` and `secret` file from that workstation (`/etc/opt/novell/zenworks/zmd` on SLES 9 and OES, `/etc/zmd` on SLES 10 and SLED 10) to the `zlmmirror.conf` file in the <User> and <Password> tags of the <RemoteServer> section.

4 Mirror using the configuration file you created in Step 1 to Step 3.

Only software assigned to the newly registered device is available for mirroring.

For more information, see Section 25.3.4, "Testing and Performing the Mirroring Operation by Using zlmmirror," on page 307.

25.5 Mirroring Dell Update Packages to Your ZENworks Server

You can mirror Dell Update Packages from the Dell FTP site or from a CD obtained from Dell to your ZENworks server. Dell Update Packages let you update and configure hardware and system settings (including BIOS, DRAC, RAID, BMC, and FRMW configurations) on Dell PowerEdge servers.

IMPORTANT: Before you can use Dell Update Packages on your Dell servers, you must complete the steps in "Enabling Dell PowerEdge Support" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

If you plan to update Dell PowerEdge servers using Dell Update Packages, we recommend that you mirror the packages from the Dell FTP site before installing the ZENworks Agent on the managed PowerEdge servers. You can also mirror the packages after installing the ZENworks Agent on the managed PowerEdge servers but before registering them in the ZENworks Management Zone. Mirroring the Dell Update Packages prior to installing the ZENworks Agent or registering the servers in the Management Zone ensures that all Dell model numbers are loaded into the database, the standard reports are run as the servers register, and the Dell Update Packages exist in the ZENworks package repository. For more information, see Chapter 23, "Using Dell Update Package Bundles," on page 283.

To mirror Dell Update Packages from a remote server or from a CD to your ZENworks server:

1 Run the following command to generate an empty configuration file:

`/opt/novell/zenworks/bin/zlmmirror conf-generate` *filename*`.xml`

This command generates a template configuration file in the current directory.

For more information, see Section 25.3.1, "Creating the Configuration Files by using the Command Line Utility," on page 295.

2 Open the empty configuration file in a text editor.

3 In the `<RemoteServer>` section, edit the following configuration elements:

Configuration Element	Setting
`<Base></Base>`	Path to the server you want to mirror:
	`<Base>http://ftp.dell.com</Base>`
	or
	Path to the mountpoint of the CD you want to mirror:
	`<Base>file:///path/to/cd</Base>`
`<Type></Type>`	Type of server you want to mirror:
	`<Type>dell</Type>`

4 In the `<LocalServer>` section, edit the following configuration elements:

Configuration Element	Setting
`<Type></Type>`	Type of mirroring you want performed:
	`<Type>zlm</Type>`
	Specifying zlm mirrors the Dell Update Packages directly to your ZENworks Linux Management server. After mirroring, the Dell Update Packages are displayed in the ZENworks Control Center.
`<User></User>`	Name to use when connecting to your ZENworks Linux Management (local) server:
	`<User>Administrator</User>`
	The Administrator user should be specified if you want to use the default administrator account.
`<Password></Password>`	Password for the account provided in User:
	`<Password>password</Password>`
	If you are using the Administrator account, this is the password you specified during the server installation. For information about encoding your password, see Section 25.10, "Encoding the ZENworks Server Password," on page 319.

5 To list all catalogs and bundles available on the remote ftp site, execute the `zlmmirror server-list-bundles -c filename.xml` command. For more information, view help for zlmmirror by executing the following command: `zlmmirror --help`.

6 In the `<Catalog>` section, edit the following configuration elements:

Configuration Element	Setting
`<Name></Name>`	Name of the catalog you want to mirror from this remote server:
	`<Name>catalog_name</Name>`

Configuration Element	Setting
`<Folder></Folder>`	Name of the folder where the Dell Update Packages are created and updated:
	`<Folder>/folder_name</Folder>`
	Specifies the eDirectory folder (for example, `/Dell`) where bundles and catalogs are created and updated. If not specified, the catalogs and bundles are created and updated in the `/zlmmirror` folder.

Your edited zlmmirror configuration file should look similar to the following example. If your configuration file is set up to mirror a CD, the `<Base></Base>` configuration element in the `<RemoteServer>` section contains `<Base>file:///path/to/cd</Base>` instead of `<Base>http://ftp.dell.com</Base>`.

```
<ZLMMirrorConf>
    <Session>
        <RemoteServer>
            <Base>http://ftp.dell.com</Base>
            <Proxy></Proxy>
            <Type>dell</Type>
            <User></User>
            <Password></Password>
        </RemoteServer>
        <LocalServer>
            <Type>zlm</Type>
            <Base></Base>
            <User>Administrator</User>
            <Password>password</Password>
            </LocalServer>
            <Catalog>
                <Name>catalog_name</Name>
                <LocalName></LocalName>
                <Folder>/folder_name</Folder>
                <Target></Target>
                <ExcludeTarget></ExcludeTarget>
                <Bundle></Bundle>
                <ExcludeBundle></ExcludeBundle>
            </Catalog>
    </Session>
</ZLMMirrorConf>
```

7 Save the file.

This downloads all the bundles available in the specified catalog. If you want to download a specific bundle, specify the bundle name as shown below:

```
<Bundle>Bundle_Name</Bundle>
```

8 Mirror the Dell Update Packages by running the following command:

```
zlmmirror m -c=filename.xml
```

where `filename.xml` is the name of the zlmmirror configuration file you created in Step 1 on page 309.

After the mirroring operation is complete, the Dell Update Packages are automatically bundled and displayed in the ZENworks Control Center on the Bundles page. The first time you mirror Dell Update Packages, all available packages are mirrored; subsequent mirror sessions obtain upgraded packages only.

To determine if there are updated Dell Update Package bundles available for the servers in your system, in the ZENworks Control Center, click the *Devices* tab, then click *Servers*. A link in the *Dell Updates* column indicates whether there is a Dell Update Package bundle available in the ZENworks package repository for each Dell PowerEdge server in the list. You can click the link to view the name of the Dell Update Package bundle appropriate for the device.

If the Dell Update Package bundle is already installed on the device, but a newer version of the bundle is available, you can deploy the newer version. For more information, see Section 23.4, "Deploying an Updated Version of a Dell Update Package Bundle," on page 287.

If the Dell Update Package bundle is not assigned to the device, you assign devices as you would for any bundle. For more information, see Section 23.2, "Assigning Dell Update Package Bundles," on page 283.

If you assign the Dell Update Packages to devices using bundles, the packages are always installed. For this reason, it is possible to downrev your firmware using Dell Update Packages distributed via bundles.

If you assign the Dell Update Packages to devices using catalogs, the packages are installed only in an upgrade situation. It is not possible to downrev firmware using Dell Update Packages distributed via catalogs.

To create catalogs and assign devices, continue with Section 22.1, "Understanding Catalogs," on page 271.

During installation of the Dell Update Packages, if you get an error message stating that your system needs more contiguous RAM, reboot the system and retry the installation.

You should periodically run the zlmmirror utility to obtain updated Dell Update Packages. You can automate the process by creating a cron job to perform the mirror session as often as needed (monthly, for example).

25.6 Mirroring Bundles Between ZENworks Linux Management Servers Located in Different Management Zones

You can mirror bundles in a catalog from a remote primary ZENworks Linux Management server located in one management zone to a local primary ZENworks Linux Management server located in another management zone. The servers use the HTTPS protocol at TCP port 443 to communicate with each other. You can mirror RPM package bundles, patch bundles, file bundles, and DUP bundles from the remote ZENworks server to the local ZENworks server. When you mirror bundles

from the remote server, only the version of the bundle that is currently deployed is mirrored to the local server. A new version of the bundle is created on the local server irrespective of the deployed version of the bundle on the remote server.

1 Before registering to the remote server, delete the existing ZENworks service on the local server by entering the following command:

```
Local-ZLM-Server# rug sd <URL_of_the_existing_ZLM_server>
```

2 Register the local primary ZENworks Linux Management server to the remote primary ZENworks Linux Management server as a ZENworks service by entering the following command:

```
Local-ZLM-Server# rug sa <URL_of_the_remote_ZLM_server>
```

You are required to register the server only once, so that the local server updates its credentials to the remote server.

3 Add the bundles that you want to mirror to a catalog on the remote server, and assign the catalog to the local Primary Server from the remote server.

4 Assign the catalog on the remote server to the local server by using the *Assign Catalog* option in the ZENworks Control Center, or by entering the following command at the command line:

```
zlman server-add-catalog
```

For more information, see Section 22.3, "Assigning Catalogs," on page 276 and the zlman (1) (page 562).

5 Create a mirror configuration file.

For more information, see "Creating the Configuration Files by using the Command Line Utility" on page 295 or "Creating a Configuration File by Using the xzlmmirror Utility" on page 300.

6 In the `<Remote Server>` section, edit the following configuration elements:

Configuration Element	Setting
`<Base></Base>`	Path to the server you want to mirror
	`<Base>https://server</Base>`
`<User></User>`	DeviceID of the local server
	`<User>aa06e91b8a7447fba83c3aaf2412c03</User>`
`<Password></Password>`	Secret of the local server
	`<Password>ee3f30ed0d1a4cee9fd61420a9898926</Password>`
`<Type></Type>`	Type of server you want to mirror
	`<Type>zlm</Type>`

7 In the `<Local Server>` section, edit the following configuration elements:

Configuration Element	Setting
`<Type></Type>`	Type of the local server you want mirrored
	`<Type>zlm</Type>`
`<User></User>`	User who uses `administrator` as the username to log in to the ZENworks Control Center.
	`<User>administrator</User>`
`<Password></Password>`	Password for the account provided in the `User` element.
	`<Password>password</Password>`

8 In the `<Catalog>` section, edit the following configuration element:

Configuration Element	Setting
`<Name></Name>`	Name of the catalog you want to mirror from the remote server.
	`<Name>catalog_name</Name>`

NOTE: While mirroring YOU patch bundles from a remote server in one management zone to a primary local server in another zone, packages for the target oes-9-i586 are added to the patch bundle on the local ZENworks Linux Management server, although the patch bundles contain packages only for target sles-9-i586.

While mirroring the YaST patches for SLES 9 platforms from the YOU repository and OES 1 platforms from the RCE repository, you must mirror the patch bundles for 32-bit target and 64-bit target to separate folders on the ZENworks Linux Management server. This is because the patches for 32-bit and 64-bit platforms are hosted in two different channels in the repository. The mirroring process skips the YOU patch bundle download or update if a bundle with the same name already exists in the folder path on the server.

25.7 Mirroring Red Hat Updates from the NU Repository by Using a YUM Subscription

You can mirror Red Hat updates from the NU repository by using YUM subscriptions and updating the RHEL devices. These updates are available from the RES catalogs for 32-bit and 64-bit target platforms. You can list the RES catalogs such as RES3, RES4, and RES5 by using an NU subscription. However, to mirror the Update bundle for a specific RES catalog, you must configure a YUM subscription. You cannot use an NU subscription because of the limitation of the distro target information in the RES catalog metadata in the NU repository.

To use a YUM subscription to mirror the RES catalogs from the NU repository:

1 Run the following command to verify if there are any RES or Red Hat catalogs on the remote NU server:

```
zlmmirror slc -c  NU_mirror_configuration_file  -v
```

This lists the catalogs on the remote NU server.

2 In the NU mirror configuration file's `<RemoteServer>` section, edit the following configuration elements:

Configuration Element	Setting
`<Base></Base>`	Specify the path to the server you want to mirror, the catalog name, and the architecture.
	`<Base>https://nu.novell.com/repo/$RCE/`*`catalog_name`*`/`*`architecture`*`</Base>`
	For example:
	The base URL for a 32-bit target of a RES5 catalog is `<Base>https://nu.novell.com/repo/$RCE/RES5/i386</Base>`.
	The base URL for a 64-bit target of a RES5 catalog is `<Base>https://nu.novell.com/repo/$RCE/RES5/x86_64</Base>`.
`<Type></Type>`	Type of server you want to mirror.
	`<Type>yum</Type>`
`<Platform></Platform>`	The platform of the device to which you want to mirror the packages.
	`<Platform>`*`platform`*`</Platform>`
	For example, if the target platform is rhel-5-i386, edit the Platform tag to be:
	`<Platform>rhel-5</Platform>`.
	The target platform must be defined in ZENworks Linux Management.
`<User></User>`	Username to log in to the remote NU server.
	`<User>`*`user`*`</User>`
`<Password></Password>`	Password for the username provided in the `User` element.
	`<Password>`*`password`*`</Password>`

3 In the `<Catalog>` section, edit the following configuration element:

Configuration Element	Setting
`<Name></Name>`	Specify the name of the catalog you want to mirror from the remote server in the following format:
	`<Name>`*`platform`*`-catalog</Name>`
	For example, if the platform is rhel-5, the catalog name must be `<Name>rhel-5-catalog</Name>`.

In the `<Catalog>` section, it is not necessary to provide a value for the `<Target>` tag, because the bundles of the catalog must be separately mirrored for each target. If you specify a value for the `<Target>` tag, you can only mirror those architecture packages that match the specified target. You must specify separate URLs for each target in the `<Base>` tag in the configuration file's `<Remote Server>` section.

To mirror catalog packages for 32-bit RHEL targets such as rhel-5-i386, the mirroring process automatically mirrors the packages of all compatible 32-bit architectures such as i386, i586, i686, and noarch.

To mirror catalog packages for 64-bit RHEL targets such as rhel-5-x86_64 to a given bundle, the packages for 32-bit architecture are added as target rhel-5-i386 in the bundle. You must convert targets of all the 32-bit architecture packages in the mirrored bundle from 32-bit to the corresponding 64-bit target by using the `zlman bap` command.

For example, to convert all the 32-bit architecture packages from rhel-5-i386 to the corresponding rhel-5-x86_64 target, you must run the `zlman bap` command as follows:

```
zlman bap --freshen=true bundle_name rhel-5-x86_64 /var/opt/novell/
zenworks/pkg-repo/bundles/first_two_letters_of_the_bundle_GUID/
bundle_GUID/bundle_version/rhel-5-i386/*.rpm.
```

4 Save the configuration file.

25.8 Mirroring Dell Updates from the OpenManage Server Administrator Repository by Using a YUM Subscription

You can mirror Dell software, and Dell drivers and updates such as BIOS and firmware, from the YUM - based OpenManage Server Administrator (OMSA) repository to update the Dell PowerEdge Linux servers that are running on Dell supported RHEL or SLES platforms. These updates for SLES and RHEL devices are available on the officially supported YUM repository for OpenManage at the Dell Linux Repository (http://linux.dell.com/repo/hardware/latest/).

You can add the YUM service to the managed device and manually install these software from the repository by using the `rug` command as follows:

```
rug sa -t yum repo-md_URL_from_where_you_want_to_mirror service_name
```

For example, to manually install the software from `http://linux.dell.com/repo/hardware/latest/platform_independent/suse10_64/`, you must execute the `rug` command as follows:

```
rug sa -t yum http://linux.dell.com/repo/hardware/latest/platform_independent/
suse10_64/  dell-updates
```

To mirror these updates for a specific device model, you must configure a YUM subscription.

To use a YUM subscription to mirror the DELL updates from the OpenManage Server Administrator Repository:

1 Run the following command to verify if the required catalogs for a given target platform are available on the remote Dell Repository:

```
zlmmirror slc -c yum_mirror_configuration_filename -v
```

2 In the YUM mirror configuration file's `<RemoteServer>` section, edit the following configuration elements:

Configuration Element	Setting
`<Base></Base>`	Specify the path to the server you want to mirror, the device model, and the operating system information.
	`<Base>http://linux.dell.com/repo/hardware/latest/` *`device_model`*`/`*`osinfo`*`</Base>`
	For example:
	If the device model is DELL PowerEdge R710 server, and the operating system is 64-bit SLES 10, the base URL is `<Base>http://linux.dell.com/repo/hardware/latest/per710/suse10_64/</Base>`.
`<Type></Type>`	Type of server you want to mirror.
	`<Type>yum</Type>`
`<Platform></Platform>`	The platform of the device to which you want to mirror the packages.
	`<Platform>`*`platform`*`</Platform>`
	For example, if the target platform is sles-10-x86_64, edit the Platform tag to be:
	`<Platform>sles-10</Platform>`.
	The target platform must be defined in ZENworks Linux Management.

3 In the `<Catalog>` section, edit the following configuration element:

Configuration Element	Setting
`<Name></Name>`	Specify the name of the catalog you want to mirror from the remote server in the following format:
	`<Name>`*`platform`*`-catalog</Name>`
	For example, if the platform is sles-10, the catalog name must be `<Name>sles-10-catalog</Name>`.

In the `<Catalog>` section, it is not necessary to provide a value for the `<Target>` tag, because the bundles of the catalog must be separately mirrored for each target. If you specify a value for the `<Target>` tag, you can only mirror those architecture packages that match the specified target. You must specify separate URLs for each target in the `<Base>` tag in the configuration file's `<RemoteServer>` section.

4 Rename the mirrored package bundle appropriately after mirroring.

If the catalog that is mirrored for 64-bit target (for example, sles-10-x86_64) also contains the 32-bit architecture packages, you must convert all the 32-bit architecture packages in the mirrored bundle from 32-bit target to the corresponding 64-bit target by using the zlman bap command.. You must convert targets of all the 32-bit architecture packages in the mirrored bundle from 32-bit to the corresponding 64-bit target by using the `zlman bap` command.

To convert all the 32-bit architecture packages from sles-10-i586 to the corresponding sles-10-x86_64 target, you must run the `zlman bap` command as follows:

```
zlman bap --freshen=true bundle_name sles-10-x86_64 /var/opt/novell/
zenworks/pkg-repo/bundles/first_two_letters_of_the_bundle_GUID/
bundle_GUID/bundle_version/sles-10-i586/*.rpm.
```

For example:

```
zlman bap --freshen=true zlmmirror/sles10-OMSA-bundle sles-10-x86_64  /
var/opt/novell/zenworks/pkg-repo/bundles/31/
316c0e94afa5d6f8f96964ca556d251b/2/sles-10-i586/*.rpm
```

5 Verify if all the packages are updated in the bundle to the specified target.

6 Assign the catalog or bundle to the corresponding target device and deploy the updates.

25.9 Deploying Red Hat Network Updates

When you use ZENworks Linux Management to mirror a Red Hat distribution from the Red Hat Network, the mirroring process creates a single bundle containing all of the RPM packages. This bundle is not usually assigned directly to a managed device because it contains the entire Red Hat distribution and might contain RPM packages that conflict with each other.

Following are two scenarios for updating devices with RPM packages:

25.9.1 Providing All RPM Packages and Package Bundles through a Catalog (Pulling)

If you want to provide all RPM packages via a catalog, create a catalog and add the mirrored Red Hat Network bundle to it, then assign the catalog to the managed devices. This allows users to have access through the catalog to all of the RPM packages contained in the Red Hat Network bundle.

For more information on mirroring and catalogs, see Section 25.3, "Configuring a Software Mirror," on page 294 and Section 22.2, "Creating Catalogs," on page 271.

From a managed device, there are two ways that you can force deployment and installation of the updates included in the Red Hat Network bundles contained in a catalog:

◆ **Using the ZENworks Linux Management Update Manager:** From the managed device, click *System > Software Update*, then select the catalog and click *Mark for installation > Run now*.

◆ **Using rug:** On a managed device, start a console session and enter the rug up command.

For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop (SLED 10) devices:

```
/usr/bin/rug up
```

For other managed devices:

```
/opt/novell/zenworks/bin/rug up
```

For more information, see rug (1) (page 586).

25.9.2 Delivering Specific RPM Packages (Pushing)

If you want to provide specific RPM packages, you can create a custom bundle by selecting the desired subset of RPM packages from the initial bundle that was created when mirroring the Red Hat Network. Or, you can create several custom bundles, each containing one or more RPM packages. It is best to test your custom bundles on a single device to verify that there are no conflicts within a bundle. If the test is successful, you can then assign the bundles to your managed devices.

To ensure that the packages contained in the custom bundle can meet all of their dependencies, you can create a catalog containing the mirrored Red Hat Network bundle and make it available to the desired managed devices. During the catalog creation process, you can hide this catalog from users. After you assign the custom bundle to devices, if a package requires other packages for dependency resolution, the device has access to the packages in the hidden catalog. For more information, see Section 22.2, "Creating Catalogs," on page 271.

Managed devices refresh on a schedule. Also, an administrator can trigger a device refresh through the ZENworks Control Center. When a device refreshes, it downloads the bundle automatically from the server and installs it.

The managed device requests one or more bundles from the server. In other words, the server does not actually push the bundle. However, the server can tell the managed device to refresh immediately. You can also modify the refresh interval centrally from the server for one or more managed devices. Otherwise, the client refreshes on its own schedule to look for a scheduled action.

From a managed device, you can use rug to force a refresh by entering the `rug refresh` command.

For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE Linux Enterprise Desktop (SLED 10) devices:

```
/usr/bin/rug refresh
```

For other managed devices:

```
/opt/novell/zenworks/bin/rug refresh
```

For more information, see rug (1) (page 586).

25.10 Encoding the ZENworks Server Password

When you configure the XML configuration file prior to performing a mirroring operation, you specify your ZENworks Server's password in the `LocalServer` section. To provide enhanced security, you can encode the password before placing it in the configuration file.

To encode the ZENworks Server's password, execute the following command:

```
echo mypassword | recode ../b64
```

where *mypassword* represents your ZENworks Server's password. You can then use the resulting text in place of the clear text password.

Creating RPM Packages From Tarballs

26

Novell® ZENworks® Linux Management uses Red Hat Package Manager (RPM). RPM is a powerful package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages on different devices.

ZENworks Linux Management- Dell Edition supports the RPM format.

RPM Packages are traditionally created using a `.rpm` spec file. This is the native RPM method, and includes a number of steps, including building the software to be packaged from sources. This method is the most powerful and flexible because it can exercise all of the options available in RPM.

This section describes the simplest method to create a `.rpm` file. At the same time, it is also the least flexible.

The following sections contain additional information:

26.1 Alien Package Converter Overview

The Alien package converter is a simple program to convert packages from one format to another format. However, converting package formats does not usually work very well; package dependencies and other metadata do not carry over from one distribution to another, much less across packaging systems.

For our purposes, however, it works nicely. The Alien package converter allows the transformation from a tarball to a `.rpm` file, which can then be added to a ZENworks Server for distribution.

Additional information and download information about Alien package converter can be found on the Alien Package Converter page (http://www.kitenet.net/programs/alien/).

26.2 Installing Alien Package Converter

1 Ensure that you Perl version 5.004 or later.

2 Download the Alien package converter utility from the Alien Package Converter page (http://www.kitenet.net/programs/alien/alien_8.53.tar.gz).

3 Unpack, make, and install the utility using the following commands:

```
$ tar zxvf alien_8.53.tar.gz
$ cd alien
$ perl Makefile.PL
$ make
```

4 Log in as `root` or use sudo:

```
$ sudo make install
```

26.3 Example Usage

The following example describes the procedure to deliver a file called readme to the `/usr/share/myapp` directory:

1 Enter the following commands to create the directory structure and create the .tar file:

```
$ mkdir -p usr/share/myapp
```

```
$ echo "Hello World" >usr/share/myapp/readme
```

```
$ tar zcvf helloworld.tgz usr
```

When the tarball is unpacked, it will create the `/usr/share/myapp` directory containing the readme file.

2 Use Alien package converter to make an RPM package of the tarball by entering the following command:

```
$ alien -r helloworld.tgz
```

The Alien package converter creates the `helloworld-1-2.noarch.rpm` package.

3 Verify that the package is valid and list its contents by entering the following commands:

```
$ rpm -qlp helloworld-1-2.noarch.rpm
```

```
/usr
```

```
/usr/share
```

```
/usr/share/myapp
```

```
/usr/share/myapp/README
```

The alien utility has other options, such as to set the version and description of the package. See "man alien" for more information.

Preboot Services

VI

The following sections provide information on Novell® ZENworks® Linux Management Preboot Services features and procedures:

Preboot Services Overview

27

Novell® ZENworks® Linux Management Preboot Services contains functionality that allows you to perform tasks on devices before their operating systems boot. Currently for ZENworks Linux Management, "devices" are servers and workstations.

The following sections provide an overview of Preboot Services:

27.1 Preboot Services Functionality

Preboot Services allows you to automatically or manually do any of the following to a Linux device when it boots:

- Run AutoYaST and kickstart installations
- Run ZENworks scripts on the device
- Make an image of the device's hard drives
- Restore an image to the device
- Apply an existing image to multiple devices
- Configure Dell devices

To accomplish these tasks automatically using the ZENworks Control Center, you simply need to have PXE (Preboot Execution Environment) enabled on your devices, and have preboot bundles configured and assigned to the devices. Then, the devices can automatically execute these bundles when they boot.

You can also execute some Preboot tasks on devices using CDs, DVDs, or a ZENworks partition, rather than using PXE.

27.2 Preboot Services Strategies

The following are some ways you can use Preboot Services:

- **Automate Linux installations.** You can automate kickstart or AutoYaST installations.
- **Create and restore base images.** You can create base images from existing devices, as well as restoring images to any manageable device.
- **Restore devices to a clean state.** You can quickly and efficiently reset devices to an initial state, such as in a lab.
- **Set up devices for future reimaging.** You can set up devices so that the next time they reboot, they do the imaging work that is contained in their assigned bundle.

- **Multicast images.** You can apply an image of one device to many other devices. This is an excellent feature for initially setting up a lab.
- **Configure Dell devices.** You can configure basic boot settings on Dell devices.

27.3 Preboot Bundles

In the ZENworks Control Center, Preboot Services tasks are contained in Preboot bundles. The following five Preboot bundle types are available:

- **AutoYaST bundle:** Describes the location and access protocol of an AutoYaST response file and network installation directory for SUSE® Linux. This bundle allows you to use Preboot Services to launch an AutoYaST automated installation of SUSE Linux. This is only available for Linux devices that are PXE-enabled. AutoYaST bundles cannot be run using a boot CD or a ZENworks partition.
- **Dell Configuration bundle:** Describes the location of files and scripts for configuring Dell servers. This bundle allows you to use Preboot Services to configure the server's BIOS, BMC, RAID, and DRAC settings and to create a Dell utility partition. This is only available for Linux devices that are PXE-enabled. Dell Configuration bundles cannot be run using a boot CD or a ZENworks partition.
- **Kickstart bundle:** Describes the location and access protocol for a kickstart response file. This bundle allows you to use Preboot Services to launch an automated kickstart installation of Red Hat Linux. This is only available for Linux devices that are PXE-enabled. Kickstart bundles cannot be run using a boot CD or a ZENworks partition.
- **ZENworks Image bundle:** Lists one or more ZENworks images (base plus add-ons) that can be restored on a device. This bundle allows you to define simple imaging operations.
- **ZENworks Multicast bundle:** Specifies an image that can be sent using the multicast protocol. This bundle allows you to send an image to a large number of devices in a single operation, thus minimizing network traffic. It is ideal for labs, classrooms, and staging areas.
- **ZENworks Script bundle:** Allows you to write a custom Linux bash script. This provides detailed control over ZENworks imaging operations, as well as most Linux-based preboot tasks.

To create one of these bundles: In the ZENworks Control Center interface, click *Bundles > New > Bundle > Preboot bundle > Next*, then select a bundle type. For more information, see .

27.4 Configuring Preboot Services

In the ZENworks Control Center, you can set up default Preboot Services configurations for all of your devices. Some settings can be overridden at the device, group, or folder level.

You can configure the following settings per "ZENworks Management Zone":

- **Preboot Services Menu options:** The menu contains seven options: 1) *Start ZENworks imaging*, which automatically executes the bundle; 2) *Start ZENworks imaging maintenance*, which accesses the bash prompt; 3) *Disable ZENworks partition*; 4) *Enable ZENworks partition*; 5) *Start DELL DTK*; 6) *Start DELL DTK (Maintenance Mode)*; and, 7) *Exit*, which resumes booting. You can configure whether the Preboot Services Menu is displayed upon booting, not displayed, or allowed to be displayed only when Ctrl+Alt is pressed during booting.

- **Image storage security:** You can restrict where to save image files on the imaging server.

- **Non-registered device settings:** You can use Preboot Services to automatically name your non-registered devices using such criteria as prefixes, BIOS information (like asset tags or serial numbers), DNS suffixes, and you can set up DHCP or IP addresses.

- **Preboot work assignment rules:** Work assignment rules are used to determine which bundle should be applied to which device. The work rules use logic to determine whether a device meets the requirements for applying the Preboot bundle. A rule is comprised of filters that are used to determine whether a device complies with the rule. The AND and OR logical operators are used for creating complex filters for the rule.

- **Preboot referral lists:** When a device boots, it is necessary for it to find its home ZENworks Management Zone to get its assigned preboot work. If multiple management zones exist on the network, referral lists provide a method for allowing a managed device to find its home zone.

- **Intel Active Management Technology (AMT):** Intel* AMT provides Preboot Services with persistent device identification.

To configure these settings, click *Configuration > Preboot Services*. For more information, see Section 29.4, "Configuring Preboot Services Defaults," on page 379.

27.5 Setting Up Devices to Use Preboot Bundles

In order for a device to automatically use a Preboot bundle, you must first assign a Preboot bundle to the device, its parent folder, or its group; and then you must set up the device to apply the bundle.

Preboot Services utilizes PXE and other boot mechanisms and media to trigger the preboot work.

There are many methods for accessing the *Add* button to assign bundles to devices, or devices to bundles, including the following:

- Click *Devices*, select the box next to *Name*, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the *Servers* and *Workstations* folders.

- Click *Devices*, select the box next to *Servers*, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the *Servers* folder.

- Click *Devices*, select the box next to *Workstations*, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the *Workstations* folder.

- Click *Devices > Servers*, select the box next to *Status Name*, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the *Servers* folder.

- Click *Devices > Servers*, select the box next to one or more servers, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the selected *Servers* and *Workstations* folders.

- Click *Devices > Workstations*, select the box next to *Status Name*, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the *Workstations* folder.

- Click *Devices > Workstations*, select the box next to one or more workstations, then click *Action > Assign bundle*.

  Assigns bundles to all of the devices in the selected *Workstations* folder.

- Click *Devices > Servers*, select a server, then click *Advanced* (in *Effective Bundles*).

Assigns bundles to the selected server.

- Click *Devices > Workstations*, select a workstation, then click *Advanced* (in Effective Bundles).

    Assigns bundles to the selected workstation.

- Click *Bundles*, select the box next to *Status Name*, then click *Action > Assign bundle*.

    Assigns all bundles to the devices that you select in the wizard.

- Click *Bundles*, select the box next to one or more bundle names, then click *Action > Assign bundle*.

    Assigns the selected bundles to the devices that you select in the wizard.

For more information on assigning bundles and how to set up devices to apply the assigned bundles, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

Understanding Preboot Services in ZENworks Linux Management

28

This section provides an understanding of Novell® ZENworks® Linux Management Preboot Services and how you can use it in your Linux network:

28.1 How Do You Implement Preboot Services?

Preboot Services utilizes the following to make its functions possible:

- **PXE (Preboot Execution Environment):** An Intel specification that allows a device to boot from the network, instead of its hard drive or other local media. ZENworks Linux Management can use PXE to launch Preboot Services.
- **Preboot Services bootable CD or DVD:** Used where PXE is not installed or where you want to manually perform a Preboot Services operation.
- **Preboot Services bootable diskette:** Enables using the Preboot Services bootable CD or DVD when the device doesn't support booting from a CD or DVD.
- **ZENworks partition:** Enables you to set up a device for unattended imaging operations where the device is not PXE enabled or does not have access to PXE network services.

28.2 What Is the Preboot Execution Environment (PXE)?

The following sections provide information on using PXE in Linux Management:

28.2.1 Understanding How Preboot Services Uses PXE

PXE uses DHCP (Dynamic Host Configuration Protocol) and TFTP (Trivial File Transfer Protocol) to locate and load bootstrap programs from the network. The PXE environment is loaded from the BIOS on the NIC.

In ZENworks Linux Management, Preboot Services uses PXE to discover if there is Preboot Services work specified for a device and to provide the device with the files necessary to execute the assigned work.

Using Preboot Services, you can automatically place an image on a device, even if the device's hard disk is blank. You do not need to use the CD or DVD, or a ZENworks partition on the device.

28.2.2 Understanding the ZENworks NBPs

The Intel PXE specification defines mechanisms and protocols that allow PXE devices to use their network interface cards (NICs) to find bootstrap programs located on network servers. In the PXE specification, these programs are called Network Bootstrap Programs (NBPs).

NBPs are analogous to the bootstrap programs found in the Master Boot Records (MBRs) of other boot media, such as hard drives, floppy disks, CDs, and DVDs. The purpose of a bootstrap program is to find and load a bootable operating system. MBRs on traditional boot media accomplish this by locating the necessary data on their respective media. NBPs accomplish this by using files found on network servers, usually TFTP servers.

ZENworks Preboot Services uses two separate NBPs working together:

- "nvlnbp.sys" on page 330
- "pxelinux.0" on page 330

nvlnbp.sys

This NBP has the following responsibilities:

- Detect various SMBIOS parameters and local hardware
- Read the ZENworks identity information from the hard drives
- Communicate with novell-zmgprebootpolicy to determine if there is any preboot work applicable to the device
- Present and manage the Preboot Services menu
- If necessary, launch pxelinux.0 to execute the assigned preboot work

pxelinux.0

The primary purpose of this NBP is to load the operating system that is required to execute the assigned preboot work.

The pxelinux.0 file is a modified version of part of an open source project called syslinux. Although pxelinux.0 is primarily a Linux loader, it is capable of loading other operating systems. It operates by using configuration files located on a TFTP server to provide boot instructions. The various pxelinux.0 configuration files used by Linux Management can be found on your imaging server in the /srv/tftp directory.

In Linux Management, when PXE devices are assigned preboot work, they are also told which pxelinux.0 configuration file they should use to execute that work. Similarly, when using the Preboot Services Menu, each menu option corresponds to a pxelinux.0 configuration file. For more information, see Section 29.3.4, "Editing the Preboot Services Menu," on page 376.

For more information on pxelinux.0 and its configuration files, see the syslinux home page (http:/ /syslinux.zytor.com/pxe.php).

For a copy of the Novell modifications to the syslinux open-source project, see Novell Forge (http:// forge.novell.com).

28.2.3 Preparing to Use PXE

Before you can use Preboot Services with PXE, you need to do the following:

1. Install ZENworks 7.3 Linux Management on your imaging server. For more information, see the *Novell ZENworks 7.3 Linux Management Installation Guide*.

2. Enable PXE on your ZENworks Linux Management devices. For more information, see Section 29.6, "Enabling PXE on Devices," on page 401.

3. Have a standard DHCP server, either on your imaging server or on another network server. For more information, see "Configuring LAN Environments for Preboot Services" on page 370.

28.3 Preboot Services Functionality

Review the following sections to understand Preboot Services functionality:

- Section 28.3.1, "Preboot Bundles," on page 331
- Section 28.3.2, "Preboot Services Menu," on page 333
- Section 28.3.3, "Image Storage Security," on page 334
- Section 28.3.4, "Non-registered Device Settings," on page 334
- Section 28.3.5, "Preboot Work Assignment Rules," on page 335
- Section 28.3.6, "Preboot Referral Lists," on page 336
- Section 28.3.7, "Intel Active Management Technology (AMT)," on page 337

28.3.1 Preboot Bundles

In ZENworks Linux Management, Preboot Services uses bundles to apply Preboot Services work to devices. For example, Preboot bundles can contain tasks, such as restoring an image, that are performed at the time a device boots.

In order for a device to utilize a Preboot bundle, the bundle must be assigned to the device, its group, or its folder.

The available Preboot bundles are:

- "AutoYaST Bundle" on page 331
- "Dell Configuration Bundle" on page 332
- "Kickstart Bundle" on page 332
- "ZENworks Image Bundle" on page 332
- "ZENworks Multicast Bundle" on page 332
- "ZENworks Script Bundle" on page 333

AutoYaST Bundle

Provides the location and access protocol for installing using AutoYaST, including the network installation directory for SUSE® Linux. This bundle allows you to launch an automated installation of SUSE Linux using Preboot Services.

Dell Configuration Bundle

Provides the location of files and scripts for configuring Dell servers. This bundle allows you to use Preboot Services to configure the server's BIOS, BMC, RAID, and DRAC settings and to create a Dell utility partition.

Kickstart Bundle

Provides the location and access protocol for installing using kickstart. This bundle allows you to launch an automated installation of Red Hat Linux using Preboot Services.

ZENworks Image Bundle

Lists one or more ZENworks images that can be restored on a computer. This bundle allows you to quickly define simple image restoration operations.

Scope

You can restore an image all of a device's hard disks, specific add-on images, and file sets.

Boot Manager Limitation

If the device you want to image has an unsupported boot manager running, such as System Commander, you must disable or remove it before attempting to image those devices. This is because boot managers create their own information in the MBR and overwrite the ZENworks boot system, preventing ZENworks imaging from being performed.

Base Images

A base image contains descriptions of all partitions and files on a hard drive. When it is restored, all existing partitions are deleted, new partitions are created from the descriptions in the base image, and all files are restored from the image.

Base images are created by taking an image of a device. You can use an option in the ZENworks Control Center or you can use imaging commands at a bash prompt to create a base image.

Add-On Images

These images are a collection of files added non-destructively to existing partitions. The existing partitions and files are left intact, except for any files that the add-on image might update.

Add-on images allow you to customize a device after a base image is restored. This allows you to use a base image for multiple purposes.

You can create add-on images using the Image Explorer utility.

ZENworks Multicast Bundle

Specifies an image that can be sent using the multicast protocol. This bundle allows you to send an existing image to a large number of devices in a single operation. It is ideal for labs, classrooms, and staging areas.

For more information, see Section 28.5.6, "Multicasting Device Images," on page 348.

Benefits

You can image multiple devices with the least amount of overhead. Devices to be imaged can have a variety of operating systems installed on them, or even no operating system installed.

Using the multicast capabilities of your network, you minimize network traffic by sending the image file across the network once for all devices to be imaged, rather than individually per device.

Limitations

Using the same image on multiple devices means they all have the same network identities. However, you can install the ZENworks Linux Management Imaging Agent (novell-zislnx) on these devices prior to performing the multicast, because this agent saves each device's network identity settings and restores them after the multicast image is applied.

ZENworks Script Bundle

Allows you to write a custom Linux bash script that is executed on PXE-enabled Linux devices. This provides detailed control over ZENworks imaging operations, as well as most Linux-based preboot tasks.

28.3.2 Preboot Services Menu

Where PXE is enabled on a device, the Preboot Services Menu can be displayed during the boot process. The following menu choices are displayed on the Preboot Services Menu:

- **Start ZENworks Imaging:** Executes the effective Preboot Services imaging bundle.
- **Start ZENworks Imaging maintenance:** Displays the bash prompt, where you can execute imaging commands.
- **Disable ZENworks partition:** Prevents an existing ZENworks partition from being used during booting to execute the assigned Preboot bundles.
- **Enable ZENworks partition:** Allows an existing ZENworks partition to be used during booting to execute the effective Preboot bundle.
- **Start DELL DTK:** Starts the Dell OpenManage Deployment Toolkit (DTK) v2.1 in the automated mode where assigned work is automatically performed.
- **Start DELL DTK (Maintenance Mode):** Starts the DTK in the maintenance mode, where you can use the DTK bash prompt to manually configure the scripts and files used by the Dell Configuration bundle.
- **Exit:** Resumes normal booting of the device.

You can use the ZENworks Control Center to configure whether this menu should be displayed on a PXE-enabled device by selecting one of the following options:

- *Always Show Preboot Menu*
- *Never Show Preboot Menu*
- *Show Preboot Menu if CTRL+ALT is Pressed*

IMPORTANT: Do not select *Always Show Preboot Menu* if you have AutoYaST or kickstart bundles assigned to any devices, because the Preboot Services Menu interrupts the PXE boot process, keeping the AutoYaST or kickstart bundles from being deployed on the device. The Preboot Services Menu only has options for doing imaging work, not for installing operating systems.

Therefore, select either *Never Show Preboot Menu* or *Show Preboot Menu if CTRL+ALT is Pressed* for your Preboot Services Menu option, which allows PXE-enabled Linux devices to automatically implement the AutoYaST or kickstart bundles.

For the procedures in configuring whether to display the menu, see Section 29.4.1, "Configuring Preboot Services Menu Options," on page 380.

28.3.3 Image Storage Security

You can determine the degree of security you want by restricting where to save image files on your imaging server. The following options in the ZENworks Control Center provide this storage security:

 - **Allow Preboot Services to overwrite existing files when uploading:** Select this option only if you want existing image files to be overwritten during imaging.
 - **Only allow uploads to the following directories:** This option allows you to determine where images can be restored on the imaging server. You specify a full path to the directory in the *Add* field, then click *Add* to enter it into the list box. These are the directories where images are allowed to be saved on the imaging server. These are the locations that can be selected when configuring where to store image files.

For the procedures in configuring imaging storage, see Section 29.4.2, "Configuring Image Storage Security," on page 381.

28.3.4 Non-registered Device Settings

Devices that are new to the ZENworks Management Zone and have received their first image need certain IP configuration information to successfully access the network and network services. You can use Preboot Services to automatically name your non-registered devices using such criteria as prefixes, BIOS information (like asset tags or serial numbers), DNS suffixes, and you can set up DHCP or IP addresses.

For example, the device needs a unique IP address and the address of at least one DNS name server. In many networks, this information is distributed through the DHCP services, but it can also be configured through the default Preboot Services configuration settings in the ZENworks Control Center.

After a device has registered with ZENworks, its configuration is set and the non-registered device settings in the ZENworks Management Zone no longer apply to it, because the ZENworks Linux Management server now knows its identity. After the device is imaged, it can become a member of the zone or continue to be a non-registered device, depending on whether the image applied to the device contains the ZENworks Linux Management Imaging Agent (novell-zislnx).

The settings that can be adjusted for a ZENworks Management Zone are:

 - **NDS suffix:** Provides a suffix for all of your devices' names. For example, provo.novell.com.

- **Name servers:** Controls which DNS servers a device uses. You can specify multiple DNS name servers.

- **Device name:** Configured device names can include a prefix, the BIOS asset tag, the BIOS serial number, or none of these.

- **IP configuration:** For the IP configuration, you can specify to use DHCP or a specific IP address. If you select to use IP addresses, you can provide a list using a range or by specifying specific IP addresses. As devices are registered, they assume one of the available addresses. For IP addresses, you can also specify a subnet mask and a default gateway.

For the procedures in configuring defaults for non-registered devices, see Section 29.4.3, "Configuring Non-registered Device Settings," on page 383.

28.3.5 Preboot Work Assignment Rules

You can set up hardware-based rules for your Preboot bundles. Work assignment rules are used to apply bundles to devices with specific hardware, or to match a broad set of hardware requirements.

For example, you can create a rule that applies a bundle to any device with a specific MAC address or BIOS serial number. Rules like this can only match to a single device. On the other hand, you can create a rule that applies to any device with at least 512 MB of RAM and 150 GB of hard drive space.

A work rule is comprised of filters that are used to determine whether a device complies with the rule. The rules use logic to determine whether a device meets the requirements for applying the Preboot bundle. The AND and OR logical operators are used for creating complex filters for the rule.

When a device is seeking work to be done, it scans the rules until it finds a rule where all of the rule's filters match the device, then executes the bundle assigned to the rule.

Filter information that you can provide:

- **Device component:** Any of the following:

  BIOS Asset Tag
  BIOS Serial Number
  BIOS Version
  CPU Chipset
  Hard Drive Controller
  Hard Drive Size (in MB)
  Hardware Type
  IP Address
  MAC Address
  Model
  Network Adapter
  RAM (in MB)
  Sound Card
  System Manufacturer
  Video Adapter

- **Relationship:** This defines the relationship for a filter between the *Device component* field and the value you specify for it.

  Possibilities for the *Hard drive size* and *RAM* fields:

  < (less than)
  > (greater than)
  = (equal to)
  >= (greater than or equal to)
  <= (less than or equal to)
  <> (not equal to)

  Possibilities for all other device components:

  Contains
  Equal To
  Starts With

- **Component value:** This corresponds to the match you want for the component. For example, you select *RAM (in MB)* for the filter and enter 512 for its value. Then, the relationship you select determines whether it's less than, less than or equal to, equal to, not equal to, greater than or equal to, or just greater than 512 MB.

You can have multiple filters and sets of filters in a single rule, using the AND and OR operators, and you can have multiple rules associated with the same Preboot bundle. This allows you to specify exactly to which devices a particular Preboot bundle can be applied.

For the procedures in configuring work assignment rules, see .

28.3.6 Preboot Referral Lists

When a PXE device boots, it makes a broadcast request on the network for PXE services. The ZENworks Proxy DHCP server (novell-proxydhcp) responds to this request with information that includes the IP address of an imaging server where the device can send requests for assigned preboot work.

It is essential that the PXE device contact PXE services associated with its home zone so that it can correctly determine if there is any preboot work assigned to it. When there is only a single ZENworks Management Zone, this is fairly easy to do because all Proxy DHCP servers provide addresses to services that belong to the same zone. Any device can request preboot work from any imaging server in the same zone and get the same response. However, when multiple ZENworks management zones exist in the same network, things become more difficult, particularly when each zone has its own set of PXE services.

The PXE device's initial request for PXE services is sent as a broadcast to the network, and all Proxy DHCP servers respond with information pertaining to their respective zones. Because it is impossible to determine which Proxy DHCP server responds first, if multiple Proxy DHCP servers respond, or which response is used by the device, it is impossible to ensure that each PXE device will contact servers in its home zone.

A Preboot Referral List allows you to ensure that all devices contact their home zone for preboot work assignments. The list should contain the IP address of an imaging server in each known ZENworks management zone. When a device requests preboot work from a server, the server first

determines if the device belongs to the same zone as the server. If it does not, the server refers the request to each server in its referral list until it finds the device's home zone. The device is then instructed to send all future requests to the correct daemon.

After you have specified all of the necessary servers in the referral list, you must place certain files in the `\tftp` directories of each server in the list. Which files are copied and modified depends on the version of ZENworks running on that server.

Note that the Preboot Referral Lists are only used by PXE devices, and only one ZENworks Management Zone needs to have an active Proxy DHCP server and Preboot Referral List.

For the procedures in configuring referral lists, see Section 29.4.5, "Configuring the Server Referral List," on page 393.

28.3.7 Intel Active Management Technology (AMT)

Review the following to understand how the Intel AMT functionality is used by ZENworks Linux Management:

- "Using AMT in ZENworks Linux Management" on page 337
- "Understanding AMT Provisioning" on page 338
- "Accessing AMT Resources" on page 338

For more information on Intel AMT, see the Intel Web site (http://www.intel.com/technology/platform-technology/intel-amt/).

Using AMT in ZENworks Linux Management

The Intel AMT functionality allows you to accurately identify devices, even if they have had physical drive replacements. This provides ZENworks Preboot Services with persistent device identification by providing ZENworks with nonvolatile memory for storing the unique device identity.

With AMT and Preboot Services, if a device has a new, unformatted hard drive, ZENworks Linux Management can instantly and accurately identify the device and apply the appropriate Preboot bundle. If a device's hard drive is inactive or its drive is replaced, ZENworks can automatically identify the device in a preboot environment and provide the appropriate ZENworks Linux Management-created image during a system rebuild.

AMT with ZENworks also provides easier hardware upgrading capability. For example, to upgrade applications, some of your device hardware might not meet the minimum requirements. With AMT and Preboot Services, as soon as the hard drives are replaced and before any agents or operating systems are installed, you can continue to assign Preboot bundles using the device's ZENworks identity without having to re-register the device.

If you are using Intel AMT, support for it should be enabled in the `novell-zmgprebootpolicy.conf` file.

Understanding AMT Provisioning

For security purposes, AMT devices generally ship with all AMT features disabled. In this configuration, AMT devices act like normal computers, but none of the AMT features are available. To enable the AMT features, each device must go through a process that Intel refers to as "provisioning," which sets up the device's AMT resources for access.

- "The Provisioning Modes" on page 338
- "The Provisioning Process" on page 338

The Provisioning Modes

An AMT device may be provisioned into one of two modes: enterprise or small business. Both modes offer the same off-line and remote management capabilities, but in enterprise mode AMT devices use local Certificate Authority credentials to grant remote access, and may require HTTPS protocol for communication rather than just HTTP. In small business mode, remote access is granted through standard HTTP authentication services.

While ZENworks Linux Management works equally well with devices provisioned in either enterprise or small business mode, only the small business mode is required. Therefore, ZENworks Linux Management does not provide a mechanism to provision AMT devices in enterprise mode.

If you use another AMT-enabled application that does require provisioning in enterprise mode, you should use the provisioning utilities of that application. Make sure you provision each AMT device with at least one "enterprise name."

The Provisioning Process

The provisioning process for AMT devices allows you to specify many AMT-related configuration settings. Examples include users, passwords, enterprise names, and allocation of NVRAM space to specific AMT-enabled applications.

To use the AMT features in ZENworks Linux Management, all that is necessary is each AMT device be provisioned with at least one valid enterprise name, which is used to access the NVRAM where Linux Management stores the ZENworks identity information.

Intel suggests that the enterprise name be chosen to indicate the device's general location. For example, all the devices in the home office may be given an enterprise name of "Company_HQ," and all devices in field offices may be given enterprise names reflecting their geographical locations.

While it is not required, it is assumed that large numbers of devices will have the same Enterprise name. Each AMT device itself may have up to four different enterprise names.

ZENworks Linux Management provides a utility (`smb-provisioning.exe`) to help provision AMT-devices in small business mode with enterprise names. This utility can be found in the `/opt/novell/zenworks/zdm/winutils` directory on your imaging server. It requires .NET framework.

For the procedures in providing Intel AMT enterprise names to ZENworks Linux Management, see Section 29.4.6, "Configuring Intel Active Management Technology (AMT)," on page 395.

Accessing AMT Resources

For more information, see "Downloading and Installing the iAMT Redirection Drivers" on page 395.

28.4 The Preboot Services Processes

The following sections explain how the Preboot Services processes work:

- Section 28.4.1, "A Typical Preboot Services Operation," on page 339
- Section 28.4.2, "Illustrating the Preboot Services Processes," on page 339

28.4.1 A Typical Preboot Services Operation

A typical Preboot Services operation flows as follows:

1. A Preboot bundle is created in the ZENworks Control Center and assigned to a PXE-enabled device.

2. The PXE-enabled device starts to boot.

3. The device sends a DHCP discovery request to determine the IP address of the Preboot Services imaging server.

4. The DHCP server responds with an IP address for the device to use.

5. The novell-proxydhcp daemon responds with the IP addresses of the TFTP server, as well as the filename of the Preboot Services bootstrap program (`nvlnbp.sys`).

6. The PXE device downloads the Preboot Services bootstrap program using novell-tftp.

7. After the Preboot Services bootstrap program is downloaded and executed, the device checks novell-zmgprebootpolicy to see if there is any imaging work to do.

8. If there is imaging work to do (as contained in a Preboot bundle that is assigned to the device), the device downloads the Linux Management imaging environment from the server so that the it can be booted to Linux.

9. Any imaging tasks contained in the Preboot bundle are performed.

10. If there are no imaging tasks to perform, files are not downloaded and the device proceeds to boot to its operating system.

In addition to using PXE for automation, you can also execute Preboot work manually using one of the following:

Preboot Services Menu (if enabled for the device)
Preboot Services bootable CD or DVD
ZENworks partition

For more information, see Section 30.1.2, "Performing Manual Imaging Tasks," on page 415.

28.4.2 Illustrating the Preboot Services Processes

The following illustrations show the interaction between a Preboot Services (PXE) device and a Preboot Services imaging server, starting when the PXE device is turned on and begins to boot, and ending when imaging work begins on that device.

The following example assumes that the devices and imaging servers are in the same network segment.

- "Phase 1: Beginning the Process" on page 340
- "Phases 2 through 8: Continuing the Process" on page 342

Phase 1: Beginning the Process

Depending on whether novell-proxydhcp is configured on the same server as the standard DHCP server or on a different server, the imaging process begins differently. The following sections illustrate how the process begins for each configuration, then the phases illustrated in "Phases 2 through 8: Continuing the Process" on page 342 are the same for them.

- "Standard DHCP and Novell Proxy DHCP Configured on Separate Servers" on page 340
- "Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part A" on page 340
- "Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part B" on page 341

Standard DHCP and Novell Proxy DHCP Configured on Separate Servers

For this example, the DHCP server and the Preboot Services imaging server are two separate servers on the network.

Figure 28-1 *DHCP Configuration on Separate Servers*
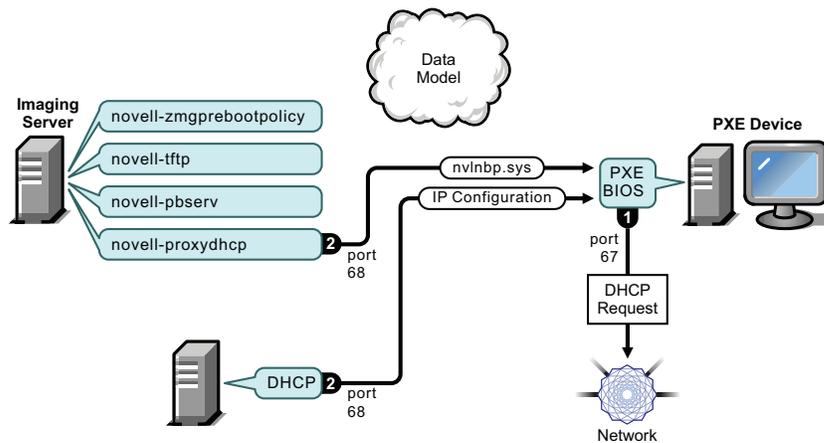
Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.
2. The DHCP server responds with IP configuration information on port 68, and the Proxy DHCP server responds on port 68 with the name of the bootstrap program (`nvlnbp.sys`) and the IP address of the TFTP daemon where it can be found.
3. Continue with "Phases 2 through 8: Continuing the Process" on page 342.

Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part A

For this example, the DHCP server and the Preboot Services imaging server are configured on the same server on the network. See "Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part B" on page 341 for the second part of this example.

Figure 28-2 *DHCP Configuration on the Same Server, Part A*
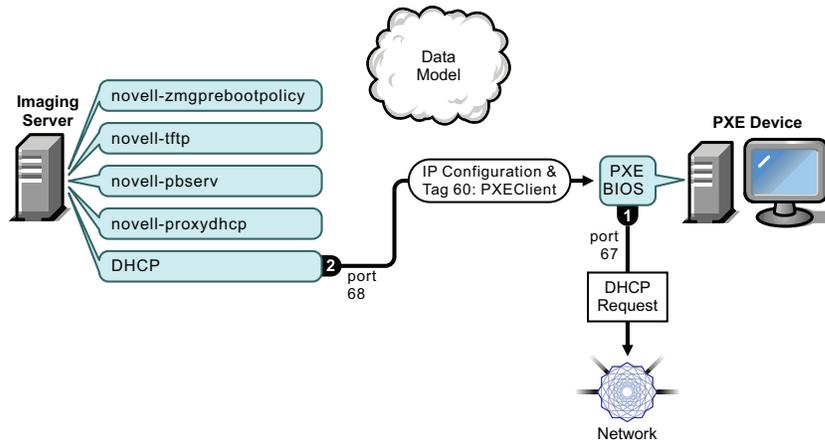
Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.

2. The DHCP server responds with IP configuration information on port 68, including tag 60 for PXEClient, which indicates that novell-proxydhcp is running on the same server.

Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part B

Figure 28-3 *DHCP Configuration on the Same Server, Part B*
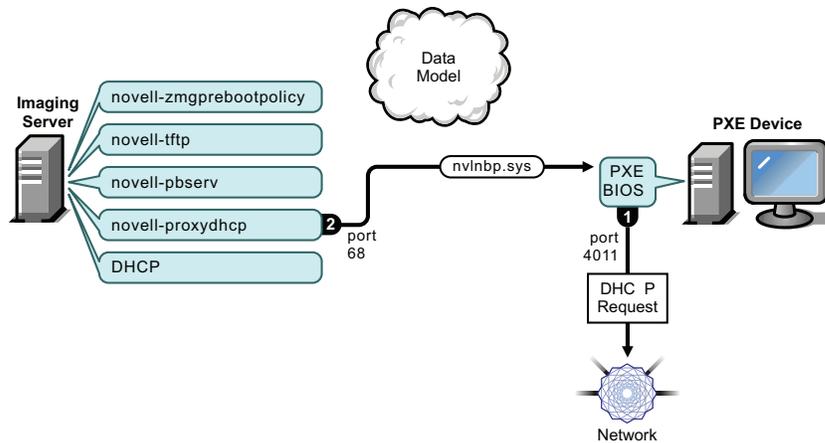
Processes:

1. When the device sees tag 60 in the DHCP response, the PXE BIOS reissues the DHCP request on port 4011.

2. The Proxy DHCP server responds on port 68 with the name of the bootstrap program (nvlnbp.sys) and the IP address of the TFTP daemon where it can be found.

3. Continue with "Phases 2 through 8: Continuing the Process" on page 342.

Phases 2 through 8: Continuing the Process

The following sections explain how the Preboot Services process continues after Phase 1:

Phase 2

Figure 28-4 *Phase 2 of the Preboot Services Process*
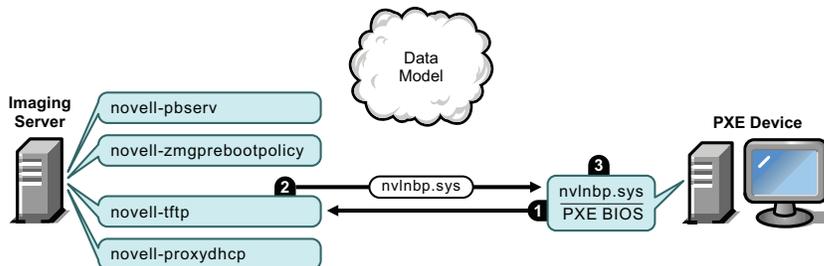
Processes:

1. The PXE BIOS requests `nvlnbp.sys` from the TFTP server.
2. The TFTP server sends `nvlnbp.sys` to the PXE device.
3. The PXE device loads `nvlnbp.sys` into memory.

Phase 3

Figure 28-5 *Phase 3 of the Preboot Services Process*
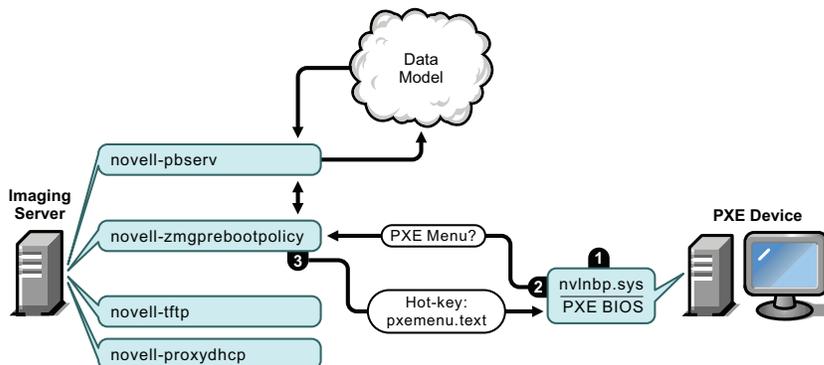
Processes:

1. Hardware detection is performed by `nvlnbp.sys` and it reads the image-safe data.

2. `Nvlnbp.sys` requests the Preboot Services Menu configuration from the Data Model via the novell-zmgprebootpolicy daemon.

3. The novell-zmgprebootpolicy daemon returns the Preboot Services Menu configuration. In this case, the menu described in `pxemenu.txt` is displayed when a user presses the hot key.

Phase 4

Figure 28-6 Phase 4 of the Preboot Services Process
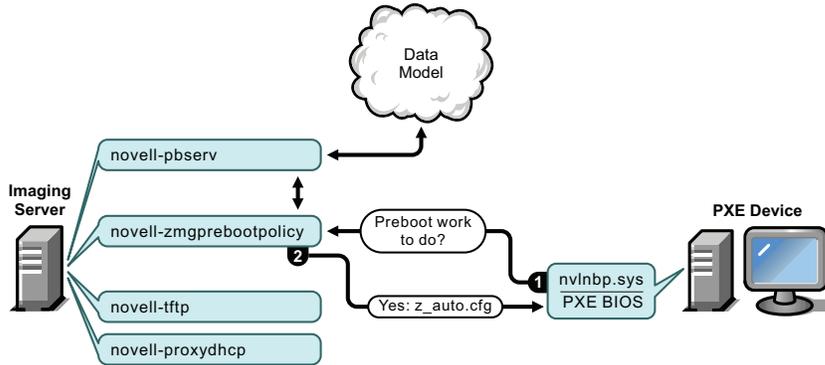
Processes:

1. Assuming no Preboot Services Menu is displayed, the device asks the Data Model (via novell-zmgprebootpolicy) if any work is assigned.

2. Assuming work is assigned, the novell-zmgprebootpolicy daemon responds with the name of the configuration file to use in performing the preboot work (`z_auto.cfg` in this example).

Phase 5

Figure 28-7 Phase 5 of the Preboot Services Process
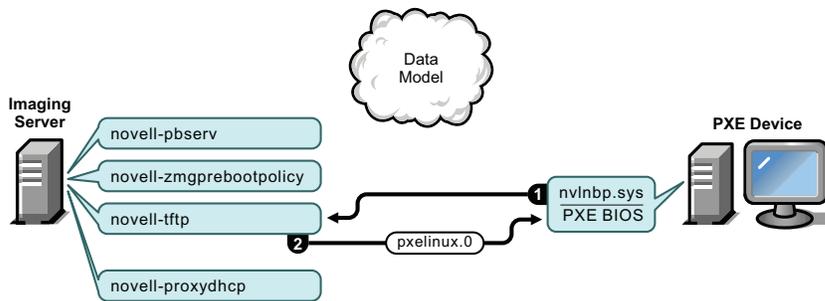
Processes:

1. The PXE device requests `pxelinux.0` from the TFTP server.

2. The TFTP server sends `pxelinux.0` to the device.

Understanding Preboot Services in ZENworks Linux Management **343**

Phase 6

Figure 28-8 *Phase 6 of the Preboot Services Process*
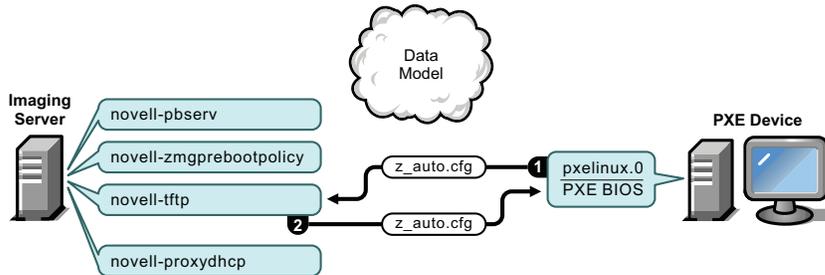
Processes:

1. Pxelinux.0 replaces `nvlnbp.sys` in memory and requests `z_auto.cfg` from the TFTP server.
2. The TFTP server sends the `z_auto.cfg` file to the device.

Phase 7

Figure 28-9 *Phase 7 of the Preboot Services Process*
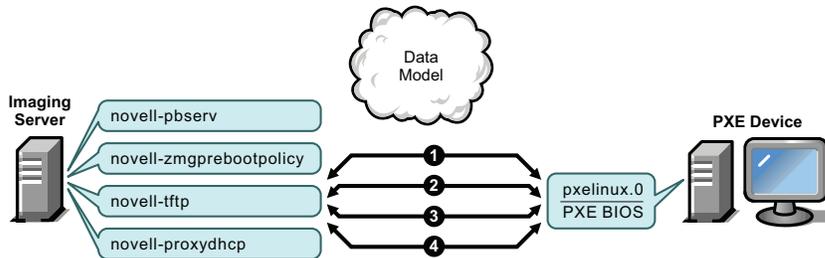
Processes:

1. `Pxelinux.0` requests and receives `/boot/kernel` from the TFTP server.
2. `Pxelinux.0` requests and receives `/boot/initid` from the TFTP server.
3. `Pxelinux.0` requests and receives `/boot/root` from the TFTP server.
4. `Pxelinux.0` requests and receives `/boot/updateDrivers.tgz` from the TFTP server, but is denied because the file does not exist (it is used to provide post-release software updates).

Phase 8

Figure 28-10 *Phase 8 of the Preboot Services Process*
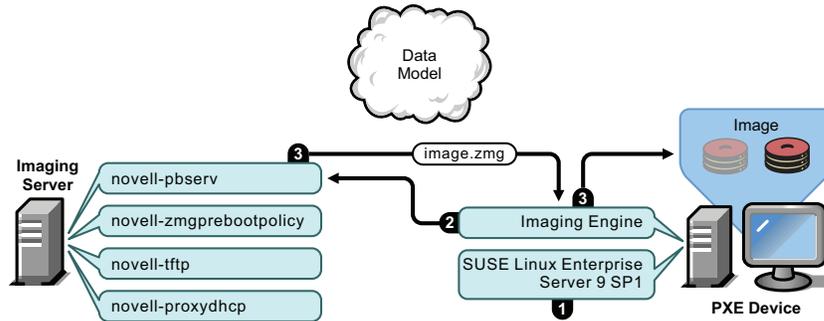
Processes:

1. SUSE Linux Enterprise Server (SLES) 9 SP1 is loaded and run on the device.

2. The ZENworks Imaging Engine (img) requests the assigned Preboot Services work details and performs the work.

3. The image is laid down on the device and it automatically reboots.

28.5 Preboot Strategies

The following sections present possible approaches to using Preboot Services. Use the following sections to determine which procedures to perform. The steps are documented in subsequent sections.

28.5.1 Automating Updates and Installations

You can automate Linux installations and software updates using Preboot Services in the following ways:

- **SUSE Linux installation:** The AutoYaST bundle can automate installation of SUSE Linux on a Linux device.
- **Red Hat Linux installation:** The kickstart bundle can automate installation of Red Hat Linux on a Linux device.
- **ZENworks script execution:** The ZENworks Script bundle can automate execution of any ZENworks script on a Linux device, including imaging commands.
- **Device imaging:** The ZENworks Imaging bundle can be used to place an image on a Linux device.

◆ **Imaging multiple devices:** The ZENworks Multicast bundle can be used to place an image on multiple Linux devices with one pass of the image file over the network, such as in resetting lab devices.

All you need to do to accomplish any of these actions is to create and configure one of the five Preboot bundle types, then assign the bundle to the desired devices.

When a device boots, the assigned bundle is automatically applied before the device's operating system starts.

You can also manually accomplish these tasks per device using the Preboot Services Menu's *Start ZENworks Imaging Maintenance* option to access the bash prompt, if you have enabled the Preboot Services Menu for the device. Or, you can use a Preboot Services bootable CD or DVD, which does not require PXE to be enabled on the device. For more information, see Section 30.1.2, "Performing Manual Imaging Tasks," on page 415.

28.5.2 Creating, Installing, and Restoring Standard Images

As new devices are purchased and before deploying them, you can install a standard software platform and enable the device for future unattended reimaging.

1. Create a model device of each type that you intend to deploy.

2. Create an image of each model device on a ZENworks Linux Management imaging server. For more information, see "Manually Taking an Image of a Device" on page 415.

   These images should include the Novell ZENworks Linux Management Imaging Agent (novell-zslnx).

3. Optionally, you can create a preboot imaging bundle for this image. This allows the image to be assigned automatically for later use.

4. If you are using Preboot Services, install ZENworks Linux Management on your imaging server. For more information, see Section 29.1, "Preparing a Preboot Services Server," on page 353.

   or

   If you are using a bootable CD or DVD, or a ZENworks partition, create a boot CD or DVD that points to the ZENworks Linux Management imaging server where the model images are stored. For more information, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

As each new device comes in, do the following if you are using Preboot Services:

1. Check to see if the device is PXE capable. Enable PXE if it isn't enabled by default. For more information, see Section 29.6, "Enabling PXE on Devices," on page 401.

2. Physically connect the device to the network.

3. Boot the device from the Preboot Services imaging server.

If you are not using Preboot Services, boot the device with the imaging boot CD or DVD and consider installing the ZENworks partition to enable auto-imaging without needing to supply the CD or DVD. For more information, see Step 3 on page 363 of Section 29.7.2, "Enabling a Device for Imaging Operations," on page 403. After you have installed the partition, reboot the device from the ZENworks partition.

28.5.3 Reimaging Corrupted Devices

Without data loss or undue disruption to users, you can fix devices that have become misconfigured or corrupted.

1. When a device needs to be fixed, have the user back up any files to the network that he or she wants to keep (if possible).

2. Create and/or assign an appropriate imaging bundle to the device.

3. If it is a device with a ZENworks partition or it is PXE-enabled, the user should boot the device from the ZENworks partition or the Preboot Services imaging server (via PXE) to find and execute the assigned bundle. If you are using PXE, make sure that Preboot Services is installed on your imaging server. For more information, see Chapter 30, "Using Preboot Services," on page 407.

    or

    If the device does not have a ZENworks partition and is not PXE-enabled, the user should boot the device with the imaging boot CD or DVD and restore the appropriate images manually.

4. After the image is laid down, restore any user files that were backed up to the network.

28.5.4 Restoring Lab Devices to a Clean State

You can restore devices to a clean state, removing any changes or additions made since the last time you restored the image on that device. This is useful for updating lab devices.

The following steps assume that the devices are unregistered.

1. Create an image of a clean model device and store it on a ZENworks Linux Management imaging server. For more information, see "Manually Taking an Image of a Device" on page 415.

2. If you are using Preboot Services, make sure that ZENworks Linux Management is installed on your imaging server. For more information, see Section 29.1, "Preparing a Preboot Services Server," on page 353.

3. If you are using Preboot Services and the devices are PXE capable, make sure that PXE is enabled. For more information, see Section 29.6, "Enabling PXE on Devices," on page 401.

    or

    If you are not using Preboot Services or the Linux partition, create an imaging boot CD or DVD that points to the ZENworks Linux Management imaging server where the clean image is stored. For more information, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

Deploy each lab device as follows:

1. Physically connect the device to the lab network.

2. If you are using Preboot Services, boot the device from the Preboot Services imaging server.

    or

    If you are not using Preboot Services, boot the device with the imaging boot CD or DVD and install the ZENworks partition. For more information, see Step 3 on page 363 of Section 29.7.2, "Enabling a Device for Imaging Operations," on page 403. After you have installed the partition, reboot the device from the ZENworks partition.

3. At the end of each lab session, assign the Preboot bundle to the lab devices.

4. Reboot each device and let it be auto-imaged by its assignment to a ZENworks Preboot bundle.

28.5.5 Setting Up Devices for Future Reimaging

With minimal disruption to users, you can enable existing devices for possible future reimaging.

This process might need to be phased in by local administrators. Each administrator can do the following:

1. Install the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) on each device.

2. If the devices are PXE capable, make sure PXE is enabled (see Section 29.6, "Enabling PXE on Devices," on page 401) and make sure that ZENworks Linux Management is installed on your imaging server (see Section 29.1, "Preparing a Preboot Services Server," on page 353).

   or

   Prepare a few sets of imaging CDs or DVDs that users can use when they run into trouble (see Section 29.2, "Setting Up the Preboot Services Methods," on page 354). These devices should point to an imaging server that contains the same clean images used for new devices.

3. If a user runs into trouble, use the strategy for reimaging corrupted devices. For more information, see Section 28.5.3, "Reimaging Corrupted Devices," on page 347.

28.5.6 Multicasting Device Images

The following sections explain the multicasting images feature:

- "Understanding Multicasting" on page 348
- "Practical Uses For Multicasting" on page 349
- "Automatic Multicasting Example" on page 350

For instructions on using multicasting, see Section 30.2, "Multicasting Images," on page 429.

Understanding Multicasting

Multicasting is a way to send the same image to multiple devices without sending that image multiple times across the network. It is done by inviting participants to join a multicast session. Multicasting is similar to broadcasting on the network, because you send the image once to the network and only those devices belonging to the multicast session can see and receive it. This saves on network bandwidth usage.

For example, if you have 10 devices in the multicast session and the image is 3 GB in size, your network experiences only 3 GB of network traffic to image all 10 devices. Without multicasting, the network experiences 30 GB of network traffic to image all 10 devices individually.

The devices to be imaged must be physically connected to the network. They can be devices with existing operating systems of any kind, or they can be new devices with no operating system installed.

IMPORTANT: For multicasting to work properly, all routers and switches on the network must have their multicast features configured. Otherwise, multicast packets might not be routed properly.

Multicasting can be done automatically or manually:

- "Automatic Multicasting" on page 349
- "Manual Multicasting" on page 349

Automatic Multicasting

In the ZENworks Control Center, multicasting is accomplished by configuring a Multicast bundle. The bundle contains a base image that is taken previously from a device and is stored on an imaging server. This base image is applied to all multicast session participants.

When using a Preboot bundle to perform multicasting, the imaging server is the session master, which sends the .zmg image file to the session participants. The novell-pbserv daemon is used in this process. All problems are reported and displayed on the session master device.

For more information, see Section 30.2, "Multicasting Images," on page 429.

Manual Multicasting

At a bash prompt, you can enter commands to configure and initiate a multicasting session. You enter the appropriate commands on a bash prompt at each device, specifying one of them to be the session master. An image of the session master's hard drive is sent to each of the session participants.

For more information on the imaging commands, see Section E.5, "Session (Multicast) Mode (img session)," on page 639.

If you plan to set up multicasting by visiting each device, you need either an imaging boot CD or DVD, or the devices must be PXE-enabled. For more information, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

Practical Uses For Multicasting

Multicasting is ideal for labs, classrooms, and staging areas, or for any place where you need to quickly create the same configuration on multiple devices, instead of taking the time to set up each device individually.

Benefits of Multicasting Images

Multicasting is the way to use ZENworks Imaging Engine for mass reimaging with the least amount of overhead. It is useful if you have one device with a clean software configuration that you want to duplicate on several other devices, or if you have a single image that you want to set up on multiple devices.

Limitations of Multicasting Images

One significant limitation of using multicast without installing any ZENworks Linux Management software is that it results in a set of devices that have duplicate network identities. The IP addresses (if the network is using static IP addressing) and device hostname are all the same and can cause conflicts if deployed on the network without change.

For a handful of devices, this might not be a problem. But for a larger number of devices, you should install the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) on each device before doing the multicast (see Section 29.7.2, "Enabling a Device for Imaging Operations," on page 403). The Imaging Agent saves the device's network identity settings before the multicast session and restores them afterwards.

Automatic Multicasting Example

To automatically multicast an image to multiple devices using the ZENworks Control Center:

1. In the ZENworks Control Center, create a Multicast bundle using a wizard.
2. Specify the source image for the bundle.

   You can multicast an existing image from your imaging server.
3. Configure the trigger for multicasting the bundle, as in the following examples:

   Client count: When the specified number of clients specified in the bundle have booted and registered, the multicast session begins.

   Time count: When the specified length of time has passed with no new clients having registered, the multicast session begins regardless of the number of client participating.

   The first trigger to be realized causes the multicast session to begin.
4. Assign the Multicast bundle to the desired devices.

   The ZENworks Control Center provides a way to enable or disable a Multicast bundle, allowing you to temporarily stop the bundle from executing. This is more efficient than unassigning the bundle from many devices.
5. Wait for the trigger to happen.

   Each device booting into the session has its boot process delayed until the session begins, which is determined by fulfillment of one of the triggers.

   The multicast happens automatically when a device assigned to the Multicast bundle boots, according the configuration you set up for the Multicast bundle and for the devices you assigned to the bundle. This bundle is applied to each session device before it boots its operating system. The ZENworks Multicast bundle is sent over the wire just once, using the multicast capability of your network, and executed simultaneously on all participating devices.

28.5.7 Configuring Dell Linux Devices

Certain Dell computer models can be automatically configured using ZENworks Preboot Services. You can configure the following for Dell devices:

- **BIOS/BMC/DRAC 5 Configuration File:** You can use syscfg to auto-generate a BIOS, BMS, or DRAC 5 file with a specific configuration for the device.
- **RAID Configuration Script:** You can use a supplied example script to configure your RAID settings for the device.
- **DRAC Configuration File:** You can run a supplied script to create your DRAC 4 or earlier configuration file.
- **Dell Utility Partition:** You can create a Dell utility partition when imaging the device, including setting its size, specifying the target disk, indicate whether to use a specific Dell utility partition file, and indicate whether to overwrite any existing utility files.

- **Preboot Bundle:** You can immediately perform an operating system installation after configuring the Dell device by specifying the Preboot bundle containing that installation configuration.

The above options are only for configuring, not for updating these settings. These configurations are applied to the Dell device when it boots and uses the Dell Configuration Preboot bundle that it is assigned to.

To properly configure Dell devices, you can also do the following:

- Keep your Dell DTK upgraded to the latest version (see Appendix G, "Upgrading the Dell DTK," on page 663).

- Create Dell configuration scripts and files to be used in the Dell Configuration Preboot bundle (see Section 30.5.1, "Creating Dell Configuration Scripts and Files," on page 454).

- Create a Dell Configuration Preboot bundle (see Section 30.5.2, "Creating Dell Configuration Bundles," on page 457).

- Troubleshoot Dell Configuration Preboot bundles (see "Dell DTK" in the *Novell ZENworks 7.3 Linux Management Troubleshooting Guide*).

Setting Up Preboot Services

<div style="text-align: right">29</div>

The section provides instructions for setting up Novell® ZENworks® Linux Management Preboot Services:

IMPORTANT: The Preboot Services software is automatically installed when you install ZENworks Linux Management.

29.1 Preparing a Preboot Services Server

When you install Novell ZENworks Linux Management on a server, the server is nearly ready to act as a Preboot Services server. To avoid confusion, the Proxy DHCP daemon (novell-proxydhcp) is installed, but not enabled. For PXE devices to be able to communicate with Preboot Services, this daemon must be started manually on at least one server on each network segment. Exactly how many servers and which specific servers should run this daemon is dictated by your network topology. As a rule of thumb, for every DHCP server deployed in your network, you should have a corresponding Proxy DHCP server.

For information on setting up management of your devices, see Section 29.3, "Deploying and Managing Preboot Services," on page 364 and Section 29.4, "Configuring Preboot Services Defaults," on page 379.

In addition to the specific hardware requirements for a ZENworks Linux Management server, the server used to store image files must meet the following requirements:

- **A fixed IP address:** When you connect to the imaging server during an imaging operation, you must do so using the fixed IP address or DNS name of the imaging server.
- **Enough space to store device images:** Unless you use compression (which is enabled by default) for your device images, they are nearly the same size as the data on the device hard disk, which could be many gigabytes.

  If you want to store an image locally (on a CD, DVD, or hard disk) rather than on an imaging server, see "Using a CD or DVD for Disconnected Imaging Operations" on page 424 and "Using a Hard Disk for Disconnected Imaging Operations" on page 426.

29.2 Setting Up the Preboot Services Methods

The Novell ZENworks Imaging Engine that performs the actual imaging of a device is a Linux application. Unless you use automated Preboot Services with PXE-enabled devices, you need to prepare a boot medium that has the Linux kernel, ZENworks Imaging Engine, and network drivers installed.

The following sections contain additional information:

- Section 29.2.1, "Using Preboot Services (PXE)," on page 354
- Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354
- Section 29.2.3, "Using the ZENworks Imaging Media Creator," on page 356
- Section 29.2.4, "Managing ZENworks Partitions," on page 362

29.2.1 Using Preboot Services (PXE)

Preboot Execution Environment (PXE) is an Intel specification that allows a device to boot from the network, instead of its hard drive or other local media. ZENworks Linux Management can use PXE to launch Preboot Services.

In ZENworks Linux Management, Preboot Services uses PXE to find out if there is imaging work specified for a device and to provide the device with the files necessary to boot to the ZENworks Linux Management imaging environment.

Before you can use Preboot Services with automated Preboot bundles, you need to do the following:

- Install the ZENworks Linux Management Imaging and Preboot Services (PXE Support) components on your imaging server.
- Enable PXE on the device.
- Have a standard DHCP server, either on your imaging server or on another network server.

Automated Preboot Services functions can also be performed using a ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

Manual Preboot Services functions can be performed using CDs or DVDs. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.

29.2.2 Preparing Imaging Boot CDs or DVDs

If you have software for burning CDs or DVDs, you can create an imaging boot CD or DVD for imaging operations. You have two options:

- "Creating a Boot CD or DVD with Additional Files" on page 354
- "Creating a Boot CD or DVD without Additional Files" on page 355

For information on how to use the CD or DVD to perform disconnected imaging operations, see Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424.

Creating a Boot CD or DVD with Additional Files

This section describes how to create an imaging CD or DVD that contains more than the files provided in the `bootcd.iso` image.

This method allows you to include the settings.txt file on the boot CD or DVD to provide the required imaging parameters. For more information on the settings.txt file, see Section D.5, "Imaging Configuration Parameters (settings.txt)," on page 618.

This method also allows you to add other files and drivers that you need to do the imaging.

To create an imaging boot CD or DVD that includes settings.txt and other files:

1 Copy the bootcd.iso file to a temporary location.

> The bootcd.iso file is located in the /opt/novell/zenworks/zdm/winutils directory on the imaging server where ZENworks Linux Management is installed.

2 In an ISO editor, open the temporary copy of the bootcd.iso file.

> If you experience ISO corruption after adding files into the ISO, such as a checksum error, use a more reliable ISO editor. Also, some ISO editors do not work very well with DVDs.

3 Using the temporary bootcd.iso file, copy the settings.txt file to the root of the bootcd.iso image.

> The settings.txt file is located in the /opt/novell/zenworks/zdm/winutils directory on the imaging server where ZENworks Linux Management is installed.

4 Copy any other files or drivers that you want included on the CD or DVD to the /addfiles directory in the temporary bootcd.iso image.

> Any files or subdirectories that you add under the /addfiles directory are placed at the root of the client when booting the CD or DVD.

> **IMPORTANT:** When booting from the CD or DVD, the imaging engine is read into RAM. Because the imaging engine uses some of the RAM that exists on the client device, the combined size of any files that you add under the /addfiles directory cannot exceed amount of remaining RAM.

5 Save the updated bootcd.iso image file to its temporary location.

6 Use your software for burning CDs or DVDs to burn the updated bootcd.iso image onto the CD or DVD.

7 Boot the device to be imaged from your newly created imaging boot CD or DVD.

> Booting from a SCSI CD-ROM device is currently not supported.

Creating a Boot CD or DVD without Additional Files

If you do not want to include the settings.txt file or any other files or drivers in the imaging boot CD or DVD, you can simply create the imaging boot CD or DVD from the bootcd.iso image provided with ZENworks.

However, you will need to provide the settings.txt file on a floppy diskette to provide the required imaging parameters. For more information on the settings.txt file, see Section D.5, "Imaging Configuration Parameters (settings.txt)," on page 618.

To create an imaging boot CD or DVD that contains only the bootcd.iso image:

1 Copy the settings.txt file containing the settings you want for the imaging boot process onto a floppy diskette.

> This file is located in the /opt/novell/zenworks/zdm/winutils directory on the imaging server where ZENworks Linux Management is installed.

2 Use your software for burning CDs or DVDs to burn the `bootcd.iso` image onto the CD or DVD.

The `bootcd.iso` file is located in the `/opt/novell/zenworks/zdm/winutils` directory on the imaging server where ZENworks Linux Management is installed

3 Boot the device to be imaged from your newly created imaging boot CD or DVD.

You will be prompted for the diskette that contains the `settings.txt` file.

Booting from a SCSI CD-ROM device is currently not supported.

29.2.3 Using the ZENworks Imaging Media Creator

This utility allows you to do the following:

- "Managing the Settings.txt File" on page 356
- "Creating a Bootable Diskette" on page 359
- "Creating a Preboot Bootable Image" on page 361

IMPORTANT: This utility is a .NET application, and therefore requires the .NET framework to be installed on the Windows device being used to run it.

Managing the Settings.txt File

There two `settings.txt` files shipped with ZENworks Linux Management:

- **/srv/tftp/boot/settings.txt:** PXE devices use this version of the file for automated preboot work. This file exists on the imaging server and usually does not need to be modified. During the boot process, this `settings.txt` file is read and the necessary settings information is discovered and used.
- **/opt/novell/zenworks/zdm/winutils/settings.txt:** The imaging server copy of this file needs to be modified for your network environment and a working copy of it should be maintained at the root of the imaging boot device (imaging CD or DVD, or a blank floppy diskette). When burning the imaging CD or DVD, be sure to include the edited copy of this `settings.txt` file.

  You can manage the content of this copy of the `settings.txt` file with the ZENworks Imaging Media Creator utility, as outlined in the following steps.

  To manually edit the `settings.txt` file, see Section D.5, "Imaging Configuration Parameters (settings.txt)," on page 618.

For more information, see Section D.5, "Imaging Configuration Parameters (settings.txt)," on page 618.

To manage the `settings.txt` file using the ZENworks Imaging Media Creator utility:

1 On a Windows device, browse to the `opt/novell/zenworks/zdm/winutils` directory on your Linux imaging server and run `zmediacreator.exe`.

You might need to configure Samba on the Linux server in order for the Windows device to have access to this directory.

The following dialog box is displayed:
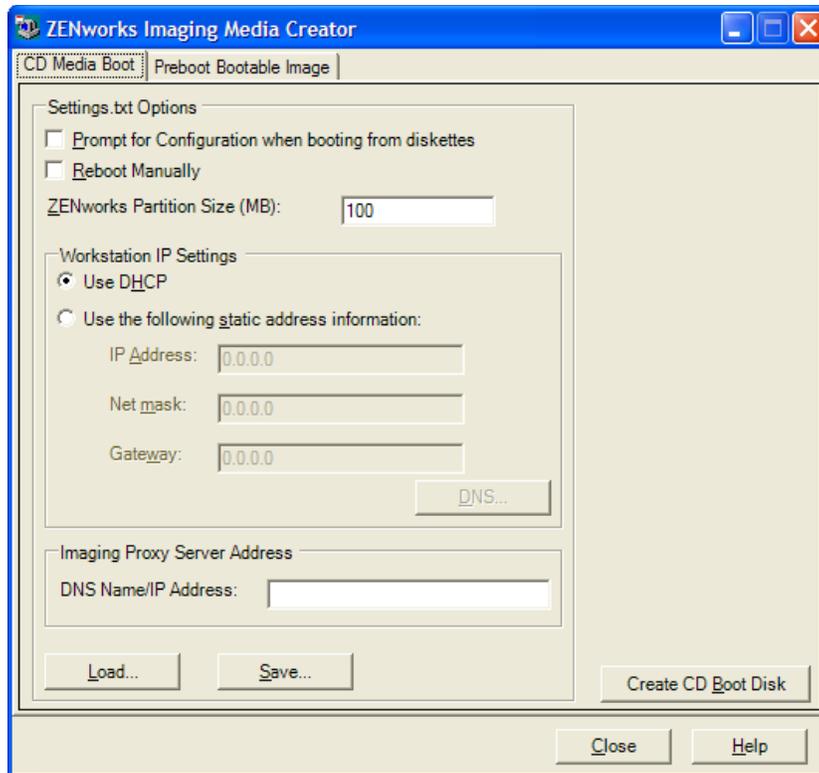
2 Click *Load*, browse for the `settings.txt` file, then click *Open*.

The default location is `A:\`. Browse to the `/opt/novell/zenworks/zdm/winutils/` directory for the copy to be modified.

When the file is loaded, the fields in this dialog box are populated from the information contained in the `settings.txt` file.

3 (Optional) In the *Settings.txt Options* section on the CD Media Boot page, fill in the fields:

Prompt for Configuration When Booting from Diskette: Specifies whether to prompt for these configuration settings when you boot a device with the bootable diskette and CD or DVD. If you leave this option deselected, the device boots using the configuration settings that you make here and you are not able to override the settings during bootup. If you select this option, you are given the chance to change each setting during bootup.

Reboot Manually: Specifies whether you must reboot a device manually after it was booted with the bootable diskette in automatic mode. (If the device was booted with the bootable diskette in manual mode, you must always reboot the device manually.)

If you boot a device with the bootable diskette and you let the bootup process proceed in automatic mode, the imaging engine starts and checks the Preboot server to see if an automatic imaging operation should be performed. If so, it performs the imaging operation on the device and quits. If not, it quits without doing anything. What happens next depends on whether you select this option.

If you leave this option deselected, you are prompted to remove the bootable diskette and press any key to reboot the device automatically to its native operating system. If you select this option, the device doesn't reboot automatically, but instead displays the Linux bash prompt,

allowing you to perform additional imaging-related tasks at the command line. This is helpful if you want to do things like check the current partition information or the image-safe data before rebooting to the native operating system.

ZENworks Partition Size (MB): Specifies the number of megabytes to allocate to the ZENworks partition if you choose to create one locally on a device when you boot the device with the bootable diskette. The default size is 150 MB, which is the smallest you should make the partition. The maximum size allowed is 2048 MB (2 GB).

4 (Optional) In the *Workstation IP Settings* section on the CD Media Boot page, fill in the fields:

Use DHCP: Specifies to obtain an IP address dynamically through DHCP. Use this option only if DHCP is configured on your network.

For Red Hat Enterprise Linux, using the DHCP option causes a "Could not look up Internet address..." message to be displayed during bootup. This is because zislnx does not know the IP address when DHCP is being used, so the /etc/hosts file contained in the image does not have the new IP address and host name. Simply select the *Log In Anyway* option to continue. Then to prevent this message from displaying each time the device boots, edit the /etc/hosts file on the device and add in its IP address.

Use the Following Static Address Information: Specifies to use a static IP address. If you select this option, fill in the IP address, subnet mask, and gateway to be used.

DNS button: This option is active only if a static IP address for the device is specified.
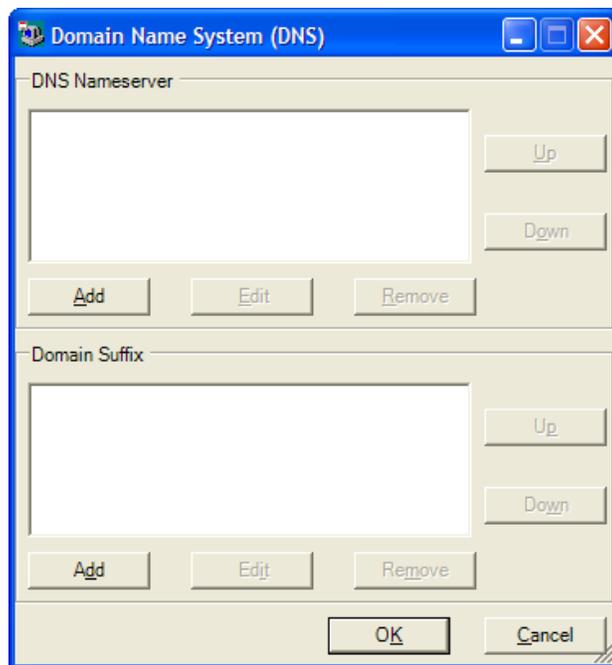
- ◆ **DNS Nameserver:** You must specify a nameserver if you want to use DNS to connect to servers.

  You can specify the addresses of as many DNS nameservers as you want. You can edit or remove the nameserver addresses, or you can move the addresses up and down in the list to specify the order used for contacting them.

- ◆ **Domain Suffix:** You can also specify as many DNS domain suffixes as you want. The editing, moving, and removal functions are also available for the suffixes.

5 (Required) In the *Imaging Proxy Server Address* section on the CD Media Boot page, specify either the fixed IP address or the full DNS name of Preboot server (where novell-pbserv is running).

This specifies which Preboot server to connect to when you boot a device with the bootable diskette.

Use a DNS name only if it is working on your network and the imaging server has an entry in your DNS server's name resolution table.

6 Click *Save*, browse for where you want to save the `settings.txt` file, then click *Save*.

Saves the configurations made in the *Settings.txt Options* section to the `settings.txt` file in the specified location. The default location is `A:\`, such as for a bootable diskette (see "Creating a Bootable Diskette" on page 359).

You can save to a different location for use in burning to an imaging CD or DVD.

7 When you are finished using this utility, click *Close*.

IMPORTANT: If you manually edit the `settings.txt` file to provide paths to executables, make sure that you provide the full path, or the executable might not run.

Creating a Bootable Diskette

If you have devices that cannot normally boot a CD or DVD, but has the CD or DVD hardware installed, you can use the ZENworks Imaging Media Creator utility to create a diskette that enables the device to boot from a CD or DVD.

To create a bootable diskette:

1 On a Windows device, browse to the `opt/novell/zenworks/zdm/winutils` directory on your Linux imaging server and run `zmediacreator.exe`.

You might need to configure Samba on the Linux server in order for the Windows device to have access to this directory.

The following dialog box is displayed:
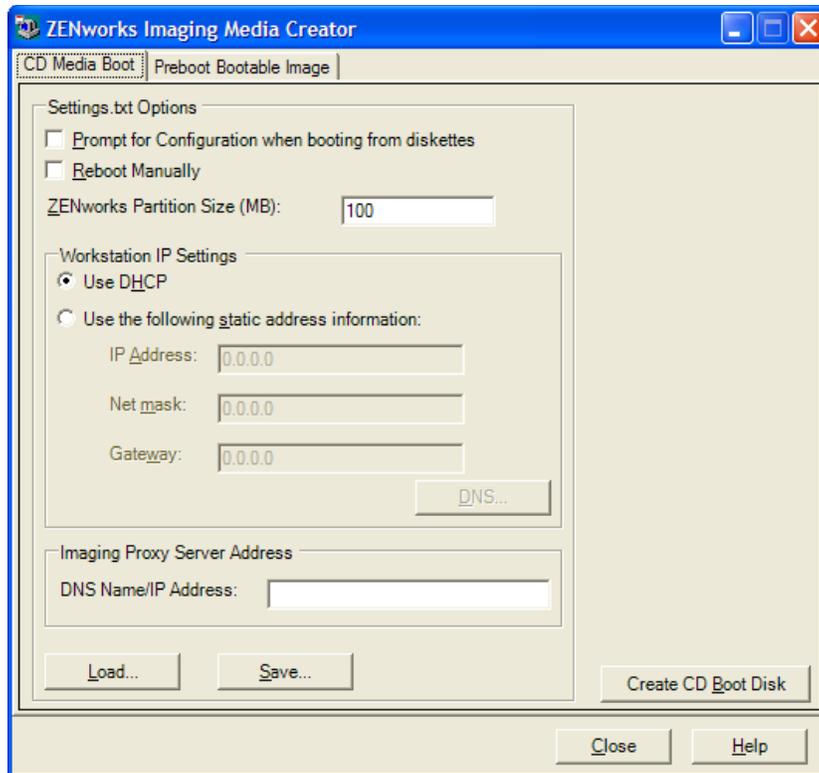
2 If you want to modify a `settings.txt` file that is to be included on this diskette, follow Step 2 through Step 4 in "Managing the Settings.txt File" on page 356, then continue with Step 3 in this section.

3 (Required) In the *Imaging Proxy Server Address* section on the CD Media Boot tab, specify either the fixed IP address or the full DNS name of Preboot server (where novell-pbserv is running).

This specifies which Preboot server to connect to when you boot a device with the bootable diskette.

Use a DNS name only if it is working on your network and the imaging server has an entry in your DNS server's name resolution table.

4 Format one high-density diskette, or insert a preformatted blank diskette in the diskette drive of the Windows device.

5 Click *Create CD Boot Disk*.

This creates a bootable diskette that enables a device that cannot otherwise boot from a CD or DVD to boot from the imaging CD or DVD. Any `settings.txt` configurations made here are included in the copy written to the bootable diskette.

6 After the diskette is created, click *Close*.

7 Insert both this diskette and the imaging CD or DVD on the device to be imaged, then boot the device.

The diskette enables the imaging CD or DVD to be booted by the device.

Creating a Preboot Bootable Image

You can create a PXE Linux configuration file that points to a Preboot Bootable Image (PBI) file, which is a raw image of a bootable diskette. This enables you to use PXE to utilize the bootable diskette information from a `.pbi` file on a TFTP server, instead of booting from the diskette for that Preboot information.

To create a PBI configuration file and then the PBI file:

1 On a Windows device, browse to the `opt/novell/zenworks/zdm/winutils` directory on your Linux imaging server and run `zmediacreator.exe`.

You might need to configure Samba on the Linux server in order for the Windows device to have access to this directory.

The following dialog box is displayed after you click the *Preboot Bootable Image* tab:
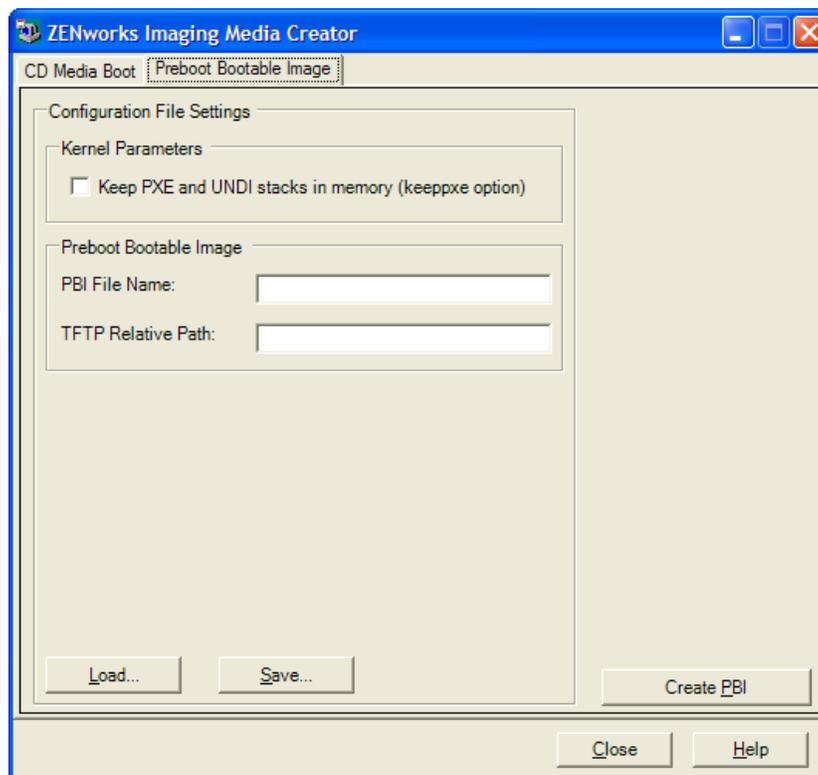
2 In the *Configuration File Settings* section on the Preboot Bootable Image page, fill in the fields:

Kernel Parameters: To use the kernel parameters in the keeppxe option, select the *Keep PXE and UNDI Stacks in Memory* option.

PBI Filename: Specify a filename for the PBI file, including the `.pbi` filename extension. Do not specify a path here.

TFTP Relative Path: Enter the path for the PBI file, relative to the TFTP server's default path. This is where the PBI file will be accessed by the device booting with PXE.

Load: Load a previously defined PBI configuration file, which populates the fields on this page with its information. You can edit those settings.

Save: Save the PBI configuration file to a location where you can access it again from this dialog box.

3 To create the PBI file, click *Create PBI* and fill in the fields:
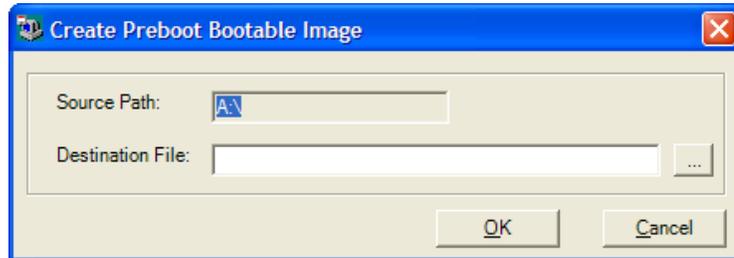
Source Path: Source of the information to be imaged to a PBI file. This is normally a bootable diskette that was created on the *CD Media Boot* tab of this dialog box.

Destination File: Where the PBI file should be written. Browse for the location and type the PBI filename. The `.pbi` filename extension is automatically added.

4 After the BPI is created, click *Close*.

This PBI file can now be used by a PXE-enabled device when booting so you can access Preboot Services functionality as if you were booting the device with the bootable diskette.

29.2.4 Managing ZENworks Partitions

A ZENworks partition is used by a device when booting for automated Preboot Services work when the device does not have PXE available. The following sections explain how to manage ZENworks partitions:

- ◆ "Creating a ZENworks Partition" on page 362
- ◆ "Disabling a ZENworks Partition" on page 363
- ◆ "Removing a ZENworks Partition" on page 363

Creating a ZENworks Partition

If you want to set up a device for unattended imaging operations and are unable to use Preboot Services (PXE), you can create a ZENworks partition on the hard disk. If you make the partition large enough, you can even store an image of the device's hard disk, which can be useful if the device becomes misconfigured or corrupted when the network connection is lost.

WARNING: Installing the ZENworks partition destroys all data on that hard drive. Use this only on devices where you plan to reinstall the operating system and software programs.

To create a ZENworks partition, you must first create an imaging CD or DVD to boot the device from. (If the device cannot boot from a CD or DVD, see Section 29.2.3, "Using the ZENworks Imaging Media Creator," on page 356.) Then, do the following:

1 Boot the device with the imaging CD or DVD, then select *Install/Update ZEN partition* from the menu.

This starts the process of creating the ZENworks partition in the first partition slot. It destroys all existing partitions, except an existing ZENworks partition or the Dell or Compaq configuration partitions. By default, the ZENworks partition size is 150 MB.

If the ZENworks partition already exists, it is upgraded, and your existing partitions are left intact.

2 After the ZENworks partition is installed or updated, remove the CD or DVD and press any key to continue.

3 After removing the CD or DVD and reboot the device, install the operating system on the device.

IMPORTANT: During installation of the operating system, you must install the boot loader where the root (/) partition is being installed. In other words, the active partition must be the root partition. You can use `fdisk` to verify that the active partition is root.

4 To take an image of the device using the ZENworks partition, see "Creating an Image Using the Bash Prompt" on page 426.

5 When the bash prompt is displayed, reboot the device.

The device should boot to Linux. If the bash prompt is displayed again, enter `lilo.s` and reboot a second time.

Disabling a ZENworks Partition

If you decide to enable PXE on a device, but have previously installed a ZENworks partition on it, you can disable or delete the partition, because it is no longer necessary. For information on deleting the partition, see "Removing a ZENworks Partition" on page 363.

When you boot to Linux using any imaging boot device or method other than booting from the ZENworks partition, you can disable (or enable) the ZENworks partition. Just select the menu option to do so when the Preboot Services Menu is presented.

Removing a ZENworks Partition

Because you should not delete the ZENworks partition if you booted using the partition, you should boot the device from an imaging boot method other than the ZENworks partition.

WARNING: After you have deleted the ZENworks partition, you need to make sure that the image you put on the device was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot. You should only remove the ZENworks partition if you are going to restore an image that does not have the partition to the device.

The following are ways you can remove a ZENworks partition from a device:

 * "Using an Imaging CD or DVD" on page 363
 * "Using a ZENworks Script Bundle" on page 364
 * "Using Fdisk" on page 364

Using an Imaging CD or DVD

If you cannot perform a full restoration at this time, you should consider disabling the ZENworks partition.

To remove a ZENworks partition:

1 Boot the device using the ZENworks 7.3 Linux Management imaging CD or DVD.

2 Select the *Manual mode* option.

3 At the bash prompt, enter:

```
img zenPart remove
```

4 After the removal is complete, eject the CD or DVD (if you are not going to use it to re-image the device).

5 If you want to restore an image before rebooting, enter the following at the bash prompt:

```
unset ZENDEVICE
```

Otherwise, reboot the device when ready.

6 Restore an image or install an operating system.

When the device boots, its ZENworks partition is removed, then the device can be imaged from the CD or DVD without a ZENworks partition.

If the device is assigned to a Preboot Services bundle, it is imaged according to that bundle.

Using a ZENworks Script Bundle

If you are using Preboot Services, but formerly booted from the ZENworks partition on the device, you can delete the ZENworks partition at the same time you put down an image. However, the new image should not contain a ZENworks partition.

For example, you can do the following:

1 In the ZENworks Control Center, create a ZENworks Script bundle.

2 In the *Script text* field in the Create New Preboot Bundle wizard, enter:

```
img zenPart remove
```

3 In the *Script text* field (after the above command), enter the other commands necessary for the imaging work you want for this device.

For more information, see Appendix E, "ZENworks Imaging Engine Commands," on page 631.

4 On the Summary page of the wizard, click *Finish* (not *Next*).

5 Reboot the device.

Using Fdisk

You can remove a ZENworks partition by simply using `fdisk` to reconfigure the device's hard drive. Then, you can either image the device using a ZENworks imaging CD or DVD, or enable PXE on the device and assign a Preboot bundle to it, then reboot it to use that bundle.

29.3 Deploying and Managing Preboot Services

The following sections explain how to set up, deploy, and manage Preboot Services:

◆ Section 29.3.1, "Checking the Preboot Services Imaging Server Setup," on page 365
◆ Section 29.3.2, "Deploying Preboot Services In a Network Environment," on page 366

For information on using Preboot, see Chapter 30, "Using Preboot Services," on page 407.

29.3.1 Checking the Preboot Services Imaging Server Setup

This section provides information on how to check the configuration of Preboot Services after it is installed, and how to set up standard DHCP and novell-proxydhcp daemons on the same server.

◆ "Overview of Preboot Services Components" on page 365

◆ "Checking the Setup" on page 365

Overview of Preboot Services Components

The following components are installed as part of Preboot Services:

Table 29-1 *Preboot Service Components*

Daemon	Description
novell-pbserv	The novell-pbserv daemon provides imaging services to devices.
novell-proxydhcp	The novell-proxydhcp daemon runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server. The Proxy DHCP server also responds to PXE devices to indicate which bootstrap program (`nvlnbp.sys`) to use.
novell-tftp	The novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these imaging files, such as the Linux kernel, initrd, and `nvlnbp.sys`. A PXE device uses this server to download the bootstrap program (`nvlnbp.sys`).
novell-zmgprebootpolicy	The PXE devices use the novell-zmgprebootpolicy daemon to check if there are any Preboot bundles that are assigned to the device.

The novell-proxydhcp daemon must be started manually and does not need to be run on all imaging servers.

The other three daemons are started automatically when installing ZENworks Linux Management, or any time the server is rebooted, and must run on all imaging servers.

For more information on these daemons, see Section D.7, "Imaging Server," on page 621.

Checking the Setup

After the Preboot Services components are installed, the following daemons should be installed and running on the server:

Table 29-2 *Preboot Services Daemons*

Service	Command to Check Its Status
novell-pbserv	`/etc/init.d/novell-pbserv status`
novell-tftp	`/etc/init.d/novell-tftp status`
novell-zmgprebootpolicy	`/etc/init.d/novell-zmgprebootpolicy status`

You should not need to change the default configuration of these daemons.

If the server where the Preboot Services components are installed is also a DHCP server, see .

29.3.2 Deploying Preboot Services In a Network Environment

To implement the network deployment strategies outlined in this section, you must have a solid understanding of the TCP/IP network protocol and specific knowledge of TCP/IP routing and the DHCP discovery process.

Deploying Preboot Services (with PXE) in a single network segment is a relatively simple process. However, Preboot Services deployment in a multi-segment network is far more complex and might require configuration of both the Preboot Services daemons and the network switches and routers that lie between the server and the PXE devices.

Configuring the routers or switches to correctly forward Preboot Services network traffic requires a solid understanding of the DHCP protocol, DHCP relay agents, and IP forwarding. The actual configuration of the switch or router must be performed by a person with detailed knowledge of the hardware.

We strongly recommend that you initially set up Preboot Services in a single segment to ensure that the servers are configured correctly and are operational.

This section includes the following information:

-
-
-
-

Server Configuration

There are three important points about configuring servers for Preboot Services:

- **DHCP server:** The Preboot Services environment requires a standard DHCP server. It is up to you to install your standard DHCP server.
- **Preboot Services daemons:** The four Preboot Services daemons (novell-pbserv, novell-tftp, novell-proxydhcp, and novell-zmgprebootpolicy) are all installed on the imaging server when you install ZENworks Linux Management. These daemons must run together on the same server.

- **Imaging server:** The Preboot Services daemons can be installed and run on the same or different server than DHCP.

The following sections give general information about these services:

- "The DHCP Server" on page 367
- "The novell-pbserv daemon" on page 367
- "The novell-proxydhcp daemon" on page 367
- "The novell-tftp daemon" on page 367
- "The novell-zmgprebootpolicy daemon" on page 367

It is seldom necessary to make changes to the default configuration of these services. However, if you need more detailed configuration information, see "Configuring Preboot Services Imaging Servers in Linux" on page 374.

The DHCP Server

The standard DHCP server must be configured with an active scope to allocate IP addresses to the PXE devices. The scope options should also specify the gateway or router that the PXE devices should use.

If Preboot Services (specifically novell-proxydhcp) is installed on the same server as the DHCP server, then the DHCP server must be configured with a special option tag. For more information, see "Configuring LAN Environments for Preboot Services" on page 370.

The novell-pbserv daemon

The Preboot Services novell-pbserv daemon provides imaging services to devices.

This includes sending and receiving image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so on.

The novell-proxydhcp daemon

The Preboot Services Proxy DHCP server runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server, the IP address of the server where novell-zmgprebootpolicy is running, and the name of the network bootstrap program (`nvlnbp.sys`).

The novell-tftp daemon

The Preboot Services novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these files.

A PXE device uses one of these servers to download the network bootstrap program (`nvlnbp.sys`).

The novell-zmgprebootpolicy daemon

PXE devices uses novell-zmgprebootpolicy to check if there are any imaging actions that need to be performed on the device. It forwards requests to novell-pbserv on behalf of PXE devices.

If you are using Intel AMT, support for it should be enabled in the `novell-zmgprebootpolicy.conf` file. (This feature is not currently supported in Novell ZENworks Linux Management.)

Network Configuration

The configuration required to run Preboot Services in your network depends on your network setup. Design your network so that PXE devices can effectively connect to the server where the Preboot Services daemons are running. Make sure you consider the number of PXE devices to be installed on the network and the bandwidth available to service these devices. To understand how the devices and servers need to interact during the Preboot Services process, see Section 28.4, "The Preboot Services Processes," on page 339.

You can configure Preboot Services where Preboot Services and DHCP are running on the same server or on different servers in both LAN and WAN/VLAN environments:

- "Understanding Preboot Services in LAN and WAN/VLAN Environments" on page 368
- "Comparing Preboot Services Setups in LAN and WAN/VLAN Environments" on page 368
- "Configuring LAN Environments for Preboot Services" on page 370
- "Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server" on page 370
- "Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers" on page 371

Understanding Preboot Services in LAN and WAN/VLAN Environments

Imaging servers should be installed so that PXE devices have access to imaging services within their LAN. A good design ensures that a client does not need to connect to imaging services through a slow WAN link.

Although you can have any number of imaging servers, generally only one Proxy DHCP server should be enabled per DHCP server scope.

In a WAN, the PXE device is usually separated from the Proxy DHCP and DHCP servers by one or more routers. The PXE device broadcasts for DHCP information, but by default the router does not forward the broadcast to the servers, causing the Preboot Services session to fail.

In a VLAN (Virtual LAN) environment, the PXE device is logically separated from the Proxy DHCP server and the DHCP server by a switch. At the IP level, this configuration looks very similar to a traditional WAN (routed) environment.

In a typical VLAN environment, the network is divided into a number of subnets by configuring virtual LANs on the switch. Devices in each virtual LAN usually obtain their IP address information from a central DHCP server. In order for this system to work, it is necessary to have Bootp or IP helpers configured on each gateway. These helpers forward DHCP requests from devices in each subnet to the DHCP server, allowing the DHCP server to respond to devices in that subnet.

Comparing Preboot Services Setups in LAN and WAN/VLAN Environments

The following illustrates the differences for a LAN configuration between installing Preboot Services on the same server as DHCP, or on a separate server. In this case, only the PXE devices on the LAN connect to the Preboot Services imaging server.

Table 29-3 *LAN Configuration Differences Between the Same and Separate Servers*

Information	On the Same Server	On Separate Servers
Configuration	Because Preboot Services and DHCP are running on the same server, option tag 60 must be set on the DHCP server. For information on setting this tag, see "Configuring LAN Environments for Preboot Services" on page 370.	None required.
Advantages	◆ Easy installation and setup. ◆ No network configuration is required.	◆ Easiest installation and setup. ◆ No network configuration is required. ◆ No DHCP server configuration is required.
Disadvantages	◆ DHCP server configuration is required (option tag 60). ◆ Limited use, because a single-LAN environment only exists in small lab-type networks.	◆ Limited use, because a single-LAN environment only exists in small lab-type networks.

The following illustrates the differences for a WAN/VLAN configuration between installing Preboot Services on the same server as DHCP, or on a separate server. In this case, all PXE devices over the entire WAN/VLAN connect to the Preboot Services imaging server.

Table 29-4 *WAN/VLAN Configuration Differences Between the Same and Separate Servers*

Information	On the Same Server	On Separate Servers
Configuration	The routers/switches have been configured with IP helpers to forward network traffic to the DHCP server. Because Preboot Services and DHCP are running on the same server, option tag 60 is set on the DHCP server. For information on setting this tag, see "Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server" on page 370.	A DHCP relay agent or IP helper is configured on the router/switch serving the subnet that the PXE device belongs to. The helper is configured to forward all DHCP broadcasts that are detected in the subnet to the DHCP and Proxy DHCP servers. This normally requires two helpers to be configured: the first to forward DHCP broadcasts to the DHCP server, and the second to forward the DHCP broadcasts to the Proxy DHCP server.
Advantages	◆ No network equipment (routers/switches) needs to be configured to forward network traffic to the TFTP server.	◆ Common network setup. ◆ Multiple Preboot Services imaging servers can be installed so that each server provides service only for certain subnets.

Information	On the Same Server	On Separate Servers
Disadvantages	- DHCP server configuration required (option tag 60). - Only one Preboot Services imaging server can be installed because it needs to run on the same server as the DHCP server (and there is usually only one DHCP server).	The network equipment (routers/switches) must be configured with additional IP helpers. Some network equipment might not function properly when more than one additional IP helper is configured.

Configuring LAN Environments for Preboot Services

For the case where you have Preboot Services and DHCP running on separate servers, no network configuration is required.

For the case where you have Preboot Services and DHCP are running on the same server, option tag 60 must be set on the DHCP server. Do the following to set up standard DHCP and Proxy DHCP on the same server:

1 Stop the DHCP services on the Linux imaging server.

2 On this server, open the `dhcp.conf` file in an editor.

3 Insert the following line in the file:

```
option vendor-class-identifier "PXEClient";
```

4 Save the file.

5 Restart the DHCP service.

Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server

You can install ZENworks Linux Management (which includes Preboot Services) on the same server where DHCP is installed and running. However, you must do the following to make it work:

- Set option tag 60 on the DHCP server so that it can work with the novell-proxydhcp daemon. See the steps in the previous section ().

- On the Linux server, edit the `/etc/opt/novell/novell-proxydhcp.conf` file and change:

```
LocalDHCPFlag = 0
```

to

```
LocalDHCPFlag = 1
```

Then restart the daemon so that the change is recognized by entering the following command on the Linux server:

```
/etc/init.d/novell-proxydhcp restart
```

IMPORTANT: If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers

You can install ZENworks Linux Management (which includes Preboot Services) on a separate server than where DHCP is installed and running. However, you must configure the network equipment so that it correctly forwards Preboot Services network traffic.

IMPORTANT: If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

An example deployment is given below of a WAN/VLAN environment with Preboot Services and DHCP running on the same server. The following sections provide the specific steps required to configure network equipment so that it correctly forwards Preboot Services network traffic.

Example Deployment

In this example, three VLANs are configured on a Bay Networks Accel 1200 switch running firmware version 2.0.1. One VLAN hosts the Proxy DHCP server, the second VLAN hosts the DHCP server, and the third VLAN hosts the PXE device. The PXE device's DHCP broadcast is forwarded by the switch to both the Proxy DHCP server and the DHCP server. The response from both servers is then routed correctly back to the PXE device, and the PXE device starts the Preboot Services session correctly.

The three VLANs are all 24-bit networks; their subnet mask is 255.255.255.0.

The first VLAN gateway is 10.0.0.1. This VLAN hosts the PXE device that is allocated an IP in the range of 10.0.0.2 to 10.0.0.128. This VLAN is named VLAN1.

The second VLAN gateway is 10.1.1.1. This VLAN hosts the DHCP server with IP 10.1.1.2. This VLAN is named VLAN2.

The third VLAN gateway is 196.10.229.1. This VLAN hosts the server running novell-proxydhcp and novell-zmgprebootpolicy. The server's IP is 196.10.229.2. This VLAN is named VLAN3.

Routing is enabled between all VLANs. Each VLAN must be in its own spanning tree group.

Configuring Cisco Equipment

1 Go to the Global configuration mode.

2 Type `ip forward-protocol udp 67,` then press Enter.

3 Type `ip forward-protocol udp 68,` then press Enter.

4 Go to the LAN interface that serves the PXE device.

5 Type `ip helper-address 10.1.1.2,` then press Enter.

6 Type `ip helper-address 196.10.229.2,` then press Enter.

7 Save the configuration.

Configuring Nortel Network Equipment

1 Connect to the router with Site Manager.

2 Ensure that IP is routable.

3 Enable the *Bootp* check box on the PXE device subnet/VLAN.

4 Select the interface that the PXE devices are connected to.

5 Edit the circuit.

6 Click *Protocols*.

7 Click *Add/Delete*.

8 Ensure that there is a check mark in the *Bootp* check box.

9 Click *OK*.

10 Click *Protocols > IP > Bootp > Relay Agent interface table*.

The interface where Bootp was enabled is visible in the list.

11 Click *Preferred server*.

12 Change the *Pass through mode* value to Bootp and DHCP.

13 Set up the relay agents:

13a Click *Add*.

13b In the *Relay agent IP address* box, type the local LAN IP address.

13c In the *Target server IP address* box, type the DHCP server IP address.

13d Click *OK*.

13e Change the *Pass through mode* value to Bootp and DHCP.

13f Perform Step 1 to Step 5 again and specify the Proxy DHCP server IP address at Step 3.

13g Apply the configuration.

Configuring Bay Network Equipment

Perform the following steps on the switch:

1 Enable DHCP for the client VLAN using the following command lines:

```
# config vlan1 ip
# dhcp enable
```

2 Configure IP helpers to forward DHCP requests from the device subnet to the TFTP server, using the following command lines:

```
# config ip dhcp-relay
# create 10.0.0.1 10.1.1.2 mode dhcp state enable
# create 10.0.0.1 196.10.229.2 mode dhcp state enable
```

The create command has the form `create agent server mode dhcp state enable`, where *agent* is the IP address of the gateway that serves the PXE device, and *server* is the IP address of the server that the DHCP frame should be forwarded to.

3 Save the configuration.

Configuring Filters on Switches and Routers

Some network devices filter network traffic that passes through them. Preboot Services makes use of several different types of traffic, and all of these must be able to successfully pass through the router or switch for the Preboot Services session to be successful. The Preboot Services session uses the following destination ports:

Table 29-5 *Destination Ports for Preboot Services*

Component	Port
DHCP and Proxy DHCP servers	UDP Port 67, 68, and 4011
TFTP server	UDP Port 69
novell-zmgprebootpolicy	UDP Port 13331

IMPORTANT: If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

Spanning Tree Protocol in Switched Environments

The spanning tree protocol (STP) is available on certain switches and is designed to detect loops in the network. When a device (typically a network hub or a device) is patched into a port on the switch, the switch indicates to the device that the link is active, but instead of forwarding frames from the port to the rest of the network, the switch checks each frame for loops and then drops it. The switch can remain in this listening state from 15 to 45 seconds.

The effect of this is to cause the DHCP requests issued by PXE to be dropped by the switch, causing the Preboot Services session to fail.

It is normally possible to see that the STP is in progress by looking at the link light on the switch. When the device is off, the link light on the switch is obviously off. When the device is turned on, the link light changes to amber, and after a period of time changes to a normal green indicator. As long as the link light is amber, STP is in progress.

This problem only affects PXE devices that are patched directly into an Ethernet switch. To correct this problem, perform one of the following:

- Turn off STP on the switch entirely.
- Set STP to Port Fast for every port on the network switch where a PXE device is attached.

After the problem is resolved, the link light on the port should change to green almost immediately after a device connected to that port is turned on.

Information about STP and its influence on DHCP can be found at Using PortFast and Other Commands to Fix End-Station Startup Connectivity Problems (http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1923.htm#xtocid897350).

29.3.3 Administering Preboot Services

This section includes information about administering and configuring Preboot Services:

Configuring Preboot Services Imaging Servers in Linux

In Preboot Services, the daemons do not use switches. Instead, to configure a daemon to do something that is not a default, you need to edit the configuration files.

You can edit configuration files while the daemon is running, because they are only read when the daemon starts. Therefore, after editing the file you must restart the daemon for the changes to take effect.

For more information on the daemon configuration files, see Section D.7, "Imaging Server," on page 621.

The following sections explain how to configure the following ZENworks Linux Management imaging servers:

Configuring the TFTP Server

It is seldom necessary to change the default TFTP server configuration values. If you need to change them, use the following procedure:

1 Open the following file in an editor:

```
/etc/opt/novell/novell-tftp.conf
```

2 Edit the configuration settings per instructions within the file.

3 Save the changes.

4 In a shell console, enter the following command:

```
/etc/init.d/novell-tftp restart
```

Configuring the Proxy DHCP Server

The Proxy DHCP server provides PXE devices with the information that they require to be able to connect to the Preboot Services system.

Use the following steps to modify the settings of novell-proxydhcp:

1 Open the following file in an editor:

```
/etc/opt/novell/novell-proxydhcp.conf
```

2 Edit the configuration settings per instructions within the file.

3 Save the changes.

4 In a shell console, enter the following command:

```
/etc/init.d/novell-proxydhcp restart
```

You can set any of the IP address fields in the configuration utility to 0.0.0.0. The server replaces these entries with the IP address of the first network adapter installed in the server.

Configuring the Novell-pbserv Daemon

The novell-pbserv daemon provides imaging services to the devices.

Use the following steps to modify the settings of novell-pbserv:

1 Open the following file in an editor:

```
/etc/opt/novell/zenworks/preboot/novell-pbserv.conf
```

2 Edit the configuration settings per instructions within the file.

3 Save the changes.

4 In a shell console, enter the following command:

```
/etc/init.d/novell-pbserv restart
```

Configuring Novell-zmgprebootpolicy

The novell-zmgprebootpolicy daemon is used to check if there are any imaging actions that need to be performed on the device. It forwards requests to novell-pbserv on behalf of PXE devices.

Use the following steps to modify the settings of novell-zmgprebootpolicy:

1 Open the following file in an editor:

```
/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf
```

2 Edit the configuration settings per instructions within the file.

3 Save the changes.

4 In a shell console, enter the following command:

```
/etc/init.d/novell-zmgprebootpolicy restart
```

Configuring the DHCP Server

The DHCP server needs to have option 60 (decimal) added to the DHCP tags if the Proxy DHCP and DHCP servers are running on the same physical server. This option should be a string type and must contain the letters PXEClient.

For more information, see "Configuring LAN Environments for Preboot Services" on page 370.

Configuring IP Port Usage

This section describes the network ports used by Preboot Services. Using the information in this section, you can configure routers to correctly forward the network traffic generated by Preboot Services. For further information about configuring routers, see Section 29.3.2, "Deploying Preboot Services In a Network Environment," on page 366.

Preboot Services uses both well-known and proprietary IP ports.

The well-known IP ports include:

- **67 decimal:** The Proxy DHCP server listens on this port for PXE information requests. This is the same port used by a standard DHCP server.
- **68 decimal:** The DHCP/Proxy DHCP server responds to client requests on this port. This is the same port used by a standard DHCP server.
- **69 decimal:** The TFTP server listens on this port for file requests from PXE devices.
- **4011 decimal:** When running on the same server as the DHCP daemon, the Proxy DHCP server listens on this port for PXE information requests.

The proprietary IP ports include:

- **998 decimal:** novell-pbserv client connection port. The novell-pbserv daemon receives all connection requests from the Preboot Services devices on this port.
- **13331 decimal:** novell-zmgprebootpolicy client connection port. The novell-zmgprebootpolicy daemon receives all connection requests from the PXE devices on this port.

Although PXE devices make their initial requests to the novell-tftp and novell-zmgprebootpolicy daemons on the ports listed above, the remainder of the transactions can occur on any available port. For this reason, imaging servers cannot be separated from their clients by a firewall.

IMPORTANT: The novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

29.3.4 Editing the Preboot Services Menu

Depending on the configuration settings for Preboot Services in the ZENworks Control Center, PXE devices may be able to display the Preboot Services Menu during the boot process. The menu has the following options:

- *Start ZENworks Imaging*
- *Start ZENworks Imaging Maintenance*
- *Disable the ZENworks Partition*
- *Enable the ZENworks Partition*
- *Start DELL DTK*
- *Start DELL DTK (Maintenance Mode)*
- *Exit*

For more information on configuring whether to display the menu, see Section 29.4.1, "Configuring Preboot Services Menu Options," on page 380.

There might be circumstances when you want to modify the options on the Preboot Services Menu. You can customize these options by editing a text file contained on the imaging server. For example, you can:

- Add, delete, and modify menu options

- Change the color scheme
- Change the menu title and screen name

The following procedure should be done on each imaging server where you want to customize the menu.

To edit the Preboot Services Menu:

1 In a text editor, open the following file on an imaging server where novell-proxydhcp is running:

`/srv/tftp/pxemenu.txt`

IMPORTANT: If you want to save the default options for this menu, we recommend that you make a backup copy of `pxemenu.txt`, such as `pxemenu_orig.txt`.

A `pxemenu65.txt` file also exists for use by ZENworks 6.5 PXE devices that attach to ZENworks 7.3 servers through Preboot Services server referrals (see Section 28.3.6, "Preboot Referral Lists," on page 336). Its content and format is the same as `pxemenu.txt`, so instructions in this section apply equally to `pxemenu65.txt`, except where data is different for ZENworks 6.5.

The following is the content of the default Preboot Services Menu's `pxemenu.txt` file:

```
#This file describes a PXEMenu

ScreenName = Novell Preboot Services Menu
ScreenInfo = Version 1.0 August, 2005
MenuTitle = ZENworks Preboot Options

#The screen colors determine the color of the main part of the menu screen
ScreenColor = bright_white
ScreenBackgroundColor = blue

#The info colors determine the color of the screen information at the top
#of the menu screen
InfoColor = yellow
InfoBackgroundColor = blue

#The hint colors determine the color of the hint line at the bottom of the
screen
HintColor = lt_cyan
HintBackgroundColor = blue

#The menu colors determine the color of the menu box and menu title
MenuColor = yellow
MenuBackgroundColor = blue

#The option colors determine the color of the menu option
OptionColor = BRIGHT_WHITE
OptionBackgroundColor = BLUE

#The chosen colors determine the color of the high-lighted option
ChosenColor = BRIGHT_WHITE
ChosenBackgroundColor = RED

#Maximum of 9 menu items
MenuOptionCount = 7

option1 = Start ZENworks Imaging
option2 = Start ZENworks Imaging Maintenance
option3 = Disable ZENworks Partition
option4 = Enable ZENworks Partition
option5 = Start DELL DTK
option6 = Start DELL DTK (Maintenance Mode)
option7 = Exit

CFG1 = z_auto.cfg
CFG2 = z_maint.cfg
CFG3 = z_zpdis.cfg
CFG4 = z_zpen.cfg
CFG5 = dell-dtk.cfg
CFG6 = dell-dtk_maint.cfg
CFG7 = 0

Hint1 = ZENworks Imaging in Automated Mode
Hint2 = ZENworks Imaging Linux Session in Interactive Mode
Hint3 = Disable Existing ZENworks Partition
Hint4 = Re-enable a Disabled ZENworks Partition
Hint5 = DELL Deployment Toolkit v2.1 in Automated Mode
Hint6 = DELL Deployment Toolkit v2.1 in Maintenance Mode
Hint7 = Boot to Local Hard Drive
```

2 To change the appearance of the menu, edit the first seven sections (title and colors).

To change colors, the mnemonics you enter must be selected from the following:

BLACK	RED	GRAY	LT_GREEN
BLUE	MAGENTA	YELLOW	LT_CYAN
GREEN	BROWN	BRIGHT_WHITE	LT_RED
CYAN	WHITE	LT_BLUE	LT_MAGENTA

3 To change the menu options, edit the last four sections, beginning with "MenuOptionCount."

The menu options, their code, and their hint descriptions are correlated by the number (see "#" where used below).

MenuOptionCount: This number must match the total number of options defined in the next three sections. The limit is 9 menu options.

option#: Displayed in the menu as the option's text.

CFG#: The configuration file that is used upon selecting the menu option.

Hint#: Displayed in the bottom of the screen to explain the highlighted menu option's function. It changes as you highlight a menu option.

IMPORTANT: If you add or subtract a menu option, make sure that you do the same thing to each of the last three sections. The numbering should be consecutive (such as 1 through 5). Be sure to keep the corresponding items matched in each of the last three sections.

4 When finished, save the `pxemenu.txt` file.

29.4 Configuring Preboot Services Defaults

You can configure Preboot Services default settings for a ZENworks Management Zone. These are settings that apply globally to all devices in the management zone.

Some of these settings enable you to automatically register devices with the ZENworks Linux Management server, and some can be overridden by configurations done for devices or folders containing devices. For more information, see Section 29.5, "Overriding Preboot Services Defaults," on page 399.

The following default settings can be configured in the ZENworks Control Center:

- Section 29.4.1, "Configuring Preboot Services Menu Options," on page 380
- Section 29.4.2, "Configuring Image Storage Security," on page 381
- Section 29.4.3, "Configuring Non-registered Device Settings," on page 383
- Section 29.4.4, "Configuring Preboot Work Assignments," on page 386
- Section 29.4.5, "Configuring the Server Referral List," on page 393
- Section 29.4.6, "Configuring Intel Active Management Technology (AMT)," on page 395

29.4.1 Configuring Preboot Services Menu Options

To determine whether the Preboot Services Menu should be displayed on your devices when they boot:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following *Management Zone Settings* section:

Management Zone Settings		
Category	**Description**	**Is Configured**
System Variables	Configure system variables.	Yes
Device Refresh Schedule	Configure the device refresh interval.	No
Device Inventory	Configure inventory settings.	No
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
Preboot Services	Configure Preboot Services.	Yes
Remote Management	Enable and configure remote management.	Yes
Centralized Message Logging	Configuration of settings related to logging performed by the central server.	Yes
Content Replication Schedule	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
Platforms	Configuration of the available target platforms.	Yes

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the *Preboot Menu Options* section:

Preboot Menu Options	
Determine if the Preboot eXecution Environment (PXE) menu should be displayed when a client boots.	
○ Always show Preboot menu	
○ Never show Preboot menu	
● Show Preboot menu if CTRL+ALT pressed	

4 Select one of the following:

   ◆ *Always Show Preboot Menu*

   ◆ *Never Show Preboot Menu*

   ◆ *Show Preboot Menu if CTRL+ALT Pressed*

IMPORTANT: Do not select *Always Show Preboot Menu* if you have AutoYaST or kickstart bundles assigned to any devices, because the Preboot Services Menu interrupts the PXE boot process, keeping the AutoYaST or kickstart bundles from being deployed on the device. The Preboot Services Menu only has options for doing imaging work, not for installing operating systems.

Therefore, select either *Never Show Preboot Menu* or *Show Preboot Menu if CTRL+ALT is Pressed* for your Preboot Services Menu option, which allows PXE-enabled Linux devices to automatically implement the AutoYaST or kickstart bundles.

5 Click either *Apply* or *OK* to save the change.

This sets the default Preboot Services Menu display mode for the ZENworks Management Zone. This can be overridden at the folder or device level. For more information, see Section 29.5, "Overriding Preboot Services Defaults," on page 399.

IMPORTANT: PXE must be enabled on the device for the menu to be displayed.

The Preboot Services menu provides options for how Preboot Services can be used on your devices. The following options are presented when the menu is displayed:

Table 29-6 *Preboot Services Menu Options*

Menu Option	Function
Start ZENworks Imaging	Executes the assigned Preboot Services imaging bundles.
Start ZENworks Imaging Maintenance	Displays the bash prompt, where you can execute imaging commands.
Disable ZENworks Partition	Prevents an existing ZENworks partition from being used when booting to execute the assigned Preboot bundles.
Enable ZENworks Partition	Allows an existing ZENworks partition to be used when booting to execute the assigned Preboot bundles.
Start DELL DTK	Starts the DELL Deployment Toolkit v2.1 in the automated mode where it checks for details on assigned work, performs the assigned work, and reboots. No user input is allowed or required.
Start DELL DTK (Maintenance Mode)	Starts the DELL Deployment Toolkit v2.1 in the maintenance mode by loading it into a RAM drive so that you can configure the scripts and files used in the Dell Configuration bundle.
Exit	Resumes booting of the device without doing any Preboot bundle work.

Generally, if your Preboot Services work is completely automated, you should select to never display the Preboot Services Menu on the device when it boots. Conversely, if you need to do manual Preboot Services functions for some or all devices, then select to always display the menu. A compromise is where you select to display the menu if Ctrl+Alt is pressed, allowing unattended Preboot Services work while allowing you the opportunity to display the menu when needed.

29.4.2 Configuring Image Storage Security

To determine the degree of security you want with respect to saving image files:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following *Management Zone Settings* section:

Management Zone Settings			⌃
Category	**Description**		**Is Configured**
System Variables	Configure system variables.		Yes
Device Refresh Schedule	Configure the device refresh interval.		No
Device Inventory	Configure inventory settings.		No
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.		Yes
Preboot Services	Configure Preboot Services.		Yes
Remote Management	Enable and configure remote management.		Yes
Centralized Message Logging	Configuration of settings related to logging performed by the central server.		Yes
Content Replication Schedule	Configuration of the refresh schedule used for replicating content between ZENworks servers.		Yes
Platforms	Configuration of the available target platforms.		Yes

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the *Image Storage Security* section:

4 Select one or both of the following options:

Allow Preboot Services to overwrite existing files when uploading: Select this option only if you want existing image files to be overwritten during imaging.

Only allow uploads to the following directories: This option allows you to determine where images can be restored on the imaging server.

Specify a full path to the directory in the *Add* field, then click *Add* to enter it into the list box. These are the directories where images are allowed to be saved on the imaging server. These are the locations that can be selected when configuring where to store image files.

Use *Move up* or *Move down* to rearrange the order of the locations, including the order of the imaging servers that are listed.

To remove a directory path from the listing, select the path and click *Remove*. You can select multiple paths for removing.

5 Click either *Apply* or *OK* to save the changes.

This sets the default image storage settings for the ZENworks Management Zone.

29.4.3 Configuring Non-registered Device Settings

The following configurations can be set after a device is imaged. The settings are applied to devices not registered in the ZENworks Management Zone.

For more information, see Section 28.3.4, "Non-registered Device Settings," on page 334.

To configure default ID settings for non-registered devices:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following *Management Zone Settings* section:

Management Zone Settings		
Category	**Description**	**Is Configured**
System Variables	Configure system variables.	Yes
Device Refresh Schedule	Configure the device refresh interval.	No
Device Inventory	Configure inventory settings.	No
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
Preboot Services	Configure Preboot Services.	Yes
Remote Management	Enable and configure remote management.	Yes
Centralized Message Logging	Configuration of settings related to logging performed by the central server.	Yes
Content Replication Schedule	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
Platforms	Configuration of the available target platforms.	Yes

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the *Non-Registered Device Settings* section:

4 Fill in the fields:

DNS suffix: Provides a suffix for all of your device's names.

For example, if you enter "provo.novell.com" and a device's name is "device1," that device's full name becomes "device1.provo.novell.com."

Name servers: To control what DNS servers the device uses, specify a DNS name server, then click *Add* to place it into the listing.

So that a booting device can find a name server efficiently, specify multiple DNS name servers.

For optimal availability of a DNS server for a device, you can rearrange the order using *Move up* and *Move down*, one name server entry at a time.

You can delete multiple name servers by selecting them and clicking *Remove*.

Device name: You can determine the default device names for non-registered devices. The name is applied after the device is imaged.

This can be useful for when you have multiple devices to be imaged. You can automatically provide unique names for each device (from its BIOS asset tag or its BIOS serial number), as well as group devices by providing the same prefix for their names.

Options:

- **Use prefix: _____:** This provides a common prefix to the device names, such as Lab1 to distinguish them from the devices in Lab2. This can be useful when doing bulk imaging of certain groups of devices. It is limited to 8 characters.

  If this option is used, the prefix you enter here is appended with a random string of letters and numbers to make the device name 15 characters long. Underscores and hyphens are valid in your prefix. The remaining random string uniquely names the device.

  For example, if you enter Lab1_, then ten other characters are randomly generated to complete the name with Lab1 separated from the random characters by the underscore for readability.

- **Use BIOS asset tag:** This is the asset tag stored in the device's BIOS, which is unique for every device. This can be useful for tracking a device based on its asset tag.

- **Use BIOS serial number:** This is the serial number stored in the device's BIOS, which is unique for every device. This can be useful for tracking a device based on its serial number.

- **Do not automatically assign a name:** Select this option if you do not want to use any of the above options. This is the default option.

IP configuration: You can select either *Use DHCP* or *Specify address List* to identify devices for Preboot Services work.

These are the settings that the device is told to use after it is imaged. It uses them for Preboot Services work any time it reboots.

⬥ **Use DHCP:** Allows the devices to be dynamically assigned IP addresses.

For Red Hat Enterprise Linux, using the DHCP option causes a "Could not look up Internet address..." message to be displayed during bootup. This is because zislnx does not know the IP address when DHCP is being used, so the `/etc/hosts` file contained in the image does not have the new IP address and host name. Simply select the *Log In Anyway* option to continue. Then to prevent this message from displaying each time the device boots, edit the `/etc/hosts` file on the device and add in its IP address.

⬥ **Specify address list:** Uses IP addresses to identify your devices. The addresses you add to the list are available to be used by your devices. This way, you can specify a range of IP addresses or individual IP addresses that you want your devices to use. For example, you can ensure that all of your lab devices use addresses between 10.0.0.5 and 10.0.0.25.

If you select this option, the following fields are displayed:

Subnet mask: (Optional) For assigning devices to a specific subnet mask.

Default gateway: (Optional) For assigning devices to a specific gateway for access to the Internet or network after the device is imaged and rebooted.

IP addresses available for machines: According to the information you provide in this section, this list box displays the available IP addresses for your devices to use.

Start and end of IP address range: Do either of the following:

- ◆ Specify one IP address at a time in the first field and click *Add* each time to place it into the list box.

- ◆ Specify a range of IP addresses and click *Add* to place them into the list box. Each IP address in a range is listed independently, allowing you to selectively remove any of them from within the range.

You can select multiple IP addresses for removal.

IP addresses currently assigned: This display-only list box shows which IP addresses from the *IP Addresses Available for Machines* list have been assigned to a device. When they are displayed here, they are no longer displayed in the list box above.

After a device is imaged, IP settings are applied to the device. The IP address that is assigned to the imaged device is no longer in the available list, but is instead listed in this currently assigned list.

5 Click either *Apply* or *OK* to save the changes.

This sets the default device ID method for the ZENworks Management Zone.

29.4.4 Configuring Preboot Work Assignments

This section allows you to set up Preboot work assignments for your defined bundles for non-registered devices, or registered devices that do not have an effective bundle defined.

In this section of the Preboot Services page, you can set up rules for your Preboot bundles. Work assignment rules are hardware keys used to determine which bundle should be applied to which device. When a device is seeking work to be done, it scans the rules until it finds a rule where all of the rule's filters match the device, then executes the bundle assigned to the rule.

For more information, see .

To configure work assignment rules:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following *Management Zone Settings* section:

Management Zone Settings		☆
Category	**Description**	**Is Configured**
System Variables	Configure system variables.	Yes
Device Refresh Schedule	Configure the device refresh interval.	No
Device Inventory	Configure inventory settings.	No
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
Preboot Services	Configure Preboot Services.	Yes
Remote Management	Enable and configure remote management.	Yes
Centralized Message Logging	Configuration of settings related to logging performed by the central server.	Yes
Content Replication Schedule	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
Platforms	Configuration of the available target platforms.	Yes

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the *Preboot Work Assignment* section:

4 If you plan to select *Hardware Type* when constructing a rule (see), you must first configure the hardware type in one of the following fields:

   ◆ **Servers:** Specify a full or partial string that identifies a server's BIOS from a match in its *Product Name* field, then click *Add* to place the string into the *Servers* list. You can add multiple strings to the list in order to identify all of the servers that you want a rule to select. To remove a string from the list, select the string, then click *Remove*.

   ◆ **Laptops:** Specify a full or partial string that identifies a laptop's BIOS from a match in its *Product Name* field, then click *Add* to place the string into the *Laptops* list. You can add multiple strings to the list in order to identify all of the laptops that you want a rule to select. To remove a string from the list, select the string, then click *Remove*.

When defining a rule, you can define hardware types so that the rule can be specifically applied to either servers or laptops.

To determine the BIOS product names of your servers or laptops, use the `img i` command at a bash prompt, which displays various BIOS information. The BIOS information that you need is listed in the *Product Name* field. For servers and laptops, you can enter partial strings to select all with BIOS product names containing that string.

Servers, *Laptops*, and *Workstations* are the three options available when defining a work assignment rule based on a hardware type. Devices whose BIOS identification matches one of the strings listed in the *Servers* or *Laptops* fields above are classified for the rule as either a server or a laptop.

A workstation is a hardware type that does not require a BIOS string definition. Therefore, if you select *Servers* or *Laptops* in the Rule Construction dialog, but you have not entered BIOS identification strings for them here, they are treated as workstations by the rule.

These hardware type definitions are applicable only to rules; they do not otherwise apply to the ZENworks Management Zone.

5 Click *Add* to configure a rule.

The information configured in the Rule Construction dialog box comprises one rule. You can add multiple rules. The rules are used to determined whether there is a device that should have any preboot work done. If so, it only does the effective preboot work assigned to it.
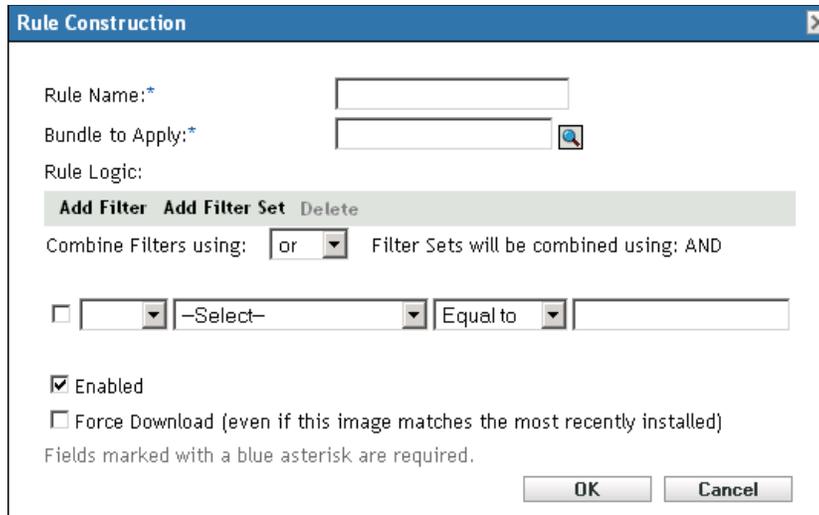
6 In the Rule Construction dialog box, provide a name for the work rule in the *Rule name* field.

This is the name that is displayed in the rules listing on the Preboot Services page in the *Preboot Work Assignment* section. Make it descriptive enough that you can later remember its purpose.

7 In the *Bundle to apply* field, browse for or specify the bundle where you want to apply this rule.

Each rule can be applied to only one bundle. However, you can apply multiple rules to a bundle.

When a device boots and searches the *Preboot Work Assignment* section for work, if the device meets a rule's criteria, the rule's applicable bundle is applied to the device.

Because the rules, not the bundles, are listed in the *Preboot Work Assignment* section, you can apply multiple rules to a given bundle. In that case, such a bundle has multiple chances to be selected for preboot work.

When multiple rules are listed, the first rule to have criteria to match a device causes that rule's assigned bundle to be applied to the device.

If no rules match a device, then the effective bundle is not applied to the device.

8 To determine which boot parameters to use, select one of the following for the *PXE Kernel Boot Parameters* field:

Use Kernel Boot Parameters from Zone's Settings: Uses the ZENworks Management Zone's settings as configured in the *Preboot Menu Options* section.

Use These Kernel Boot Parameters: Specify the boot parameters to be used with one of the Preboot Services Menu options.

9 Review the following to understand how to configure the work rule logic:
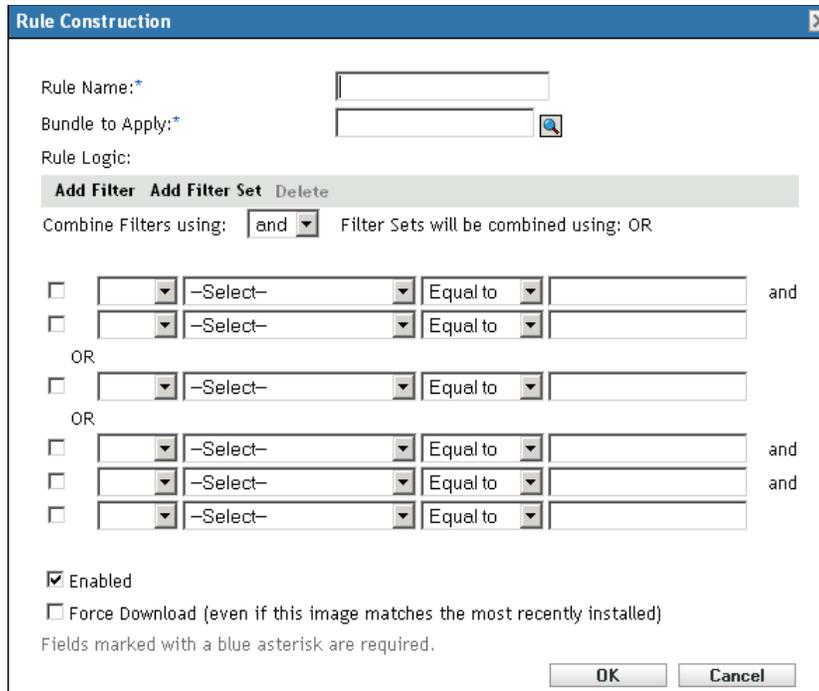
A rule is made up of one or more filters that are used to determine whether a device complies with the rule. The Rule Construction dialog box begins with one empty filter. A device must match the entire filter list of a rule (as determined by the logical operators that are explained below) for the rule to apply to the device.

A filter is a row of fields providing a condition that must be met by a device in order for the bundle to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order to be accepted by the rule, and you can add another filter to specify that the hard drive be at least 20 GB in size. There is no technical limit to the number of filters that you can add in the rule, but there are practical limits, such as:

- Designing a rule that is easy to understand

- Devising the rule so that you do not accidentally create conflicting filters

- Being able to view the dialog box as it grows in size because of the filters that you add

Filters can be added individually or in sets. Each set contains logical operators within the set. The logical operator OR is displayed by default for the filters within a set in the *Combine filters using* field, which you can change, and AND is displayed in the *Filter sets will be combined using* field, which is display-only. In other words, the logical operator that is used within a set must be opposite the operator that is used between the sets.

You can think of filters and filter sets using algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (AND and OR) separate the filters within a the parentheses, and the operators are used to separate the parentheticals.

For example, "(u AND v AND w) OR (x AND y AND z)" means "match either uvw or xyz." In the Rule Construction dialog box, this looks like:

u AND v AND w OR x AND y AND z

Filter sets cannot be nested. You can only enter them in series, and the first filter set to match the device is used to validate using the applied bundle to do preboot work on the device. Therefore, the order they are listed does not matter. You are simply looking for a match to cause the bundle to be applied to the device.

TIP: You can easily run a test to see how these logical operators work. Access the Rule Construction dialog box, click both the *Add filter* and *Add filter set* options a few times each to create a few filter sets, then switch between AND and OR in the *Combine filters using* field and observe how the operators change. Click *Cancel* to exit the Rule Construction dialog box when you are finished.

You can set up the conditions for a rule by adding all of the filters and filter sets that you need to identify the type of device you want to match. You typically do not need to set up complex rules. However, because you can apply multiple rules to a bundle, you can further complicate the use of logical operators, because each rule is considered to be an OR condition for the bundle, causing the bundle to be applied if any one of the rules matches the device. Therefore, keep in mind the OR condition of multiple rules for a bundle when designing your rules.

For example, you could create several rules for the bundle with each rule being a long listing of AND conditions to be met. Therefore, each rule becomes a specific set of criteria for a device to meet, causing the bundle to be applied if one is met. Conversely, if you have that same amount of information in one rule (using filter sets for the AND and OR conditions), it might make the dialog box so long that it becomes unmanageable.

To determine whether you need one filter set with multiple filters, multiple filter sets with only one or a few filters per set, multiple filter sets each with multiple filters, or even multiple rules per bundle, remember that the logical operators for filters within a set are the opposite of the operators between the sets, and all rules for a bundle use the OR condition.

For example, when selecting the operator in the *Combine filters using* field:

Operator Selected	Within Filter Sets	Between Filter Sets	Multiple Rules Per Bundle
OR	Only one filter in the set needs to apply to the device (OR condition). The first filter that applies is used.	Each filter set must have one filter in it that applies to the device (AND condition).	The first rule that applies is used (OR condition).
AND	All filters within the set must apply to the device (AND condition).	Only one filter in the set must apply to the device (OR condition). The first filter that applies is used.	The first rule that applies is used (OR condition).

Obviously, adding filter sets complicates the use of logical operators, and adding multiple rules to the bundle further complicates it. Therefore, carefully plan how to place your information before using this dialog box.

10 To add or remove filters and filter sets, select from the following:

- ◆ **Add filter:** Adds one filter (a row of fields) after the last filter in this dialog box.

  Subsequent clicks of the *Add filter* option add those filters to the end of the current set, which is the last listed filter set when there are multiple filters in the set (see Add Filter Set below). You cannot insert a new filter between existing filters.

The order of the filters in a set does not matter, and you cannot reorder the filters after you have created them. What matters in this structure is properly grouping the filters with respect to the selected *OR* and *AND* operator options.

- **Add filter set:** Adds the next filter as a filter set with either AND or OR placed between the filter sets, as dictated by your selection in the *Combine filters using* field.

   To create filter sets, first click *Add filter set*, then click *Add filter* as many times as necessary to add filters into that set.

   You cannot insert filter sets between existing filter sets.

- **Delete:** Deletes any filters that are selected (see Check box below in Step 12).

11 To determine the filter and filter set logic, select *AND* or *OR* from the *Combine filters using* drop-down list.

The logical operator you select here determines which operator is used within the filter sets. The operator for this field applies to multiple sets.

To provide multiple sets for the rule, indicate whether the sets should all be required (select *AND*) or are all optional (keep *OR*). If OR, then the values in only one of the sets need to match the device for the rule to apply. If AND, then all values in the entire rule must match the device for the rule to apply.

If you only have one filter set (which could contain several filters), AND is the default logical operator within the set, because OR defaults in the *Combine filters using* field, which you can change.

Filter sets will be combined using is a display-only field. When providing multiple sets for the rule, this field displays the opposite logical operator from the one you select for the *Combine filters using* field.

To require all filters within a filter set, but only one of the filter sets, select *OR* in the *Combine filters using* field. To require all filter sets, but only one of the filters within each set, select *AND* in the *Combine filters using* field.

12 To configure rule filters, fill in the fields:

- **Check box:** Selects filters for deletion.

- **Drop-down list:** If blank, this field means to do as worded in the filter. If you select *NOT*, it means to do the opposite of what the filter says.

   For example, if you select *NOT* and the RAM size is configured to be "less than 512 MB," then the device must have at least 512 MB of RAM for the bundle to be applied. In other words, the filter reads "not less than 512 MB of Ram." Conversely, if you configured it as "more than 512 MB," then left the field blank, any computer containing exactly 512 MB of RAM is excluded, which you might not intend. So, be sure that you think the logic through for your filter configurations with respect to whether you use NOT.

- **Device component:** A drop-down list provides the various items available for matching on the device in order to determine whether the work rule applies for the bundle. The options are:

   BIOS Asset Tag
   BIOS Serial Number
   BIOS Version
   CPU Chipset
   Hard Disk Controller
   Hard Drive Size (in MB)

Hardware Type

IP Address

MAC Address

Model

Network Adapter

RAM (in MB)

Sound Card

System Manufacturer

Video Adapter

If the drop-down list on the left displays NOT, then the work rule is stating that the device should not match the component as described in the next two fields.

To use the *Hardware Type* option effectively, you must first configure the settings for either the *Server* or *Laptop* field in the *Hardware Type Definitions* section in the work assignment configuration. The *Workstation* hardware type is the default and requires no configuration for it to be used. In other words, if you do not provide a BIOS identification string for a server or laptop, then select *Server* or *Laptop* in the *Value for Component* field, the devices are treated as workstations, where a BIOS identification is not used.

◆ **Relationship to:** This defines the relationship for a filter between the *Device component* field listed above and the value provided in the *Value for the component* field.

The possible options for the *Hard drive size* and *RAM* fields are:

< (less than)

> (greater than)

= (equal to)

>= (greater than or equal to)

<= (less than or equal to)

<> (not equal to)

For all other components, the options are:

Contains

Equal To

Starts With

If the drop-down list on the left displays NOT, then the work rule is stating that the component does the opposite. For example, does NOT Contain, is NOT Equal To, does NOT Start With, is NOT >, is NOT >=, is NOT =, is NOT <>, and so on.

◆ **Value for the component:** Enter the information that exactly describes the device component's value that the device must match to accept the rule. For example, 512 could be entered for the *RAM* field value in *Device component* field, meaning the device must have that amount of RAM, or more or less, depending on the selections you make in the other fields in the filter.

If you select *Hardware Type* from the *Device Component* drop-down list, this field becomes a drop-down list where you can select *Server*, *Laptop*, or *Workstation*. *Server* and *Laptop* must be defined to be useful, or the effect is the same as selecting *Workstation*, which is the default hardware type and does not need a BIOS identification defined.

IMPORTANT: Be aware of the possibility of creating conflicting filters. For example, if the *RAM (in MB)* field is used in multiple filters, make sure the effective logical operators where each is used make sense for the MB values that you enter. You could have one filter requiring exactly 512 MB of RAM and another accepting a device having at least 512 MB of RAM. If those filters are both required for the device to match the rule (this is with the AND condition existing between them), you'd have a conflict that causes the filter to fail its purpose.

13 Because you can create multiple rules to be listed here, and the information configured in the Rule Construction dialog box comprises one rule, repeat Step 10 through Step 12 as necessary.

14 To enable this work rule, select the check box for the *Enabled* field.

After you exit this dialog box, you can see whether the work rule is enabled by viewing the work rules listing on the Preboot Services page.

To enable or disable a rule after creating it, you must edit the work rule from the Preboot Services page.

15 To force the image to be reapplied to the device, select the check box for the *Force download* field.

By default, ZENworks imaging does not reimage a device containing the same image. This option allows you to force the image to be reapplied to the device. For example, you might want to refresh all of your lab devices for the next use of the lab.

IMPORTANT: Use this option cautiously, because you can create an endless loop when the option remains selected after an image is applied. If you image a device that remains non-registered after it is imaged, it is reimaged with the same image over and over each time it boots. To prevent this, deselect this option after you have imaged the applicable devices.

16 After exiting the Rule Construction dialog box, you can manipulate the order and existence of the listed rules:

Edit: Opens the Rule Construction dialog box in edit mode.

Move up/down: After adding rules, you can change the order in which they are to be executed. You can only move one rule at a time. This order is important because the first rule that is found in the listing to match the device is used to apply the bundle, and the remainder of the rules are ignored.

Remove: Removes the selected rules.

17 Click either *Apply* or *OK* to save the changes.

29.4.5 Configuring the Server Referral List

Referral lists are used to make sure managed devices belonging to other ZENworks Management Zones can access their home zone. For more information, see Section 28.3.6, "Preboot Referral Lists," on page 336.

To set up referral lists:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following *Management Zone Settings* section:

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the *Server Referral List* section:
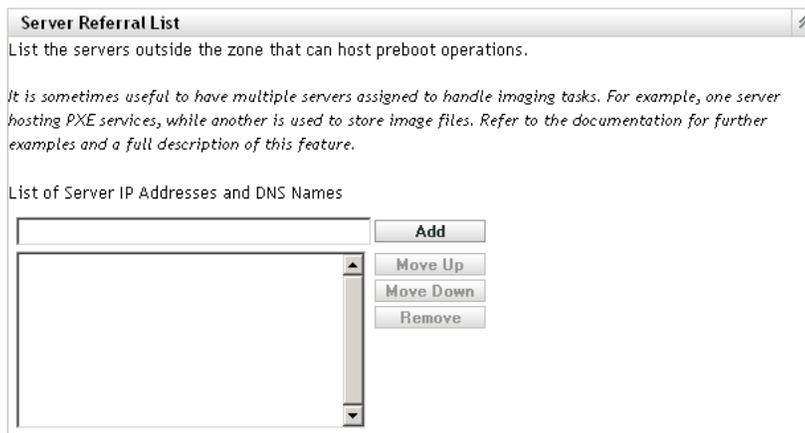
4 Specify the ZENworks Linux Management servers:

List of server IP addresses and DNS names: Specify the DNS name or IP address of a server that can host Preboot operations, then click *Add* to place the server into the referral list.

Move up/Move down: Arranges the order in which the servers are contacted. You can move only one server at a time.

Remove: To remove a server from the list, select the server, then click *Remove*.

5 Click either *Apply* or *OK* to save the changes.

6 Depending on the ZENworks version of the server, do the following to copy the necessary files from the ZENworks Linux Management imaging server to your \tftp directory on the servers in your referral list:

ZENworks Version	Files to Copy	Action
ZENworks 6.5	/svr/tftp/z_auto65.cfg	Copy the files.
	/svr/tftp/pxelinux.0	

ZENworks Version	Files to Copy	Action

ZENworks 7 (running on a NetWare or Windows server)	`/svr/tftp/z_auto.cfg`
	
	`/svr/tftp/pxelinux.0`
		Copy both of the files, but rename `z_auto.cfg` to `z_auto65.cfg`.

The `/svr/tftp/z_auto.cfg` file may not contain the same information as `/svr/tftp/z_auto65.cfg`, so that when you rename it with the `65`, it might have different content than the file used for ZENworks 6.5 servers. Therefore, for ZENworks 7.3 do not simply copy the `z_auto65.cfg` file instead of renaming the `z_auto.cfg` file.

No files need to be copied for servers running the following ZENworks versions:

ZENworks 7 (running on a Linux server)

ZENworks 7 Linux Management

29.4.6 Configuring Intel Active Management Technology (AMT)

To set up global Intel AMT enterprise names:

◆ "Downloading and Installing the iAMT Redirection Drivers" on page 395

◆ "Provisioning the AMT Devices" on page 396

◆ "Setting Up the Global Intel AMT Enterprise Names" on page 398

Downloading and Installing the iAMT Redirection Drivers

After a device has had its AMT resources provisioned, those resources can be accessed locally by the ZENworks implementation of AMT. However, before you can provision a device's resources, you need to install the iAMT Redirection Drivers from Intel. You can do this on one device, then send the result to the other devices that need the drivers, as outlined in the steps below.

The following are required to be installed and operational on the device where you initially install the drivers:

◆ The Linux kernel source

◆ GCC (gnu c compiler)

To download and install the device drivers:

1 In a Web browser, access Intel(R) PRO/10/100/1000/10GbE Drivers (http://sourceforge.net/projects/e1000/) on the SourceForge Web site.

2 Click the green *Download Intel(R) PRO/10/100/1000/10GbE Drivers* option.

3 In the *Latest File Releases* section, select the *iAMT Redirection Drivers* option.

4 Click the green *Download* option.

5 In the *Filename* column under *iAMT Redirection Drivers*, click the *iamt-1.1.8.tar.gz* option (or later version) and save the file to a location on your network.

6 Unzip the `.tar.gz` file and decompress the `iamt-1.1.8.tar` (or later version) file.

7 To install the drivers, follow the instructions contained in the `Readme` file that is contained in the `.tar` file.

This creates binaries of the drivers.

8 After following the instructions to compile the iAMT Redirect Drivers, make RPMs of the binaries, then distribute the RPMs to the other devices that need the drivers.

For more information, see Chapter 20, "Using RPM and File Bundles," on page 217.

Provisioning the AMT Devices

You can provision your AMT devices in either of two ways:

- "Provisioning in Enterprise Mode" on page 396
- "Provisioning in Small Business Mode" on page 396

Provisioning in Enterprise Mode

If you use another AMT-enabled application that requires the AMT devices to be provisioned in Enterprise mode, do the following:

1 During the boot process for a device, access the AMT BIOS.

Refer to your device's documentation for instructions.

2 When prompted, enter the device's AMT administrator username and password.

You are required to change the administrator username and password before you can proceed. See your computer documentation for instructions on changing the password.

3 Set the provisioning mode to "Enterprise."

4 Configure the other settings as appropriate.

Refer to your device's or AMT-enabled application's documentation for instructions.

5 Configure the provisioning server supplied with the application to assign at least one enterprise name to the device.

Refer to your AMT-enabled application's documentation for instructions.

6 Repeat Step 1 through Step 5 for each device to be provisioned with the Enterprise mode.

7 To provide the provisioned enterprise names to ZENworks Linux Management, continue with "Setting Up the Global Intel AMT Enterprise Names" on page 398.

Provisioning in Small Business Mode

To provision an AMT device in small business mode for use with ZENworks Linux Management, do the following:

1 During the boot process for a device, access the AMT BIOS.

Refer to your device's documentation for instructions.

2 When prompted, enter the device's AMT administrator username and password.

You are required to change the administrator username and password before you can proceed. See your computer documentation for instructions on changing the password.

3 Set the provisioning mode to "Small Business."

4 Configure the other settings as appropriate.

Refer to your device's documentation for instructions.

5 If you configured the AMT device to use DHCP mode for IP addressing, you might need to boot the device into an operating system to discover a currently valid IP address.

You can use the ZENworks Linux Management imaging CD or DVD for this, if necessary. Boot from the CD or DVD, select the ZENworks Maintenance Mode, then at the bash prompt enter `ifconfig eth0`. This provides the currently assigned IP address.

6 Run `/opt/novell/zenworks/zdm/winutils/smb-provisioning.exe` on a Windows XP workstation running .NET framework to display the following dialog box:
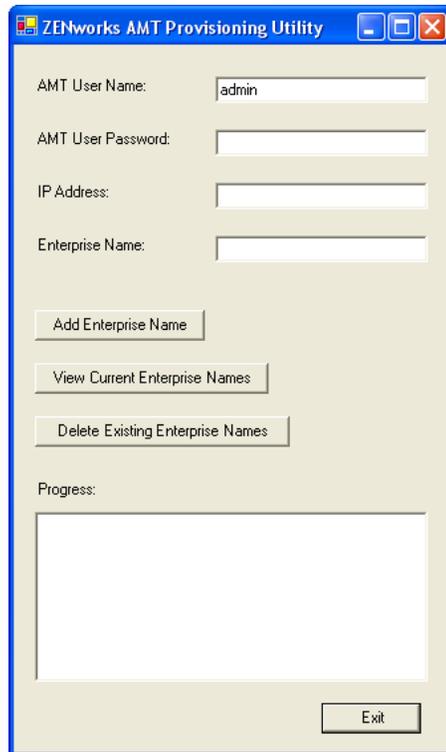
This must be run on a different device than is being provisioned.

7 Fill in the fields:

    7a Enter the appropriate administrator account and passwords in their respective fields.

       This is the same as you entered in Step 2.

    7b Enter the currently valid IP address for the device.

    7c Enter an enterprise name.

       Intel suggests that the enterprise name be chosen to indicate the device's general location. For example, all the devices in the home office may be given an enterprise name of "Company_HQ," and all devices in field offices may be given enterprise names reflecting their geographical locations.

       While it is not required, it is assumed that large numbers of devices will have the same enterprise name. Each AMT device itself may have up to four different enterprise names.

       You can use the *View Current Enterprise Names* or the *Delete Existing Enterprise Names* to manage the names in the *Progress* list box.

8 Select *Add Enterprise Name*, then click *Exit*.

This adds the defined enterprise name into the *Progress* list box and to the device.

9 Repeat Step 1 through Step 8 for each device to be provisioned with the Small Business mode.

10 To provide the provisioned enterprise names to ZENworks Linux Management, continue with "Setting Up the Global Intel AMT Enterprise Names" on page 398.

Setting Up the Global Intel AMT Enterprise Names

The Intel AMT functionality allows you to accurately identify devices, even if they have had physical drive replacements. This sets up Preboot Services with persistent device identification by providing ZENworks with nonvolatile memory for storing the unique device identity.

For more information, see Section 28.3.7, "Intel Active Management Technology (AMT)," on page 337.

To configure Intel AMT for Preboot Services:

1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings		☆
Category	**Description**	**Is Configured**
System Variables	Configure system variables.	Yes
Device Refresh Schedule	Configure the device refresh interval.	No
Device Inventory	Configure inventory settings.	No
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
Preboot Services	Configure Preboot Services.	Yes
Remote Management	Enable and configure remote management.	Yes
Centralized Message Logging	Configuration of settings related to logging performed by the central server.	Yes
Content Replication Schedule	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
Platforms	Configuration of the available target platforms.	Yes

2 In this section, click *Preboot Services* to display the configuration sections.

3 Locate the Intel Active Management Technology (AMT) section:

Intel Active Management Technology (AMT)	☆
Enter the global AMT Enterprise names.	
Name List	
[_____] Add	
[▲] Move Up	
Move Down	
Remove	
[▼]	

4 Fill in the fields:

Name list: Enterprise names are given to AMT devices when they are provisioned. This list should contain at least one valid AMT enterprise name for every AMT device in the ZENworks Management Zone. Click *Add* to place each one into the list box.

Move up/Move down: Arranges the order in which the AMT names are listed. You can move only one at a time.

Remove: To remove a name from the list, select the name, then click *Remove*.

5 Click either *Apply* or *OK* to save the changes

29.5 Overriding Preboot Services Defaults

You can determine which Preboot Services Menu displays a configuration to use and whether the menu should be displayed on a device when it boots. By default, the ZENworks Management Zone configuration applies to all folders and devices. You can override this at the folder or device level.

For more information on the Preboot Services Menu options, see Section 28.3.2, "Preboot Services Menu," on page 333.

The Preboot Services Menu can be customized by editing the `pxemenu.txt` file. For more information, see Section 29.3.4, "Editing the Preboot Services Menu," on page 376.

To override the default configuration at the folder or device level:

1 In the ZENworks Control Center, click the *Devices* tab to display the Devices page:

2 Select one of the following on this page:

- The *Details* option next to the *Servers* or *Workstations* folder
- The *Servers* folder, then a server contained in the folder
- The *Workstations* folder, then a workstation contained in the folder

3 On the page that is displayed, click the *Settings* tab to display the Settings page options:
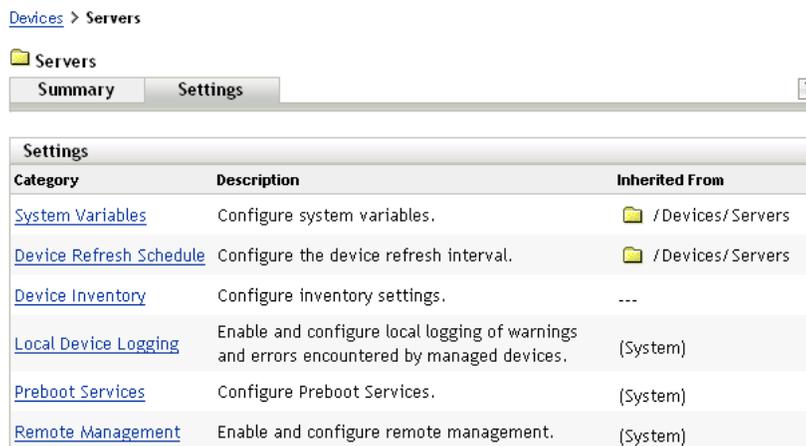
4 Click *Preboot Services* to display the Preboot Services configuration page:

Devices > Servers > sdf1.provo.novell.com > **Preboot Services**

sdf1.provo.novell.com

Preboot Services ✕

Configure Preboot Services for this device. Unless you choose to override settings, the values specified in the system configuration, or in individual folder settings, will be used.

Current: /Devices/Servers/sdf1.provo.novell.com

Revert to settings from: (System)

Preboot Menu Options ⌃

Determine if the Preboot eXecution Environment (PXE) menu should be displayed when a client boots.

○ Always show Preboot menu
○ Never show Preboot menu
● Show Preboot menu if CTRL+ALT pressed

[OK] [Apply] [Reset] [Cancel]

If you have not previously configured for this folder or device, the following is displayed:

```
Current: (System) (Override settings)
```

and the *Preboot Menu Options* section is disabled for editing. The above text varies depending on whether you are at the folder or device level.

5 To configure the settings for the folder or device, click *Override*.

The following is displayed:

```
Current: /Devices/Servers
Revert to settings from: (System)
```

and the *Preboot Menu Options* section is enabled for editing. The above text varies depending on whether you are at the folder or device level.

6 Select which option to use (PXE must be enabled on the device for the menu to be displayed):

- *Always Show Preboot Menu*
- *Never Show Preboot Menu*
- *Show Preboot Menu if CTRL+ALT is Pressed*

IMPORTANT: Do not select *Always Show Preboot Menu* if you have AutoYaST or kickstart bundles assigned to any devices, because the Preboot Services Menu interrupts the PXE boot process, keeping the AutoYaST or kickstart bundles from being deployed on the device. The Preboot Services Menu only has options for doing imaging work, not for installing operating systems.

Therefore, select either *Never Show Preboot Menu* or *Show Preboot Menu if CTRL+ALT is Pressed* for your Preboot Services Menu option, which allows PXE-enabled Linux devices to automatically implement the AutoYaST or kickstart bundles.

7 Click *Apply* or *OK*.

OK: Enables the change and exits the page.

Apply: Enables the change and retains focus on the page, so you can click *Revert* to temporarily disable the configuration change.

8 To temporarily disable the change, click *Revert* and the ZENworks Management Zone settings for the menu remain in effect.

29.6 Enabling PXE on Devices

To image a device using Preboot Services, you need to find out if the device is PXE capable, and then make sure that PXE is enabled.

PXE code is typically delivered with newer devices (PC 99 compliant or later) on the NIC.

This section includes the following information:

- ◆ Section 29.6.1, "Enabling PXE on a PXE-Capable Device," on page 401
- ◆ Section 29.6.2, "Verifying That PXE Is Enabled on a Device," on page 402

29.6.1 Enabling PXE on a PXE-Capable Device

When PXE is enabled, it can lengthen the time of the boot process slightly, so most NICs have PXE turned off by default. To enable PXE on a PXE-capable device:

1 Access the computer system BIOS and look at the *Boot Sequence* options.

The PXE activation method for a device varies from one manufacturer to another, but generally one of the following methods is used:

- ◆ Some BIOSs have a separate entry in the BIOS configuration to enable or disable the PXE functionality. In this case, set either the *PXE boot* setting or the *Network boot* setting to Enabled.
- ◆ Some BIOSs extend the entry that allows you to configure boot order. For example, you can specify that the system should try to boot from a diskette before trying to boot from the hard drive. In this case, set the system to try *Network boot* before trying to boot from a diskette or from the hard disk.

2 If PXE is not listed in the *Boot Sequence* options and if the NIC is embedded in the motherboard, look at the *Integrated Devices* section of the BIOS, which might have an option to enable PXE. PXE might be called by another name, such as MBA (Managed Boot Agent) or Pre-Boot Service.

After enabling PXE in the *Integrated Devices* section, look at the *Boot Sequence* options and move PXE so that it is first in the boot sequence.

3 Save any changes you have made and exit the system BIOS.

4 Reboot the device.

If the device does not have the network adapter and PXE integrated into the motherboard, it uses the installed NIC management software to prompt you to start PXE configuration during the boot process.

For example, many network adapters that are PXE-aware prompt you to press Control+S during the boot process to allow you to configure the PXE functionality. Other network adapters might prompt you to press Control+Alt+B or another key combination to configure PXE.

If the computer system does not have an integrated NIC, you might need to use NIC management software to configure your NIC to support PXE. Refer to your NIC documentation for support of PXE.

29.6.2 Verifying That PXE Is Enabled on a Device

After you have activated PXE, it becomes available in the *Boot* section of the BIOS. PXE is correctly enabled on a device when the device attempts to establish a PXE session during the boot process. You can see this happening when the device pauses during the boot process and displays the following on the screen:

```
CLIENT MAC ADDR: 00 E0 29 47 59 64

DHCP...
```

The actual message displayed varies from one manufacturer to another, but you can identify it by the obvious pause in the boot process as the device searches for DHCP.

29.7 Setting Up Devices for Imaging

The following sections cover procedures to prepare devices for imaging. The procedures that are applicable to you depend on your imaging deployment strategy. For more information, see Section 29.3.2, "Deploying Preboot Services In a Network Environment," on page 366.

If you are using Preboot Services (PXE) as your imaging method, you need to enable PXE on the device. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.

If you are using a ZENworks partition as your imaging method, you need to create the partition on the device. For more information, see "Creating a ZENworks Partition" on page 362.

If your cloned virtual or physical machine does not boot up properly, you must disable the use of persistent device names for networks and storages for CODE 10 products. For more information, see Section 29.7.3, "Disabling Persistent Device Names," on page 404.

The following sections contain additional information:

- Section 29.7.1, "Device Requirements," on page 402
- Section 29.7.2, "Enabling a Device for Imaging Operations," on page 403
- Section 29.7.3, "Disabling Persistent Device Names," on page 404

29.7.1 Device Requirements

This section gives the requirements for using a network-connected device.

It is possible (but usually not as convenient) to image a device without connecting to the network. Such operations can't be fully automated.

The following are the requirements for the device:

Table 29-7 *Device Requirements*

Device Must Have	Because
A supported Ethernet card	The device must connect with the imaging server to store or retrieve the images. This connection is made when the device is under the control of the ZENworks Imaging Engine. Therefore, make sure the device has a supported Ethernet card. For more information, see "Supported Ethernet Cards" on page 665.
Free disk space for a ZENworks partition (optional)	Unless you are using PXE, unattended operations require a ZENworks partition to be installed on the device hard disk, so that the ZENworks Imaging Engine can gain control when booting. The default partition size is 150 MB, and the minimum partition size is 50 MB. This partition is not required if you are performing manual imaging operations using bootable CDs, DVDs, or diskettes. Partition size can be in megabytes of disk space.
Standard hardware architecture	NEC* PC98 architecture is not supported.
PXE enabled	If you are using Preboot Services, PXE must be enabled in the BIOS. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
Supported imaging partition type	The only supported partition types for imaging are the ReiserFS, Ext2, and Ext3 file systems.

NOTE: ZENworks Linux Management imaging does not support devices running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the device from communicating with the imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

29.7.2 Enabling a Device for Imaging Operations

Use one of the following methods to enable a device for auto-imaging operations:

- "Using PXE" on page 403
- "Using a ZENworks Partition" on page 403
- "Using a CD or DVD" on page 404

Using PXE

You can set up a device to be automatically imaged from Preboot bundles by enabling PXE on the device.

For more information, see Section 29.6.1, "Enabling PXE on a PXE-Capable Device," on page 401.

Using a ZENworks Partition

If you cannot enable PXE on the device, you can use a partition to perform unattended imaging operations.

For more information, see "Creating a ZENworks Partition" on page 362.

Using a CD or DVD

If you cannot use the PXE or ZENworks partition methods to automate imaging of your devices, you can manually image a device using an imaging CD or DVD.

For information, see Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424.

29.7.3 Disabling Persistent Device Names

If you try to boot a cloned virtual machine or a physical machine, the following problems might occur:

* Unable to find file systems
* The network is not up
* Change in the network device names

To fix these issues, you must disable the persistent device names for network and storage before cloning the devices.

* "Disabling the Persistent Network Device Names" on page 404
* "Disabling the Persistent Storage Device Names" on page 405

Disabling the Persistent Network Device Names

Review the following sections to understand how to disable the persistent network device names for SLES 10, SLED 10, SLES 9, and NLD:

* "Disabling the Persistent Network Device Names for SLES 10 / SLED 10" on page 404
* "Disabling the Persistent Network Device Names for SLES 9 / NLD" on page 405

Disabling the Persistent Network Device Names for SLES 10 / SLED 10

1 Reset the udev configuration for the network devices by executing the following command:

    cat < /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules command.

2 Rename the Ethernet configuration files to initialize the Ethernet devices on boot.

    2a Go to `/etc/sysconfig/network`.

    2b Find the `ifcfg-eth` file for each Ethernet device. In the filename, the trailing identifier for an Ethernet device represents the MAC address for the device.

        For example, in the `ifcfg-eth-id-00:AA:BB:11:22:33` file, the trailing identifier, `AA:BB:22:33`, is the MAC address for the device.

    2c Rename the file to `ifcfg-ethX,` where X represents the number of Ethernet devices on the system. For example, the name for the configuration `eth0` is `ifcfg-eth0`.

3 In the `/etc/sysconfig/network/config` file, change the value of `FORCE_PERSISTENT_NAMES` to `No`.

4 Reboot the device.

Disabling the Persistent Network Device Names for SLES 9 / NLD

You must rename the Ethernet configuration file to initialize the Ethernet devices on boot.

1 Go to `/etc/sysconfig/network`.

2 Find the `ifcfg-eth` file for each Ethernet device. In the filename, the trailing identifier for an Ethernet device represents the MAC address for the device.

For example,

```
In the ifcfg-eth-id-00:AA:BB:11:22:33 file, the trailing identifier,
AA:BB:22:33, is the MAC address for the device.
```

3 Rename the file to `ifcfg-ethX,` where X represents the number of Ethernet devices on the system. For example, the name for the configuration `eth0` is `ifcfg-eth0`.

Disabling the Persistent Storage Device Names

To disable the persistent storage device names for SLES9/SLES10/SLED9/SLED10:

1 Search for the `/dev/disk/by-*` references in the boot loader configuration file `/boot/grub/menu.lst` and the file system table `/etc/fstab`.

2 Store the mapping of `/dev/disk/by-*` symlinks to their targets in a scratch file: `ls -l /dev/disk/by-* > /tmp/scratchpad.txt`.

3 Remove storage-specific entries, such as SAN or iSCSI volumes, that are not local to the system.

4 In `/boot//grub/menu.lst and/etc/fstab` files, replace the `/dev/disk/by-*` entries from the scratch file with the device names the symlinks point to.

5 Reboot the device.

Using Preboot Services

<div style="text-align: right; font-size: 3em;">30</div>

This section provides instructions on how to use Novell® ZENworks® Linux Management Preboot Services:

- Section 30.1, "Imaging Devices," on page 407
- Section 30.2, "Multicasting Images," on page 429
- Section 30.3, "Configuring AutoYaST or Kickstart Installation Script Bundles," on page 440
- Section 30.4, "Configuring ZENworks Script Bundles," on page 450
- Section 30.5, "Using Dell Configuration Bundles," on page 454
- Section 30.6, "Assigning Unassigned Preboot Bundles," on page 461
- Section 30.7, "Editing Preboot Services Work," on page 463

30.1 Imaging Devices

Preboot Services provides tools for creating and compressing images of device hard disks, as well as images of specific add-on applications or file sets. ZENworks Linux Management also provides tools for customizing such images and for making images available to auto-imaging operations.

You can take images of devices, re-image them with those images, and image other devices with the images. In ZENworks 7.3 Linux Management, the available devices are servers and workstations.

ZENworks Linux Management imaging supports devices that physically connect to the network that meet the minimum requirements for devices. ZENworks Linux Management imaging does not support imaging operations (creating or restoring images) using wireless connectivity. Devices with logical volumes (LVMs) are not supported for imaging.

NOTE: ZENworks Linux Management imaging does not support devices running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the device from communicating with the imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

Some imaging tasks can be performed manually on a device, some in the ZENworks Control Center, and some in both:

- Section 30.1.1, "Imaging Using the ZENworks Control Center," on page 407
- Section 30.1.2, "Performing Manual Imaging Tasks," on page 415
- Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424

30.1.1 Imaging Using the ZENworks Control Center

The following imaging tasks are available in the ZENworks Control Center:

- "Taking a Base Image of a Device" on page 408

- "Configuring the ZENworks Image Bundle for Automatic Imaging" on page 410
- "Imaging a Device Using a Script" on page 414

Taking a Base Image of a Device

A *base* image is an image of all partitions and data on a source device's hard disks. Normally, such an image is prepared with the intent to completely replace the contents of a target device's hard disks.

You can take an image of an existing device and use it to image a similar device, or use it as a backup image for reimaging the device.

1 In the ZENworks Control Center, click the *Devices* tab.

2 Click *Servers* or *Workstations*, then select the check box next to a device.

This selects the device for taking the image.

3 Click *Actions > Take image*.

You can also select the check box next to *Servers* or *Workstations* to start this wizard, then click *Actions > Take image*. If you do so, you are asked to select a device from the group. Then the File Information page is displayed.

4 Click *Next* to display the File Information page:
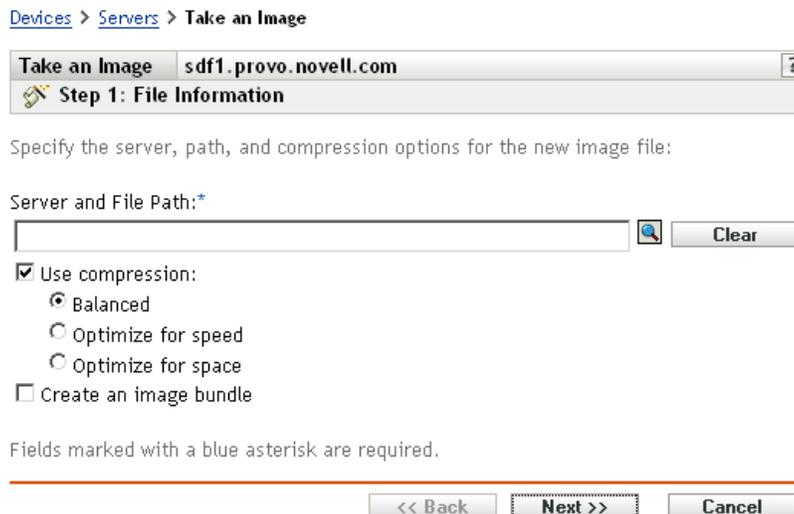
5 Fill in the fields:

Server and file path: (Required) Browse for the object, DNS name, or IP address of the server where the image file is to be stored, then specify the path to the storage location. This must be a server where ZENworks Linux Management is installed.

Images can take up a large amount of disk space. Make sure your imaging server has the disk space available before selecting it.

Use compression: Compression is required. Choose one of the following:

- ◆ **Balanced:** Automatically balances compression between an average of the reimaging speed and the available disk space for the image file.

- ◆ **Optimize for speed:** Optimizes the compression to allow for the fastest reimaging time. Use this option if CPU speed is an issue.

- ◆ **Optimize for space:** Optimizes the compression to minimize the image file's size to conserve disk space. This can cause reimaging to take longer.

Create an image bundle: If you select this option, another wizard page is displayed (see Step 6) where you can configure the new bundle. Otherwise, the Summary is your next wizard page (skip to Step 9).

6 If you selected to create an image bundle, the New Image Bundle page is displayed:

7 Fill in the fields:

Name: Specify a unique name for the bundle, because many other bundle names might be listed in the same folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Destination folder: Specify a folder where you want to list the new bundle. This is a location in the ZENworks Control Center, not a file location on a device.

Description: Enter information to help you later recognize the purpose and scope of this image bundle. For example, "Image taken after Linux OS was installed, but before GroupWise was installed."

8 Click *Next* to display the Summary page.

9 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Finish: Click to take the image. If you completed Step 7, the image is assigned to the bundle when it is created.

This base image can be used in under "Configuring the ZENworks Image Bundle for Automatic Imaging" on page 410.

To create an add-on image for use in , see "Creating an Add-On Image" on .

Configuring the ZENworks Image Bundle for Automatic Imaging

Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a ZENworks Image bundle and assign devices to the bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New > Bundle* to start the Create New Bundle Wizard:

3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.

4 On the Select Preboot Bundle Type page, select *ZENworks Image bundle*.

5 Click *Next* to display the Set General Information page:

6 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Image bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the ZENworks Image bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this ZENworks Image bundle.

7 Click *Next* to display the Bundle Configuration page:

| Create New Bundle | ZENworks Image 1 | ? |

Step 4: Preboot Bundle Creation

Configure the preboot information

Base Image File:

[   ] 🔍 [Clear]

Add-On Image Files:

[   ] [**Add**]
                                       [Edit]
                                       [Move Up]
                                       [Move Down]
                                       [Remove]

File Set: [1 ▼]

☐ Use IP Address from the preboot bundle rather than from Image Safe Data
☐ Use Identity Information from the preboot bundle rather than from Image Safe Data

[<< Back] [Next >>] [Cancel]

8 Fill in the fields:

Base image file: This is an image file existing on an imaging server. You must provide the full path and filename here. The image filename must end in `.zmg` (case-sensitive). For information on creating a base image, see "Taking a Base Image of a Device" on page 408.

Add-on image files: These are existing image files that you can add onto the device after it is re-imaged with the base image file. You must provide the full paths and filenames here. The image filename must end in `.zmg` (case-sensitive). For information on creating an add-on image, see "Creating an Add-On Image" on page 419.

File set: File sets are assigned to the current ZENworks Image bundle using this *File set* field. File sets are defined on the imaging server from the base image using the Image Explorer utility, which can be run on a Windows device from a Linux server running Samba. The Image Explorer utility is located at `/opt/novel/zenworks/zdm/winutils/ImgExp.exe` on the Linux server.

When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.

For example, `device1image.zmg` is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of `device1image.zmg`.

File sets provide an advantage because you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets will include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.

There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.

IMPORTANT: If you create 10 different file sets, the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you don't select a file set when using this wizard.

Add: Accesses the Server and Path Information dialog box:

- **Server object, IP, or DNS:** The identity of the imaging server where the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) is installed and running, and where the base image file is stored.

- **File path on server:** The full path to the base image file.

A device's Image Safe Data, such as the device's IP address and other identity information that is defined for its ZENworks Control Center object, is contained on the hard drive that the device boots from. This information can be lost if that hard drive needs to be replaced. However, the following options allow you to retain a device's IP address and other identity information when replacing the hard drive.

These options are only applicable when this Preboot bundle is applied to a specific device. The image used in this bundle must contain the device's previous IP address and ZENworks Control Center object information.

(Optional) Select one or both of the following options:

- **Use the IP Address from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

  Use this option if you have previously taken an image of the device and are using that image with this Preboot bundle. This option causes the imaging process to write the device's IP address that is contained in this image to the Image Safe Data location on the replacement hard drive.

  Do not use this option if the image being used for this bundle was not previously made from this device.

  If you do not select this option, then:

  - If the device that this Preboot bundle is applied to is still using its primary hard drive to boot from, the IP address in its Image Safe Data continues to be used.

    or

  - If the device that this Preboot bundle is applied to has been given a new hard drive to boot from, but you do not have a previous image of the old hard drive, then the IP address is assigned according to your ZENworks Management Zone configuration for non-registered devices.

- **Use the Identity Information from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

  If you are using a previous image of this device, this option writes ZENworks Control Center object identity information as contained in the image to the new hard drive's Image Safe Data location, which allows the device to retain its ZENworks Control Center object.

However, if the image contained in this bundle was not previously made from this device, it receives the new ZENworks Control Center object that is defined in the image.

If you do not select this option and the device that this Preboot bundle is applied to has been given a new hard drive to boot from, then a new ZENworks Control Center object is created according to your ZENworks Management Zone configuration for non-registered devices.

9 Click *Next* to display the Summary page.

10 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Click to perform the following tasks before creating the bundle:

- ◆ Specify device assignments for this bundle
- ◆ Specify groups for this bundle

Continue with to assign the bundle and complete the wizard.

Finish: Creates the ZENworks Script bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When a device assigned to the ZENworks Image bundle boots, the bundle's work is performed on the device before its operating system starts.

Imaging a Device Using a Script

You can perform scripted imaging using the ZENworks Script bundle. Any imaging commands can be entered for the script.

For example, if you want to mount a DVD and restore an image from it, you could enter something similar to the following in the *Script text* field in the Create New Preboot Bundle Wizard when defining a ZENworks Script bundle:

```
echo "Please insert the DVD containing the image into the drive."
mount /dev/cdrom /mnt/cdrom
img rl /mnt/cdrom/myimagefile.zmg
umount /mnt/cdrom
eject /dev/cdrom
```

This example is a combination of automatic and manual tasks, where you define the bundle in the ZENworks Control Center, assign it to the device, then when the device boots, it runs the bundle's script, prompting you to insert the DVD containing an image into the device's DVD drive. The script then runs the commands to restore the image on the device and ejects the DVD when finished.

For information on creating a ZENworks Script bundle, see Section 30.4, "Configuring ZENworks Script Bundles," on page 450.

30.1.2 Performing Manual Imaging Tasks

The following manual imaging tasks are available:

- "Manually Taking an Image of a Device" on page 415
- "Using Image Explorer to Customize an Image" on page 418
- "Creating an Add-On Image" on page 419
- "Manually Putting an Image on a Device" on page 420
- "Making an Image Available for Automatic Imaging" on page 422

These instructions assume that you have already prepared the imaging server (see Section 29.1, "Preparing a Preboot Services Server," on page 353), prepared devices for imaging (see Section 29.7, "Setting Up Devices for Imaging," on page 402), and set up imaging defaults (Section 29.4, "Configuring Preboot Services Defaults," on page 379).

ZENworks Linux Management imaging supports devices that physically connect to the network and that meet the minimum requirements for devices. ZENworks Linux Management imaging does not support imaging operations (creating or restoring images) using wireless connectivity.

Manually Taking an Image of a Device

This section explains how to take an image of a device by booting from an imaging method and entering a particular imaging command. The image is stored on your imaging server.

If you want to store an image locally rather than on an imaging server, see "Using a CD or DVD for Disconnected Imaging Operations" on page 424 and "Using a Hard Disk for Disconnected Imaging Operations" on page 426.

Ensure that your imaging server has enough disk space for the image. Otherwise, you receive a "Failed to write to proxy" error.

The following sections contain additional information:

- "Manually Taking an Image of a Device Using the Bash Prompt" on page 415
- "Manually Taking an Image of a Device Using the ZENworks Imaging Engine Menu" on page 417

Manually Taking an Image of a Device Using the Bash Prompt

1 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` at the bash prompt.

or

Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.

3 (Optional) At the bash prompt, type `img dump`, then press Enter.

This displays a list of the partition slots on the device. For your reference, note the number and type of partitions and which one is active.

4 Enter a command at the bash prompt using one of the following formats:

◆ To create an image and store it on the imaging server, enter:

```
img makep serverIPaddr_or_DNSname //uncpath/newimg.zmg [comp=comp
level]
```

The makep parameter stands for "make on proxy," which creates an image and stores it on the imaging (proxy) server.

The IP address or DNS name should be that of your imaging server.

The UNC path specifies the location and filename where the new image is to be stored.

The .zmg filename extension is case-sensitive.

The directories in the path must exist. You can use the following characters in the path and filename:

◆ Letters: a through z (uppercase and lowercase)

◆ Numbers

◆ Special Characters: $ % ' - _ @ { } ~ ` ! # ( )

comp level is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.)

For example:

```
img makep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg comp=6
```

◆ To create an image and store it locally, enter:

```
img makel filepath [comp=comp level]
```

The makel parameter stands for "make locally," which creates an image and stores it on a local hard disk.

NOTE: Unless you mount a drive before using makel, the image is created in RAM and is lost during a reboot of the device.

---

filepath is the image filename, including the .zmg extension (case-sensitive) and the complete path from the root of the partition.

The directories in the path must exist. You can use the following characters in the path and filename:

◆ Letters: a through z (uppercase and lowercase)

◆ Numbers

◆ Special Characters: $ % ' - _ @ { } ~ ` ! # ( )

comp level is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates

the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.)

For example:

```
img makel /imgs/dellnt.zmg comp=6
```

IMPORTANT: Make sure to use *forward slashes* in the UNC path as shown above. Backslashes are not recognized by Linux. Or, you can use backslashes and enclose the entire UNC path in quotes. The path you specify must exist on your imaging server.

For more information on the parameters you can use and usage examples, see Section E.3, "Make Mode (img make)," on page 633.

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

5 After the image is created and the bash prompt is displayed, remove any CD or DVD from the drive and reboot the device.

6 (Optional) Verify that the image file was created on your imaging server. You might also want to check its size.

Manually Taking an Image of a Device Using the ZENworks Imaging Engine Menu

1 Boot the device using one of the following methods:

- ◆ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.

- ◆ Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.

- ◆ Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` at the bash prompt.

or

Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.

3 Enter `img` to display the ZENworks Imaging Engine menu.

4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your reference, note the number and type of partitions and which one is active.

5 Click *Imaging > Make image*.

6 In the Make Image Wizard window, specify the destination where the image is stored (Local or Server), then click *Next*.

The directories in the path must exist. You can use the following characters in the path and filename:

- ◆ Letters: a through z (uppercase and lowercase)

- ◆ Numbers

- ◆ Special Characters: $ % ' - _ @ { } ~ ` ! # ( )

7 Browse to and specify the path to the image archive.

8 Select the partitions that you want to include in the image.

9 Select a compression option:

None: No compression is used.

Speed: Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.

Balanced: Represents a compromise between compression time and image file size.

Size: Creates the smallest image file but takes longer to compress.

10 Click *Next*.

11 (Optional) Fill in the fields:

Author: The name of the person creating this image.

Computer: The name of the computer being imaged.

Image description: A description of the image.

Comments: Any additional comments about the image.

12 Click *Next*.

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

13 After the image is created, exit from the ZENworks Imaging Engine menu, remove any CD or DVD from the drive, then reboot the device.

14 (Optional) Verify that the image file was created on your imaging server. You might also want to check its size.

Using Image Explorer to Customize an Image

After you have created a base or add-on image as explained in the previous sections, you can customize it with the Image Explorer utility. Specifically, you can:

◆ **Compress the image:** You can compress an image (including images created by previous versions of ZENworks Linux Management) to 40-60% of the original file size, if you have not done so already during the imaging process. There are three compression options. *Optimize for speed* takes the least amount of time but creates the largest compressed image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size. This option is used by default when an image is created.

ZENworks Linux Management provides the following compression methods:

 ◆ **Compress:** Use this option to compress an image file that you currently have open in Image Explorer. For more information, see "Compressing an Open Image" on page 610.

 ◆ **QuickCompress:** Use this option to compress an image file without waiting for the file to fully load into Image Explorer. For more information, see "Compressing Any Image without Waiting for the File to Fully Load into Image Explorer" on page 611.

◆ **Split the image:** You can specify a device image file that you want to split into separate files so that the entire image can be spanned across several CDs or DVDs. Splitting a device image is helpful for putting down or restoring images in a disconnected environment. For more information, see Section D.1.15, "Splitting an Image," on page 611.

- **Resize a partition in an image:** For base images, you can edit the value in the *Original size* text box to allow you to change how big the ZENworks Imaging Engine makes the partition when the image is restored. For more information, see Section D.1.16, "Resizing a Partition in an Image," on page 612.

- **Purge deleted files:** Excluded or hidden files and folders can be completely removed from an open image. This saves space in the image if you no longer want to include the files. For more information, see Section D.1.5, "Excluding a File or Folder from a File Set in the Open Image," on page 609.

- **Exclude individual files and folders from the image:** In doing this, you create subsets of the image by specifying which of ten possible file sets to exclude a given file or folder from. This exists merely as internal attributes of the same image archive. For more information, see Section D.1.7, "Purging Files and Folders Marked for Deletion from the Open Image," on page 609.

  IMPORTANT: Do not exclude BPB files from a base image or the device won't be able to boot the new operating system after receiving the image.

- **Add files and folders to the image:** By default, any file or folder you add is included in all file sets. To change this, you must explicitly exclude the file or folder from one or more file sets. For more information, see Section D.1.3, "Adding a File or Folder to an Open Image," on page 608.

For information on starting Image Explorer, see Section D.1, "Image Explorer (imgexp.exe)," on page 607.

Creating an Add-On Image

An *add-on* image is an archived collection of files to be applied to an existing installation on a target device. This is sometimes referred to as an application overlay. The existing partitions and files on the target device are left intact, except for any files that the add-on image might update.

An add-on image typically corresponds to an application or utility, or simply to a set of data files or configuration settings.

To create an add-on image:

1 Run the Image Explorer utility, which is located on the Linux imaging server at:

```
/opt/novell/zenworks/zdm/winutils/ImgExp.exe
```

2 Drag files and folders from an existing device into a new image archive.

For more information, see Section D.1, "Image Explorer (imgexp.exe)," on page 607.

3 Save this image with the .zmg extension (case-sensitive) in the same directory on the imaging server where you store base images.

Generally, an add-on image created in this manner doesn't require any post-processing on the target device. It is simply a set of files that are copied to the appropriate locations on the hard disk, much like what happens when you unzip an archive. For more information, see "Using Image Explorer to Customize an Image" on page 418.

This add-on image can be used in Step 8 on page 412 under "Configuring the ZENworks Image Bundle for Automatic Imaging" on page 410.

Manually Putting an Image on a Device

The section explains how to put an image on the device by booting from an imaging method and entering a particular imaging command. The image is retrieved from your imaging server.

Ensure that the device receiving a new image has enough disk space for the image. Otherwise, you receive a "Failed to write to proxy" error.

The following sections contain additional information:

* "Manually Putting an Image on a Device Using the Bash Prompt" on page 420
* "Manually Putting an Image on a Device Using the ZENworks Imaging Engine Menu" on page 421

Manually Putting an Image on a Device Using the Bash Prompt

1 If you haven't already done so, create the image to put on the device, as instructed in "Manually Taking an Image of a Device" on page 415.

Make sure that the image is of the same type of device (same hardware configuration) and is stored on your imaging server. You can use a previous image of the same device.

> **IMPORTANT:** If you are putting an image on a device without a ZENworks partition, make sure the image was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot.

2 (Optional) Boot the device from a Windows startup disk and run `fdisk` to remove all partitions from the hard disk.

Running `fdisk` is not required, but it is recommended for purposes of comparing workstation or server partitions before and after the imaging operation.

3 Boot the device using one of the following methods:

* If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
* Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
* Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

4 Enter `manual` at the bash prompt.

This step is not the same as in the previous step's manual processes.

5 (Optional) At the bash prompt, type `img dump`, then press Enter to display a list of the partition slots on the device.

For your reference, note the number and type of partitions and which one is active. If you removed all partitions using `fdisk`, each slot should be empty and none should be active.

6 Enter a command at the bash prompt using one of the following formats:

* To restore an image from the imaging server and put it down on a device, enter:

      img restorep *serverIPaddr_or_DNSname* //*uncpath*/*newimg*.zmg

The restorep parameter stands for "restore from proxy," which retrieves an image from the imaging (proxy) server and puts it on this device. The IP address or DNS name should be that of your imaging server, and the UNC path specifies the location and filename where the image is to be retrieved from.

For example:

```
img restorep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg
```

  ◆ To retrieve an image from a local device and put it down on a device:

```
img restorel filepath
```

The restorel parameter stands for "restore from local," which retrieves an image from a local device and puts it on this device. *Filepath* represents the filename of the image to retrieve, including the .zmg extension (case-sensitive) and the complete path from the root of the partition.

IMPORTANT: Make sure to use *forward slashes* in the UNC path as shown above. Backslashes aren't recognized by Linux. However, you can use backslashes and enclose the entire UNC path in quotes. The server portion of the path must be the name of your imaging server.

If you want to manually restore an image from a folder that uses extended or double-byte characters in its name, you should perform an automatic image restoration. For more information, see Section 28.5.2, "Creating, Installing, and Restoring Standard Images," on page 346 or Section 28.5.4, "Restoring Lab Devices to a Clean State," on page 347.

For more information on the parameters you can use and usage examples, see Section E.4, "Restore Mode (img restore)," on page 635.

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.

7 (Optional) After the image is put down and the bash prompt is displayed, type img dump, then press Enter.

As before, this displays a list of the partition slots on the device. You should now see information about the new partitions that are created and activated by the image that you just put down.

8 At the bash prompt, type lilo.s, then press Enter.

9 Remove any CD or DVD from the drive and reboot the device.

10 Verify that the device boots to the operating system that was installed by the new image.

Manually Putting an Image on a Device Using the ZENworks Imaging Engine Menu

1 If you haven't already done so, create the image to put on the device, as instructed in "Manually Taking an Image of a Device" on page 415.

Make sure that the image is of the same type of device (same hardware configuration) and is stored on your imaging server. You can use a previous image of the same device.

IMPORTANT: If you are putting an image on a device without a ZENworks partition, make sure the image was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot.

---

2 (Optional) Boot the device from a Windows startup disk and run fdisk to remove all partitions from the hard disk.

Running `fdisk` is not required, but it is recommended for purposes of comparing the workstation or server partitions before and after the imaging operation.

3 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.

- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.

- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

4 Enter `manual` at the bash prompt.

or

Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.

5 Enter `img` to display the ZENworks Imaging Engine menu.

6 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your reference, note the number and type of partitions and which one is active. If you removed all partitions using `fdisk`, each slot should be empty and none should be active.

7 Click *Imaging > Restore image*.

8 In the Restore Image Wizard window, specify the source location of the image (Local or Server), then click *Next*.

9 Browse to and specify the path to the image archive.

10 (Optional) Specify a file set.

11 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.

For details on this and other related `img` command parameters, see "ZENworks Imaging Engine Commands" on page 631.

12 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.

13 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

As before, this displays a list of the partition slots on the device. You should now see information about the new partitions that are created and activated by the image that you just put down.

14 Exit the ZENworks Imaging Engine menu.

15 Run `lilo.s` from the bash prompt.

16 Remove any CD or DVD from the drive and reboot the device.

17 Verify that the device boots to the operating system that was installed by the new image.

Making an Image Available for Automatic Imaging

When you boot a device from an imaging method and allow the boot process to proceed in auto-imaging mode, the imaging operation that is performed on the device is determined by default Preboot Services settings that you define in the ZENworks Control Center.

Creating a Preboot Services bundle also allows you to combine a base image and one or more add-on images into a single entity that can be put down on target devices. You can specify a standard image file to put down, or you can create a script to further customize your imaging operation. You can also specify that a particular file set of an image be used.

The sections that follow give instructions for performing these tasks:

◆ "Creating a Base Image" on page 423

◆ "Associating an Add-On Image with a Base Image" on page 423

◆ "Using a File Set of an Image" on page 424

Creating a Base Image

1 Create the base image using one of the following methods:

   ◆ **ZENworks Control Center:** See "Taking a Base Image of a Device" on page 408.

   ◆ **Manually from a bash prompt:** See "Manually Taking an Image of a Device" on page 415.

2 After the base image is created, perform one of the following procedures in the ZENworks Control Center:

   ◆ If you created the image using a Preboot bundle, assign the bundle to the devices to be imaged:

      1. In the ZENworks Control Center, click *Bundles*, click the bundle containing the base image that you want to associate the add-on images with, then click *Details*.

      2. In the Assignments section, click *Add* to start the Assign Bundle wizard.

      3. Click *Add* to open the Select Objects dialog box.

      4. Select the devices or groups containing devices, then click *OK*.

      5. Click *Next* to display the Summary page, then click *Finish > OK* to assign the devices to the bundle and exit the wizard.

   ◆ If you created the image manually, assign the image to a Preboot Image bundle, then assign that bundle to the devices to be imaged:

      1. Follow the instructions in "Configuring the ZENworks Image Bundle for Automatic Imaging" on page 410.

      2. In Step 10 on page 414, click *Next* to assign the bundle to the devices.

The next time these devices boot, they are imaged from this Preboot bundle.

Associating an Add-On Image with a Base Image

1 Create the add-on image to associate with the base image. For more information, see "Creating an Add-On Image" on page 419.

2 Copy the add-on image file to a ZENworks Linux Management imaging server that is accessible as a server object in your eDirectory tree.

You might want to copy your add-on images to the same location as the base image.

3 In the ZENworks Control Center, click *Bundles*, click the bundle containing the base image that you want to associate the add-on images with, then click *Details*.

4 For the Add-On Image Files section, click *Add*.

5 Browse for and select an add-on image.

You can associate more than one add-on image with a base image. Repeat this step for each add-on image.

6 Click *Apply*.

When a device boots that is assigned to this bundle, the add-on images are put down after the base image in the order listed on this page.

Using a File Set of an Image

As explained in "Using Image Explorer to Customize an Image" on page 418, you can exclude individual files and folders from any of 10 possible file sets of an image.

Table 30-1   *Image File Set Usages*

Type of imaging operation	How to specify the file set to use
Automatic (Preboot Services based on default settings)	In the Multicast Wizard in the ZENworks Control Center, specify the number of the file set in the *File set* field. You must create the file set using the Image Explorer utility. For more information, see Section D.1, "Image Explorer (imgexp.exe)," on page 607. You can create multiple Preboot bundles that point to the same base image, but to different file sets of that image.
Manual (command line or menu)	Use the `s` parameter on the `img restore` command. For example, to specify file set number 3: `img restorel dellnt4.zmg s3` or You can enter `img` at the bash prompt to display a menu, select *Restore an image*, then select *Local image*. Specify s*fileset* (for example, s3) in the *Advanced parameters* field. For details, see "ZENworks Imaging Engine Commands" on page 631.

30.1.3 Setting Up Disconnected Imaging Operations

Disconnected imaging operations are inherently manual. To perform a disconnected imaging operation on a device, you must have a storage device to hold the image to be created or put down, and that storage device must be locally accessible to the ZENworks Imaging Engine (in Linux) when you boot the device from the imaging boot media.

The following sections explain how to set up and perform disconnected operations:

- "Using a CD or DVD for Disconnected Imaging Operations" on page 424
- "Using a Hard Disk for Disconnected Imaging Operations" on page 426

Using a CD or DVD for Disconnected Imaging Operations

In ZENworks Linux Management, you can use CDs and DVDs only as the storage medium for an image to put down, not for an image to be created.

You can put down an image from a bootable or non-bootable imaging CD or DVD using either the bash prompt or using the ZENworks Imaging Engine menu.

The following sections contain additional information:

- "Putting Down an Image Using the Bash Prompt" on page 425
- "Putting Down an Image Using the ZENworks Imaging Engine Menu" on page 425

Putting Down an Image Using the Bash Prompt

1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.

2 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

3 Enter `manual` from the bash prompt.

4 Insert the CD or DVD that contains the source image.

5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.

This mounts the CD or DVD to `/mnt/cdrom`.

6 Enter a command using the following format:

```
img restorel /mnt/cdrom/path/image_name.zmg
```

where *path* and *image_name* are the path and filename of the image relative to the root of the CD or DVD.

7 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

7a At the Linux prompt, type `lilo.s`, then press Enter.

7b Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

Putting Down an Image Using the ZENworks Imaging Engine Menu

1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.

2 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

3 Enter `manual` from the bash prompt.

4 Insert the CD or DVD that contains the source image.

5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.

This mounts the CD or DVD to `/mnt/cdrom`.

6 Enter `img` to display the ZENworks Imaging Engine menu.

7 Click *Imaging*, then click *Restore image*.

8 Click *Local*, then click *Next*.

9 Browse to and specify the path to the image archive.

10 (Optional) Specify a file set.

11 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.

For details on this and other related `img` parameters, see "ZENworks Imaging Engine Commands" on page 631.

12 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.

13 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

13a At the Linux prompt, type `lilo.s`, then press Enter.

13b Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

Using a Hard Disk for Disconnected Imaging Operations

When you boot a device from a ZENworks Linux Management imaging boot media, you can create an image on, or put down an image from, any primary partition on an IDE or SCSI hard drive. You can also use the local ZENworks partition if one is installed. Any target partition must have sufficient space.

When you create an image, the partition where you store the image is itself excluded from the image. When you put down an image, the source partition is not altered.

You can create or put down an image on a hard disk using either the bash prompt or using the ZENworks Imaging Engine menu.

The following sections contain the instructions:

- "Creating an Image Using the Bash Prompt" on page 426
- "Creating an Image Using the ZENworks Imaging Engine Menu" on page 427
- "Putting Down an Image Using the Bash Prompt" on page 428
- "Putting Down an Image Using the ZENworks Imaging Engine Menu" on page 428

Creating an Image Using the Bash Prompt

1 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` from the bash prompt.

3 At the Linux prompt, enter `img dump` to view the available partitions.

Note the number of the partition where you will store the new image.

4 Enter a command using the following format:

`img makel[`*pNumber*`] /`*path*`/`*image*`.zmg [comp=`*comp_level*`]`

where *pNumber* is the number of the partition to store the image in, and *comp_level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed*. 6 is the same as *Balanced* and is used by default if you do not specify this parameter. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.) *Path* and *image* are the path and filename of the new image relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related `img` command parameters, see "ZENworks Imaging Engine Commands" on page 631.

Creating an Image Using the ZENworks Imaging Engine Menu

1 Boot the device using one of the following methods:

- ◆ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.
- ◆ Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.
- ◆ Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` from the bash prompt.

3 Enter `img` to display the ZENworks Imaging Engine menu.

4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your information, note the number of the partition where you will store the new image.

5 Click *Imaging > Make image*.

6 In the Make Image Wizard window, click *Local > Next*.

7 Browse to and specify the path to the image archive.

8 Select the partitions that you want to include in the image.

9 Select a compression option.

None: No compression is used.

Speed: Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.

Balanced: Represents a compromise between compression time and image file size.

Size: Creates the smallest image file but takes longer to compress.

10 Click *Next*.

11 (Optional) Fill in the fields:

Author: The name of the person creating this image.

Computer: The name of the computer being imaged.

Image description: A description of the image.

Comments: Any additional comments about the image.

12 Click *Next*.

Depending on the amount of data on the hard disk, the image might take several minutes to create.

13 After the image is created, exit from the ZENworks Imaging Engine menu, remove any CD or DVD from the drive, then reboot the device.

14 (Optional) Verify that the image file was created. You might also want to check its size.

Putting Down an Image Using the Bash Prompt

1 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.

- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.

- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` from the bash prompt.

3 (Optional) At the Linux prompt, enter `img dump` to view the available partitions.

For your information, note the number of the partition where the source image is stored.

4 Enter a command using the following format:

```
img restorel[pNumber] /path/image.zmg
```

where *pNumber* is the number of the partition where the source image is stored, and *path* and *image* are the image path and filename relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related `img` command parameters, see "ZENworks Imaging Engine Commands" on page 631.

5 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

  5a At the Linux prompt, type `lilo.s`, then press Enter.

  5b Press Ctrl+Alt+Delete.

   If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

Putting Down an Image Using the ZENworks Imaging Engine Menu

1 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see Section 29.2.1, "Using Preboot Services (PXE)," on page 354.

- Boot the device using an imaging boot CD or DVD. For more information, see Section 29.2.2, "Preparing Imaging Boot CDs or DVDs," on page 354.

- Boot the device from the ZENworks partition. For more information, see "Creating a ZENworks Partition" on page 362.

2 Enter `manual` from the bash prompt.

3 Enter `img` to display the ZENworks Imaging Engine menu.

4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your reference, note the number of the partition where the source image is stored.

5 Click *Imaging > Restore image*.

6 Click *Local > Next*.

7 Browse to and specify the path to the image archive.

8 (Optional) Specify a file set.

9 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.

For details on this and other related `img` command parameters, see "ZENworks Imaging Engine Commands" on page 631.

10 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

11 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

11a At the Linux prompt, type `lilo.s`, then press Enter.

11b Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

30.2 Multicasting Images

ZENworks Linux Management's Preboot Services includes a multicasting capability for its imaging software. You can perform multicasting of images either in the ZENworks Control Center or manually:

- Section 30.2.1, "Multicasting in the ZENworks Control Center," on page 429
- Section 30.2.2, "Multicasting Manually," on page 435

30.2.1 Multicasting in the ZENworks Control Center

- "Configuring Multicast Bundles" on page 430
- "Enabling a Multicast Session" on page 434

Configuring Multicast Bundles

With Preboot Services, multicasting is an automated procedure. As described in "Automatic Multicasting Example" on page 350, you simply define a Multicast bundle and assign it to the devices. The multicast session starts when the trigger event that you configured occurs.

Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a Multicast bundle and assign devices to the bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New > Bundle* to start the Create New Bundle Wizard:

3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next* to display the Select Preboot Bundle Type page:

4 Select *ZENworks Multicast bundle*, then click *Next* to display the Set General Information page:

5 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Multicast bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the ZENworks Multicast bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this ZENworks Multicast bundle.

If you are using subsets of an image, be sure to indicate which file set this bundle is configured for.

6 Click *Next* to display the Master Image Source page:

Create New Bundle | ZENworks Multicast 1 | ?
Step 4: Set Multicast Session Attributes

Master Image Source:

File Path: *

[   ] 🔍 [Clear]

File Set:
[1 ▾]

Start the session as soon as:
[1] clients have joined, or
[5] minutes have elapsed since a new client has joined

Fields marked with a blue asterisk are required.

[<< Back] [Next >>] [Cancel]

7 Fill in the fields:

ZENworks Multicast bundles use an image that is taken previously from a device and is stored on an imaging server. The image is sent to multiple devices at one time to re-image them, rather than sent one time for each device, thus saving on network bandwidth usage. For example, if you have 10 devices in the multicast session and the image is 3 GB in size, your network experiences 3 GB of network traffic to image all 10 devices. Without multicasting, the network experiences 30 GB of network traffic.

For multicasting to work properly, all routers and switches on the network must have their multicast features configured. Otherwise, multicast packets might not be routed properly.

File path: The location on the imaging server where the image file to be used by the ZENworks Multicast bundle is stored.

File set: File sets are assigned to the current ZENworks Image bundle using this *File set* field. File sets are defined on the imaging server from the base image using the Image Explorer utility, which can be run on a Windows device from a Linux server running Samba. The Image Explorer utility is located at `/opt/novel/zenworks/zdm/winutils/ImgExp.exe` on the Linux server.

When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.

For example, `device1image.zmg` is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of `device1image.zmg`.

The advantage file sets provide is that you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets will include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.

There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.

IMPORTANT: If you create 10 different file sets, then the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you do not select a file set when using this wizard.

8 Fill in the fields:

There are two triggers that you can use to determine when to start the ZENworks Multicast session. The first trigger to be realized starts the session.

A session consists of all clients (devices) that are assigned to the ZENworks Multicast bundle that are booting (joining), but must wait for a start trigger. Therefore, the boot processes for the devices can be held up until one of the triggers is realized, even for as long as you specify in an elapsed time or number of clients entry.

After a session has started, if other devices boot that are assigned to this bundle, they do not become part of this session, but become part of the next session when it triggers.

Start the session as soon as: You have two choices:

- ◆ _____ clients have joined

    This trigger, if met first, limits the session to the number of clients that you specify. The default is 1.

- ◆ _____ minutes have elapsed since a new client has joined

    This trigger, if met first, causes the session to start, regardless of the number of clients that have joined, except that at least one client must have joined (otherwise there is no device to multicast to).

    A "new client" means that it is the first device to boot that starts this round of waiting for a trigger to be realized. The default is 5.

These triggers are useful if you want economy of scale in multiple clients joining, but don't want to stall the session too long from starting.

9 Click *Next* to display the Summary page.

10 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Click to perform the following tasks before creating the bundle:

- ◆ Specify device assignments for this bundle
- ◆ Specify groups for this bundle

Continue with Section 30.6, "Assigning Unassigned Preboot Bundles," on page 461 to assign the bundle and complete the wizard.

Finish: Creates the Multicast bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When the Multicast bundle's trigger event occurs (configured in Step 8), the Multicast session begins.

Enabling a Multicast Session

A wizard allows you to cause each device assigned to the ZENworks Multicast bundle to be enabled for receiving the bundle when it reboots, even if the configuration for the device is to "do nothing" (see Step 5 through Step 7 in Section 30.7, "Editing Preboot Services Work," on page 463).

The wizard does not assign a bundle to any device, nor does it make it the effective bundle for any device. It only sets up a device to do ZENworks Multicast Bundle work for its effective bundle the next time it boots.

To enable a ZENworks Multicast bundle:

1 In the ZENworks Control Center, click the *Bundles* tab to display the Bundles page:

Bundles

	Status Name ⩒	Type	Size
☑	🟢 ZENworks Multicast Bundle	ZENworks Multicast Bundle	

◄ ▶ 1 - 10 of 12   show 10 ▾ items
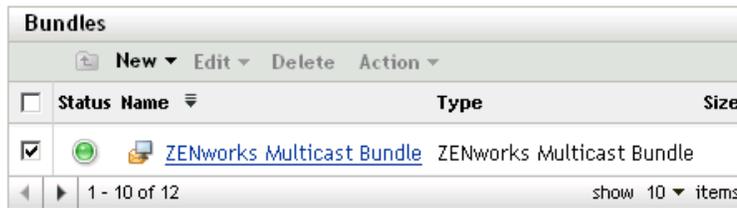
2 Select the check box next to a *ZENworks Multicast bundle*.

Bundles

New ▾ Edit ▾ Delete Action ▾

	Status Name ⩒		Size
☑	🟢 ZENworks Multicast	Assign Bundle… Assign Catalog… Add To Group… Add To Catalog… Enable Multicast Session… Disable Multicast Session	ast Bundle

◄ ▶ 1 - 10 of 12   show 10 ▾ items
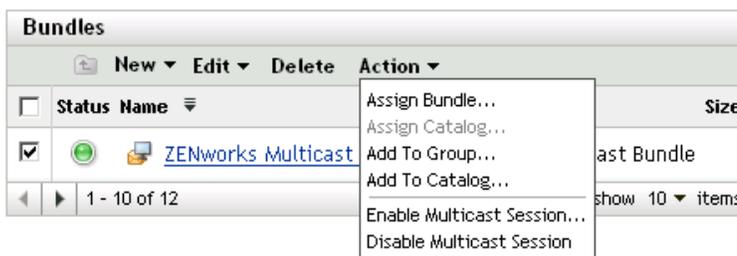
3 Click *Actions > Enable multicast session* to start the Enable Multicast Session Wizard:
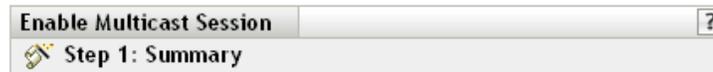
4 Click *Finish* to enable multicasting for the selected device.

5 Click *OK* to the message that indicates multicasting is successfully enabled.

The next time a device assigned to the multicast bundle boots, it can become part of that multicast session. For more information, see Section 30.2, "Multicasting Images," on page 429.

30.2.2 Multicasting Manually

If you want to perform a manual multicast session, you need to start the multicast session from the ZENworks imaging server and physically visit each participating device. Performing a manual multicast session is particularly useful in a lab environment in which a small number of devices participate.

The following sections contain step-by-step information about performing a manual multicast session. You must perform the steps in both of the following sections; however, the order in which you perform these tasks does not matter.

- ◆ "Initiating a Multicast Session from the ZENworks Imaging Server" on page 435
- ◆ "Initiating a Multicast Session from Each Client" on page 437

Initiating a Multicast Session from the ZENworks Imaging Server

On the ZENworks Linux Management imaging server, do the following to initiate the multicast session:

1 In the shell console, enter the following command to make sure the imaging software is running:

```
/etc/init.d/novell-pbserv -status
```

If it is not running, then enter:

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

2 In the shell console, enter the following command to enable a multicast session:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -mcast arguments
```

where *arguments* represents the following that you can append to the command line:

Argument	Description
session_name	(Required) The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network.
-p *path*	(Required) The path to the image to be multicast, which is located on the imaging server. This must be the full path.
-i *IP_address*	(Optional) The IP address of the imaging server.
-f *file_set_number*	(Optional) File sets are assigned to the current ZENworks Image bundle using this information. File sets are defined on the imaging server from the base image using the Image Explorer utility, which can be run on a Windows device from a Linux server running Samba. The Image Explorer utility is located at `/opt/novel/zenworks/zdm/winutils/ImgExp.exe` on the Linux server.

When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.

For example, `device1image.zmg` is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of `device1image.zmg`.

File sets provide an advantage because you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.

There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.

IMPORTANT: If you create 10 different file sets, then the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you don't select a file set when using this wizard. |
| -t *time_wait* | (Optional) If not enough devices have booted to fulfill the Client Count requirement, the multicast session begins if a participating device boots and a certain amount of time passes without another participating device booting. Specify this amount of time. The default is 5 minutes. |
| -c *client_count* | (Optional) The number of participating devices you want to have booted before the multicast session begins. If you do not specify a number, the default is 1. |

IMPORTANT: The image is sent to and put down on each participating device only after you initiate the multicast session from each participating client.

3 To view the status of the multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -status -i
proxy_IP_address
```

The -i argument is optional.

4 To view the list of multicast sessions, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -list -i proxy_IP_address
```

The -i argument is optional.

5 To stop a multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -stop session_name -i
proxy_IP_address
```

The *session_name* is required and the -i argument is optional.

6 Continue with "Initiating a Multicast Session from Each Client" on page 437.

Initiating a Multicast Session from Each Client

You can use the bash prompt or the ZENworks Imaging Engine menu to perform the multicast session as you physically visit each device.

The following sections contain additional information:

◆ "Using the Bash Prompt to Perform the Multicast Session" on page 437
◆ "Using the ZENworks Imaging Engine Menu to Perform the Multicast Session" on page 438

Using the Bash Prompt to Perform the Multicast Session

1 (Optional) Install the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) on each of the participating devices.

If you do not install the Imaging Agent on each participating device, the devices have duplicate network identities. For more information, see "Limitations of Multicasting Images" on page 349.

2 Create an imaging boot CD or DVD for each person who will assist with the multicast session, or enable PXE on the participating devices.

If you don't know how to do this, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

3 At each device, including the master device (unless you are starting the multicast session from the imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

4 Enter `manual` at the bash prompt.

5 To identify each participating device in the multicast session, enter the following command at the bash prompt of every device:

```
img session session_name
```

where *session_name* is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating devices in this multicast session. You can specify any multicast session, including one that originates from the imaging server (as long as you specify the session name used by the imaging server).

Example: `img session mcast01`

The `img session` command can take other parameters that allow you to designate the master device and the imaging start time beforehand. See "ZENworks Imaging Engine Commands" on page 631 for details.

6 (Conditional) If you have not already done so, start the multicast session from the master device or from the imaging server.

Master device: To start the multicast session from the master device, after all of the other devices have registered as participants, click *Start session*.

If you start the session from the master device, the session master must be a device. If you start the session from the imaging server, the session master must be an imaging server using a previously saved image file.

The ZENworks Imaging Engine begins creating the image of the master device and the image is sent to and put down on each participating device. Any problems are reported and displayed on the master device.

Imaging server: To start the multicast session from the imaging server, follow the steps under "Initiating a Multicast Session from the ZENworks Imaging Server" on page 435.

7 At each participating device, when the imaging is done, do the following to boot the device with the new operating system:

7a At the Linux prompt, type `lilo.s`, then press Enter.

7b Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

Using the ZENworks Imaging Engine Menu to Perform the Multicast Session

1 (Optional) Install the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) on each of the participating devices.

If you do not install the Imaging Agent on each participating device, the devices have duplicate network identities. For more information, see "Limitations of Multicasting Images" on page 349.

2 Create an imaging boot CD or DVD for each person who will assist with the multicast session, or enable PXE on the participating devices.

If you don't know how to do this, see Section 29.2, "Setting Up the Preboot Services Methods," on page 354.

3 At each device, including the master device (unless you are starting the multicast session from the imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

4 Enter `manual` at the bash prompt.

or

Select *Start ZENworks Imaging Maintenance* from the Preboot Services Menu.

5 To identify each participating device in the multicast session, type `img` at the bash prompt to display the ZENworks Imaging Engine screen.

6 Click *Imaging*, then click *Multicast session* (or on the task bar, click *F7 Multicast*) to start the Multicast Wizard.

7 Enter a session name.

The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating devices in this multicast session. You can specify any multicast session, including one that originates from the imaging server (as long as you specify the session name used by the imaging server).

8 Select a *Session role* option:

Master: Select this option if this is the session master.

Client: Select this option if this is a participating device.

9 (Optional) If you chose Master in Step 8, click *Specify additional options*, click *Next*, then fill in the fields:

Compression level: Specify the compression level you want to use for this multicast session:

◆ **None:** No data compression is used. Data is sent immediately across the network to participating devices. You might use this option if the master device has a slow CPU; the amount of time to compress the data is eliminated and the data is immediately sent across the network. However, this option creates more network traffic than if you selected one of the other compression levels (*Speed*, *Balanced*, or *Size*).

◆ **Speed:** Takes the least amount of time to compress the data before the data is sent across the network to participating devices. You might use this option if the master device has a slow CPU; the amount of time to compress the data is reduced before the data is sent across the network. With this option, however, the multicast session creates more network traffic than if you selected either the *Balanced* or *Size* compression level.

◆ **Balanced:** Represents a compromise between data compression and the amount of network traffic that the multicast session creates.

◆ **Size:** Takes the most amount of time to compress the data before sending it across the network to participating devices. You might use this option if the master device has a fast CPU. Using this option requires the most CPU resources to compress the data but creates less network traffic to transfer the data to the participating devices.

Automated session: Click *Enabled* to specify the number of participating devices (clients) that must register before starting the automated multicast session and to specify the amount of time, in minutes, that can expire without the number of participating devices to register before starting the automated multicast session. If you do not click the *Enabled* check box, you must manually start the multicast session.

10 Click *Next*, then click *Start session*.

You can cancel the session by clicking *Abort session > Yes > OK > Close*.

11 At each participating device, when the imaging is done, do the following to boot the device with the new operating system:

11a At the Linux prompt, type `lilo.s`, then press Enter.

11b Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

30.3 Configuring AutoYaST or Kickstart Installation Script Bundles

The following sections explain how to create, configure, and assign AutoYaST and kickstart bundles:

IMPORTANT: Do not select *Always Show Preboot Menu* if you have AutoYaST or kickstart bundles assigned to any devices, because the Preboot Services Menu interrupts the PXE boot process, keeping the AutoYaST or kickstart bundles from being deployed on the device. The Preboot Services Menu only has options for doing imaging work, not for installing operating systems.

Therefore, select either *Never Show Preboot Menu* or *Show Preboot Menu if CTRL+ALT is Pressed* for your Preboot Services Menu option, which allows PXE-enabled Linux devices to automatically implement the AutoYaST or kickstart bundles.

30.3.1 Configuring an AutoYaST Bundle

Use the wizard described in this section to create a new AutoYaST bundle for installing SUSE® Linux. Using ZENworks Linux Management, you can then install the software by using this bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure an AutoYaST bundle, and assign devices to the bundle:

1 In the ZENworks Control Center, click the *Bundles* tab to display the Bundles page:
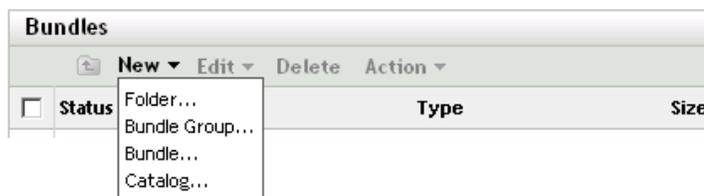
2 Click *New > Bundle* to start the Create New Bundle Wizard:
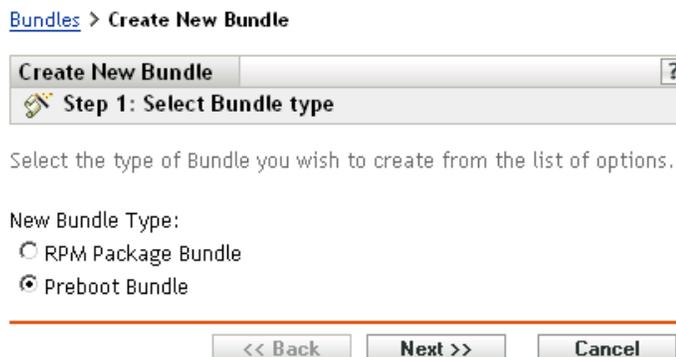
3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next* to display the Select Preboot Bundle Type page:

Bundles > Create New Bundle

| Create New Bundle | asdf | ? |

Step 2: Select Preboot Bundle Type

Select the type of Preboot Bundle you wish to create from the list of options.

Preboot Bundle Type:
- AutoYaST Bundle
- Dell Configuration Bundle
- Kickstart Bundle
- ZENworks Image Bundle
- ZENworks Multicast Bundle
- ZENworks Script Bundle

Type Description:
AutoYaST Bundle - Describes the location and access protocol of an AutoYaST configuration file and network install directory for SUSE Linux. This bundle allows you to launch an automated installation of SUSE Linux using Preboot Services.

[<< Back] [Next >>] [Cancel]

4 On the Select Preboot Bundle Type page, select *AutoYaST bundle*, then click *Next* to display the Set General Information page:

Bundles > Create New Bundle

| Create New Bundle | | ? |

Step 3: Set General information

Name:
[ ]

Folder:
[/Bundles] 🔍

Description:
[ ]

[<< Back] [Next >>] [Cancel]

5 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the AutoYaST bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the AutoYaST bundle to be displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this AutoYaST bundle.

6 Click *Next* to display the Set AutoInstall Attributes page:

7 Fill in the fields:

Linux kernel file: The path should be relative to the home directory of the novell-tftp daemon. For example, you might do the following:

a. Copy the kernel file, whose default location is `/boot/loader/linux` on a SLES 9 SP1 bootable CD.

b. Place the copy in a location on your imaging server. For example, `/srv/tftp/autoyast/ linux`.

c. In this field, enter the path that is relative to the daemon. For example, `autoyast/linux`.

Initial RAM drive: The path should be relative to the home directory of the novell-tftp daemon. For example, you might do the following:

a. Copy the RAM drive file, whose default location is `/boot/loader/initrd` on a SLES 9 SP1 bootable CD.

b. Place the copy in a location on your imaging server. For example, `/srv/tftp/autoyast/initrd`.

c. In this field, enter the path that is relative to the daemon. For example, `autoyast/initrd`.

Protocol and IP address (or DNS name) required to access the network installation directory: Select *NFS*, *FTP*, *HTTP*, or *TFTP* from the drop-down list, then specify the IP address or DNS name of the device containing the network installation directory.

Path to the network installation directory (relative to protocol): The path should be relative to the home directory of the selected protocol daemon.

For example, if you specify the HTTP protocol, enter *myserver.provo.novell*.com as the DNS name, and specify the path as `/installs/scripts/myscript.cfg`, then the URL to the installation directory is `http://myserver.provo.novell.com/installs/scripts/myscript.cfg`, where `/installs/scripts/myscript.cfg` is relative to the protocol and server ID.

Protocol and IP address required to access the script: Select *NFS*, *FTP*, *HTTP*, *TFTP*, or *FILE* from the drop-down list, then specify the IP address or DNS name of the device containing the script.

If you select *FILE*, you must manually copy the AutoYaST XML file that you specify on this wizard page into the initial RAM drive file that you specify in the *Initial RAM Drive* field.

For example, if `initrd` is your initial RAM drive file and `autoyast.xml` is your AutoYaST XML file, perform the commands in the following tables:

Table 30-2 *Obtaining and Preparing the RAM Drive File*

Command	Description
`cd /path_to_RAM_drive_file`	Change to the directory where `initrd` exists.
`cp initrd initrd.bak`	Make a backup copy of your original RAM drive file (recommended).
`mv initrd initrd.gz`	Rename `initrd` to a temporary gzipped file.
`gzip -d initrd.gz`	Decompress the `.gz` file. This changes the `initrd.gz` filename back to `initrd`, but in an uncompressed mode.
`mkdir temp`	Create a temporary working directory.
`file initrd`	Determine which type of file system `initrd` is. If the type is cpio, perform the commands in Table 30-3, "Updating a cpio File Type," on page 444; otherwise, perform the commands in Table 30-4, "Updating a non-cpio File Type," on page 444.

Table 30-3 *Updating a cpio File Type*

Command	Description
`cd temp`	Move to the temporary directory.
`cpio -idmuv < ../initrd`	Extracts cpio archive to the current directory.
`cp /path_to_autoyast.xml_file/` `autoyast.xml.`	Copy your AutoYaST XML file to the temp directory.
`find .	cpio -o -H newc > ../initrd`	Re-creates the archive with the AutoYaST XML file included.

`cd ..`
`gzip -v9 initrd`
`mv intird.gz initrd`
	Return the file back to its compressed state with the AutoYaST XML file in it.

Table 30-4 *Updating a non-cpio File Type*

Command	Description
`mount -o loop initrd temp`	Create a `temp` directory and mount the initial RAM drive file to `temp`.
`cp autoyast.xml temp`	Copy your AutoYaST XML file to the temp directory.

`umount temp`
`gzip -v9 initrd`
`mv intird.gz initrd`
	Return the `initrd` file back to its compressed state with the AutoYaST XML file in it.

After performing these commands, the initial RAM drive file (`initrd`) can be used with the AutoYaST XML file when this AutoYaST bundle is executed on the device.

AutoYaST script name and path (relative to the protocol default directory): The path should be relative to the home directory of the selected protocol daemon.

For example, if you select the HTTP protocol, enter *myserver.provo.novell*.com as the DNS name, and enter the path and filename as `/scripts/autoyast.xml`, then the URL to the installation directory is `http://myserver.provo.novell.com/scripts/autoyast.xml`, where `/scripts/autoyast.xml` is relative to the protocol and server ID.

Additional kernel parameters: Specify additional kernel parameters. These are not Preboot Services or ZENworks parameters. They are parameters that your Linux kernel needs. For more information, see your Linux documentation.

A device's Image Safe Data, such as the device's IP address and other identity information that is defined for its ZENworks Control Center object, is contained on the hard drive that the device boots from. This information can be lost if that hard drive needs to be replaced. However, the following options allow you to retain a device's IP address and other identity information when replacing the hard drive.

These options are only applicable when this Preboot bundle is applied to a specific device. The image used in this bundle must contain the device's previous IP address and ZENworks Control Center object information.

(Optional) Select one or both of the following options:

◆ **Use the IP Address from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

Use this option if you have previously taken an image of the device and are using that image with this Preboot bundle. This option causes the imaging process to write the device's IP address that is contained in this image to the Image Safe Data location on the replacement hard drive.

Do not use this option if the image being used for this bundle was not previously made from this device.

If you do not select this option, then:

  ◆ If the device that this Preboot bundle is applied to is still using its primary hard drive to boot from, the IP address in its Image Safe Data continues to be used.

   or

  ◆ If the device that this Preboot bundle is applied to has been given a new hard drive to boot from, but you do not have a previous image of the old hard drive, then the IP address is assigned according to your ZENworks Management Zone configuration for non-registered devices.

◆ **Use the Identity Information from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

If you are using a previous image of this device, this option writes ZENworks Control Center object identity information as contained in the image to the new hard drive's Image Safe Data location, which allows the device to retain its ZENworks Control Center object.

However, if the image contained in this bundle was not previously made from this device, it receives the new ZENworks Control Center object that is defined in the image.

If you do not select this option and the device that this Preboot bundle is applied to has been given a new hard drive to boot from, then a new ZENworks Control Center object is created according to your ZENworks Management Zone configuration for non-registered devices.

8 Click *Next* to display the Summary page.

9 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Allows you to perform the following tasks before creating the bundle:

  ◆ Specify device assignments for this bundle

  ◆ Specify groups for this bundle

Continue with to assign the bundle and complete the wizard.

Finish: Creates the AutoYaST bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When any device assigned to the AutoYaST bundle boots, the bundle's SUSE Linux installation work is performed on the device.

30.3.2 Configuring a Kickstart Bundle

A kickstart bundle contains software for installing Red Hat Linux.

Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a kickstart bundle and assign devices to the bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New > Bundle* to start the Create New Bundle Wizard:

3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.

4 On the Select Preboot Bundle Type page, select *Kickstart bundle*, then click *Next* to display the Set General Information page:

5 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the kickstart bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the kickstart bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this kickstart bundle.

6 Click *Next* to display Set AutoInstall Attributes page:

Bundles > Create New Bundle

Create New Bundle	kickstart 1	?

Step 4: Set AutoInstall Attributes

Describe how to access the Linux boot files. These files should have been copied to the Preboot TFTP server from the CD.

Linux Kernel File:

(Path should be relative to the default directory of the TFTP daemon. e.g.: redhat/8.0/vmlinuz)

Initial RAM Drive:

(Path should be relative to the default directory of the TFTP daemon. e.g.: redhat/8.0/initrd.img)

Additional Kernel Parameters:

Protocol and IP address (or DNS name) required to access the configuration file:

NFS

Path to the kickstart configuration file (relative to the protocol default directory):

(e.g.: config/ks.cfg)

☐ Use IP Address from the preboot bundle rather than from Image Safe Data
☐ Use Identity Information from the preboot bundle rather than from Image Safe Data

<< Back   Next >>   Cancel

7 Fill in the fields:

Linux kernel file: The path should be relative to the home directory of the novell-tftp daemon. For example, you might do the following:

a. Copy the kernel file, whose default location is `/isolinux/vmlinuz` on a Red Hat Enterprise Linux 4 bootable CD.

b. Place the copy in a location on your imaging server. For example, `/srv/tftp/kickstart/vmlinuz`.

c. In this field, enter the path that is relative to the daemon. For example, `kickstart/vmlinuz`.

Initial RAM drive: The path should be relative to the home directory of the novell-tftp daemon. For example, you might do the following:

a. Copy the RAM drive file, whose default location is `/isolinux/initrd.img` on a Red Hat Enterprise Linux 4 bootable CD.

b. Place the copy in a location on your imaging server. For example, `/srv/tftp/kickstart/initrd.img`.

c. In this field, enter the path that is relative to the daemon. For example, `kickstart/initrd.img`.

Protocol and IP address required to access the script: Select *NFS* or *HTTP* from the drop-down list, then specify the IP address or DNS name of the device containing the script.

Kickstart script name and path (relative to the protocol default directory): The path should be relative to the home directory of the selected protocol daemon.

For example, if you select the HTTP protocol, enter *myserver.provo.novell*.com as the DNS name, and enter the path and filename as `/config/ks.cfg`, then the URL to the installation directory is `http://myserver.provo.novell.com/config/ks.cfg`, where `/config/ks.cfg` is relative to the protocol and server ID.

Additional kernel parameters: Specify additional kernel parameters. These are not Preboot Services or ZENworks parameters. They are parameters that your Linux kernel needs. For more information, see your Linux documentation.

A device's Image Safe Data, such as the device's IP address and other identity information that is defined for its ZENworks Control Center object, is contained on the hard drive that the device boots from. This information can be lost if that hard drive needs to be replaced. However, the following options allow you to retain a device's IP address and other identity information when replacing the hard drive.

These options are only applicable when this Preboot bundle is applied to a specific device. The image used in this bundle must contain the device's previous IP address and ZENworks Control Center object information.

(Optional) Select one or both of the following options:

- **Use the IP Address from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

  Use this option if you have previously taken an image of the device and are using that image with this Preboot bundle. This option causes the imaging process to write the device's IP address that is contained in this image to the Image Safe Data location on the replacement hard drive.

  Do not use this option if the image being used for this bundle was not previously made from this device.

  If you do not select this option, then:

  - If the device that this Preboot bundle is applied to is still using its primary hard drive to boot from, the IP address in its Image Safe Data continues to be used.

    or

  - If the device that this Preboot bundle is applied to has been given a new hard drive to boot from, but you do not have a previous image of the old hard drive, then the IP address is assigned according to your ZENworks Management Zone configuration for non-registered devices.

- **Use the Identity Information from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

  If you are using a previous image of this device, this option writes ZENworks Control Center object identity information as contained in the image to the new hard drive's Image Safe Data location, which allows the device to retain its ZENworks Control Center object.

  However, if the image contained in this bundle was not previously made from this device, it receives the new ZENworks Control Center object that is defined in the image.

  If you do not select this option and the device that this Preboot bundle is applied to has been given a new hard drive to boot from, then a new ZENworks Control Center object is created according to your ZENworks Management Zone configuration for non-registered devices.

8 Click *Next* to display the Summary page.

9 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Click to perform the following tasks before creating the bundle:

- Specify device assignments for this bundle
- Specify groups for this bundle

Continue with to assign the bundle and complete the wizard.

Finish: Creates the kickstart bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When any device assigned to the kickstart bundle boots, the bundle's Red Hat installation work is performed on the device.

30.4 Configuring ZENworks Script Bundles

A ZENworks Script bundle can contain any ZENworks script.

Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a ZENworks Script bundle and assign devices to the bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New > Bundle* to start the Create New Bundle Wizard:

3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.

4 On the Select Preboot Bundle Type page, select *ZENworks Script bundle*, then click *Next* to display the Set General Information page:

5 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Script bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the ZENworks Script bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this ZENworks Script bundle.

6 Click *Next* to display the Preboot Bundle Creation page:

Bundles > Create New Bundle

Create New Bundle	ZENworks Script 1	?
🔧 Step 4: Preboot Bundle Creation		

Configure the preboot information

Script Text:

```
#!/bin/sh
```

☐ Use IP Address from the preboot bundle rather than from Image Safe Data
☐ Use Identity Information from the preboot bundle rather than from Image Safe Data

[<< Back]   [Next >>]   [Cancel]
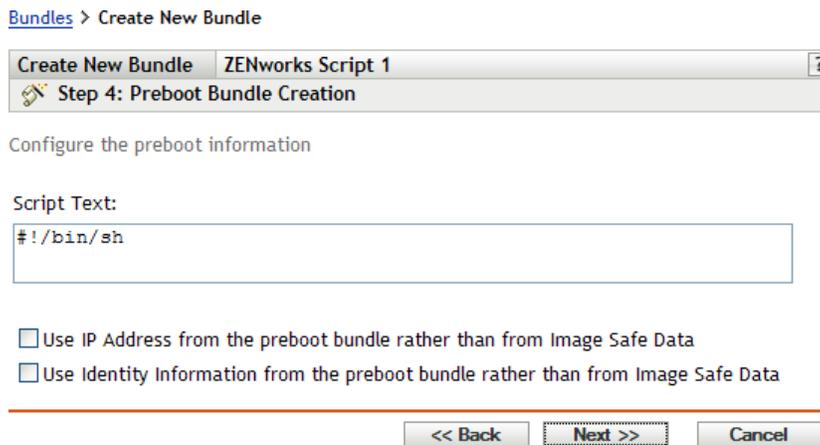
7 Fill in the fields:

Script text: Specify the text of the ZENworks script. The script is restricted to doing preboot work prior to the device booting.

IMPORTANT: If you provide any paths to executables in a script, make sure that you provide the full path, or the executable might not run.

For information on using this bundle to perform scripted imaging, see "Imaging a Device Using a Script" on page 414.

A device's Image Safe Data, such as the device's IP address and other identity information that is defined for its ZENworks Control Center object, is contained on the hard drive that the device boots from. This information can be lost if that hard drive needs to be replaced. However, the following options allow you to retain a device's IP address and other identity information when replacing the hard drive.

These options are only applicable when this Preboot bundle is applied to a specific device. The image used in this bundle must contain the device's previous IP address and ZENworks Control Center object information.

(Optional) Select one or both of the following options:

   ◆ **Use the IP Address from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

Use this option if you have previously taken an image of the device and are using that image with this Preboot bundle. This option causes the imaging process to write the device's IP address that is contained in this image to the Image Safe Data location on the replacement hard drive.

Do not use this option if the image being used for this bundle was not previously made from this device.

If you do not select this option, then:

- If the device that this Preboot bundle is applied to is still using its primary hard drive to boot from, the IP address in its Image Safe Data continues to be used.

  or

- If the device that this Preboot bundle is applied to has been given a new hard drive to boot from, but you do not have a previous image of the old hard drive, then the IP address is assigned according to your ZENworks Management Zone configuration for non-registered devices.

- **Use the Identity Information from Content in the Preboot Bundle Rather Than from the Device's Image Safe Data**

  If you are using a previous image of this device, this option writes ZENworks Control Center object identity information as contained in the image to the new hard drive's Image Safe Data location, which allows the device to retain its ZENworks Control Center object.

  However, if the image contained in this bundle was not previously made from this device, it receives the new ZENworks Control Center object that is defined in the image.

  If you do not select this option and the device that this Preboot bundle is applied to has been given a new hard drive to boot from, then a new ZENworks Control Center object is created according to your ZENworks Management Zone configuration for non-registered devices.

8 Click *Next* to display the Summary page.

9 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Click to perform the following tasks before creating the bundle:

- Specify device assignments for this bundle
- Specify groups for this bundle

Continue with Section 30.6, "Assigning Unassigned Preboot Bundles," on page 461 to assign the bundle and complete the wizard.

Finish: Creates the ZENworks Script bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When a device assigned to the ZENworks Script bundle boots, the bundle's work is performed on the device before its operating system starts.

30.5 Using Dell Configuration Bundles

When a server boots, the ZENworks Dell Configuration bundle is executed on the server before the operating system boots. The Dell Configuration bundle is used in server provisioning to do the following:

- Use scripts and files to configure the BIOS, BMC, RAID, and DRAC
- Install a Dell utility partition
- Overwrite an existing Dell utility partition
- Update the files in an existing Dell utility partition
- Execute another Preboot bundle to install an operating system after updating the Dell device

For more information on the Dell OpenManage Deployment Toolkit (DTK), see the guides (`dtk20cli.pdf` and `dtk20ug.pdf`) contained in the DTK download.

In using Dell Configuration bundles, you should first create the Dell Configuration scripts and files, if they are needed, then create the Dell Configuration bundle:

- Section 30.5.1, "Creating Dell Configuration Scripts and Files," on page 454
- Section 30.5.2, "Creating Dell Configuration Bundles," on page 457

IMPORTANT: If a newer version of the DTK is available from Dell, and you want to use it for your Dell Configuration bundle work, see Appendix G, "Upgrading the Dell DTK," on page 663 for instructions on updating the DTK.

30.5.1 Creating Dell Configuration Scripts and Files

When you create a Dell Configuration bundle you might need specialized scripts or files to already exist, depending on which settings you employ in the bundle. Novell recommends that you follow the instructions in the Dell DTK documentation to create the necessary configuration files and scripts.

To help do this, ZENworks provides the Dell DTK (Maintenance Mode) option when booting a Preboot Services Imaging CD, which provides a complete DTK environment where configuration scripts and files can be created and tested. This environment is identical to the environment provided by booting the Dell DTK CD, but includes additional configuration information needed for placing files and scripts on the ZENworks servers.

After you create them, you need to copy all of the scripts and files to be used in the Dell Configuration bundle to the ZENworks TFTP server. You will need to do this before you reboot the device that you used to create the scripts and files, because the scripts and files are created in a RAM drive, which is replaced in rebooting.

The DTK environment provides a TFTP client utility that allows you to upload your configuration files directly to your ZENworks servers, because the Dell DTK (Maintenance Mode) also provides an environment variable ($TFTPIP) that always resolves to the IP address of the TFTP service on the ZENworks server.

IMPORTANT: In the following sections you are instructed to upload files to your ZENworks TFPT server. Because this is not enabled by default, you must first configure TFTP before attempting to upload those files.

To create the scripts and files that you might need when creating a Dell Configuration bundle:

- "Creating a BIOS/BMC/DRAC 5 Configuration File" on page 455
- "Creating a RAID Configuration Script" on page 456
- "Creating a DRAC 4 or Earlier Configuration File" on page 456

Creating a BIOS/BMC/DRAC 5 Configuration File

This bundle option only configures the BIOS, BMC, or DRAC 5; it cannot be used to update them. Updates are done using a Dell Update Package.

1 Make sure the novell-proxydhcp daemon is running on a server in your network.

This service must be available so that the device's PXE can access files from the ZENworks server, such as the Preboot Services Menu and Dell DTK (Maintenance Mode).

2 Boot a Dell device that is PXE-enabled and press the Ctrl-Alt keys during booting.

Press these keys when a string starting with "Novell ..." is displayed during the boot process.

IMPORTANT: Choose the correct device to boot for creating the BIOS, BMC, or DRAC 5 file. The devices to receive the update must be the same as the device you are using to configure the file. For example, if the boot device is a Dell 2950, then the configured file can only be used to update other Dell 2950 devices.

3 When the bash (#) prompt is displayed, auto-generate the file using the following command:

```
syscfg -o BIOS-BMC_filename
```

where `BIOS-BMC_filename` is the name of the BIOS or BMC file to be used. In Dell 9G devices, DRAC 5 is included in the BIOS, rather than a separate file.

WARNING: Do not reboot the device at this time, because the file you created is in a RAM drive. (You can safely reboot after you upload the file to the TFTP server.)

4 To upload the new configuration file to your ZENworks TFTP server, enter:

```
tftp -l local_BIOS-BMC_filename -r remote_BIOS-BMC_filename_and_path -p
$TFTPIP
```

where `local_BIOS-BMC_filename` is the name of the configuration file that you are saving, and `remote_BIOS-BMC_filename_and_path` is both the name and the location for where you want the file on your ZENworks server.

The path on the ZENworks server for the remote filename should be relative to the TFTP server's home path, because the remote file is placed in that location. The Dell Configuration bundle is designed to look for files relative to the TFTP server's home path.

5 Continue with the appropriate section:

- "Creating a RAID Configuration Script" on page 456
- "Creating a DRAC 4 or Earlier Configuration File" on page 456
- "Creating Dell Configuration Bundles" on page 457

Creating a RAID Configuration Script

This bundle option only configures RAID; it cannot be used to update it. Updates are done using a Dell Update Package.

1 Make sure the novell-proxydhcp daemon is running on a server in your network.

This service must be available so that the device's PXE can access files from the ZENworks server, such as the Preboot Services Menu and Dell DTK (Maintenance Mode).

2 Boot a Dell device that is PXE-enabled and press the Ctrl-Alt keys during booting.

Press these keys when a string starting with "Novell ..." is displayed during the boot process.

IMPORTANT: Choose the correct device to boot for creating the RAID script. The devices to receive the update must be the same as the device you are using to configure the script. For example, if the boot device is a Dell 2950, then the configured script can only be used to update other Dell 2950 devices.

---

3 When the bash (#) prompt is displayed, to edit the following sample script file, first make a copy of it where you have editing rights:

```
cp -a /opt/dell/toolkit/template/scripts /tmp
```

then to edit the copy:

```
vi /temp/scripts/raidcfg.sh
```

Modify the file as needed, then save the changes. You can save the file using any filename; however, the filename you save it as must be provided in the Dell Configuration bundle. Therefore, if you save to a different name, make a note of it.

WARNING: Do not reboot the device at this time, because the script you created is in a RAM drive. (You can safely reboot after you upload the script to the TFTP server.)

---

4 To upload the new configuration script to your ZENworks TFTP server, enter:

```
tftp -l local_RAID_filename -r remote_RAID_filename_and_path -p $TFTPIP
```

where *local_RAID_filename* is the name of the configuration script that you are saving, and *remote_RAID_filename_and_path* is both the name and the location for where you want the script on your ZENworks server.

The path on the ZENworks server for the remote filename should be relative to the TFTP server's home path, because the remote script is placed in that location. The Dell Configuration bundle is designed to look for scripts relative to the TFTP server's home path.

5 Continue with the appropriate section:

Creating a DRAC 4 or Earlier Configuration File

This bundle option only configures DRAC 4 or earlier; it cannot be used to update it. Updates are done using a Dell Update Package.

Do this only for Dell devices that are 8G or earlier.

1 Make sure the novell-proxydhcp daemon is running on a server in your network.

This service must be available so that the device's PXE can access files from the ZENworks server, such as the Preboot Services Menu and Dell DTK (Maintenance Mode).

2 Boot a Dell device that is PXE-enabled and press the Ctrl-Alt keys during booting.

Press these keys when a string starting with "Novell ..." is displayed during the boot process.

IMPORTANT: Choose the correct device to boot for creating the DRAC 4 file. The devices to receive the update must be the same as the device you are using to configure the file. For example, if the boot device is a Dell 2950, then the configured file can only be used to update other Dell 2950 devices.

---

3 When the bash (#) prompt is displayed, execute the following script:

```
/opt/dell/toolkit/template/scripts/raccap.sh
```

4 While the script is running, provide a name for the DRAC 4 or earlier configuration file.

The DRAC configuration file is saved in your current directory.

WARNING: Do not reboot the device at this time, because the file you created is in a RAM drive. (You can safely reboot after you upload the file to the TFTP server.)

---

5 To upload the new configuration file to your ZENworks TFTP server, enter:

```
tftp -l local_DRAC_filename -r remote_DRAC_filename_and_path -p $TFTPIP
```

where *local_DRAC_filename* is the name of the configuration file that you are saving, and *remote_DRAC_filename_and_path* is both the name and the location for where you want the file on your ZENworks server.

However, the path on the ZENworks server for the remote filename should be relative to the TFTP server's home path, because the remote file is placed in that location. The Dell Configuration bundle is designed to look for files relative to the TFTP server's home path.

6 Continue with Section 30.5.2, "Creating Dell Configuration Bundles," on page 457.

30.5.2 Creating Dell Configuration Bundles

The Dell Configuration bundle allows you to configure certain Dell devices with specific BIOS/BMC/DRAC 5, RAID, DRAC 4 or earlier, and Dell utility partition configurations, and then have a Preboot bundle executed to image the device with an operating system.

To create a Dell Configuration bundle:

1 In the ZENworks Control Center, click the *Bundles* tab.

2 Click *New > Bundle* to start the Create New Bundle Wizard:

3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.

4 On the Select Preboot Bundle Type page, select *Dell Configuration bundle*, then click *Next* to display the Set General Information page:

5 Fill in the fields:

Name: (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed in, you should develop a naming scheme that differentiates the Dell Configuration bundles that are listed together in a folder.

For more information, see Appendix C, "Naming Conventions in the ZENworks Control Center," on page 605.

Folder: Browse for the location where you want the Dell Configuration bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

Description: Provide a description to help you later recognize the exact purpose of this Dell Configuration bundle.

6 Click *Next* to display the Dell Configuration Bundle Options page:

Bundles > Create New Bundle

Create New Bundle	Dell Configuration 2	?

Step 4: Dell Config Bundle Options

Enter options for creating the Dell Configuration bundle. All files and scripts should be relative to the TFTP directory.

☐ BIOS/BMC/DRAC 5 Configuration File: [   ]
☐ RAID Configuration Script: [   ]
☐ DRAC Configuration File: [   ]
  (not for use with DRAC 5 systems)
☐ Create Dell Utility Partition

Partition Size: [   ]
  (size in MegaBytes. i.e.: 32)

Target Disk: [   ]
  (example: /dev/hda)

File: [   ]
  (example: /dell-dtk/pe1850/upimg.bin)

  ☐ Overwrite existing Dell Utility Partition
☐ Preboot Bundle: [   ]
  (Preboot bundle will be applied after the selected configuration steps have been taken.)

[<< Back] [Next >>] [Cancel]

7 Fill in the fields:

BIOS/BMC/DRAC 5 Configuration File: To configure the BIOS, BMS, or DRAC 5, specify the path and filename of the configuration file, relative to the TFTP server's home path. Do not specify the TFTP location or any of the path that precedes it.

For information on creating this file, see Section 30.5.1, "Creating Dell Configuration Scripts and Files," on page 454.

RAID Configuration Script: To configure RAID, specify the path and filename of the configuration script, relative to the TFTP server's home path. Do not specify the TFTP location or any of the path that precedes it.

For information on creating this script, see Section 30.5.1, "Creating Dell Configuration Scripts and Files," on page 454.

DRAC Configuration File: To configure DRAC 4 or earlier, specify the path and filename of the configuration file, relative to the TFTP server's home path. Do not specify the TFTP location or any of the path that precedes it.

For information on creating this file, see Section 30.5.1, "Creating Dell Configuration Scripts and Files," on page 454.

Create Dell Utility Partition: To create a new Dell utility partition, select this check box, then fill in the fields:

WARNING: If you use this option, all existing partitions on the identified disk are replaced by the Dell utility partition. However, you can select the *Overwrite Existing Dell Utility Partition* check box to update only an existing Dell utility partition. In that case, all existing partitions are kept and the Dell server diagnostics utility files are written to the existing Dell utility partition using the entry that you provide in the *File* field.

- ◆ **Partition Size:** This partition requires 32 MB for the Dell server diagnostics utilities. Use this field only when creating a new Dell utility partition.

- ◆ **Target Disk:** This is the disk's identifier, such as `/dev/hda`. This ID is used to determine the disk for creating the new partition, or for updating an existing partition.

- ◆ **File:** Specify the path to the Dell utility partition file. The path must be relative to the TFTP server's home path.

  The file is written to the partition in the process of creating a new partition or when updating an existing partition.

  Dell utility partition files are contained on the *Dell Installation and Server Management* CD. For example, for a PowerEdge 1850 system, the file is at `d:\server_assistant\pe1850\upimg.bin`. Copy the necessary files from the CD to a path relative to the TFTP server's home path for use in this field.

- ◆ **Overwrite Existing Dell Utility Partition:** If a Dell utility partition already exists on the selected target disk, select this check box to simply update the partition with the newer utility files, instead of replacing the partition.

You cannot use a ZENworks partition for the same purpose as the Dell utility partition. However, both a Dell utility partition and a ZENworks partition can exist on the same server, each being used for its own purposes.

IMPORTANT: The Dell utility partition relies on its version of the MBR (master boot record) to function correctly. Grub also uses the MBR for its boot loader. If you install the Dell utility partition, then installing the Linux operating system, the Dell version of the MBR is overwritten by the grub version. Do one of the following to resolve this issue:

◆**Grub on the boot partition:** When installing Linux, you can select to put grub on the boot partition, rather than in the MBR (the default). However, you must set this boot partition as *Active*. Then, when the Dell utility partition writes its MBR information, it does not conflict with grub, because its boot loader is not located in the same place.

◆**Grub menu item for the Dell utility partition:** If the devices are not using the Dell utility partition boot loader, you can use grub in the MBR (the default) and still provide an F10 menu option to the Dell utility partition. Edit the `/boot/grub/menu.1st` file and add the following lines:

```
title Dell Utility Partition
chainloader (hd0,0)+1
```

Preboot Bundle: This option allows Preboot Services to complete the above configurations, then immediately apply a destructive image or installation script from another Preboot bundle. Select this option, then browse for or specify the path and filename of the Preboot bundle.

8 Click *Next* to display the Summary page.

9 Review the configuration, then click one of the following:

Back: Allows you to make changes after reviewing the summary.

Next: Click to perform the following tasks before creating the bundle:

- ◆ Specify device assignments for this bundle
- ◆ Specify groups for this bundle

Continue with Section 30.6, "Assigning Unassigned Preboot Bundles," on page 461 to assign the bundle and complete the wizard.

Finish: Creates the Dell Configuration bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When a device assigned to the Dell Configuration bundle boots, the bundle's work is performed on the device before its operating system starts.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

For more information on the Dell DTK, see the Dell guides (`dtk20cli.pdf` and `dtk20ug.pdf`) contained in the DTK download.

30.6 Assigning Unassigned Preboot Bundles

IMPORTANT: If you are assigning a Preboot bundle that has been created on a management device inside the firewall to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

---

1 If you click *Next* on the Summary page of a wizard, or if you access this page through the *Devices* or *Bundles* tabs in the ZENworks Control Center, the Bundle Assignments page is displayed:

Create New Bundle | Script Bundle X | ?
Step 6: Bundle Assignments

Specify the assignments for this bundle:

Add Remove
☐ **Name** | **In Folder**
No items selected, click add to select items

<< Back | Next >> | Cancel
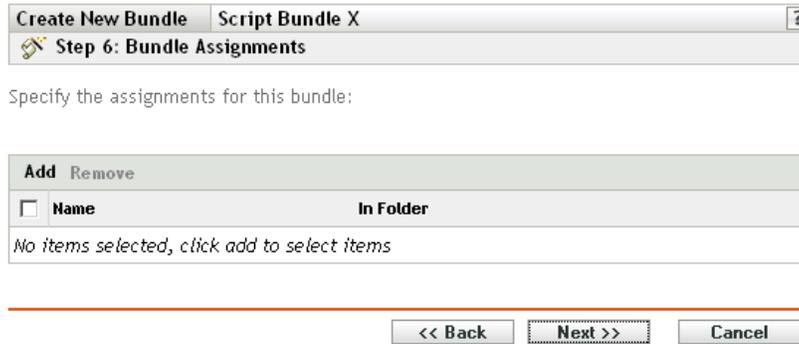
The wizard's step number depends on where you access the wizard from. The examples in these instructions are based on accessing this wizard when creating a ZENworks Script bundle.

2 Click *Add* to display the Select Assignments dialog box:

Select Assignments | ✕

Look in: | Selected:
/Devices | Remove | Name | Folder
Item name: | Items of type:
* | All Types

Name ▲ | **Type**
📁 Servers | Folder
📁 Workstations | Folder

◄ ► | 1 - 2 of 2 | show 10 ▼ items
2 Items | Select All | 0 Items Selected | Remove All

OK | Cancel
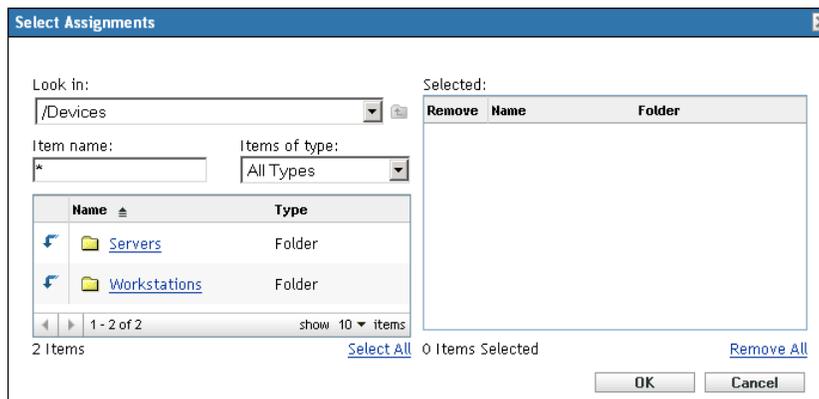
3 Browse for and select the devices that you want to be assigned to this bundle, then click *OK*.

You can select individual devices, or the *Servers* or *Workstations* folders containing such devices, or mixtures of folders and devices.

4 Click *Next* to display the Bundle Groups page:

Create New Bundle | Script Bundle X | ?
Step 7: Bundle Groups

Specify the groups for this bundle:

Add Remove
☐ **Name** | **In Folder**
No items selected, click add to select items

<< Back | Next >> | Cancel
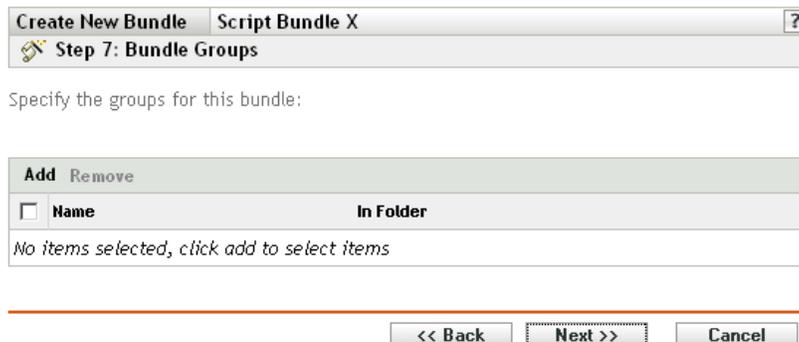
This is optional. You can click *Next* to display the Summary page without assigning a bundle group. In this case, skip to Step 8.

5 Click *Add* to display the Select Groups dialog box:
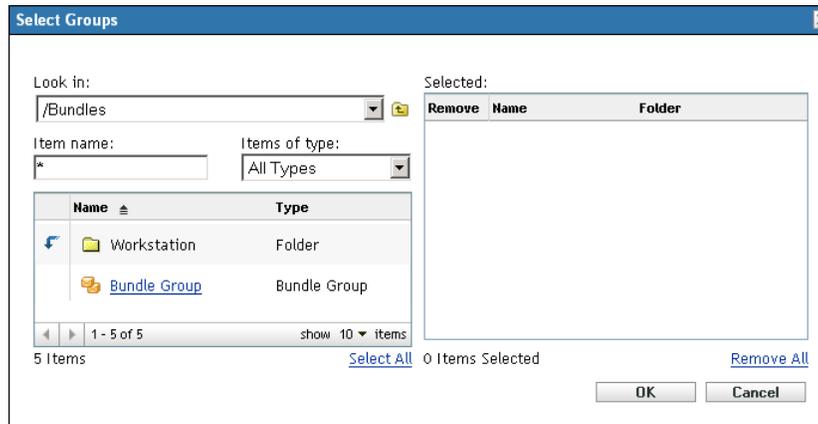
6 Browse for and select the groups that you want to be assigned to this bundle, then click *OK*.

You can select individual groups, including browsing the folders containing groups.

7 Click *Next* to display the Summary page.

8 Review the configuration, then click one of the following:

Back: If necessary, use this to make changes before finishing.

Finish: Click to create the bundle and assign the devices or groups to the bundle when it is created.

30.7 Editing Preboot Services Work

The Edit Preboot Work page allows you to view all images that are recently applied to the selected device, and the image that is currently assigned (known as its "effective" image).

To edit a server's or workstation's Preboot Services work:

1 In the ZENworks Control Center, click the *Devices* tab to display the Devices page:

2 Click *Servers* or *Workstations*, then select a device to display the page with the Preboot Work section:

3 In the Preboot Work section, click *Advanced*.

This starts the Edit Preboot Work Wizard:

4 In the Preboot Work section, select one of the following from the drop-down list for the *Scheduled work* field:

Do nothing: Continue with Step 5.

Apply Preboot bundle: Continue with Step 6.

Take an image: Continue with Step 7.

5 If you select *Do nothing*, review the image files, then skip to Step 8.

The Applied Image Files section displays the image files most recently applied to this device.

6 If you select *Apply Preboot bundle*, fill in the field under Bundle to Apply, then skip to Step 8:

Bundle: Select or specify the bundle. Its bundle name, folder, and description are displayed.

The *Bundle* field displays the currently effective bundle. You can select the bundle to apply from the drop-down list, which changes the effective bundle for the device.

The next time the device boots, or when you manually apply a Preboot bundle (such as from a ZENworks imaging CD or DVD), the selected bundle is applied.

7 If you select *Take an image*, fill in the fields, then continue with Step 8:

The image is taken the next time the device boots, or when you manually apply a Preboot bundle, such as from a ZENworks imaging CD or DVD.

Server and path of new image file: Browse for or enter the full path to where you want the image file saved.

Image compression options: Select one:

- ◆ **Balanced:** Automatically balances compression between an average of the reimaging speed and the available disk space for the image file.

- ◆ **Optimize for speed:** Optimizes the compression to allow for the fastest reimaging time. Use this option if CPU speed is an issue.

- ◆ **Optimize for space:** Optimizes the compression to minimize the image file's size to conserve disk space. This can cause reimaging to take longer.

8 Click *OK* to exit the wizard.

Your changes should be displayed in the Preboot Work section for the device.

Imaging Utilities and Components

31

The following sections provide reference information on Novell® ZENworks® Linux Management imaging utilities, commands, and configuration settings.

31.1 Starting Image Explorer

There are no command line parameters for the Image Explorer utility.

1 To start Image Explorer, run the following file:

```
/opt/novell/zenworks/preboot/bin/zmgexp
```

31.2 Determining the Image Explorer Version

To determine which version of Image Explorer you are using:

1 Click *Help > About*.

31.3 Image Explorer versus Linux Konquerer

Although ZENworks Imaging Explorer looks and functions like Linux Konquerer in most situations, some functionality differences exist between the two programs. The following describes the key differences between ZENworks Image Explorer and Linux Konquerer:

- **Replacing Files in an Image:** During the life cycle of an image, files might be deleted or updated through Image Explorer. When you replace an existing file in an image by using Image Explorer, the original file is not deleted from the image. Image Explorer purges only deleted files; it does not purge files that have been updated.

  When files are added to an image where the file already exists, Image Explorer appends the entry to the end of the image. When images are restored, all files that have been previously updated are sequentially restored.

  To avoid performance problems, you should manually delete and purge each instance of a duplicate file in order to have the duplicates purged from the image. In Linux Konquerer, replaced files are automatically deleted.

◆ **Dragging Files from Image Explorer:** You cannot drag files from Image Explorer in order to extract them, which you can do in Linux Konquerer. However, you can drag and drop files and folders into an image by using Image Explorer.

31.4 Opening an Image

1 Start Image Explorer.

2 Browse for and select the image file.

Large image files might take a few moments to open.

31.5 Saving Image Changes and Exiting the Utility

To save your changes when exiting the utility:

1 Click *File > Save* or *Save As*.

2 Browse for and save the image file in .zmg format.

3 Click *File > Exit* to close the utility.

31.6 Managing Image Properties

You can view the properties of an image file or any item in its content, including modifying some of the properties:

31.6.1 Viewing and Modifying the Properties of the Image File

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select the top line of the opened image file.

This is the line that displays the path to the .zmg file.

4 Click *File > Properties*.

You can also right-click the top line, then select *Properties*.

5 (Optional) Fill in the fields:

Description: Specify useful information, such as its purpose or its important content.

Author: Specify the author of this version of the image.

Comments: Specify any information that is helpful.

6 Save the image file to save your properties changes.

7 To close the properties dialog box, click *OK*.

31.6.2 Viewing the Properties of an Image File Item

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select a partition, directory, or file in the image.

For other information on a partition's properties, see Section 31.6.3, "Changing a Partition's Size," on page 469.

4 Click *File > Properties*.

You can also right-click the item, then select *Properties*.

5 To close the properties dialog box, click *OK*.

31.6.3 Changing a Partition's Size

You can change a partition's size for the next time the image is applied to a device. You can edit this value for base images only; you cannot edit this value for add-on images.

If the number that you specify in the *Original Size* text box exceeds the size of the target hard drive, ZENworks automatically uses the entire disk. Therefore, you can specify a value larger than exists on the target device.

However, if you specify a smaller disk space size than is on the target device, only that amount of disk space is used, so the remaining disk space is unused. For example, if you create a base image of a device with a 20 GB hard drive and you want to then place that image on a new device with a 60 GB hard drive, 40 GB of that drive is unused.

You cannot decrease the number in the *Original Size* text box to a smaller value that what is shown in the *Minimum Size* text box.

To modify the partition's size:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select a partition.

4 Click *File > Properties*.

You can also right-click the partition, then select *Properties*.

5 In the *Original Size* field, specify the new partition size.

6 Click *OK* to save the change.

This only saves the partition size change. You must save the image file for it to be in effect the next time the image is applied.

31.7 Image File Operations

You can do the following with an image file:

◆ Section 31.7.1, "Compressing an Image File," on page 470

31.7.1 Compressing an Image File

You can compress an uncompressed image (including images created by previous versions of ZENworks) by 40 to 60 percent of the original file size.

You can compress an image in two ways:

- "Compressing an Opened Image File" on page 470
- "Compressing an Unopened Image File" on page 471

Compressing an Opened Image File

Use this dialog box to set compression options so that it takes less time to restore the image file or less space to store the file on your Imaging server.

IMPORTANT: If you have used *Delete* to hide files in the image, they are removed from the image during compression.

To compress the image file:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Click *File > Compress Image*.

4 Fill in the fields:

Image File to Compress: Specifies the name of the existing imaging file to compress.

Save Compressed Image As: Click the browse button next to this field to specify the location and filename under which to save the image.

Compression Level: Specify an image-compression level:

- **Compress for Speed:** Takes the least amount of time to compress but creates the largest compressed image file.
- **Balanced Compression:** Represents a compromise between compression time and image file size. This option is used by default when an image is created.
- **Compress for Size:** Creates the smallest image file but takes longer to compress.

5 Click *Compress* to compress the image file, using the settings you specified.

Compressing an Unopened Image File

Use this dialog box to set compression options to quickly compress an image file without waiting for the file to fully load into Image Explorer.

To quickly compress an image file:

1 Click *Tools* > *QuickCompress*.

2 Fill in the fields:

Image File to Compress: Specify or browse to an existing imaging file to compress.

Save Compressed Image As: Specify the location and filename under which to save the image, or click the browse button next to this field to locate and select it.

Compression Level: Specify an image-compression level:

- ◆ **Compress for Speed:** Takes the least amount of time to compress but creates the largest compressed image file.
- ◆ **Balanced Compression:** Represents a compromise between compression time and image file size. This option is used by default when an image is created.
- ◆ **Compress for Size:** Creates the smallest image file but takes longer to compress.

3 Click *Compress* to compress the image file using the settings you specified.

31.7.2 Splitting an Image

You can split an image file into separate files so that you can span the entire image across several CDs or DVDs.

When you split a device image and span it across several CDs or DVDs, you are essentially creating a base image on the first CD or DVD. The remaining CDs or DVDs are add-on images.

Because images are split by placing individual files into different images, an image cannot be split if it contains any single file that is larger than the specified maximum file size.

To restore a device image that has been spanned across several CDs or DVDs you should restore the first CD or DVD before restoring the remaining CDs or DVDs containing the add-on images. For more information, see "Manually Putting an Image on a Device" on page 420.

Restoring split Images is done using bundles, such as restoring a base plus add-ons. For more information, see "Creating an Add-On Image" on page 419.

To split an image:

1 Click *Tools* > *Split Image*.

2 Fill in the fields:

Image File to Split: Enter or browse to an existing base image file to split.

Directory to Store Split Images: Specify the location and filename under which to save the split-image files, or click the browse button next to this field to locate and select it.

The split-image files are named automatically. For example, if you enter `image.zmg` in the *Image File to Split* field, the first split-image file is named `image_base.zmg`, the second file is named `image_a1.zmg`, the third file is named `image_a2.zmg`, and so forth. The `image_base.zmg` file contains files that allow the device to boot to the operating system. The add-on images (`image_a1.zmg`, `image_a2.zmg`, etc.) contain additional files.

Maximum Split File Size _ MB: Specify the maximum size of each split-image file. Depending on the size of the original image and the number you enter in this field, ZENworks creates as many files as necessary to split the entire image into separate split-image files.

3 To split the image file into as many files as necessary, using the settings you specified, click *Split*.

31.7.3 Hiding and Removing Content in the Image File

You can hide a directory or file from being used when the image is applied to a device. You can also permanently remove hidden or excluded directories and files from an image file.

Hiding Directories or Files in the Image

You can hide directories or files so that they are not used when the image is applied to a device. This enables you save their existence so that you can later unhide them to be applied to the imaged device.

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select the directories and files to be hidden.

IMPORTANT: When editing a base image, do not hide BPB files or the device won't be able to boot the new operating system after receiving the image.

4 Click *Image > Delete*.

You can also right-click the selected directories and files, then select *Delete*.

Deleting a file in the Image Explorer merely marks it for deletion; it can still be retrieved. A file marked as deleted is not removed from the image until the image is purged; files and folders marked as deleted are not restored during imaging.

Unhiding Directories or Files in the Image

You can unhide directories or files so that they are available when the image is applied to a device.

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select the directories and files that were previously hidden that you want to unhide.

4 Click *Image > Undelete*.

You can also right-click the selected directories and files, then select *Undelete*.

This makes them available in the image when it is applied to a device.

Removing Hidden Directories and Files from the Image File

To permanently remove hidden directories and files from the open image in order to create a different version of the image file:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Click *File > Purge Files*.

4 Browse to the image filename or specify a new image filename, then click *OK*.

You can save over the original image file to make this modification, or create another version of the image with the hidden directories and files removed.

31.7.4 Configuring File Sets

To configure a file set:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Select the directories and files in the image that you want excluded from the image.

Ways that you can select content:

- ◆ Click a single file in the right pane.

- ◆ Use the Shift and Ctrl keys to select multiple files in the right pane.

- ◆ Individually select partitions and directories in the left pane. Any partition or directory that you select includes everything under it.

- ◆ Select a partition or directory in the left pane, then click *Edit > Select All* to select all files listed in the right pane. Subdirectories are not included.

4 Do one of the following to exclude the selected files and directories from the image:

- ◆ Click *Edit > File Sets*, then select one of the options from *Exclude from Set 1* through *Exclude from Set 10*.

  You can also right-click your selection to access the *File Sets* menu options.

- ◆ Click *Edit > File Sets > Edit* to open the File Sets dialog box, do the following as applicable, then click *OK* to exit the dialog box:

  - ◆ **Exclude Specific Items:** To exclude the selected directories and files from specific file set numbers, click the check box for each set number.

    This causes all selected directories and files to be excluded from the image for any Image bundle assigned to the specified file set numbers.

  - ◆ **Exclude All Items:** To exclude the selected directories and files from all file sets of this image, click *Exclude All*.

    This causes all selected directories and files to be excluded from the image for any Image bundle assigned to any file set number.

◆ **Include All Items:** To clear all of the check boxes, click *Exclude None*.

This allows all selected directories and files to be included in the image.

You can also right-click your selection to access the *File Sets* menu options.

31.7.5 Extracting Content as Files

To extract a file or directory from the open image and copy it to a directory:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Click *File > Save*.

If any changes have been made, this must be done before you can extract the information.

4 Click *File > Extract > As Files*.

5 Browse to and select a directory for the files, then click *OK*.

31.7.6 Extracting Content as an Add-on Image

To extract a file or directory from the open image as an add-on image:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Click *File > Save*.

If any changes have been made, this must be done before you can extract the information.

4 Click *File > Extract > As Add-on Image*.

5 Specify the name and location of the new add-on image, then click *OK*.

31.7.7 Creating an Add-on Image

You can create an add-on image from existing directories and files on your system and add partitions to the new add-on image.

1 Click *File > New*.

2 To add a partition, click the root of the image, click *Image*, then click *Create Partition*.

You cannot add a partition to an existing image.

3 Do any of the following to add content:

◆ Browse to the directories and files you want the add-on image to contain, then drag or copy the directories and files into the right pane from your file browser.

◆ Click *Image > Add Files* and select the files to be added.

◆ Click *Image > Add Directory* and select the directories to be added.

◆ Click the *Add Directory* icon and select the directories to be added.

◆ Click the *Add File* icon and select the files to be added.

4 Click *File > Save As*, then specify the filename of the add-on image, including the `.zmg` filename extension.

31.8 Modifying Image Content

You can modify the content of an image file in the following ways:

31.8.1 Adding Directories and Files

To add directories and files to the open image:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Do any of the following to add content:

- Browse for the directories and files you want the add-on image to contain, then drag or copy the directories and files into the right pane from your file browser.
- Click *Image > Add Files* and select the files to be added.
- Click *Image > Add Directory* and select the directories to be added.
- Click the *Add Directory* icon and select the directories to be added.
- Click the *Add File* icon and select the files to be added.

4 Brows for and select the files or directory, then click *Add* or *OK*.

You can select multiple files using the Shift and Ctrl keys.

5 Repeat these steps as necessary.

31.8.2 Creating a New Directory

To create a directory in the open image:

1 Click *File > Open*.

2 Browse for and select the image file.

Large image files might take a few moments to open.

3 Browse for the partition or directory in the left pane where you want to create the directory, then click *Image > Create Directory*.

You can also click the *New Directory* icon.

4 Specify the name of the directory, then click *OK*.

31.8.3 Creating a New Partition

New partitions cannot be created in an existing base or add-on image that you opened for editing. You can only create a new partition in a new image file. For more information, see "Adding Partitions" on page 476.

31.8.4 Resizing a Partition

You can resize the partitions in a base image, but not an add-on image. For more information, see "Changing a Partition's Size" on page 469.

31.9 Creating a New Image File

Do the following to create a new image file:

- Section 31.9.1, "Creating, Configuring, and Saving the New Image File," on page 476
- Section 31.9.2, "Selecting New Image File Options," on page 476

31.9.1 Creating, Configuring, and Saving the New Image File

1 Click *File > New*.

2 Configure the new image file using the instructions in "Selecting New Image File Options" on page 476, then return to Step 3.

3 To save the new image file, click *Save As*.

4 Specify an image filename, including the .zmg filename extension, then click *Save*.

31.9.2 Selecting New Image File Options

You can do the following in this new image file:

- "Adding Partitions" on page 476
- "Adding Content" on page 477
- "Configuring File Sets" on page 477

Adding Partitions

1 Select the top line of the new image file.

This is the line that will display the path to the new .zmg file when you save it.

2 Click *Image > Create Partition*.

3 Repeat Step 1 through Step 2 as necessary.

4 To add content to the partitions, continue with "Adding Content" on page 477.

Adding Content

1 See Section 31.8, "Modifying Image Content," on page 475 for instructions on adding new content.

2 Continue with "Configuring File Sets" on page 477, or return to Step 3 in "Creating, Configuring, and Saving the New Image File" on page 476.

Configuring File Sets

1 See "Configuring File Sets" on page 473 for instructions on configuring file sets.

2 Return to Step 3 in "Creating, Configuring, and Saving the New Image File" on page 476.

Hardware and Software Inventory

VII

The following sections provide information on Novell® ZENworks® Linux Management hardware and software inventory features:

Inventory Overview

<div style="text-align: right; font-size: 3em;">32</div>

The Server Inventory component of Novell® ZENworks® Linux Management allows you to collect hardware and software inventory information from local and remote servers or workstations of your enterprise. This inventory information is scanned and stored in a database that can be accessed by the ZENworks administrator.

The Inventory scanning capability of ZENworks Linux Management performs the following tasks:

- Collects hardware and software inventory information from workstations and servers managed within your enterprise.
- Stores the inventory information in a database that can be accessed by the ZENworks administrator.
- Rolls up the hardware inventory data from the database to the ZENworks 7 Server Management database or the ZENworks 7 Desktop Management Inventory database so you can view the inventory data at the enterprise level.

Reviewing the Device Inventory

33

From the ZENworks® Control Center you can view the complete hardware and software inventory of servers and workstations. This section discusses the following topics:

33.1 Accessing the Device Inventory

To view a device's hardware and software inventory:

1 In the ZENworks Control Center, click the *Devices* tab.

2 Navigate the folder structure to locate the desired device, then click the device to show its details.

3 Click the *Inventory* tab.

Refer to the following sections for descriptions of the inventory information:

33.2 Reviewing Device Inventory Summaries

The Inventory page provides the following inventory information about each device:

Table 33-1 *Inventory Information for Devices*

Scan Data Item	Description
Last Scan Date	The last time the selected managed device was scanned for inventory information
Alias	The alternative name for the managed device
Host Name	The network name that should resolve to the managed device's IP address
Mac Address	The hardware address of the managed device's network interface card
IP Address	The unique address of the managed device on the TCP/IP network
Subnet Mask	The network segment the managed device is on

Scan Data Item	Description
Location	The server location

33.3 Reviewing Hardware (General)

The Inventory page provides the following general information about the device's hardware. For detailed hardware information, see

Table 33-2 *General Information about Device Hardware*

Scan Data Item	Description
Asset Tag	The asset identification number assigned to the machine by the company
Serial Number	A unique number assigned to the machine by the manufacturer
Vendor	The product supplier, such as Dell or Compaq*
Model	Model name of the device provided by the manufacturer
Operating System	The operating system currently installed on the machine
OS Patch Level	The support pack version of the operating system currently installed on the device
Code Page	The selected character set of the machine
Visible Memory	Total physical memory available to the operating system
Virtual Memory	Amount of virtual memory assigned

33.4 Reviewing Software (General)

The Inventory page provides the following information about the device's software. Click *Bundles* (Details) or *Packages* (Details) or *Dell Applications* (Details) for detailed information about each.

Table 33-3 *General Information about Device Software*

Scan Data Item	Description
Bundles	Software bundled with the server
Packages	Additional software deployed on the server
Dell Applications	Dell applications installed on the selected managed device

33.5 Reviewing Hardware Details

The following table provides common device information that might be useful for troubleshooting. For detailed information about each device, click the hardware component name in the interface.

Table 33-4 *Common Device Information*

Inventory Item	Attributes	Description
Batteries	Name	Battery name.
	Manufacturer	Battery manufacturer name.
	Serial Number	Battery serial number.
	Chemistry	The battery chemistry, for example, lithium-ion or nickel metal hydride.
BIOS	Name	BIOS name.
	Manufacturer	BIOS manufacturer name.
	Version	The version or revision level of the BIOS.
Busses	Name	Bus type, such as PCI, ISA, and others.
	Description	Bus description.
CD ROMs	Name	CD-ROM name.
	Manufacturer	CD-ROM manufacturer.
Chassis	Name	Chassis name.
	Manufacturer	Chassis manufacturer.
	Asset Tag	A code for property and product identification.
	Serial Number	Serial number assigned by the manufacturer.
Dell Device	Name	Dell hardware name.
	Version	Dell version.
	Component ID	Dell Component ID.
	Dell PCI Information	Click for additional details.
	Dell Applications	Click for a list of all applications associated with this Dell device.
Desktop Monitors	Name	Monitor name. When a monitor is connected through a KVM (keyboard, video, mouse) switch, the system might pass two instances of the desktop monitor. This is because of manufacturing limitations for the device.
	Manufacturer	Monitor manufacturer.
	Model	Identifying information of the monitor.

Inventory Item	Attributes	Description
	Size	Monitor screen size.
Floppy Disks	Name	Floppy disk name.
	Capacity	Floppy disk capacity.
	Description	Floppy disk description.
Keyboards	Name	Keyboard brand name and model.
	Description	Description of the keyboard, such as interface, ergonomics, system requirements, and so on.
Logical Disks	Volume Label	Name of the logical disk volume.
	Filesystem Type	Type of file system, such as File Allocation Table (FAT).
	Filesystem Size	Drive's actual size in MB.
	Available Space	Available space on the logical disk.
Modems	Name	Modem name.
	Manufacturer	Modem manufacturer.
Motherboards	Name	Motherboard name.
	Manufacturer	Motherboard manufacturer name.
	Version	The version of the motherboard.
	Slots	The number of expansion slots in the motherboard for adding more memory, graphic capabilities, and support for special devices.
Network Adapters	Name	Network adapter name.
	Manufacturer	Network adapter manufacturer.
	Maximum Speed	Rate at which the information is transferred over the LAN.
	Mac Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.
Parallel Ports	Name	Port name.
	Description	Port description.
Physical Disks	Name	Disk name.
	Manufacturer	Disk manufacturer.
	Capacity	Capacity of the disk.
	Free Space	Remaining free space on the disk.

Inventory Item	Attributes	Description
Pointing Devices	Name	Pointing device name.
		When a pointing device is connected through a KVM (keyboard, video, mouse) switch, the system might not pass the correct name and configuration of the device, because of manufacturing limitations for the device.
	Buttons	Number of buttons.
	Description	Description of the pointing device.
Power Supplies	Name	Name of the power supply.
	Description	A description of the power supply.
Processors	Name	Processor name.
	Family	The name of the class or group to which the processor belongs, such as Pentium II, Pentium III, and others.
	Speed	The speed at which a microprocessor executes instructions. Every computer contains an internal clock that regulates the rate at which instructions are executed and that synchronizes all the various computer components. Clock speeds are expressed in megahertz (MHz) or gigahertz (GHz).
Serial Ports	Name	Serial port name.
	Description	Serial port description.
Sound Adapters	Name	Sound adapter name.
	Description	A description of the sound adapter.
Video Adapters	Name	Video adapter name.
	Manufacturer	Manufacturer name.

NOTE: For XEN Guest OS managed device, the inventory scanner does not scan for all the items listed in the Table 33-2, "General Information about Device Hardware," on page 484. It might scan and report only the following inventory items: Processor, Network Adapter, MotherBoard, Chassis, and BIOS.

33.6 Refreshing Device Inventory

Device inventory is broken down into three areas:

- Software
- Hardware
- System (disk size, usage, and operating system information)

Inventory data is refreshed in three ways:

1. At client (zmd) start up.

   - The device sends hardware and system information to the server where the device is registered.

   - A new software hash is calculated to check if there has been a change, for example, if a new package or bundle has been installed. If the hash has changed, the device sends the new software inventory to the server where the device is registered.

2. When new software in installed on a client, that software inventory information will be sent to the server immediately.

3. At a scheduled refresh, which refreshes data as described in the client start up above.

Device inventory is refreshed at start up and then every twenty-four hours by default. This schedule cannot be directly changed on the server side, but it can be changed on the client side using `rug refresh-interval-hardware` *time_in_second*s, `rug refresh-interval-software` *time_in_seconds*, and `rug refresh-interval-system` *time_in_seconds*. If you want to change the inventory refresh schedule for multiple managed devices, you can use a Remote Execute policy. For more information, see Section 16.6, "Remote Execute Policy," on page 164.

IMPORTANT: The Device Refresh Schedule setting does not affect refresh inventory information.

Rolling Up Hardware Inventory

34

You can roll up the hardware inventory data from the Novell® ZENworks® Linux Management database to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory database to view the inventory data at the enterprise level.

Review the following sections:

- Section 34.1, "Preparing to Roll Up Inventory," on page 489
- Section 34.2, "Configuring the Inventory Roll-Up Policy," on page 489
- Section 34.3, "Understanding the Roll-Up Process," on page 490
- Section 34.4, "Understanding the Components Involved in the Inventory Roll-Up," on page 491
- Section 34.5, "Viewing the Inventory Data Stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database," on page 492

34.1 Preparing to Roll Up Inventory

Ensure that the following prerequisites are met:

- ❑ ZENworks 7.3 Linux Management has been successfully installed.
- ❑ The hardware inventory data has been stored in the ZENworks Linux Management database.
- ❑ The ZEN Loader service is up and running on the ZENworks Linux Management server.
- ❑ The Inventory server and Inventory database components of ZENworks 7 Server Management or ZENworks 7 Desktop Management have been successfully installed and set up.
- ❑ One of the following roles for the ZENworks 7 Inventory server has been configured:
  - Root Server
  - Root Server with Workstations
  - Intermediate Server with Database
  - Intermediate Server with Database and Workstations
- ❑ The Inventory service is up and running on the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server.

34.2 Configuring the Inventory Roll-Up Policy

1 In the ZENworks Control Center, click *Configuration*.

2 In the *Management Zone Settings* pane, click the *Device Inventory* category.

3 In the *Inventory Roll-Up Settings* pane, do the following:

3a Specify the DNS name or the IP address of the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server to which you want to roll up the hardware inventory data.

3b Specify the time interval between roll-ups. By default, the time interval is 168 hrs.

4 Click *Apply*, then click *OK*.

34.3 Understanding the Roll-Up Process

ZENworks uses the following process to collect inventory and roll it up to the Inventory server

1. The Sender converts the hardware inventory stored in the ZENworks 7 Linux Management database into `.str` files, and places the files into the `/var/opt/novell/zenworks/inventory/entmerge` directory.

2. The Sender moves the `.str` files from the `entmergedir` directory to the `entpushdir` directory, and compresses the files as a `.zip` file.

3. The Sender sends the `.zip` file from the `entpushdir` directory to the Receiver on the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server.

4. The Receiver places the `.zip` files in the `/entpushdir/zipdir` directory.

5. The Receiver copies the `.zip` files to the `/entpushdir` directory and deletes the `.zip` files from the `entpushdir\zipdir` directory.

6. The Receiver copies the `.zip` files to the database directory (`dbdir`) if a database is attached to the Inventory server.

7. The Sender-Receiver logs the status in Novell eDirectory™.

34.4 Understanding the Components Involved in the Inventory Roll-Up

The Sender on the Inventory servers transfer the scan files from the ZENworks 7.3 Linux Management Inventory server to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server. The following sections contain more information:

34.4.1 Understanding the Sender

The Sender is a Java component that runs on any ZENworks 7.3 Linux Management server. The Sender is a service loaded by the ZEN Loader.

The flow of information from the Sender in the roll-up of inventory information is as follows:

1. The ZEN Loader starts the Sender on the Inventory server. At the time specified in the Roll-Up Schedule, the Sender moves the scan data files (`.str`) from the enterprise merge directory (`entmergedir`) to the enterprise push directory (`entpushdir`).

   The Sender compresses these `.str` files in the `\entpushdir` directory of the Inventory server as a `.zip` file and then deletes the `.str` files. This `.zip` file is again compressed with the `.prp` file into a `.zip` file. The `.prp` file is an internal file containing information about the `.zip` file.

2. Based on the Discard Scan Data Time in the Inventory Service object properties of the Receiver, the Sender deletes the compressed `.zip` files in the `\entpushdir` directory that were created earlier than the specified discard scan data time. This removes unwanted scan information being sent in the roll-up.

3. The Sender sends the compressed `.zip` files to the Receiver, with the oldest compressed files sent first.

4. After transferring the `.zip` file, the Sender deletes the compressed files in the `\entpushdir` directory.

If the Sender is unable to connect to the Receiver, the Sender retries to connect after 10 seconds. The time interval increases exponentially by a factor of 2. After 14 retries, the Sender stops trying to connect to the Receiver. The Sender retries for approximately 23 hours before it discontinues trying. The Sender does not process any other information while it is establishing the connection.

34.4.2 Understanding the Compressed Scan Data File

The Sender compresses the scan data files (`.str`) into a `.zip` file. This `.zip` file is again compressed with the `.prp` file into a `.zip` file. The `.zip` file (containing the `.zip` files and `.prp`) is named using the following naming conventions:

scheduledtime_inventoryservername_treename_storedstatus`.zip`

where *scheduledtime* refers to the date and time when the `.zip` file is created, *inventoryservername* refers to the Inventory server on which the `.zip` file was compressed, *treename* refers to the unique tree name in which the `.zip` file is currently located, *storedstatus* refers to the storage status of the `.zip` file, and *zip* is the file extension for the compressed files. The *storedstatus* displays 0, 1, or 2. 0 indicates the `.zip` file has not yet been stored. 1 indicates the `.zip` file will be stored for the first time in the Inventory server. 2 indicates the `.zip` file has already been stored once.

The `.zip` filename changes depending on if the database is attached to the Inventory server.

The `.zip` file contains the `.zip` files and a property file. The property file is named using the following conventions:

scheduledtime_inventoryservername`.prp`

The property file contains the scheduled time, Inventory server name, and signature. The signature helps to authenticate the `.zip` file.

Each `.zip` file can contain a maximum of 50 `.str` files.

34.5 Viewing the Inventory Data Stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database

You can view the inventory data stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory database using the following Inventory ConsoleOne® utilities:

- Inventory Query
- Inventory Reports

For more information on how to invoke and work with these utilities, see the "Workstation Inventory" section in the Novell ZENworks 7 Desktop Management Administration Guide (http://www.novell.com/documentation/zenworks7)or the see the "Server Inventory" section in the Novell ZENworks 7 Server Management Administration Guide (http://www.novell.com/documentation/zenworks7).

Remote Management

VIII

The Remote Management component of Novell® ZENworks® 7.3 Linux Management gives you the ability to remotely manage devices from the management console. Remote Management allows you to:

- Remotely control the managed device
- Remotely view the managed device
- Remotely login to the managed device
- View log information about any Remote Management sessions performed on any managed device from anywhere in your network

Remote Management can save you and your organization time and money. For example, you or your organization's help desk can analyze and remotely fix problems on the devices without visiting the user's device, which reduces problem resolution time and increases productivity.

The following sections will help you understand and use Remote Management:

Remote Management Overview

35

You can use Novell® ZENworks® 7.3 Linux Management to remotely manage all the supported platforms. To see details on supported platforms, see "Managed Device Requirements" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

The following sections provide information to help you understand the functionality of Remote Management components:

◆ Section 35.1, "Remote Management Terminology," on page 495
◆ Section 35.2, "Understanding the Remote Management Components," on page 495

35.1 Remote Management Terminology

Managed device: A device that you want to remotely manage. To remotely manage a managed device, you must install the ZENworks 7.3 Linux Management Agent on it.

Management server: A server where ZENworks 7.3 server is installed.

Management console: A Windows or Linux device that provides console to manage ZENworks. The management console provides the interface to manage and administer your workstations.

Administrator: A person who can perform various Remote Management operations.

Remote Control Service: A component that is installed on a managed device, enabling the administrator to remotely control and remote view the managed device. The Remote Control Service starts automatically when the managed device boots up. It verifies whether the administrator is allowed to perform Remote Control operations on the managed device before the Remote Management session proceeds with authentication.

Remote Login Service: A component that is installed on a managed device, enabling the administrator to remotely login into the managed device. The Remote Login Service starts automatically when the managed device boots up. It verifies whether the administrator is allowed to perform Remote Login on the managed device before the Remote Management session proceeds with authentication.

Remote Management Viewer: A window displaying the desktop session of the managed device.

35.2 Understanding the Remote Management Components

The following sections provide information to help you understand the functionality of Remote Management components. You must install the Remote Management Agent on the managed devices to perform the Remote Management operations.

◆ Section 35.2.1, "Understanding Remote Control," on page 496
◆ Section 35.2.2, "Understanding Remote View," on page 496
◆ Section 35.2.3, "Understanding Remote Login," on page 496

35.2.1 Understanding Remote Control

Remote Control lets you control a managed device desktop from the management console so you can provide user assistance and help resolve problems on the devices.

Remote Control establishes a connection between the management console and the managed device. With remote control connections, the administrator can go beyond viewing a managed device to taking control of it.

During a Remote Control session, you can now switch between the active applications running on the managed device using Alt+Z in the Remote Management Viewer.

35.2.2 Understanding Remote View

Remote View lets you view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered by observing how the user at a managed device performs certain tasks.

35.2.3 Understanding Remote Login

Remote Login lets you login into a managed device from the management console. This helps you to start a new graphical session without disturbing the user on the managed device. The user on the managed device would not be able to view a Remote Login session.

During a Remote Login session, you can now switch between the active applications running on the managed device using Alt+Z in the Remote Management Viewer.

Setting Up Remote Management

36

The following sections provide information on deploying the Remote Management component of Novell® ZENworks® 7.3 Linux Management in a production environment:

36.1 Configuring the Remote Management Settings

Remote Management Settings allows you to configure the Remote Management settings for the management zone. This includes enable and disable options for remote management operations as well as configurations for custom ports. The Remote Management Settings can be applied at Zone, Folder, and Device levels.

36.1.1 Configuring Remote Management Settings at the Zone Level

1 In the ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings section, click *Remote Management*.
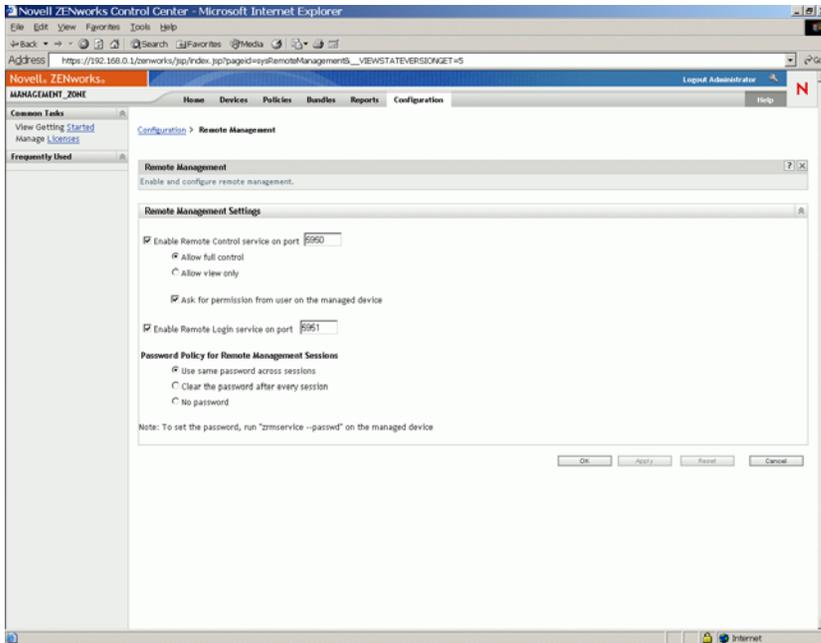
3 To enable the Remote Control Service on a particular port, select the *Enable remote control service on port* option.

By default, the Remote Control Service listens on port number 5950.

4 Select *Allow full control* or *Allow view only*.

Select *Allow full control* to enable the user to perform both remote control and remote view operation to a managed device. Select *Allow view only* to enable the user to perform only remote view operations to a managed device. Selecting *Allow view only* disallows the user to perform remote control operation.

5 Select the *Ask for permission from user on the managed device* option to request the permission of a user on the managed device before starting a Remote Control or Remote View session.

6 To enable Remote Login Service on a particular port, select the *Enable remote login service on port* option.

By default, the Remote Login Service listens on port 5951.

7 In the Password Policy for Remote Management Sessions section, select the desired option.

Select *Use same password across sessions* to use the same password across all sessions. By default, this option is selected. Select *Clear the password after every session* to set the password for every session. If you select this option, the password is cleared after every successful or unsuccessful attempt for a Remote Management operation. If you want to launch a Remote Control, Remote Login, or Remote View operation without asking for a password, select *No password*.

NOTE: We recommend you to use the *No password* option judiciously as it allows access to the managed device without any password.

8 Click *Apply*.

These changes will be effective on the managed devices on their next Settings Refresh Schedule.

36.1.2 Configuring Remote Management Settings at the Folder Level

1 In the ZENworks Control Center, click *Devices*.

2 Click the folder you wish to configure.

3 Click *Settings*, then click *Remote Management*.
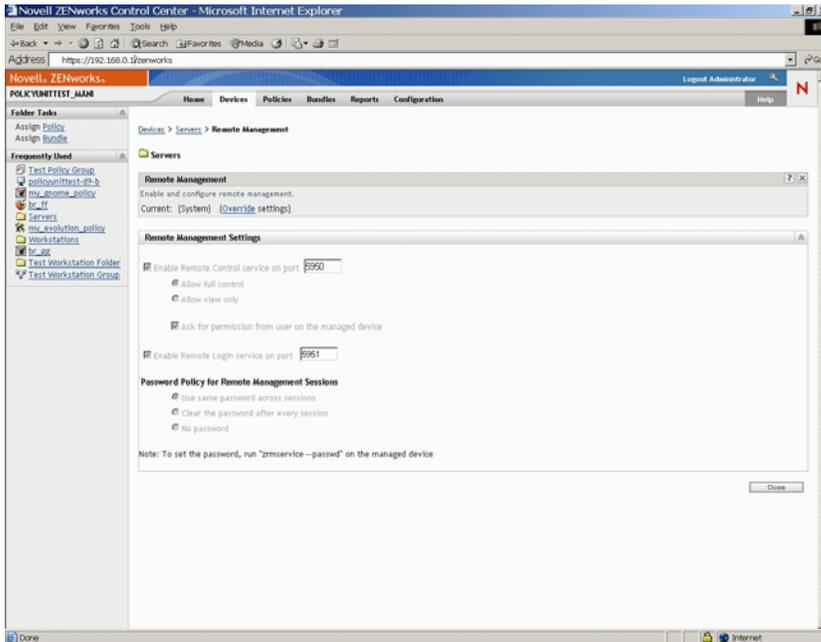
4 Click *Override*.

5 Edit the Remote Management Settings as required.

6 Click *Apply*.

These changes will be effective on the managed devices on their next Settings Refresh Schedule.

36.1.3 Configuring Remote Management Settings at the Device Level

1 In the ZENworks Control Center, click *Devices*.

2 Click *Servers* or *Workstations* to display the list of managed devices.

3 Click the name of a device for which you want to configure Remote Management.

4 Click *Settings*, then click *Remote Management*.
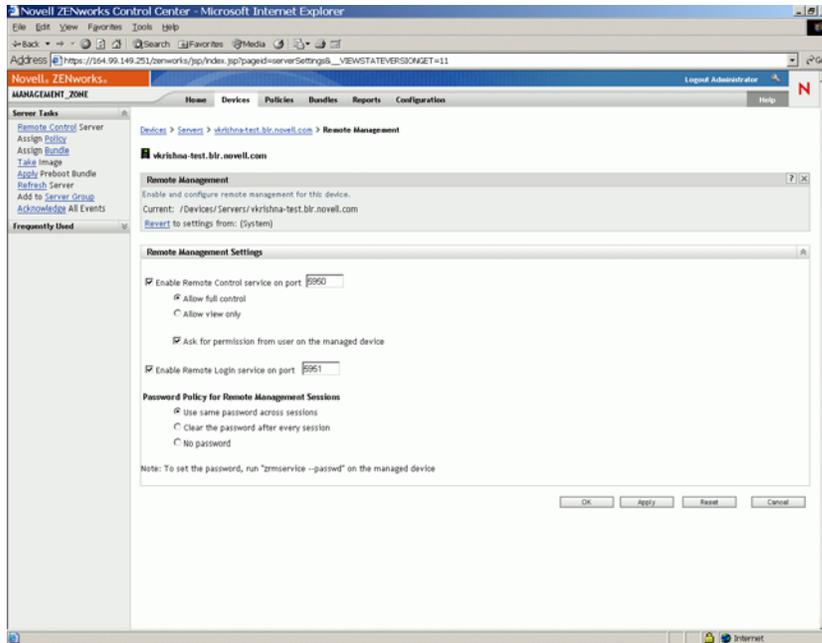
5 Click *Override*.

6 Edit the Remote Management Settings as per your requirements.

7 Click *Apply*.

These changes will be effective on the managed device on its next Settings Refresh Schedule.

36.2 Configuring Remote Management Agent

The Remote Management Agent allows you to remotely manage the device and configure the following:

36.2.1 Setting Up the Remote Management Agent Password on the Managed Device

The user on the managed device must set a Remote Management Agent password and communicate the password to the administrator.

To set the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --passwd
```

The password is case-sensitive and should be between three to eight characters in length.

NOTE: This step is not necessary if the Password Policy is configured to *No password*.

36.2.2 Clearing the Remote Management Agent Password

To clear the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --clrpasswd
```

36.2.3 Clearing Remote Management Agent Log Files

To clear the Agent log files on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --clearlog
```

36.3 Starting Remote Management Operations Using the ZENworks Control Center

The ZENworks Control Center is the comprehensive web-based control interface for ZENworks 7 Linux Management. It provides an intuitive and task-driven console to manage various ZENworks components including Remote Management.

You can initiate various Remote Management operations from the following locations:

36.3.1 Initiating a Remote Management Session from Common Tasks

1 In the ZENworks Control Center, click *Devices*.

2 In Device Tasks in the left pane, click *Remote Control Device* to open the following dialog box:
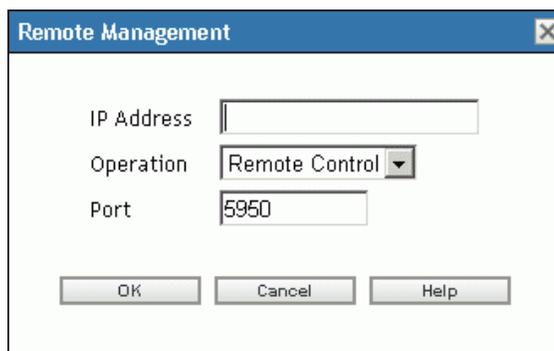
3 In the *IP address* field, specify the IP address or DNS name of the device you want to remotely control.

4 Select the Remote Management operation to be performed on the device. The available options are *Remote control*, *Remote view*, and *Remote login*.

The following table lists and explains all the operations you can select from the drop-down list:

Option	Description
Remote control	Allows you to take control of the managed device.
Remote view	Allows you to view the managed device.
Remote login	Allows you to remotely log in to a new desktop session on the managed device. This desktop cannot be viewed by the users on the managed device.

5 Specify the port number configured for the selected operation.

The auto-populated port numbers are those which are configured in the Remote Management Settings at Zone Level.

6 Click *OK*.

7 Read the Java Security message and click *Yes* to accept the Certificate of the Signed Applet. To avoid the message to be displayed again, select *Always*.

8 If the *Ask for permission from user on the managed device* setting is enabled, click *Yes* in the permission change dialog-box on the managed device.

9 Specify the password at the management console, then click *OK*.

IMPORTANT: We recommend you to use Java plug-in 1.5.x in the browser of the Management Console.

36.3.2 Initiating a Remote Management Session from the Device Context

You can perform Remote Management operations on a specific device.

1 In the ZENworks Control Center home page, click *Devices*.

2 Click *Servers* or *Workstations*.

3 Select the device you want to remotely control.

or

Click the device name, then click *Remote Control* in Server Tasks (if you have selected Server) or *Workstation Tasks* (if you have selected Workstation) in left pane.

4 If you have selected the device in step 3, click *Remote control* in the *Action* menu to open the Remote Management dialog box:
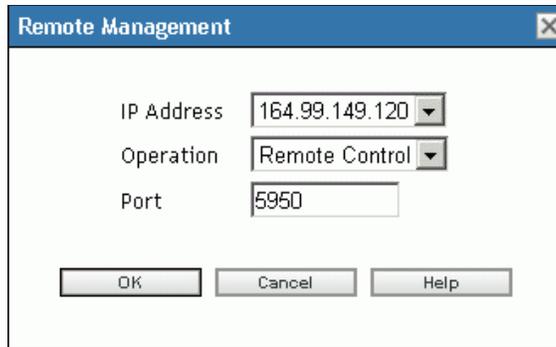
5 Select the IP address of the device.

6 Select the Remote Management operation to be performed on the device.

The drop-down list of operations is based on the effective Remote Management Settings for the managed device. The available options are *Remote control*, *Remote view*, and *Remote login*.

The following table lists and explains all the operations you can select from the drop-down list:

Option	Description
Remote Control	Allows you to take control of the managed device.
Remote View	Allows you to view the managed device.
Remote Login	Allows you to remotely login to a new desktop session on the managed device. This desktop cannot be viewed by the users on the managed device.

7 Specify the port number configure for the selected operation.

The auto-populated port numbers are those which are configured in the effective Remote Management Settings for the selected device.

8 Click *OK*.

9 Read the Java Security message and click *Yes* to accept the Certificate of the Signed Applet. To avoid the message to be displayed again, select *Always*.

10 If the *Ask for permission from user on the managed device* setting is enabled, click *Yes* on the permission change dialog-box on the managed device.

11 Specify the password at the management console, then click *OK*.

36.4 Starting Remote Management Operations Using the Native VNCViewer

The following sections contain additional information:

- Section 36.4.1, "Starting Remote Management Operations Using the Windows VNC Viewer," on page 504
- Section 36.4.2, "Starting Remote Management Operations Using the Linux VNC Viewer," on page 504

36.4.1 Starting Remote Management Operations Using the Windows VNC Viewer

1 Download the latest stable version of the native VNC Viewer from the TightVNC web site (http://www.tightvnc.com/download.html).

2 Install Tight VNC from the executable you have downloaded.

3 Launch the Tight VNC Viewer from *Start > Programs > Tight VNC > Tight VNC Viewer.*

> **IMPORTANT:** We recommend using Tight VNC Viewer (Fast Compression) over fast links and Tight VNC Viewer (Best Compression) over slow links.

4 In *Connection details*, specify the IP address with a port number as configured, then click *OK*.

You can specify the port number after the IP address with a double colon (::) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify as 192.168.0.1::5950.

You can specify the display number after the IP address with a single colon (:) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify the IP address as 192.168.0.1:50.

You can also specify a DNS name instead of an IP address.
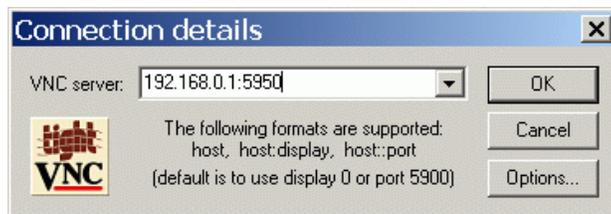
5 In *VNC authentication*, specify the correct password, then click *OK*.

Now, you will have an access to the desktop of the managed device you have specified.

36.4.2 Starting Remote Management Operations Using the Linux VNC Viewer

1 Download the latest stable version of native VNC Viewer from the TightVNC Web site at TightVNC web site (http://www.tightvnc.com/download.html).

2 Install Tight VNC from the RPM Package you have downloaded.

3 Launch Tight VNC Viewer by specifying the following command at the Shell prompt:

```
$ vncviewer
```

4 In serverDialog, specify the IP address with a port number as configured, then click *OK*.
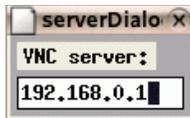
You can specify the port number after the IP address with a double colon (::) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify the IP address as 192.168.0.1::5950.

You can specify the display number after the IP address with a single colon (:) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify as 192.168.0.1:50.

5 In passwordDialog, specify the correct session password, then click *OK*.

Now, you will have an access to the desktop of the IP address you have specified.

36.5 Establishing SSH Tunneling

The VNC protocol and data are unencrypted between the management console and the managed device. If you perform Remote Management operations over an insecure network like Internet, you should tunnel the VNC protocol using SSH for secure communication.

1 Establish SSH tunneling to use VNC between management console and managed device.

2 Launch the Remote Control session from Device Tasks at the top left of the ZENworks Control Center on the Devices page.

3 Specify the IP address and port of the configured SSH tunnel.

4 Select the desired operation from drop-down list.

5 Click *OK*.

36.6 Improving Remote Management Performance

The performance during a Remote Management session over a slow link or a fast link varies depending on the network traffic. For better response time, try one or more of the following strategies:

On the Management Console

On the Remote Management viewer window at the console, click *Options* and set the following values:

- Set the Encoding value to Tight
- Adjust the Compression level and JPEG image quality depending on the quality of the image required.

- Set Cursor Shape Updates to No.
- Set the CopyRect option to Yes.
- Use 8 bit color mode by setting Restricted Colors to Yes.

On the Managed Device

- The speed of the Remote Management session depends upon the processing power of the managed device. We recommend that you use Pentium* III, 500MHz (or later) with 64 MB RAM or higher.
- Disable the wallpaper.
- Configure the following settings at the managed device:
    - Reduce the screen resolution.
    - Reduce the depth of color pixels.

More Performance Tuning Tips

For additional information on performance tuning tips, refer to the following Web sites for specific components:

- www.tightvnc.com (http://www.tightvnc.com)
- www.realvnc.com (http://www.realvnc.com)
- FAQs on x11VNC (http://www.karlrunge.com/x11vnc)

Event Monitoring

IX

Novell® ZENworks® Linux Management includes a Message Logger component that tracks and logs significant system events. Administrators can use this information to monitor events related to devices, policies, and bundles. Specifically, event monitoring allows you to do the following:

- Monitor problems associated with devices, policies, and bundles
- Track successful events
- Log events and run reports
- View a summary of problems on a hot list

This section contains the following topics:

Event Monitoring Overview

37

Event monitoring allows you to manage your environment by taking messages from the Message Logger and displaying them in various event logs, making it easy to track errors, problems, and successful events for your devices, policies, and bundles.

You can capture and store specific events related to devices, policies, and bundles that you or your organization's help desk can analyze and use to monitor problems without visiting the server or workstation, which can reduce problem resolution times and increase productivity. The captured information includes a description, time stamp, severity status, and message ID.

To keep your environment running at its maximum efficiency, you can use the event logs to stay abreast of critical errors and help you to troubleshoot and fine-tune your environment.

The following sections provide additional information:

37.1 Event Monitoring Terminology

Event: Something that happens, such as a successful installation, that triggers a message to be created and sent.

Local Log: A list of the event messages generated by the ZENworks® Agent that resides on the server or workstation.

System Log: A list of event messages displayed only for servers that are functioning as primary or secondary ZENworks Servers. The log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its Management Zone.

Message: A detailed description of an event. A message explains an exception such as an error or warning, provides information to a user, or includes a debug statement used for debugging the module.

Community String: The protocol password for SNMP. Applications use community strings for access control. You can use the trap receiver console to define the set of community strings to accept the trap. The agent, in turn, accepts or rejects the operation. When none of the community string matches, the trap is discarded.

37.2 Monitoring Device Events

When you use Novell® ZENworks Linux Management to remotely install applications, you need feedback on the success and failure of certain events so you can keep your systems working at an optimal level. With event monitoring, you can track things such as software installation on client devices, whether or not a device has been refreshed, whether or not sessions were started, and so on. These messages are logged into a database and the information displayed in the event logs.

37.3 Monitoring Policy Events

ZENworks Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. The Message Logger tracks problems with setting policies and displays them in the event logs. The resulting messages alert you to any problems that arise, such as failed connections and the inability to create schedules.

37.4 Monitoring Bundle Events

ZENworks Linux Management enables you to create bundles and catalogs to distribute RPM packages to managed devices. In the process of pushing the bundles to managed devices, problems can arise, such as a bundle failing to install or problems with removing a bundle. These events are logged in the event log so you can address them.

37.5 Using the Hot List

When a device, policy, or bundle has been identified as having a critical or warning event (non-system) that has not been acknowledged or cleared, it is displayed in the Hot List. You can use this list as a summary of problems that need attention. Events on the Hot List are ordered by severity: first are those devices, policies, or bundles with critical events, then those with warning events. Those with the most problems are listed first. With the Hot List, you can see at a glance which device, policy, or bundle needs the most attention.

Figure 37-1   *Summary Page and Hot List*

To view the Hot List, click *Home* on the toolbar. This page shows the System Summary and the Hot List. The System Summary page shows the various categories—servers, workstations, policies, and bundles—and their respective status counts. In this example, there are four policies and none have had a warning or critical event; one server that has not had any warning or critical events; and seven bundles that haven't had any warnings or critical events. In the workstation category, one workstation has had at least one critical event. You can click the workstation name to view a summary, which includes details of the problem events.

37.6 Backing Up the Log Files

You can take a backup of `/var/opt/novell/log/zenworks/tomcat/catalina.out` or any other log file using the logrotate utility.

The logrotate utility is available with the operating system. The utility eases the administration of systems that generate large numbers of log files. It allows automatic rotation, compression, and removal of log files. Each log file might be handled daily, weekly, monthly, or when it grows too large. For more information on the usage of the logrotate utility, see the logrotate man page.

ZENworks 7.3 Linux Management with IR2 provides a logrotate file, `/etc/logrotate.d/zlm-server-logrotate`, on the server. The logrotate utility uses the file to rotate the existing and the new log files created in `/var/opt/novell/log/zenworks` on the ZENworks Linux Management server. These server log files are compressed with date extension, rotated, and backed up daily for 33 days before being discarded.

The tomcat server logs rotated within the `tomcat` directory are not affected by the `zlm-server-logrotate` file. The rotation of the `catalina.out` log file that resides in the `tomcat` directory is based on its size.

To allow the rotation of the `catalina.out` log file, do the following:

- Rename the `log4j` configuration file from `/etc/opt/novell/zenworks/log4j.properties.disabled` configuration file to `/etc/opt/novell/zenworks/log4j.properties`

- Restart the ZENworks services by using the `zlm-config --restart` command

This configures the `log4j.properties` file as the tomcat system logger for the ZENworks Server and tomcat events.

The configuration defined in the `log4j.properties` file creates a maximum of five rotating backups for the `catalina.out` file. The maximum size of each backup log file can be upto 100 MB.

Working with Event Logs

38

Event logs are automatically created for important events, such as successful installations or critical errors.

- Section 38.1, "The Event Log Page," on page 513
- Section 38.2, "Working with the Log Pages," on page 515

38.1 The Event Log Page

The Event Log page gives you an overview of the recorded events. The Event Log lists the event messages generated by the ZENworks® Agent that resides on the server or workstation. The list is ordered by date, with the latest date first. Each event listed includes the following information:

- **Status:** An indication of the event's severity:
    - The ◉ icon indicates an event has executed successfully.
    - The ◈ icon indicates an exception condition that might cause problems but might not need immediate attention.
    - The ⊗ icon indicates that an action could not be completed because of a user or system error, and it needs immediate attention.
- **Event:** Something that happens, such as a successful installation, that triggers a message to be created and sent. Click the event message to display additional details. You can use the message details window to acknowledge the message, which causes the message to be cleared from the event log.
- **Data:** The date and time the event occurred.
- **Advanced:** A page showing both acknowledged and unacknowledged events. You can sort events by status, date, or whether an event has been acknowledged or not. You can also acknowledge events from this page.

Figure 38-1 *Event Logs*

When you click the description of an event, the following page appears:

Figure 38-2 *Detailed Information Concerning the Event*

This page can be used to acknowledge the event. Acknowledging an event removes it from the main event log, but you can still see it in the Advanced page. Clicking *Finished* closes the window.

There are two log lists, the Event Log and the System Event Log. The Event Log lists the event messages generated by the ZENworks Agent that resides on the server or workstation; the System Event Log is displayed only for servers that are functioning as primary or secondary ZENworks Servers. The System Event Log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its management zone.

38.2 Working with the Log Pages

After an event has been logged, you can view and acknowledge it.

38.2.1 Viewing an Event Log

You can view event logs for devices, policies, and bundles. To view an event log, start with the appropriate tab in the ZENworks Control Center: *Devices*, *Policies*, or *Bundles*. For example, to view the event log for a server, do the following:

1 Click the *Devices* tab on the ZENworks Control Center page to display a list of managed devices.

2 Click *Servers* to display a list of servers.

3 Click the server you want to check. A summary page appears that includes the event logs. To view additional details, click the event.

38.2.2 Acknowledging an Event

After you view the logs and identify a problem, you can acknowledge it. To acknowledge an event means you've seen it and either fixed it or decided to take care of the problem later. When you acknowledge an event, it is removed from the event and system log lists but kept in the database and on the Advanced page. You can view acknowledged events either by running a report or using the Advanced page.

You can acknowledge a single event, acknowledge multiple events, or acknowledge all events.

To acknowledge a single event:

1 Open the Summary page. (For information, see)

2 Click the event you want to acknowledge.

Message Detail Information ✕

Full Message:	The policy wes1.txt could not be successfully enforced as the file "/opt/wes1.txt" does not exist. The rollback exit code is -1.
Additional Information:	None
Severity:	Error
Date:	July 12, 2005 10:18:50 AM
Acknowledged Date:	None
Source:	/Devices/Workstations/mtalbot
Message ID:	Novell.Zenworks.PolicyEnforcers.TPE.NO_SUCH_FILE
Log ID:	11458
Related Objects:	<Unknown>

[Finished] [Acknowledge]

3 Click *Acknowledge*.

The event disappears from the list but remains in the database and is listed on the Advanced page.

To acknowledge several events:

1 Open the Summary page. (For information, see

2 Click *Advanced* on the toolbar in the *Event Log* section.

| Home | Devices | Policies | Bundles | Reports | Configuration |

Devices > Servers > sdf1.provo.novell.com > Edit System Event Log

Edit System Event Log

Events logged from this device are displayed in this list.

🟢 **System Event Log**

Acknowledge

☐	Status	Event	Date ⧨	✔
☐	🟢	Device sdf1.provo.novell.com was	7/18/05 2:01:47 PM	
☐	🟢	Device veritech was successfully updated	7/18/05 1:34:16 PM	
☐	🟢	Device mtalbot was successfully updated	7/18/05 12:31:37 PM	
☐	🟢	Device sdf1.provo.novell.com was	7/18/05 12:01:19 PM	
☐	🟢	Device veritech was successfully updated	7/18/05 11:34:16 AM	

◄ ► 1 - 5 of 426   show 5 ▼ items

3 Select the check box for each message you want to acknowledge.

4 Click *Acknowledge*.

To acknowledge all events:

1 Open the Summary page.

2 Click *Acknowledge All Events* in the upper left corner.

Clicking *Acknowledge All Events* acknowledges all system events, not just those in a single category.

38.2.3 Using the Advanced Page

You can open the Advanced page by clicking *Advanced* in the upper right corner of the event log part of the page. In the Advanced page, you can acknowledge events, view acknowledged events, and click the description of an event for more details.

38.2.4 Clearing the Event Log

After you acknowledge an event, you have two options for cleaning up the logs. You can clear the events, which deletes the events from all the lists, including the Advanced window. Once cleared, the event is only available through reports. You can also permanently delete the event, which deletes the event from both the logs and the database. You can clear events associated with servers, workstations, policies, and bundles. For each, the process is the same.

To clear the event log for a workstation:

1 Open the Devices page, then click *Workstations*.

2 Click the check box of the workstation you want cleared of events.
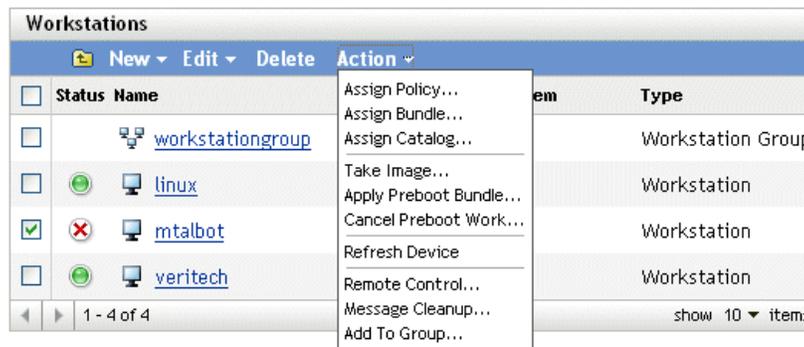
3 Click *Action* on the toolbar.

4 Click *Message Cleanup*.
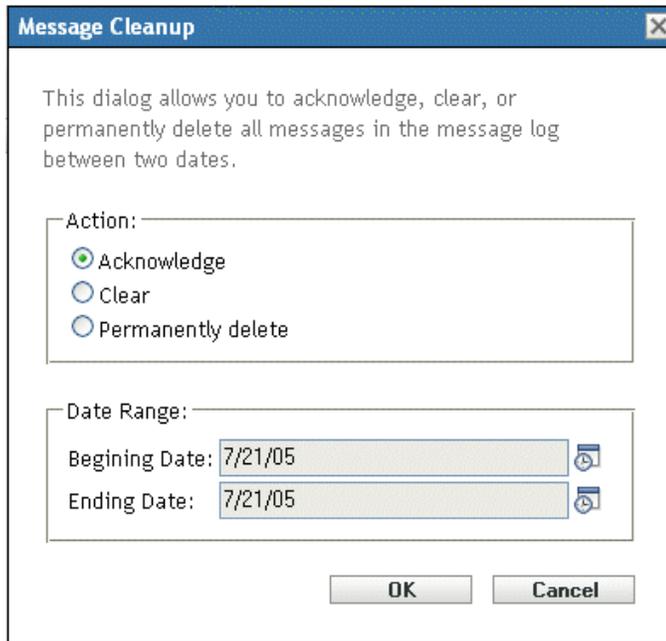
From here you can do the following:

- ◆ Acknowledge all event messages for the device. This acknowledges all events within a specified date range and deletes them from the Hot List, event log, and system event log.

- ◆ Clear all event messages. This clears all events within a specified date range from the event log, system event log, advanced event log, and advanced system event log.

- ◆ Permanently delete all event messages. This deletes all events within a specified date range from all the log lists and the database.

5 When you have selected the option you want and set a date range, click *OK* to clear the messages.

Message Logger

39

You can use the Message Logger component of Novell® ZENworks® Linux Management to log the messages on managed devices and servers.

The following sections provide information to help you understand the functionality of the Message Logger component:

- Section 39.1, "What Is Message Logger?," on page 521
- Section 39.2, "Message Severity," on page 521
- Section 39.3, "Message Format," on page 521
- Section 39.4, "Debugging and Logging ZMD," on page 522
- Section 39.5, "Viewing the Debug Logs on ZENworks Server," on page 522

39.1 What Is Message Logger?

Message Logger is the component responsible for logging the messages to different output targets. Several components of ZENworks 7.3 Linux Management use Message Logger to log messages, including zenloader and webservices on the server and the ZENworks management daemon (ZMD), Remote Management, and Policy Enforcers on the client. For more information about ZENworks services, see Section 5.1, "ZENworks Services," on page 47.

Message Logger logs the messages in different output targets, such as e-mails, SNMP traps, writes to the database, local and system log files, and the central log file.

39.2 Message Severity

Messages are classified in the following three categories:

Error: Indicates that an action cannot be completed because of a user or system error. These messages require immediate attention from an administrator.

Warning: Calls attention to an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.

Information: Provides feedback about something that happened in the product or system that is important and informative for an administrator.

39.3 Message Format

Messages are logged on the managed device and Primary Server in the following format:

```
Severity: [time] Component_Name Message_ID Message_String
Additional_Info:Value_for_Additional_Info
```

For example, ERROR: [3/15/05 3:28:45 PM] PolicyEnforcers Novell.Zenworks.PolicyEnforcers.EPE.NO_SUCH_FILE The Text File policy could not be successfully enforced as the file abc.txt does not exist.

Additional Info: PolicyEnforcer Exception: file does not exist.

39.4 Debugging and Logging ZMD

The ZENworks Management Daemon (ZMD) provides the following preferences that can be used for debugging and logging ZMD:

- **log-level:** Used to set up custom logging levels. The valid values are off, fatal, error, warn, info, and debug. To set the value of the preference, use the `rug set log-level` `'preference_value'`command. For example, to set the log-level preference to debug, use `rug set log-level 'debug'`. For more information about rug, view the rug man page (`man rug`) on a managed device or see rug (1) (page 586).

- **log-soap-xml:** Used to log SOAP messages. All messages are logged in the `zmd-messages.log` file. The file is located in the `/var/log/` directory on SLES 10 and SLED 10 devices, and in the `/var/opt/novell/log/zenworks` directory on all other devices.

For detailed ZMD logging information on SLES 10 and SLED 10, you can also refer to `/var/log/zmd-backend.log`. For extensive logging of ZYPP, configure the ZYPP_FULLOG environmental variable.

39.5 Viewing the Debug Logs on ZENworks Server

The following logs are available on ZENworks Server:

- **ZENworks Server Logs:** The ZENworks Server logs are located in the `/var/opt/novell/log/zenworks` directory. Each log file corresponds to an individual component or service. For example, the operations of ZENserver and ZENloader are logged in the `services-messages.log` and `loader-messages.log` files respectively.

  If you want to collect additional debug logging information for ZENworks Server, do the following:

  1. Edit the `etc/opt/novell/zenworks/logger-server-conf.xml` to configure the following lines:

     `<LoggerModule trace = "true">`

     `<param name="fileDebug" enable = "true" value ="true" />`

  2. Restart all the zlm services by using the `zlm-config --restart` command.

  If you want to collect additional debug logging information for ZENworks Loader or its modules, do the following:

  1. Edit the `/etc/opt/novell/zenworks/logger-loader-conf.xml` file and the `/etc/opt/novell/zenworks/logger-server-conf.xml` file to configure the following lines:

     `<LoggerModule trace = "true">`

     `<param name="fileDebug" enable = "true" value ="true" />`

  2. Edit the `/etc/opt/novell/zenworks/logger-log4j-loader-conf.xml` file to configure any specific loader module as follows:

     `<logger name="LocalLogger.ComponentName" additivity="true">`

     `<level value="debug"/>`

```
</logger>
```

where *component name* can be DataModelModule, QueueRunner, Sender, ZLMCleanupDevice, SettingsRefreshModule, etc.

3. Restart all the zlm services by using the `zlm-config --restart` command.

- **ZENworks Agent (zmd) Logs:** The ZENworks Agent (zmd) logs are in the `zmd-messages.log` and `zmd-backend.log` files. On SLES 11 devices, the backend logs are in the `zmd-satbackend.log` file. For more information, view the zmd man page (`man zmd`) on a managed device or see zmd (8) (page 548).

- **Install and Uninstall Logs:** The installation and uninstallation of the ZENworks Server and Agent are logged in the `zlm-install.log` and `zlm-uninstall.log` files.

Configuring Message Logger Settings

40

You can perform the following activities by configuring Message Logger settings:

- Write messages to a local log file
- Write messages to a system log file
- Send messages as SNMP traps
- Send messages as SMTP mail
- Purge the database entries

NOTE: The Message Logger does not log messages with severity levels other than error, warning, information, and debug.

There are two ways to configure Message Logger settings:

40.1 Configuring Message Logger Settings for the Primary Server

The following settings of the Message Logger can be configured to log messages on the Primary Server:

40.1.1 Configuring Database Maintenance Settings

These settings allow you to configure the database maintenance settings for purging the database log messages.

1 In the ZENworks® Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *Central Server*, specify the name of the server that is responsible for purging message log entries from the database.

You can also select a server by clicking ▣.

The ZENworks servers that are displayed here are the ones that are registered with Novell®
ZENworks Linux Management Server.

4 In the *Purge Log Entries After* field, select a value from the drop-down list. The available options are *30, 60,* and *90*.

Log entries older than the selected number of days are purged. Purging is done every midnight and 5 minutes after zenloader starts.

5 Click *OK* or *Apply*.

40.1.2 Configuring Centralized Log Settings

These settings allow you to use a log file to log the messages of a server and all the managed devices that are connected to this server. The name of this log file is central-message.log, and it is located in /var/opt/novell/log/zenworks.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *Centralized File Log*, select the *Log Message to a Centralized File if Severity Is* check box to enable the settings.

4 In the *Log Message to a Centralized File if Severity Is* field, select a value from the drop-down list.

   ◆ Select *Error* to store the messages that have an Error severity.

   ◆ Select *Warning and Above* to store the messages that have a severity of Warning and Error.

   ◆ Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.

5 In the *Limit File Size To* field, specify the size of a file in KB or MB. The default value is 100 MB.

The message file is backed up after reaching the specified size.

6 In the *Number of Backup Files* field, specify the number of backup files to take. The default value is 2.

The maximum number of backup files is 99. The most recent backup file is named central-message.log.1, the second most recent file has the number 2, and so on. When the maximum file size is reached, the oldest file is deleted.

7 Click *Apply* or *OK*.

40.1.3 Configuring SMTP Settings

These settings allow you to send error messages through e-mail by configuring SMTP settings.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *E-mail Notification*, select the *Send Log Message via E-mail If Severity Is* check box to enable the settings.

4 In the *SMTP Server Address* field, specify the SMTP server address.

You can specify a DNS name or IP address as a server address.

5 Select *SMTP Server Requires Authentication* to authenticate to the SMTP server.

6 Specify the username to use to authenticate to the SMTP server.

7 Specify the password to use to authenticate to the SMTP server.

> **IMPORTANT:** For security considerations, you should create a separate e-mail account and password to send ZENworks messages.

8 In the *Message Settings* section, specify the sender's e-mail address in the *From* field. The error messages are sent from this e-mail address.

9 In the *To* field, specify the e-mail address of the recipients.

You can specify more than one e-mail address by separating the addresses with commas.

10 Specify a subject for the e-mail.

The following table describes how you can customize the subject field:

Format Specifiers	Value
%s	Severity of the message
%c	Component name
%d	Device ID
%t	Time when the message is generated
%a	Alias name of the device on which the message is generated.

Format specifiers are a special set of characters that are replaced with their associated values.

For example, if you want the subject line to be displayed as "ERROR occurred on device TestDevice at 4/7/05 5:31:01 PM," then in the subject line you should specify "%s occurred on device %a at %t."

11 Click *OK* or *Apply*.

40.1.4 Configuring SNMP Settings

These settings allow you to send messages as SNMP traps. The location of the MIB file is `/opt/novell/zenworks/share/loggermodule/messageloger.mib`.

> **NOTE:** The MIB file should not be modified or deleted, or sending of traps does not work.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Under *SNMP Traps*, select the *Log to SNMP Trap if Severity Is* check box to enable all the fields.

4 In the *Log to SNMP Trap if Severity Is* field, select a value from the drop-down list.

- Select *Error* to forward as traps the messages that have Error, Information, Warning, and Debug severity.
- Select *Warning and Above* to forward as traps the messages with a severity of Warning and Error.
- Select *Information and Above* to forward as traps the messages that have a severity of Information, Warning, and Error.

5 Specify a trap target.

You can specify the IP address or DNS name of the management console as a trap target.

6 Specify the port number of the SNMP server.

By default, the port number is 162.

7 Specify the community string of the SNMP trap that is to be sent.

The default value of the community string is Public.

8 Click *OK* or *Apply*.

40.2 Configuring Message Logger Settings for a Managed Device

The following settings of the Message Logger can be configured to log the messages on a managed device:

- Section 40.2.1, "Configuring Local Log Settings," on page 528
- Section 40.2.2, "Configuring System Log Settings," on page 529

40.2.1 Configuring Local Log Settings

These settings allow you to write messages into a local file. The name of the log file for ZMD logging is `zmd-messages.log`; for ZENloader logging it is `loader-messages.log`; and for ZEN server logging it is `services-messages.log`. The path of the local log files is `/var/opt/novell/log/zenworks`.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Local Device Logging*.

3 Under *Local File*, the *Log Message to a Local File if Severity Is* check box is selected by default if you are on ZENworks 7.3 Linux Management. For a new installation of ZENworks 7.3 Linux Management with IR1IR2, this option is deselected by default. If you upgrade to ZENworks 7.3 Linux Management with IR1IR2 from an earlier version of ZENworks Linux Management, this option displays the value that you selected before upgrading.

4 In the *Log Message to a Local File if Severity Is* field, select a value from the drop-down list.

- Select *Error* to store the messages with an Error severity.
- Select *Warning and Above* to store the messages with a severity of Warning and Error.
- Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.
- Select *Debug and Above* to store the messages that have a severity of Debug, Information, Warning, and Error

5 In the *Limit File Size To* field, specify the size of the file in MB or KB. The default value is 10 MB.

The messages are backed up after reaching the specified size and the file is reset.

6 In the *Number of backup files per day* field, specify the number of backup files to take per day. The default value is 1 if you are on ZENworks 7.3 Linux Management and does not change if you upgrade to ZENworks 7.3 Linux Management with IR1IR2. For a new installation of

ZENworks 7.3 Linux Management with IR1IR2, the default value is 5. For more information, see "Event Monitoring Troubleshooting Strategies" in the *Novell ZENworks 7.3 Linux Management Troubleshooting Guide*.

The maximum number of backup files is 99. The most recent backup file is named `central-message.log.1`, the second most recent file has the number 2 and so on. When the maximum file size is reached, the oldest file is deleted.

7 Click *OK* or *Apply*.

40.2.2 Configuring System Log Settings

These settings allow you to insert messages into the system file. The path of the system log file is `/var/log/messages`.

1 In the ZENworks Control Center, click *Configuration*.

2 In *Management Zone Settings*, click *Local Device Logging*.

3 Under *System Log*, select the *Send Message to Local System Log if Severity Is* check box to enable the fields.

4 In the *Send Message to Local System Log if Severity Is* field, select a value from the drop-down list.

- ◆ Select *Error* to store the messages with an Error severity.
- ◆ Select *Warning and Above* to store the messages with a severity of Warning and Error.
- ◆ Select *Information and Above* to store the messages with a severity of Information, Warning, and Error.

5 Click *OK* or *Apply*.

Reports

X

The following sections provide information on Novell® ZENworks® Linux Management reporting features:

Reports Overview

41

Reports can contain details from a large volume of inventory, packaging, and other device or bundle information. You can create new reports, edit existing reports, delete reports, or generate one or multiple reports simultaneously. You can create folders to organize and store reports based on your own criteria.

The Reports page, accessed from the ZENworks® Control Center, displays reports and folders. A number of standard bundle, Dell, and device reports are included with ZENworks, and you can easily modify these and define your own. Reports are generated in HTML. After a report is generated, it can be printed, saved, or exported to XML or comma-separated value (CSV) format. When you create reports, the system stores them as objects in Novell® eDirectory™.

The following reports are provided with ZENworks Linux Management:

41.1 Bundle Reports

The following bundle reports are provided with ZENworks Linux Management:

Table 41-1 *Bundle Reports*

Report Name	Description
Bundle Delivery Failure	Lists bundle delivery failures per device.
Bundle Delivery in the Past 24 Hours	Displays the previous day's bundle deliveries.
Bundle Delivery Information per Device	Lists information consisting of error, warning, and success counts, as well as the last bundle delivery message and status.
Last Bundle Delivery per Device	Displays the last bundle delivery that took place per device.

41.2 Dell Reports

The following Dell reports are provided with ZENworks Linux Management:

Table 41-2 *Dell Reports*

Report Name	Description
Devices Not Having Valid Dell Update Package Bundles (template)	Use this template to create a validation report for Dell Update Package Bundles.

Report Name	Description
Devices Not Having Valid RPM Package Bundles (template)	Use this template to create a validation report for RPM Package Bundles.
Installed Dell Applications Per All Devices	Lists all devices and the installed Dell applications on each device.
Installed Dell Applications Per Model	Lists the installed Dell applications for a single model.
List of Bundled Dell Update Packages	Lists all Dell Update Package Bundles and the Dell Update Packages contained in each bundle.

41.3 Device Reports

The following device reports are provided with ZENworks Linux Management:

Table 41-3 *Device Reports*

Report Name	Description
Device Errors in the Past 24 Hours	Lists all device errors in the past 24 hours.
Device Errors in the Past Week	Lists all device errors in the past week.
Device Disk Usage	Lists disk usage for all devices.
Devices Inactive for the Past 90 Days	Lists all devices that have been inactive for the past 90 days.
Devices Registered in the Past 24 Hours	Lists all devices registered in the past 24 hours.
Devices Registered in the Past Week	Lists all devices registered in the past week.

Generating ZENworks Reports

<div style="text-align: right; font-size: 3em;">42</div>

This section includes the following topics:

42.1 Creating a Folder

You create folders to store ZENworks® reports.

1 In the ZENworks Control Center, click the *Reports* tab.

2 Click *New > Folder*.

3 Specify the name and folder location.

You can browse to select an existing folder in which to store the new folder.

4 Enter a report description, if necessary, then click *OK*.

New Folder

Name: *

`Hard Disk Reports`

Folder: *

`/Reports`

Description:

```
Contains reports for hard disk
inventory.
```

Fields marked with a blue asterisk are required.

[OK]   [Cancel]

The system displays the new folder on the Reports page, as follows:

42.2 Creating a Report

ZENworks allows you to define the devices for which the system generates report data, and to customize how the information is displayed. After you create the report, you can generate the report and view or print it in formats such as XML, HTML, or CSV (comma-separated values). You can also create new folders to store multiple reports that you can run simultaneously.

1 In the ZENworks Control Center, click the *Reports* tab.

2 Click *New > Report*.
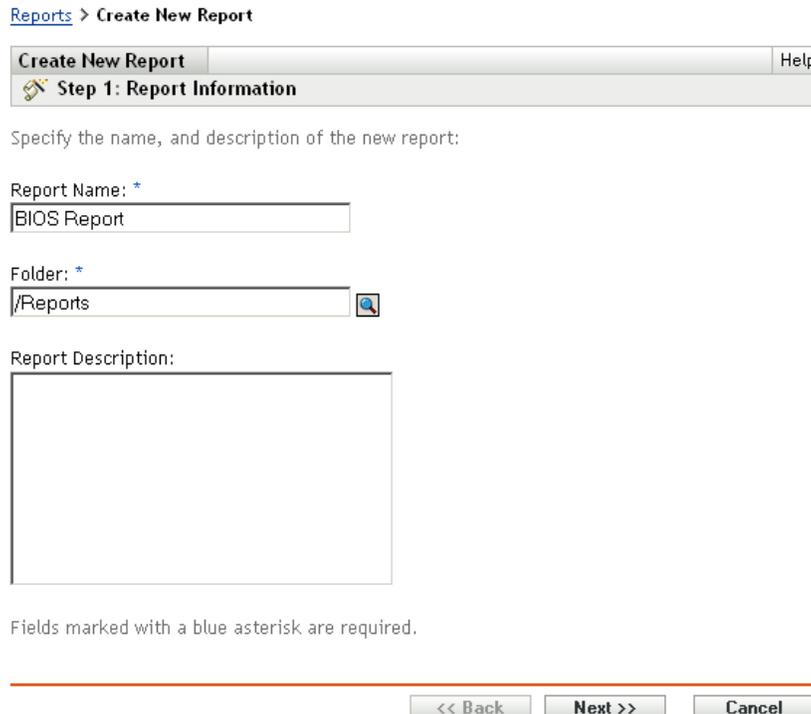
3 Use the Report Information page to specify the following information:

Report name: Specify a report name.

Folder: Specify the folder name, or browse to locate the folder in which you want to store the report. When you browse to locate a folder, the system displays the Select Folder dialog box. After you locate the desired folder, click the *Select* icon to select the folder, then click *OK*.

Report description: Specify a report description. The system displays this description beneath the report name in the generated report.

4 Click *Next*.

5 Use the Columns page to add and sort the columns that you want to display on the report.

Columns: Select a column, then click *Add*. You can select a group of items by holding the Shift key and clicking the first and last items in the group, or you can select several items by holding the Ctrl key and clicking each item. The system displays the items as you add them. Use the ZENworks interface to sort or remove the columns.

The *Software Update Available* column in Bundle Reports displays True if any package updates are assigned to a device through bundles but are not yet installed. It displays False after these updates are installed and the software inventory is updated to the server.

Primary and secondary sort: Use the drop-down menus to specify a primary and secondary sort, if needed. You can sort by a column in ascending or descending order.

6 Click *Next*.

Use the Filters page to create filter rules to manipulate the amount of queried data you want to display on the report. Filter sets enable you to create sets of individual filters, and evaluate them with another set of individual filters. The system uses Boolean logic (And, Or, and Not operators) that determines how to process filters and filter sets. Individual filters can be grouped by And or Or based on how you select the conjunction operator. If you select And to combine filters within filter sets, then the filter sets will be Or, and vice versa. Filter sets can be grouped using Or or And. If you have multiple conditions that must be met, group them using individual filter sets with an And condition.

For example, you can add a filter to report inventory data for a particular *BIOS Name*, then add a second filter to further limit (or expand) the results, such as the *BIOS Manufacturer*. You then might add another filter and use the Not operator to eliminate a certain *BIOS Release Date* value from the search.

7 Click *Add Filter* to create a filter.

Use the drop-down menu to specify whether to combine filters using And or Or. This selection also controls how the system combines filter sets. Depending on the item you select for the filter, ZENworks provides a variety of filtering criteria, such as:

- Alphanumeric (equal to / contains)
- Date and time (before, after, relative, non-existent)
- Size ($<$, $>$, $=$, and so on)
- True/false
- Has/doesn't have

For example, the following filter sets return all devices with 10 GB hard disk drives containing less than 2 GB of free space:

8 Click *Add Filter Set* to create a new set of filters, then click *Add Filter* to add filters to the new set.

For example, the following filter set returns all devices with more than 2 GB of free space that are not made by the specified manufacturer:

New filters are always added to the newest filter set.

To delete a filter, select a filter's check box, then click *Delete*.

9 Click *Next*.

Use the Summary page to review the report information.

10 Click *Finish* to create the new report, then click *OK* on the Results page to return to the Reports page.

Novell® recommends that you use the *Message From This Type Object* column only in conjunction with other message and device columns and filters. If you add other types of columns or filters, the message displayed in this column may be inaccurate. Known exceptions of device columns and filters that also cause this inaccuracy are:

- Device Code Page
- Device Virtual Memory
- Device Visible Memory

42.2.1 Using Templates to Create Dell Reports

ZENworks Linux Management includes two report templates you can use to create reports:

- Devices Not Having Valid Dell Update Package Bundles
- Devices Not Having Valid RPM Package Bundles

Because these are templates, you must modify them before you can generate a report.

1 In the ZENworks Control Center, click the *Reports* tab.

2 Click *Dell Reports*.

3 Click the check box next to the template you want to modify.

4 Click *Edit > Copy*.

5 Specify a name for the report and click *OK*.

6 Click the report name you just created.

7 Modify the report. See Section 42.4, "Modifying Report Details," on page 540.

8 Make sure you've properly filled out the filter fields. For the Dell Update Package Bundles report, the *Dell Model, Bundle,* and *Version* fields are required; for the Devices Not Having Valid RPM Package Bundles report, the required fields are *Bundle* and *Version*.

9 To generate the report, click Generate. To export the report to HTML, CSV, or XML, see Section 42.6, "Exporting Reports," on page 542.

42.3 Organizing Reports and Folders

You can simplify report management and generation by organizing the report list and storing reports in separate folders.

- Section 42.3.1, "Editing the Reports List," on page 539
- Section 42.3.2, "Deleting a Report or Folder," on page 540

42.3.1 Editing the Reports List

To edit the reports list:

1 In the ZENworks Control Center, click the *Reports* tab.

2 Select the report or folder check box, then click *Reports > Edit*.

The following table describes each task:

Table 42-1   Editing Options

Task	Description
Rename	Displays the Rename Report or the Rename Folder dialog box. Specify a new name for the object. Make sure you do not give a report or folder the same name as an existing report or folder.
Copy	Displays the Copy Report dialog box. You must specify a new, unique name for the copied report. You cannot copy folders.
Move	Displays the Move Report dialog box. Select the folder to which the report should be moved.

42.3.2 Deleting a Report or Folder

To delete a report or folder

1 In the ZENworks Control Center, click the *Reports* tab.

2 Select the report or folder check box, then click *Reports > Delete*.

This permanently removes the report from the database.

42.4 Modifying Report Details

1 In the ZENworks Control Center, click the *Reports* tab.

2 Select a report.

3 To modify the settings of an existing report, complete any of the following fields or options:

Field	Description
General	Revise the report description.
Columns	Add, delete, or change the column layout and sorting details of the report. See Section 42.2, "Creating a Report," on page 536 for more information about adding columns to a report.
	Novell recommends that you use the Message From This Type Object column only in conjunction with other message and device columns and filters. If you add other types of columns or filters, the message displayed in this column might be inaccurate. Known exceptions of device columns and filters that also cause this inaccuracy are
	◆ Device Code Page
	◆ Device Virtual Memory
	◆ Device Visible Memory
Filters	Revise, add, or delete the report filters. See Section 42.2, "Creating a Report," on page 536 for more information about naming, formatting, and filtering.
Generate	Runs the report based on the settings displayed on the page. See Section 42.5, "Generating Reports," on page 541 for more information.
Apply	Saves the new settings.
Reset	Resets the report to its original settings.

4 To generate the report, click *Generate*.

42.5 Generating Reports

You can generate an existing report, or generate multiple reports simultaneously. After the system displays the report, you can print the information or export and view the data in HTML, CSV, or XML formats.

1 In the ZENworks Control Center, click the *Reports* tab.

2 To generate a report, select the report's check box, then click *Generate*.

or

3 To generate a batch of reports, select the report folder's check box, then click *Generate*.

You can also select individual reports and run them simultaneously.

The following graphic is a sample of a generated ZENworks report.

Figure 42-1   *Report Generation Page*

42.6 Exporting Reports

There are two ways to export a report to HTML, CSV, or XML: you can generate the report and then export it, or you can export it directly without generating it first.

To generate the report and then export it:

1 Generate a report as described in Section 42.5, "Generating Reports," on page 541.

2 Click *HTML*, *CSV*, or *XML*.

To export a report directly:

1 In the ZENworks Control Center, click the *Reports* tab.

2 Select the check box of the report you want to export. (This feature is only available for single items.)

3 Click *Action* and select the desired format.

Table 42-2   *Output Types*

Output Type	Description
HTML	The system displays the report data in the default browser. However, you can choose another program to open this document, if needed. The HTML styles are embedded in the report output.
CSV	The system displays the information as CSV (comma-separated values), allowing you to view the report data in a spreadsheet.
XML	When you view a report in XML, the system displays the information using rows, rather than in table format. You can view this data in any application that can display XML.

42.7 Resetting Default Reports

Click *Reset Default Reports* to reset the default reports to their original settings when you installed ZENworks. The default reports are the bundle and device reports that come with the installed software.

NOTE: When new Dell devices are defined, *Reset Default Reports* regenerates the Dell default reports as well as adding reports for the new Dell devices.

Appendixes

XI

The following sections are accessed from other sections of the *Novell® ZENworks® 7.3 Linux Management Administration Guide*:

Command Line Utilities

<div style="text-align: right; font-size: 3em;">A</div>

zmd (8)

Name

zmd - The back-end daemon for the Novell® ZENworks® Linux Management agent.

Syntax

```
zmd [options]
```

Description

The zmd daemon performs software management functions on the ZENworks managed device, including updating, installing, and removing software, and performing basic queries of the device's package management database. Typically, these management tasks are initiated through the ZENworks Control Center or the rug, zen-installer, zen-updater, or zen-remover utilities, which means you should not need to interact directly with zmd.

The zmd daemon has built-in download interrupt support. If a download is interrupted, the zmd daemon resumes the download where it left off.

While making the HTTP requests, the zmd agent sets the HTTP User-Agent value to ZENworks Management Daemon/*<version>*, where *<version>* is a value as reported by the `rug ping` command.

The Device Black-Out feature of ZMD allows you to configure the following preferences:

- **blackout-interval "*<start_time> - <end_time>*":** The time interval for which the device is to be locked. Specify the start time and end time in the HH:MM format, with hours in 24-hour format. For example, if the device is to be locked from 9 a.m. to 6 p.m., specify the time interval as 09:00-18:00.

- **device-locked:** Valid values are "True" and "False". If the device-locked value is set to True, then zmd blocks install, removal, refresh, and register operations for packages and bundles. However, we recommend that you do not manually change the value of device-locked. The value is automatically set when you configure blackout-interval to specify the time interval when the device is to be locked. Depending on blackout-interval, the lock or unlock schedule is created and triggered. The lock or unlock schedule resets the device-locked value accordingly. If any refresh, bundle install, or bundle remove schedules are to be triggered when the device is locked, then these schedules are rescheduled to be triggered after the device is unlocked.

Options

Usage Options

-n, --non-daemon

Do not run the daemon in the background.

-m, --no-modules

Do not load any optional modules.

-r, --no-remote

Do not load any optional modules.

--no-services

Don't load the saved services.

Help Options

--help, -?

Display the help information and exit.

Files

zmd.conf

Configuration file. Options such as proxy and cache settings can be adjusted through this file directly or with the `rug set` command. The file is located in `/etc/opt/novell/zenworks/zmd/` on SLES 9, OES 1, NLD, RHEL 3/4/5; and in `/etc/zmd/` on SLES 10, SLED 10, and OES 2.

novell-zmd

Initialization script. You should use this script to start and stop zmd, rather than running it directly. The file is located in `/etc/init.d/` on SLES 9, SLES 10, SLED 10, NLD, RHEL, and OES.

zmd-messages.log

Log file. The file is located in `/var/opt/novell/log/zenworks/` on SLES 9, OES 1, NLD, and RHEL 3/4/5; and in `/var/log/` on SLES 10, SLED 10, and OES 2.

zmd

Cached information from servers. The directory is located in `/var/opt/novell/zenworks/cache/` on SLES 9, OES 1, NLD, and RHEL 3/4/5; and in `/var/cache/` on SLES 10, SLED 10, and OES 2.

initial-configuration

URL for the supported services that zmd registers at initial startup. You can provide all the options that you would have otherwise used from rug for registration. The file is located in `/etc/opt/novell/zenworks/zmd/` on SLES 9, OES 1, NLD, and RHEL 3/4/5; and in `/etc/zmd/` on SLES 10, SLED 10, and OES 2.

Examples

This program normally runs as `root`.

/etc/init.d/novell-zmd start

Runs the program in the standard way.

/opt/novell/zenworks/sbin/zmd or /usr/sbin/zmd

Runs the program directly.

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

rug (1)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

zrmservice (1)

Name

zrmservice - Configures the Novell® ZENworks® Remote Management agent.

Syntax

```
zrmservice [options]
```

Description

zrmservice is a command line interface to configure the Novell ZENworks Remote Management agent.

Options

Configuration Options

--passwd

Changes the Remote Management Agent password.

--clrpasswd

Clears the Remote Management Agent password.

--clearlog

Clears the Remote Management Agent message log files.

Help Options

--help

Displays the help information and exits.

Files

/etc/opt/novell/zenworks

Password file.

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

rug (1), zlman (1), zlmmirror (1), zmd (8), zlm-debug (1)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

zlm-debug (1)

Name

zlm-debug - The debug utility for Novell® ZENworks® Linux Management.

Syntax

```
zlm-debug [options]
```

Description

The zlm-debug utility lets you gather information to help you troubleshoot and solve problems you might encounter using ZENworks Linux Management. By default, zlm-debug gathers cache, server, client, configuration, hardware, and package data as well as log files. The information is packaged into a tarball file and placed in the location you specify. Use the options described below to limit the types of information you gather.

Options

--modules-dir=[directory_path]

Specifies the modules directory.

--tar-dir=[directory_path]

Specifies the directory to place the tarball in.

-a, --no-cache

Do not collect cache data. Cache data is located in the `/var/opt/novell/zenworks/cache/zmd` directory.

-c, --no-client

Do not collect client data. Client data is gathered from the `/var/opt/novell/zenworks/cache/zmd` directory.

-d, --no-hardware

Do not collect hardware data.

-l, --no-logs

Do not collect logs. Log files are located in the `/var/opt/novell/log/zenworks` directory.

-o, --no-config

Do not collect configuration data. Configuration data is located in the `/etc/opt/novell/zenworks` directory.

-p, --no-packages

Do not collect package data. Package data includes all version information for packages in the ZENworks Linux Management package repository. Package data is located in the `/var/opt/novell/zenworks/pkg-repo` directory.

`-s, --no-server`

    Do not collect server data. Server data includes PostgreSQL and Novell eDirectory data.

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

rug (1), zlman (1), zlmmirror (1), zmd (8), zrmservice (1)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

zlmmirror (1)

Name

zlmmirror - Mirrors bundles and catalogs of software, in whole or in part, from remote ZENworks® Linux Management, YaST Online Updates, Novell Updates, YUM, and Red Hat Network servers, to your local ZENworks Linux Management server or to a local directory. For detailed information about mirroring Dell Update Packages to your ZENworks server, see Mirroring Software in the *ZENworks 7.3 Linux Management Administration Guide*.

Syntax

```
zlmmirror [command] [options] [arguments]
```

This command reads the information necessary to connect to the local and remote server from an XML configuration file. Detailed information on creating zlmmirror configuration files is included in the *ZENworks 7.3 Linux Management Administration Guide*.

Description

zlmmirror enables you to connect to a remote server and copy software catalogs, bundles, or packages from the remote server to your server using a few simple commands. Software can be mirrored from the following servers:

- ZENworks Linux Management
- Dell Update Packages (DUPs)
- YaST Online Updates
- Red Hat* Network
- Red Carpet® Enterprise or ZENworks 6.*x* Linux Management
- Novell Updates
- YUM

Novell®, Dell, SUSE, and Red Hat each maintain servers of their respective types, enabling you to simply mirror the catalogs and bundles you are interested in without maintaining or updating these repositories. Mirroring is the preferred method of obtaining the majority of the software you distribute to managed devices.

During use, zlmmirror connects to the remote server, the local server, and to the zlman program, authenticating itself each time. It should be run on the same system as zlman and the rest of the ZENworks Linux Management server, and requires `root` privileges.

Commands

All of the commands below accept the option flags listed in the Global Options section. In addition, they accept individual options as listed with each command.

Configuration Commands

These commands are used to create, convert, and validate zlmmirror configuration files.

conf-convert (cc) [options] [file to convert] [converted filename]

> Converts the specified `rcmirror.conf` configuration file to the new XML format.

conf-generate (cg) [options] [target filename]

> Creates a new, empty configuration file showing all possible fields.

conf-validate (cv) [options] [filename]

> Checks the configuration file for errors, and display the parsed configuration information.

Catalog and Bundle Commands

These commands allow you to view the catalogs, bundles, and packages on the remote server.

bundle-list-packages (blp) [options] [bundle] [catalog]

> Lists the packages available in the specified bundle. Accepts the following option flags:
>
> -c,--conf=[filename] - Specifies the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.
>
> -t,--target - Restricts the listing to the specified target.

catalog-list-bundles(clb) [options] [catalog]

> Lists the bundles available in the specified catalog. Accepts the following option flags:
>
> -c,--conf=[filename] - Specifies the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.
>
> -t,--target - Restricts the listing to the specified target.

catalog-list-packages (clp) [options] [catalog]

> Lists the packages available in the specified catalog. Accepts the following option flags:
>
> -c,--conf=[filename] - Specifies the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.
>
> -t,--target - Restricts the listing to the specified target.

server-list-bundles (slb) [options]

> Lists the bundles available on the remote server. Accepts the following option flags:
>
> -p,--packages - For RCE servers, includes patch bundles only. (This excludes the package set bundles.)
>
> -c,--conf=[filename] - Specifies the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.
>
> -t,--target - Restricts the listing to the specified target.

server-list-catalogs (slc) [options]

> Lists the catalogs available on the remote server. Accepts the following option flags:
>
> -c,--conf=[filename] - Specifies the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.
>
> -t,--target - Restricts the listing to the specified target.

server-list-packages (slp) [options]

> Lists the packages available on the remote server. Accepts the following option flags:

-c,--conf=[filename] - Specify the configuration file to use; otherwise, the default (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.

-t,--target - Restricts the listing to the specified target.

Mirror Command

The mirror command is used to perform the actual mirroring operation contained in `zlmmirror.xml`.

`mirror (m) [options]`

Performs a mirroring operation. Accepts the following option flags:

-n, --dryrun - Prints the packages to be mirrored or added. It does not mirror anything.

-r, --re-download - Re-downloads the contents even if they are already mirrored.

-p, --packagesets - For RCE and NU servers, include patch bundles only. (This excludes the package set bundles).

-s, --sync-local - For a remote ZENworks Linux Management server, synchronizes the local server repository with the remote server repository.

--force-nevra - Allows a new package with a conflicting NEVRA (name, epoch, version, release, and architecture) to overwrite an existing package.

-c, --conf=[filename] - Specifies the configuration file to use. If not specified, the default file (`/etc/opt/novell/zenworks/zlmmirror.xml`) is used.

--category=[value] - Specifies values such as security, recommended, or optional. This value will have precedence over the values that you specify in the mirror configuration file. This command is applicable for RCE and NU servers.

-o, --remove-obsolete-patches - Removes the mirrored YOU patch bundles from the local ZENworks server if the bundles are obsolete in the YOU repository. If the YOU patch bundles are mirrored to a folder containing the obsolete patches, the obsolete patches are removed from that folder. This option is applicable only for the YOU server.

-g, --retain-guid - Retains the bundle GUID when mirroring bundles between ZENworks Linux Management Servers located in different management zones. By default, the bundles are created in the `Bundles/zlmmirror` directory. If a bundle with the same name exists on the local server, then mirroring that bundle from the remote server does not retain the bundle GUID. When you mirror bundles from the remote server, only the bundle that is currently deployed is mirrored to the local server. A new version of the bundle is created on the local server irrespective of the deployed version of the bundle on the remote server.

Options

`-h, --help`

Displays a help message.

`--log=[logfile]`

Logs messages to a file. If no log file is specified, the default (`/var/opt/novell/log/zenworks/zlmmirror.log`) is used.

`-v, --verbose`

Displays verbose output.

`--version`

> Prints zlmmirror version information and exits.

`--remote-timeout=[seconds]`

> Remote server connection timeout (seconds).

Files

`/etc/opt/novell/zenworks/zlmmirror.xml`

> The default configuration file.
>
> You must create a different XML configuration for each remote server you mirror. A template XML file can be created using the `conf-generate` command. See the *ZENworks Linux Management Administration Guide* for detailed instructions on mirroring.
>
> The following is a description of the sections contained in the zlmmirror XML configuration file. You must provide details about the remote server containing the software you want to mirror, and the local server, which is your ZLM server receiving the mirrored software, as well as information on the catalogs, bundles, and packages you want mirrored.

Remote Server

> The remote server is specified according to the following:

```
<RemoteServer>
<Base>https://zlm.novell.com/</Base>
<Type>zlm</Type>
<User>Administrator</User>
<Password>letmein</Password>
</RemoteServer>
```

> Base - Path to the server you want to mirror, in the following format depending on Type:
>
> - ZLM: `https://server`
> - DELL: `http://ftp.dell.com`
> - RCE: `https://server/path`
> - YaST: `http(s)://server/path` or `ftp://server/path`
> - RHN: `http(s)://server/path`
> - NU: `https://nu.novell.com/repo`
> - YUM: YUM respositories for SUSE such as `http://poincare.suse.de/testrepo/`
>
> Type - Type of server you want to mirror:
>
> - ZLM: ZENworks 7 Linux Management
> - DELL: Dell Update Package FTP Server
> - RCE: Red Carpet Enterprise, or ZENworks 6.*x* Linux Management
> - YaST: YaST Online Updates
> - RHN: Red Hat Network
> - NU: Novell Updates
> - YUM: Yellow Dog Updater, Modified

User - Name to use when connecting to the remote server. If no user is specified, zlmmirror reads the identity from the following location depending on Type:

- ZLM: `/etc/opt/novell/zenworks/zmd/deviceid` on SLES 9 and OES, and `/etc/zmd/deviceid` on SLES 10 and SLED 10

- RCE: `/etc/ximian/mcookie`

- YaST: `/etc/sysconfig/onlineupdate`

- NU: `/etc/opt/novell/zenworks/zmd/deviceid` on SLES 9 and OES, and `/etc/zmd/deviceid` on SLES 10 and SLED 10

- YUM: Does not require any authentication.

When connecting to an RHN server or a Dell Server, leave this element empty.

Password - Password to use when connecting to the remote server. If no password is specified, zlmmirror reads the password from the following location depending on Type:

- ZLM: `/etc/opt/novell/zenworks/zmd/secret` on SLES 9 and OES, `/etc/zmd/secret` on SLES 10 and SLED 10

- RCE: `/etc/ximian/partnernet`

- YaST: `/etc/sysconfig/onlineupdate`

- NU: `/etc/opt/novell/zenworks/zmd/secret` on SLES 9 and OES, `/etc/zmd/secret` on SLES 10 and SLED 10

- YUM: Does not require any authentication

When connecting to an RHN server or a Dell Server, leave this element empty.

Proxy - The Proxy configuration element is optional and is used with an Internet Proxy. You can add the Proxy element anywhere in the RemoteServer section. If the Internet proxy requires authentication, the format looks like the following example:

```
<Proxy>http://username:password@server:port</Proxy>
```

If the Internet proxy does not require authentication, the format looks like the following example:

```
<Proxy>https://server:port</Proxy>
```

SystemID - To mirror from the RHN server, you must add the SystemID configuration element in the zlmmirror configuration file. You can use the `systemid` file that has a valid authentication to the RHN server. You need to provide the complete path of the `systemid` file that is located on the ZENworks Server. The format looks like the following example:

```
<SystemID> /etc/opt/novell/zenworks/zlmmirror-example-rhn-conf.xml</SystemID>
```

Local Server

The local server is specified according to the following:

```
<LocalServer>
<Base></Base>
<Type>zlm</Type>
<User>Administrator></User>
<Password>letmein</Password>
</LocalServer>
```

Base - If the Type attribute is ZLM, leave this field empty. If the Type attribute is STATIC, enter the path to the local directory where you want the packages copied, in the following format: `/path/on/filesystem`.

Type - Type of mirroring you want to perform:

- ◆ ZLM: Mirrors catalogs and bundles directly to your ZENworks Linux Management server. After mirroring, mirrored catalogs and bundles are displayed in the ZENworks Control Center.

  You cannot perform ZLM mirroring on Secondary Servers.

- ◆ STATIC: Mirrors packages to the file system of your ZENworks Linux Management server, but does not add them to ZENworks.

  You can perform only static mirroring on Secondary Servers.

User - Name to use when connecting to your ZENworks Linux Management (local) server. The Administrator user should be specified if you want to use the default administrator account.

Password - Password for the account provided in User. If you are using the Administrator account, this is the password you specified during the server installation.

Catalogs, Bundles, and Packages

Each bundle and package you want to mirror must be contained in a catalog on the remote server, so Catalog is the only item necessary to mirror a catalog, bundle, or package. A configuration file can have multiple Catalog elements, and each catalog you want to mirror must have its own entry.

```
<Catalog>
<Name>Red Carpet 2</Name>
<LocalName>Red Carpet 2</LocalName>
<Target>sles-9-i586</Target>
<Package>lib.*</Package>
</Catalog>
```

Local Name - Name of the catalog you want the mirrored software placed in. If no Local Name is specified, the catalog name from the source server is used. The local name for the catalog should not be same as that reserved for the <catalogname>-patches folder.

Folder - Specifies the eDir folder (such as `/folder1/folder2`) where bundles and catalogs are created and updated. If not specified, the catalogs and bundles are created and updated in the `/zlmmirror` folder.

Target - Restricts the mirroring operation on the catalog to packages and patches that support the specified target platforms. If the target is not specified, packages for all platforms are mirrored. This element can be specified multiple times, and can contain either a target name or a regular expression string for matching target names. For example, to include targets beginning with sles such as sles-9-i586, use the regular expression *<Target>sles.*</Target>*.

ExcludeTarget - Same as Target, except packages and patches supporting the specified target platforms are excluded. ExcludeTarget is performed after Target, so platforms appearing in a Target and ExcludeTarget are ultimately excluded. For example, to exclude targets that end with i586 such as sles-9-i586, use the regular expression *<ExcludeTarget>.*i586</ExcludeTarget>*.

Bundle - Restricts the mirroring operation on the catalog to the specified bundles. If the bundle is not specified, all bundles are mirrored. This option is valid only for ZLM and YaST source servers. It can be specified multiple times, and can contain either a bundle name or a regular expression string for matching bundle names. See the note below about regular expressions for more information.

LocalBundleName - Renames the bundle name locally.This is applicable only for the RCE, NU, and RHN services in which a catalog has only one bundle on the remote server. If you specify `<LocalBundleName>`, you must not specify the `<Bundle>` tag. This tag is not applicable when you mirror OES from the RCE service with more than one bundle per catalog.

ExcludeBundle - Same as Bundle, except packages and patches contained in the specified bundle or bundles are excluded. This option is valid only for ZLM and YaST source servers, can be specified multiple times, and can contain either a bundle name or a regular expression string for matching bundle names. ExcludeBundle is performed after Bundle, so bundles appearing in a Bundle and ExcludeBundle are ultimately excluded. See the note below about regular expressions for more information.

Package - Restricts the mirroring operation on the catalog to the specified packages. If the package is not specified, all packages are mirrored. This option can be specified multiple times, and can contain either a package name or a regular expression string for matching package names. This option is not supported for patch bundles. Filtering of packages in a patch bundle is not supported for RCE, YaST, and NU type of remote servers. See the note below about regular expressions for more information.

ExcludePackage - Same as Package, except specified packages are excluded. This option can be specified multiple times, and can contain either a package name or a regular expression string for matching package names. This option is not supported for YOU patches. ExcludePackage is performed after Package, so packages appearing in a Package and ExcludePackage are ultimately excluded. See the note below about regular expressions for more information.

Category: Restricts the mirroring operation on the catalog to the specified categories of patch bundles. If the category is not specified, all patch bundles are mirrored. Valid values are recommended, optional, and security. This tag is applicable only for the RCE type servers and NU type servers of SLES 10, SLED 10, and OES 2.

ServicePackGroups - Accepts Boolean values (true or false) only. By default `<ServicePackGroups>` is set to true, and it automatically creates bundle groups. This option is supported for YOU patches only.

AutoDeploy - Mirroring the packages to existing bundle creates a newer version of the bundle and deploys it on the server. If AutoDeploy is set to false, then the mirroring operation restricts the deployment of the newer bundle. Accepts only the boolean values (true or false). By default, the option is set to true.

CreateMonolithicBundle - Automatically creates monolithic package bundles consisting of only latest package rpms. It creates a separate monolithic bundle for each Service Pack release, and a separate monolithic bundle with the updates after the latest Service Pack release. It accepts Boolean values (true or false) only. By default the option is set to true. This option is supported for YOU patches only.

FilterPatchRPM - Restricts the mirroring operation of the YOU patch bundles to filter all the packages of the `.patch.rpm` type. This option creates an equivalent RPM package bundle in the local server. Accepts only the Boolean values (true or false). By default, the option is set to false. This option is supported only for the YOU patches.

NOTE: The use of regular expressions (regexes) has changed in ZENworks 7.3 Linux Management. ZENworks Linux Management does not use wildcard character matching. In ZENworks Linux Management 6.6.*x*, you can use a wildcard expression string instead of a regular expression string. In ZENworks 7.3 Linux Management, you should use `<Bundle>patch-.*</Bundle>` to mirror all bundles with the name starting with "patch-". ZENworks Linux Management supports all the Java regular expressions. For more information on the Java regular expressions, see the Java documentation (http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/Pattern.html).

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

rug (1), zlman (1), zmd (8), zlm-debug (1), zrmservice (1)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

zlman (1)

Name

zlman - zlman is the command-line interface to Novell® ZENworks® Linux Management, which provides comprehensive Linux* server and workstation management.

Syntax

```
zlman [command] [options] [arguments]
```

In general, zlman commands have both a short form and a long form. The long form is assembled in the form object-actionobject. For example, the command `registration-list` lists all registrations in a registration folder. There are a large number of commands, but most of them are easy to remember, because there are a limited number of objects (workstation, server, bundle, catalog, policy, administrator, registration) and actions (list, create, modify, delete) to perform on them.

Arguments for a command are ordered in the same way as the command itself: for `catalog-addbundle`, the catalog is named first and the bundle second. For example, `catalog-addbundle catalog2 bundle4`. Option flags always come before any arguments.

The abbreviated form of each command uses one letter from each word in the long form: In this manner, `admin-list` is shortened to `al`. The exceptions to these general syntax rules are system commands such as `ping` and `server-version` which apply directly to the server.

For filenames, you can use standard shell globbing: `*.rpm` is used to indicate "all files ending in .rpm."

Description

ZENworks Linux Management is the next evolution in Linux server and workstation management. ZENworks Linux Management provides comprehensive Linux management, including:

- Advanced software package management, including dependency resolution, support for SUSE patches, and the ability to roll back to previous versions.
- Automated imaging and scripted installs using YaST autoinstall and Red Hat* kickstart.
- Secure and fast graphical remote management of servers and desktops.
- Hardware, software, and operating system inventory collection and reporting.
- Comprehensive policy-based management of Linux servers and desktops.
- Task-driven Web management interface.

The zlman command-line interface provides you with a full-featured application that uses scripting to simplify many operations, and provides quick access to operations. A comprehensive Web management interface with many advance features is also installed on your ZENworks Linux Management server.

Guide to Usage

This section contains a guide to general command formatting and conventions.

Administrators

> Every action in zlman is governed by the access limitations of the administrator. The initial Administrator account created during the initial installation has rights to all objects. Additional administrator accounts you create are granted read-only rights by default. These accounts must be explicitly granted rights to any objects they are to manage.

Folders

> If no folder is specified for commands that take a folder argument, the command targets the root folder. To specify a folder path, list each folder from the root separated by a forward slash (/). For example, if you have a folder named folder1 in the root, containing a subfolder named subfolder1, you would reference this folder as folder1/subfolder1. Each specified folder must already exist.

Ellipsis (...)

> An ellipsis indicates that a command accepts multiple entries of the last argument type. For example, the ellipsis in the following command indicates that `catalog-add-bundle` can accept multiple bundles:
>
> `zlman catalog-add-bundle [options] [catalog] [bundle] [...]`

Option Flags

> Commands that do not have command-specific options (they accept only the standard option flags) do not have options listed as an argument in the command reference. For example, the reference entry for the following command does not list options because it accepts only the standard flags:
>
> `zlman workstation-list [folder] [filter]`
>
> However, the following command lists options because the command has a command-specific option (-a):
>
> `zlman workstation-messages [options] [workstation name]`

RC File

Creating a `.zlmanrc` file in your home directory enables you to provide global options that are added to each command. For example, adding `-U Administrator -P password` causes each command to read your username and password from this file instead of prompting. To bypass the options stored in this file, use the `--ignore-rc-file` option.

Commands

All of the commands below accept the option flags listed in the Global Options section. In addition, they accept individual options as listed with each command.

Administrator Commands

These commands are used to create and adjust administrator accounts. Administrator commands begin with word `admin` in the long form or the letter `a` in the short form.

admin-create (ac) [options] [administrator] [password]

Creates a new administrator account. By default, this account is created with view-only rights to all objects. Use the `admin-rights-assign` command to grant additional rights to this account.

admin-delete (ad) [options] [administrator] [...]

Deletes an administrator account.

admin-list (al) [options] [folder]

Lists all administrator accounts. Accepts the following option flags:

-r,--recursive - Includes subfolders.
-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

admin-rename (arn) [options] [admin name] [new name]

Renames the administrator account specified by current name to new name.

admin-rights-assign (ara) [options] [admin name] [object name] [...]

Assigns the specified administrator rights to the object specified by object. One of the following options must be specified to indicate the object type:

-w,--workstations
-s,--servers
-a,--administrators
-b,--bundles
-p,--policies
-R,--reports
-r,--registrations

Additionally, this command accepts the following option flags:

-n,--none - All rights to the specified object are revoked.
-v,--view - Grants view-only access to the specified object.
-m,--modify - Grants rights to modify the specified object.
-c,--create - Grants rights to create new objects.

admin-rights-get (arg) [options] [admin name] [object name] [...]

Views the effective rights of a specified object. If no object is specified, all assigned rights display. A single type flag must be specified. One of the following options can be specified to indicate the object type:

-w,--workstations
-s,--servers
-a,--administrators
-b,--bundles
-p,--policies
-R,--reports
-r,--registrations

Additionally, this command accepts the following option flags:

-n,--none - All rights to the specified object are revoked.

-v,--view - Grants view-only access to the specified object.

-m,--modify - Grants rights to modify the specified object.

-c,--create - Grants rights to create new objects.

admin-set-password (asp) [options] [admin name] [password]

Sets an administrator's password. Only the administrator can change other administrator passwords. All administrators can change their own passwords.

Replicate Commands

These commands are used to replicate repositories from Primary Servers to Secondary Servers.

replicate-repositories-now [options]

Immediately replicates repositories to all the Secondary Servers.

Bundle Commands

These commands are used to create and modify bundles and folders, including adding packages to bundles and creating patch bundles. zlman treats objects and their corresponding folders as one object type. Therefore, `zlman bundle-rename` can rename bundles or bundle folders; `zlman bundle-move` can move bundles or bundle folders, etc. Bundle commands begin with the word `bundle` in the long form, or with the letter `b` in the short form, with the exception of the patch bundle command, which begins with the letter `p`.

bundle-add-file (baf) [options] [bundle] [target-platform] [destination] [file] [...]

Adds a file to a bundle. Accepts the following arguments:

Bundle - An existing bundle to which you want to add one or more files.
File - The file being added. Specify its full path.

Accepts the following option flags:

--destination=[path] - Full path where the file should be deployed on the client.
--unpack - Indicates that this file is compressed and should be decompressed and extracted on the client. The supported compression formats are `.gz` and `.bz2`.
--permissions=[xxx] - UNIX file permissions to be applied to this file after deployment (not applicable for compressed files.)

bundle-add-package (bap) [options] [bundle] [target] [package file] [...]

Adds a package to a bundle. Accepts the following arguments:

Bundle - An existing bundle to which you want to add one or more RPM packages.
Target - OS/Platform targets. (valid targets for your environment can be viewed using `zlman tl`.)
Package File - RPM format package file.

Accepts the following option flags:

--force-nevra - Force the package to add in spite of the NEVRA (name, epoch, version, release, and architecture) conflict.
 --freshen - Upgrade the package only if it is installed.

--installtype=[upgrade|install] - Specify the rpm installation type. The upgrade value triggers the rpm -u behavior and the install value triggers the rpm -i behavior.

--ver=[bundle version] - Specify the bundle version to which the package must be added. By default, the package is added to the latest version of the bundle.

`bundle-copy (bco) [options] [source bundle] [version] [name]`

Copies a bundle version to a new bundle.

`bundle-copy-package (bcp) [options] [source bundle] [target bundle] [target]`
`[package] [version] [release] [arch] [epoch]`

Copies the packages from the source bundle to the target bundle.

NOTE: Copying RPM packages from one bundle to another bundle does not update the version of the target bundle.

`bundle-create (bc) [options] [name] [folder]`

Creates a new bundle. If a folder is provided, the bundle is created in the specified folder. Accepts the following option flags:

--description=[description] - Provides a description for the bundle.

--disable-persistence - Does not apply the persistence when the bundle is installed.

`bundle-delete [options] (bd) [bundle] [...]`

Deletes one or more bundles or bundle folders.

`bundle-delete-version [options] (bdv) [bundle] [version]`

Deletes a specific version of a bundle.

`bundle-deploy (bp) [options] [bundle] [version]`

Deploys the specified version of a bundle.

`bundle-folder-create (bfc) [options] [name] [folder]`

Creates a new folder for containing bundles in the path specified by folder.

`bundle-group-add (bga) [options] [bundle group] [bundle] [...]`

Adds a bundle to a bundle group. Accepts the following option flag:

-r, --recursive - Includes subfolders.

`bundle-group-create (bgc) [options] [name] [folder]`

Creates a bundle group in the specified folder.

`bundle-group-members (bgm) [options] [bundle group]`

Lists the members of a bundle group.

`bundle-group-remove (bgr) [options] [bundle group] [bundle] [...]`

Removes a bundle from the specified bundle group.

`bundle-info (bi) [options] [bundle] [version]`

Displays detailed information about a bundle. The version can be specified for software bundles. If now version is specified, the deployed version is shown.

bundle-list (bl) [options] [folder]

Lists all bundles and bundle folders in the specified folder. Accepts the following option flags:

-r,--recursive - Includes subfolders.

-f,--filter - Displays options matching the specified filter. Wildcard characters * and ? can be used if they are enclosed in quotation marks.

bundle-list-dups (bld) [options] [bundle]

Lists the Dell Update Packages contained in a DUP bundle.

bundle-list-files (blf) [options] [bundle] [target]

Displays a list of files contained in the specified bundle, including the bundle ID.

bundle-list-packages (blp) [options] [bundle] [target]

Displays a list of packages contained in the specified bundle, including the bundle ID.

bundle-list-versions (blv) [options] [bundle]

Displays a list of the version numbers for the specified bundle.

bundle-move (bmv) [options] [bundle] [new folder]

Moves the specified bundle or bundle folder to the specified folder.

bundle-remove-dup (brd) [options] [bundle] [package ID] [[package ID] [...]]

Removes a Dell Update Package from a DUP bundle. The package ID is listed with the `bundle-list-dups` command.

bundle-remove-package (brp) [options] [bundle] [target] [package ID] [[package ID][...]]

Removes a package from a bundle. The package ID is listed with the `bundle-list-packages` command.

bundle-remove-file (brf) [options] [bundle] [target] [file ID] [...]

Removes a package from a bundle. Use the `bundle-list-files` command to find the file ID.

bundle-rename (brn) [options] [current name] [new name]

Renames the specified bundle or bundle folder to the name specified by new name.

bundle-update-package (bup) [options] [bundle] [target] [package file] [[package file] [...]]

Update the properties of a package in a bundle. Accepts the following options.

--arch=[arch] - Specifies the arch of package to update.

--freshen=[true|false] - Only upgrade package if installed.

--installtype=[install type] - Specifies the RPM installation type. The upgrade value indicates the rpm - U behavior, and the install value indicates the rpm - i behavior.

file-bundle-create (fbc) [options] [name] [folder]

Creates a new file bundle.

`patch-bundle-create (pbc) [options] [product name] [product version] [product arch] [patch file] [folder]`

> Creates a new patch bundle. Accepts the following arguments:
>
> Product Name - Name of the product to which this patch applies, must be one of the following: SUSE LINUX, SUSE SLES, SUSE CORE, Novell Linux Desktop, SuSE SLED.
>
> Product Version - Version of the product to which this patch applies.
>
> Product Arch - Product architecture. Must be one of the following: i386, x86_84
>
> Patch File - File containing the patch.
>
> Folder - Bundle folder to use for this patch bundle.

Catalog Commands

These commands are used to create and modify catalogs, including adding bundles to catalogs. Catalog commands begin with the word `catalog` in the long form, or with the letter `c` in the short form.

`catalog-add-bundle (cab) [options] [catalog] [bundle] [...]`

> Associates one or more bundles or bundle groups with a catalog. Accepts the following option flag:
>
> --relative=[DD:HH:MM] - Specifies that the action should be performed at a time relative to now. The time should be formatted as DD:HH:MM. A repeat frequency can be specified.

`catalog-create (cc) [options] [catalog name] [containing folder]`

> Creates a new catalog in the specified folder.

`catalog-delete (cd) [options] [catalog] [...]`

> Deletes the specified catalog.

`catalog-folder-create (cfc) [options] [folder name] [containing folder]`

> Creates a new folder for containing catalogs. If a folder is provided, the catalog is created in the specified folder. The containing folder can be a path to an existing catalog folder, such as folder/subfolder.

`catalog-list (cl) [options] [folder] [filter]`

> Lists catalogs in a folder. Accepts the following option flags:
>
> -r,--recursive - Includes subfolders.
>
> -f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

`catalog-list-bundles (clb) [options] [catalog]`

> Displays the list of all bundles assigned to a catalog.

`catalog-move (cmv) [options] [catalog] [new folder]`

> Moves the specified catalog to the location specified by new folder. The folder you specify using `[new folder]` must already exist or the move fails.

`catalog-rename (crn) [options] [current name] [new name]`

> Renames the specified catalog.

catalog-remove-bundle (crb) [options] [catalog] [bundle] [...]

>   Removes the specified bundle from the specified catalog.

Hotlist Commands

This command is used to view the list of devices that have unacknowledged warnings or errors.

hotlist

>   Displays a list of devices that have unacknowledged warnings or errors. Warning or errors can be acknowledged using the `workstation-ack` and `server-ack` commands. After all warnings or errors for a device are acknowledged, the device no longer appears on the hotlist.

License Commands

These commands are used to activate your server or display licensing information. License commands begin with the word `license` in the long form, or with the letter `l` in the short form.

license-activate (la) [options] [key]

>   Activates your system.

license-info (li) [options]

>   Displays licensing information.

license-set-seats (lss) [options] [count]

>   Sets the number of allowed active devices.

Package Commands

These commands are used to modify packages. Package commands begin with the word `package` in the long form, or with the letter `p` in the short form.

delete-packages (dp) [options] [package filename]

>   Deletes the specified package.

package-list-bundles (plb) [options] [package filename]

>   Displays a list of the bundles that contain the specified package.

list-packages (lp) [options]

>   Lists packages. Accepts the following option flags:
>
>   --name-filter = [name-filter] - Name filter.
>   --epoch-filter = [epoch-filter] - Epoch filter.
>   --version-filter = [version-filter] - Version filter.
>   --release-filter = [release-filter] - Release filter.
>   --arch-filter-[arch-filter] - Arch filter.
>   --target filter [target-filter] - Target filter.
>   --orphan - List the orphaned packages.
>
>   To delete orphan packages, use the `zlman lp --orphan|cut -d'|' -f1 -s | grep ^[0-9] | xargs zlman dp` command.

package-replace-packages (prp) [options] [target] [package filename] [...]

Replaces the specified package with another package with the same name, epoch, version, release, architecture, and target (NEVRAT). You can replace multiple packages by specifying multiple filenames.

NEVRAT is a term to describe a unique RPM identifier generated from the Name, Epoch, Version, Release, Architecture, and Target properties of a given `.rpm` file. This identifier is guaranteed to be unique to a given `.rpm`; however, this guarantee can be violated given the following scenarios:

- A corrupted RPM file was downloaded. The checksum of this corrupted `.rpm` does not match the known checksum of the same uncorrupted `.rpm`, as identified via NEVRAT.

- A vendor incorrectly released an improperly formatted update `.rpm` package, with newer (different) contents but still identifying itself with the same version and release numbers. This results in a different checksum being encountered for what the system identifies as the same package, based on its NEVRAT properties. This is rare, but it does occur on occasion. This problem is most often encountered when performing bulk mirroring of entire distributions.

Several workarounds exist for this problem:

- If the package is not of interest, exclude it from mirroring by using the `<ExcludeBundle/>` or `<ExcludeTarget/>` options in the `zlmmirror.conf` file. Use `<ExcludeBundle>` for ZENworks Linux Management and YaST source servers. For other source servers, use `<ExcludeTarget>`. The value of either tag is the package/patch/bundle to exclude from the mirroring.

- If the package is of interest, it must be first retrieved to the file system. This can be accomplished in a variety of ways, including static mirroring. After the given `.rpm` is available on the server's file system, it is possible to import it into the server using the `package-replace-package` command.

Using the `package-replace-packages` command results in the newer package with the same NEVRAT replacing the existing package in all bundles it is a member of.

The following example shows the correct usage:

```
rc-qa-client-402:/opt/novell/zenworks # zlman prp sles-9-i586
/root/nrmtest-same-nevrat-b.rpm
Username:administrator
Password:******
[package.command.replacePackage.success]
```

Queue Commands

These commands are used in situations when you need to make modifications to the queue. The queue processes asynchronous events such as XML file regeneration and client refreshes, and does not need to be modified under most circumstances. Queue commands begin with the word `queue` in the long form, or with the letter `q` in the short form.

queue-flush (qf) [options] [status]

Flushes the queue by deleting the contents based on the status. Accepts the following values for the status argument:

N - New
F - Failed.
S - Succeeded

I - In progress

If you don't specify a status, all entries in the queue are deleted.

`queue-list (ql) [options] [status]`

Lists all queue entries. If a status is provided, only queue entries matching the specified status are displayed. Accepts the following option flags:

-f,--filter - Displays options matching the specified filter. The * and ? wildcard characters can be used if they are enclosed with in quotation marks.

Accepts the following values for the status argument:

N - New
F - Failed
S - Succeeded
I - In progress

`queue-reset (qr) [options] [status]`

Resets the status of all entries in the queue to New.

Registration Commands

These commands allow you to create and alter registrations. Registration commands begin with the word `registration` in the long form, or with the letter `r` in the short form.

`registration-add-server-group (rasg) [options] [key] [group] [...]`

Adds membership in the specified server group to objects registering using the specified key.

`registration-add-workstation-group (rawg) [options] [key] [group] [...]`

Adds membership in the specified workstation group to objects registering using the specified key.

`registration-create-server (rcs) [options] [key] [device folder] [registration folder]`

Creates a registration specifying folder membership for servers.

`registration-create-workstation (rcw) [options] [key] [workstation folder] [registration folder]`

Creates a registration specifying membership in the specified workstation folder.

`registration-delete (rd) [options] [key] [...]`

Deletes the specified registration.

`registration-folder-create (rfc) [options] [folder name] [containing folder]`

Creates a folder specified by [folder name] in the location specified by [containing folder].

`registration-info (ri) [options] [key]`

Displays detailed information about the specified registration.

`registration-list (rl) [options] [folder] [filter]`

Lists all registrations. Accepts the following option flags:

-r,--recursive - Includes subfolders.

-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

`registration-list-groups (rlg) [options] [key]`

Displays a list of the groups associated with the specified registration. Devices registering with this key are added to the listed groups.

`registration-move (rmv) [options] [key] [new folder]`

Moves the specified registration to the specified folder.

`registration-remove-server-group (rrsg) [options] [key] [group] [...]`

Removes the membership in the specified group from the registration key. Any device that has previously registered using this key does not lose group membership. This change applies only to new devices using this registration.

`registration-remove-workstation-group (rrwg) [options] [key] [group] [...]`

Removes the membership in the specified group from the registration key. Any device that has previously registered using this key does not lose group membership. This change applies only to new devices using this registration.

`registration-update (ru) [options] [key]`

Updates a registration by allowing you to change the properties of the registration key. Accepts the following options:

-k, --newkey=[key] - Updates the name of the key with the provided name.

-u, --usage=[count] - Updates the maximum number of devices that can be registered using this key to the provided number.

--unlimited - Removes limits on the number of devices that can be created with this key.

-n, --nrule=[naming rule] - Specify a new naming rule, such as ${HostName}. Possible naming variables include ${Alias}, ${AssetTag}, ${CPU}, ${DNS}, ${DeviceType}, ${GUID}, ${HostName}, ${Location}, ${OS}. Naming rules can contain a combination of variables, such as ${HostName}-${OS}.

--workstation-folder=[folder] - Specifies a new folder for workstations that register using this key.

--server-folder=[folder] - Specifies a new folder for servers that register using this key.

Ruleset Commands

These commands are used to create and modify rule sets. Rule sets are applied to new devices registering to your server that do not present a registration key. Rule set commands begin with the word `ruleset` in the long form, or with the letters `rs` in the short form.

`ruleset-add-rule (rsar) [options] [name or position] [attribute] [operator] [value]`

Adds a rule to a rule set. Each rule defines a condition that must be met in order for a rule set to be applied to a device. Each rule in a rule set must evaluate to TRUE in order for the rule set to be applied. Accepts the following arguments:

Attribute - Valid attributes are: Alias, AssetTag, CPU, DNS, DeviceType, GUID, HostName, IPAddress, Location, MacAddress, OS, and SubnetMask.

Operator - Valid string operators are: contains, starts, ends, equals. Valid integer operators are: <, <=, =, >, >=.

Value - The format and contents of value are determined by the attribute. For additional information about attribute values see the Inventory section in the ZENworks Linux Management Administration Guide.

`ruleset-add-server-group (rsasg) [options] [name or position] [group] [...]`

Adds workstation group membership to objects imported with a given rule set. Any servers that satisfy each rule condition of the rule set are added to the specified groups.

`ruleset-add-workstation-group (rsaw) [options] [name or position] [group] [...]`

Adds server group membership to objects imported with a given rule set. Any workstations that satisfy each rule condition of the rule set are added to the specified groups.

`ruleset-create-workstation (rscw) [options] [name] [position]`

Creates a new rule set to apply when a workstation registers without a key.

`ruleset-create-server (rscs) [options] [name] [position]`

Creates a new rule set to apply when a server registers without a key.

`ruleset-delete (rsd) [options] [name or position]`

Removes a rule set.

`ruleset-info (rsi) [options] [name or position]`

Displays detailed information about a rule set.

`ruleset-list (rsl) [options]`

Lists all rule sets. Accepts the following option flags:

-f,--filter - Displays options matching the specified filter. Wildcard characters * and ? can be used if they are enclosed in quotation marks.

`ruleset-list-groups (rslg) [options] [name or position]`

Displays a list of groups that a device will be a member of when it is created with the specified rule set.

`ruleset-move (rsmv) [options] [name or position] [new position]`

Changes the position of a rule set.

`ruleset-remove-rule (rsrr) [options] [ruleset name or position] [rule position]`

Removes a rule from a rule set.

`ruleset-remove-server-group (rsrsg) [options] [name or position] [group] [...]`

Removes server group membership from a rule set. Group membership for devices that have already registered is unaffected. This applies only to new devices when they register.

**`ruleset-remove-workstation-group (rsrwg) [options] [name or position] [group]
[...]`**

> Removes workstation group membership from a rule set. Group membership for devices that have already registered is unaffected. This applies only to new devices when they register.

`ruleset-update (rsu) [options] [name or position]`

> Updates values of a rule set. Accepts the following options:
>
> -k, --newname=[key] - Specifies a new name for the given rule set.
>
> -n, --nrule=[naming rule] - Specifies a new naming rule for the given rule set.
>
> --workstation-folder=[folder] - Specifies a new folder to place workstations in when they are created with the specified rule set.
>
> --server-folder=[folder] - Specifies a new folder to place servers in when they are created with the specified rule set.

Server Commands

These commands are used to manage servers. Server commands begin with the word `server` in the long form, or with the letter `s` in the short form.

`server-ack (sa) [options] [server] [log ID] [...]`

> Acknowledges a message associated with a device.

`server-add-bundle (sab) [options] [server] [bundle]`

> Associate one or more bundles with a device. Accepts the following option flags:
>
> --dry-run - Simulates the transaction and does not make any changes on the managed device. This option is not applicable for File bundles.
>
> -a, --allow-removal - Allows removal of a bundle. This option is not applicable for File bundles.
>
> --push-now - Specifies that the action must be immediately performed. A repeat frequency can be specified. If no other schedule is specified, it defaults to Now.
>
> --prepare-time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.
>
> --prepare-date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.
>
> --time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.
>
> --date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.
>
> --relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.
>
> --weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:
>
> Monday = M
>
> Tuesday = TU
>
> Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month when the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

--bundle-lock - Locks bundles on the managed devices from the server.

`server-add-catalog (sac) [options] [server] [catalog] [...]`

Associate one or more catalogs with a device. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

--relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month when the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

`server-add-policy (sap) [options] [server] [policy] [...]`

Associates one or more policies with a device. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

--relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month when the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

server-delete (sd) [options] [server] [...]

Deletes one or more devices, folders, or groups.

server-folder-create (sfc) [options] [folder name] [containing folder]

Creates a new folder in the specified folder.

server-group-add (sga) [options] [group] [server] [...]

Adds one or more servers to a group.

server-group-create (sgc) [options] [group name] [containing folder]

Creates a new group in the specified folder.

server-group-members (sgm) [options] [group]

Lists servers that are members of the specified group.

server-group-remove (sgr) [options] [group] [server] [...]

Removes one or more servers from a group.

server-health (sh) [options] [server]

Displays the health status of a ZENworks Primary Server. Its health status is determined by pinging the core admin services on the server.

server-info (si) [options] [server]

Displays detailed information about the specified device.

server-list (sl) [options] [folder] [filter]

Lists devices in the specified folder. Accepts the following option flags:

-r,--recursive - Includes subfolders.

-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

server-list-bundles (slb) [options] [server]

Lists bundles associated with a server.

server-list-catalogs (slc) [options] [server]

Lists catalogs associated with a server.

server-list-policies (slp) [options] [server]

Lists policies associated with a device.

server-messages (sm) [options] [server]

Displays a list of unacknowledged messages associated with the specified device. Accepts the following option flag:

-a, --all - Displays all messages including acknowledged messages.

server-move (smv) [options] [server] [folder]

Moves a device to a different folder.

server-refresh (sr) [options] [server]

Refreshes all policies and bundles on one or more device, folder or group. Accepts the following option flags:

--service=[service] - Specifies a specific service to refresh. The service must be one of the following: registration, Log, policymanager, settings, inventory.

server-rename (srn) [options] [current name] [new name]

Renames a device.

server-remove-bundle (srb) [options] [server] [bundle] [...]

Removes the association between a server and one or more bundles. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in the 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

--relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

server-remove-catalog (src) [options] [server] [catalog] [...]

Removes the association between a device and one or more catalogs.

server-remove-policy (srp) [options] [server] [policy] [...]

Removes the association between a server and one or more policies.

ping [options]

Verifies whether the server is operational and responding.

Target Commands

These commands are used to create and manage the list of valid OS targets. Target commands begin with the word target in the long form, or with the letter t in the short form.

target-create (tc) [options] [name] [arch] [package manager] [primary role] [product name] [vendor] [version] [detect string]

Creates a new OS target. Accepts the following arguments:

Name - Target name, such as sles-9-i586.

Arch - Architecture, such as i586 or x86_64.

Package Manager - System package manager, such as rpm.

Primary Role - Role of the operating system, set to Server or Workstation.

Product Name - Name of the product, such as SUSE Linux Enterprise Server.

Vendor - Product vendor, such as Novell or SUSE.

Version - Product version, such as 10 for SUSE Linux Enterprise Server.

Detect String - Location where the OS and version can be read on the system. For example, the SLES 9 detect string is <file source="/etc/SuSE-release" substring="SUSE LINUX Enterprise Server 9"/>. This detect string looks for "SUSE LINUX Enterprise Server 9" in /etc/SuSE-release to find a match for this target.

target-delete (td) [options] [target]

Deletes a user-defined OS target.

target-info (ti) [options] [target]

Displays detailed information about an OS target.

target-list (tl) [options]

Displays a list of current OS targets. Accepts the following option flag:

-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

target-update (tu) [options] [target]

Modifies values for a user-created OS target. Accepts the following options:

--arch=[arch] - Specifies a new arch value.

--pkgmgr=[package manager] - Specifies a new Package Manager value.

--enable - Enables a disabled OS Target.

--disable - Disables an enabled OS Target.

--role=[primary role] - Specifies the primary role of this target.

--product=[product name] - Specifies a new product name.

--vendor=[vendor] - Specifies a new vendor.

--detect=[detect string] - Specifies the OS detection string.

--version=[version] - Specifies a new version.

Workstation Commands

These commands are used to manage workstations. Workstation commands begin with the word `workstation` in the long form, or with the letter `w` in the short form.

`workstation-ack (wa) [options] [workstation name] [log ID] [...]`

Acknowledges a message associated with a workstation.

`workstation-add-bundle (wab) [options] [workstations] [bundle] [...]`

Assigns one or more bundles to a device. Accepts the following option flags:

--dry-run - Simulates the transaction and does not make any changes on the managed device. This option is not applicable for File bundles.

-a, --allow-removal - Allows packages to be removed if there are conflicts. This option is not applicable for File bundles.

--push-now - Immediately pushes the bundle to the managed device.

--prepare-time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.

--prepare-date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

---relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month when the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

--bundle-lock - Locks bundles on the managed devices from the server.

`workstation-add-catalog (wac) [options] [workstation] [catalog]`

Associates one or more catalogs with a device. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

---relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month when the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

`workstation-add-policy (wap) [options] [workstation] [policy] [...]`

Associates one or more policies with a device. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in the 24-hour format.

--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.

--relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.

--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:

Monday = M

Tuesday = TU

Wednesday = W

Thursday = TH

Friday = F

Saturday = SA

Sunday = SU

--monthly=[DD] - Specifies the day of the month the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.

---gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

workstation-delete (wd) [options] [workstation name] [...]

Deletes one or more workstation devices, folders, or groups.

workstation-folder-create (wfc) [options] [folder name] [containing folder]

Creates a new folder.

workstation-group-add (wga) [options] [group] [workstation] [...]

Adds one or more workstations to a group.

workstation-group-create (wgc) [options] [group name] [containing folder]

Creates a new group.

workstation-group-members (wgm) [options] [group]

Lists workstations in a group.

workstation-group-remove (wgr) [options] [group] [workstation] [...]

Removes one or more workstations from a group.

workstation-info (wi) [options] [workstation]

Displays detailed information about the specified device.

workstation-list (wl) [options] [folder] [filter]

Lists the workstations contained in the specified folder. Accepts the following option flags:

-r,--recursive - Includes subfolders.

-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

workstation-list-bundles (wlb) [options] [workstation]

Lists bundles associated with a workstation.

workstation-list-catalogs (wlc) [options] [workstation]

Lists catalogs associated with a device.

workstation-list-policies (wlp) [options] [workstation]

Lists policies associated with a device.

workstation-messages (wm) [options] [workstation name]

Displays a list of unacknowledged messages associated with the specified device. Accepts the following option flag:

-a, --all - Displays all messages including acknowledged messages.

workstation-move (wmv) [workstation name] [new folder]

Moves a workstation to a different folder.

workstation-refresh (wr) [options] [workstation name]

Refreshes all policies and bundles on one or more device, folder, or group. Accepts the following option flags:

--service=[service] - Specifies a specific service to refresh. Service must be one of the following: registration, Log, policymanager, settings, inventory.

workstation-rename (wrn) [options] [current name] [new name]

Renames a workstation.

workstation-remove-bundle (wrb) [options] [workstation] [bundle] [...]

Removes the association between a device and one or more bundles. Accepts the following option flags:

--time=[HH:MM] - Specifies a time of day when the action must be performed. The time must be specified in the HH:MM format, with hours in the 24-hour format.
--date=[YYYY-MM-DD] - Specifies a date when the action must be performed. The date must be specified in the YYYY-MM-DD format.
--relative=[DD:HH:MM] - Specifies that the action must be performed at a time relative to now. The time must be in the DD:HH:MM format. A repeat frequency can be specified.
--weekly=[MWF] - Specifies the days of the week when the action must be performed. If specified, the action is repeated on the specified days every week. For example, if you specify MWF, the action is executed every Monday, Wednesday, and Friday. The values for the days of a week are:
Monday = M
Tuesday = TU
Wednesday = W
Thursday = TH
Friday = F
Saturday = SA
Sunday = SU
--monthly=[DD] - Specifies the day of the month the action must be performed. If specified, the action is repeated on the specified day every month. You can specify only one day and not multiple days.
--gmt - The specified time is taken as GMT. If this is not specified, the time is the local time of the device.

workstation-remove-catalog (wrc) [options] [workstation] [catalog] [...]

Removes the association between a device and one or more catalogs.

workstation-remove-policy (wrp) [options] [workstation] [policy] [...]

Removes the association between a device and the specified policies.

workstation-health (wh) [options]

Determines the health status of a device.

Policy Commands

These commands are used to modify and manage policies. Policies must be initially created using the ZENworks Control Center. Policy commands begin with the word `policy` in the long form, or with the letter `p` in the short form.

policy-delete (pd) [options] [policy] [...]

Deletes a policy.

policy-folder-create (pfc) [options] [name] [containing folder]

Creates a new folder for containing policies.

policy-group-add (pga) [options] [group] [policy] [...]

Adds a policy to a policy group.

policy-group-create (pgc) [options] [group name] [folder]

Creates a policy group.

policy-group-members (pgm) [options] [group]

Lists the members of a policy group.

policy-group-remove (pgr) [options] [group] [policy]

Removes a policy from a policy group.

policy-list (pl) [options] [folder] [filter]

Lists policies in a folder. Accepts the following option flags:

-r,--recursive - Includes subfolders.

-f,--filter - Displays options matching the specified filter. Wildcards * and ? can be used if they are enclosed in quotation marks.

policy-move (pmv) [options] [policy] [folder]

Moves a policy.

policy-rename (prn) [options] [existing name] [new name]

Renames a policy.

Report Commands

report-generate (rg) [options] [path] [outputfile] [format]

Generates the report located at [path], and saves the report to file specified in [outputfile] in the specified [format], which can be XML, CSV, or HTML.

Preference Management Commands

`get (get) [options]`

Lists the system preferences to be set.

`set (set) [options] [preference name] [value]`

Sets a preference variable.

Global Options

The following options can be applied to any zlman transaction:

`-?, --help`

Used without a command, this flag displays a list of commands and exits. Used with a command, it displays a list of available options for the command.

`-U, --user=[username]`

Provides a user name. If not provided, you are prompted.

`-P, --password=[password]`

Specifies a password. If not provided, you are prompted.

`--log=[logfile]`

Specifies the log file. (default: /var/opt/novell/log/zenworks/zlman.log)

`-d, --debug`

Displays debugging output.

`--version`

Prints the zlman version and exits.

`-V, --verbose`

Enables verbose output.

`--quiet`

Quiet output; prints only error messages.

`--ignore-rc-file`

Ignores the `~/.zlmanrc` file.

`--host=[host]`

Specifies the host name to connect to. (default: localhost)

`--port=[port]`

Specifies the port that the server is listening on. (default: 443)

`--cleartext`

Disables SSL for debugging purposes. The port must be set to the clear text port.

Time Formats

zlman understands a variety of time formats. You can use the following:

UNIX time

> The number of seconds since January 1, 1970. For example, 1064503775.

Written date formats

> Thu May 29 13:28:47 2003, Thu May 29 13:28:47 EDT 2003 and 29 May 2003 13:28:47 EDT are all valid.

Numeric date formats

> All-numeric date formats such as 2003-05-29 13:28:47 or 03-05-29 13:28:47 will work. Dashes indicate dates, and colons indicate times. The order of the date numerals will vary by locale settings.

24-hour or 12-hour time

> Both 13:28:47 and 1:28:47 PM are acceptable.

All times are converted to UTC, and used without regard to time zones. If you want to execute a transaction at a particular local time, you must create one transaction for each time zone.

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

rug (1), zlmmirror (1), zlm-debug (1), zrmservice (1), zmd (8)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

rug (1)

Name

rug - The command line interface for the Novell ZENworks Linux Management Agent.

Syntax

```
rug [global-options] [command] [command-options] ...
rug --version
rug --help
```

Description

rug is the command-line interface to the ZENworks Linux Management agent. It works with the ZENworks Linux Management daemon to install, update, and remove software according to the commands you give it. The software that it installs can be from ZENworks 7.*x* Linux Management, ZENworks 6.6.*x* Linux Management servers, YUM repositories, the ZYPP service, as well as local files.

ZENworks Linux Management servers sort software by category into catalogs, which are groups of similar software. For example, one catalog can contain software from the operating system vendor, and another catalog can contain the SUSE Linux Enterprise Desktop. You can subscribe to individual catalogs to control the display of available packages and prevent the accidental installation of unwanted software. By default, all operations are performed on software from within catalogs to which you are subscribed, although you may alter this with the `--allow-unsubscribed` flag. The rug utility also provides other features, such as rollback, locks, history and preferences to easily manage packages and bundles.

Depending on the type of managed device, the location of the rug utility varies.

For SUSE Linux Enterprise Server 10 (SLES 10) and SUSE LINUX Enterprise Desktop 10 (SLED 10) devices, the rug utility is located in the following directory:

```
/usr/bin
```

On all other managed devices, the rug utility is installed in the following location:

```
/opt/novell/zenworks/bin
```

Guide to Usage

This section contains a guide to general command formatting and conventions.

Folders

If no folder is specified for commands that take a folder argument, the command targets the root folder. To specify a folder path, list each folder from the root separated by a forward slash (/). For example, if you have a folder named folder1 in the root, containing a subfolder named subfolder1, you would reference this folder as folder1/subfolder1. Each specified folder must already exist.

Ellipsis (...)

An ellipsis indicates that a command accepts multiple entries of the last argument type. For example, the ellipsis in the following command indicates that `catalog-add-bundle` can accept multiple bundles:

```
rug bundle-history [options] [search-string] [...]
```

Option Flags

Commands that do not have command-specific options (they accept only the standard option flags) do not have options listed as an argument in the command reference. For example, the reference entry for the following command does not list options because it accepts only the standard flags:

```
rug list-updates (lu) [catalog]
```

However, the following command lists options because the command has a command-specific option (-a):

```
rug bundle-history [options] [search-string] [...]
```

Commands

rug provides a number of commands (shown as [command] in the Syntax section). Each command accepts the option flags listed in the Global Options section. In addition, many commands have specific option flags that are listed with the commands.

The most commonly used command is `rug update` which downloads and installs updates in catalogs to which you are subscribed.

Bundle Management Commands

bundle-history (bhi) [options] [search-string] [...]

Searches the bundle log entries for the strings specified by [search-string]. Accepts the following option flags:

-n, --search-name - Searches by bundle name (default)

-a, --search-action - Searches by action

--search-user - Searches by user

--match-all - Requires packages to match all search strings (default)

--match-any - Allows packages to match any search string

--match-substrings - Matches search strings against any part of text

--match-words - Requires packages to match all search strings

-d, --days-back - Maximum number of days to look back (default 30)

bundle-install (bin) [options] [bundlename] [...]

Installs the specified bundles. rug attempts to find the specified bundles in catalogs to which you are subscribed. Use `bundle-upgrade` to upgrade a bundle that you already have installed. Accepts the following option flags:

--entire-catalog - Installs all of the bundles from the catalogs specified.

-y,--no-confirmation - Does not prompt for confirmation.

-p,--prepare-only - Only prepares bundles; does not install.

-f,--freshen - Freshens children.

-g,--use-guid - Refer bundles by bundle GUIDs.

-r, --allow-removals - Removes all conflicting packages.

-N,--dryrun - Tests and displays, but does not actually perform the requested actions.

NOTE: The -N and -r options is not applicable for File bundles.

`bundle-list (bl)` [options] [[catalog] [catalog] [...]]

Lists available bundles in catalogs to which you are subscribed.

The output for this command is presented in the following columns: Status, Catalog, Name, Version, and Type. The columns provide the details of every bundle assigned or available for the managed device. The Catalog, Name, Version, and Type represent the catalog name, bundle name, bundle version, and bundle type respectively.

The Status field is empty if the bundle is not installed, displays "i" if the bundle is installed, "v" if the bundle is installed but is of a different version compared to the one displayed in the list, and "*" if the bundle is partially installed.

By default, the command shows the display bundle name.

Accepts the following option flags:

-i, --installed-only - Shows only installed bundles, and their bundle lock status.

-u, --uninstalled-only - Shows only uninstalled bundles.

-c, --incomplete-only - Shows only incomplete bundles.

-s, --show-name - Shows the actual name of the bundle.

-g, --show-guid - Shows the GUIDs of the bundle.

-t, --type - Shows the bundles of the type you specify. Valid values are package, file, and YOU patch. You can specify the value in one of the following formats:

rug bl -t file

rug bl -t=file

rug bl --type file

rug bl --type=file

`bundle-lock-add (bla)` [options] [bundlename] [version] [...]

Adds a bundle lock rule. This prevents changes to the installation state of the bundle that is not specified in the lock. The bundle name can be specified individually, with wildcard patterns, or even with version number relations. For example, the command `rug bla gnome*` refuses to remove any bundles beginning with "gnome". Accepts the following options:

-c, --catalog - Catalog to match in lock.

`bundle-lock-delete (bld)` [options] [lock-number] [...]

Deletes the bundle lock you specify by its number. You can find the numbers for each bundle lock with the `lock-list (bll)` command.

`bundle-lock-list (bll)` [options]

Lists the locks that have been put in place. Locks are sorted by ID number. The bundles that are locked by the administrator on the server are not listed.

`bundle-remove (brm)` [options] [bundlename] [...]

Removes the specified bundles. Accepts the following option flags:

-y,--no-confirmation - Does not prompt for confirmation.

-p,--prepare-only - Only prepare bundles, do not install.

-f,--freshen - Freshens children.

-r,--allow-removals - Removes all conflicting packages.

-N,--dryrun - Tests and displays, but does not actually perform the requested actions.

NOTE: The -N and -r options are not applicable for File bundles.

bundle-search (bse) [options] [querystring]

Searches for bundles matching the query string. Accepts the following option flags:

-i,--installed-only - Searches only the list of installed bundles.

-s, --show-name - Shows the actual name of the bundle.

-g, --show-guid - Shows the GUIDs of the bundle.

bundle-types (bt) [options]

Lists the available bundle types.

bundle-upgrade (bup) [options]

Upgrades the bundles. Accepts the following option flags:

-y,--no-confirmation - Does not prompt for confirmation.

-p,--prepare-only - Only prepares bundles, does not install.

-f,--freshen - Freshens children.

-r,--allow-removals - Removes all conflicting packages.

-N,--dryrun - Tests and displays, but does not actually perform the requested actions.

NOTE: The -N and -r options are not applicable for File bundles.

catalogs (ca) [options]

Lists the catalogs available for the services you have added. Accepts the following option flags:

-u, --uri - Show the service uri.

subscribe (sub) [options] [catalogname] [...]

Subscribes to the specified catalogs. Each specified catalog must be available from one of the services you have added. Accepts the following option flags:

-s,--strict - Fails if attempting to subscribe to a subscribed catalog.

-a,--all - Subscribes to all catalogs.

-e, --service - Specifies the service.

unsubscribe (unsub) [options] [catalogname] [...]

Unsubscribes the specified catalogs. Accepts the following option flags:

-s,--strict - Fails if attempting to unsubscribe from an unsubscribed catalog.

-a,--all - Unsubscribes to all catalogs.

-e, --service - Specifies the service.

File Management Commands

bundle-files (bf) [options] [bundle]

Shows the files in a given file bundle. Accepts the following option flag:

-g,--use-guid - Refer bundles by bundle GUIDs.

The Status column is empty if the file is not installed. It displays "i" if the file is installed,"c" if the file is in the compressed form, or "p" if the file is of a lower version than that installed on the device.

Package Management Commands

bundle-packages (bp) [option] [bundle]

Shows the packages in a given bundle. Accepts the following option flags:

--show-nevra - Shows the NEVRA details of the packages.

If the --show-nevra option is not specified, the output for this command is presented in the Status, Catalog, Name, Version, and Arch columns. These provide the details of every package that is part of the given bundle. Catalog, Name, Version, and Arch represent the catalog name, package name, package version, and package architecture respectively.

The Status column is empty if the package is not installed. It displays "i" if the package is installed, "v" if a different version of the package is installed on the device, or "s" if the package in the bundle is of a lower version than that installed on the device.

The description of these columns is the same with other package commands.

If the --show-nevra option is specified, the output for this command is presented in the Status, Catalog, Name, Epoch, Version, Release, and Arch columns.

-g,--use-guid - Refer bundles by bundle GUIDs.

checkpoint-add (cpa) [name] [date]

Adds a checkpoint. If the date is not specified, adds a check point with the current date.

checkpoint-remove (cpr) [name] [name] [...]

Removes the specified checkpoints.

checkpoints (cp)

Gets a list of saved checkpoints.

dump [output filename]

Gets a dump of system information as a SQLite database.

file-list (fl) [package name]

Lists files within a package.

history (hi) [options] [search term]

Searches package history for the search term you specify. By default, searches package names for the search term, displaying the package version history. Use the following option flags to perform a different search:

-n, --search-name - Searches by package name (default).

-a, --search-action - Searches by action.

-d, --days-back - Maximum number of days to look back (default 30)

`info (if) [options] [package name] [...]`

Displays complete information for the specified package. Accepts the following option flags:

-i, --uninstalled - Searches for uninstalled packages.

-u, --unsubscribed - Searches in unsubscribed catalogs.

`info-conflicts (ic) [package name]`

Lists all conflicts for the specified package.

`info-obsoletes (io) [package name]`

Lists all obsoletes for the specified package.

`info-provides (ip) [package name]`

Lists the information provided by the specified package.

`info-requirements (ir) [package name]`

Lists package requirements. Accepts the following option flags:

-a, --all-providers - Lists all packages that can satisfy a requirement.

-v, --show-versions - Displays full version information for packages.

`install (in) [options] [-t resolvableType] [-c catalog] resolvable1 [resolvable2]`

Installs the specified resolvables. If a user requests a package with a version, zmd installs the exact version of the package. If the package version is not specified, zmd installs the best version of the package. On SLES 10 and SLED 10 platforms, the resolvableType can be a package, pattern, product, or patch; by default it is package. Accepts the following option flags:

-u, --allow-unsubscribed - Allows unsubscribed catalogs.

-d, --download-only - Only downloads packages.

--entire-catalog - Installs all of the packages from the catalogs specified.

-N, --dry-run - Tests and displays the requested actions, but does not actually perform them

-i, --confirm - Prompts for confirmation.

-y, --no-confirm - Does not prompt for confirmation.

--agree-to-third-party-licences - Automatically agrees to third-party licences.

`list-resolvables (lr)`

Lists the available resolvable types.

`list-updates (lu) [catalog] [...]`

Displays available updates in the specified catalogs. Adding catalogs as arguments limits the list to those catalogs you specify. If you are not subscribed to a catalog, no updates will be available, even if you name the catalog as an argument; you must subscribe to list updates.

If the output from this command does not match the pending updates listed on the server, it is because the pending updates list on the server shows updates for all available catalogs, not just catalogs to which the client is subscribed. For the lists to match, the client must be subscribed to all available catalogs.

Accept the following option flags:

-t, --type - Specify the type of updates.

lock-add (la) [options] [name or pattern] [version] [...]

Adds a package lock rule. This prevents changes to the installation state of the package that is specified in the lock. The package name can be specified individually, with wildcard patterns, or even with version number relations.

The *package_name* can include wildcard characters. The following table explains the valid relational operators that can be used with the package in the command:

Relational Operator	Functionality
=	Locks only the specific package version.
<	Locks all versions of the package older than the specified version, excluding the specified version.
>	Locks all versions of the package later than the specified version, excluding the specified version.
<=	Locks all versions of the package older than the specified version, as well as the specified version.
>=	Locks all versions of the package later than the specified version, as well as the specified version.

If you want to install a specific version of the package, ZENworks first checks if the package version has been locked, then installs the package version only if it is not locked. For example, lets assume that all the later versions of the package, "X 1.7" have been locked by using the `rug la X > 1.7` command. If you try to install X 1.9 package by using the `rug in X (1.9)` command, the installation fails.

lock-delete (ld) [options] [lock-number] [...]

Deletes the package lock you specify by its number. You can find the number for each lock with the `lock-list (ll)` command.

lock-list (ll) [options] [lock-number] [...]

Lists the package locks that have been put in place. Locks are sorted by ID number.

package-file (pf) [filename]

Gets the package which contains the specified file.

packages (pa) [options] [catalog] [...]

Displays the packages in a given catalog. If no catalog is specified, all packages in all catalogs are listed. Accepts the following option flags:

-i, --installed-only - Shows only installed packages.
-u, --uninstalled-only - Shows only uninstalled packages.
--sort-by-name - Sorts packages by name (default).
--sort-by-catalog - Sorts packages by catalog.
--show-nevra - Shows the NEVRA details of the packages.

If the --show-nevra option is not specified, the output for this command is presented in the Status, Bundle, Name, Version, and Arch columns. These provide the details of every package that is part of the given bundle. Bundle, Name, Version, and Arch represent the bundle name, package name, package version, and package architecture respectively. The Status field is empty if the package is not installed, and displays "i" if the package is installed, or "v" if the package is installed but is of a different version compared to the one displayed in the list.

The description of these columns is the same with other package commands.

If the --show-nevra option is specified, the output for this command is presented in the Status, Bundle, Name, Epoch, Version, Release, and Arch columns.

patch-search (pse) [options] [querystring]

Searches for patches matching a pattern. Accepts the following option flags:

--match-all - Requires patches to match all search strings (default).
--match-any - Allows patches to match any search string.
--match-substrings - Matches search strings against any part of text.
--match-words - Requires search strings to match entire words.
-d, --search-descriptions - Searches in patch descriptions, but not patch names.
-i, --installed-only - Shows only patches that are already installed.
-u, --uninstalled-only - Shows only patches that are not currently installed.
-c, --catalog - Shows only the patches from the catalog you specify.
--sort-by-name - Sorts patches by name (default).
--sort-by-catalog - Sorts patches by catalog, not by name.

remove (rm) [options] [package] [...]

Removes the specified packages. Accepts the following option flags:

-N, --dry-run - Tests and displays, but does not actually perform the requested actions.
-i, --confirm - Prompts for confirmation.
-y, --no-confirm - Does not prompt for confirmation.

rollback (ro) [options] [date or check point]

Rolls back package transactions to the time and date you specify. Sets the rollback preference, which is disable by default. Accept the following option flags:

-d, --download-only - Only downloads packages.
-p, --package - Name of the package that needs to be rolled back.
-N, --dry-run - Tests and displays, but does not actually perform the requested actions.
-i, --confirm - Prompts for confirmation.
-y, --no-confirm - Does not prompt for confirmation.

search (se) [options] [querystring]

Searches for packages matching a pattern. Accepts the following option flags:

--match-all - Requires packages to match all search strings (default).
--match-any - Allows packages to match any search string.
--match-substrings - Matches search strings against any part of text.
--match-words - Requires search strings to match entire words.
-d, --search-descriptions - Searches in package descriptions, but not package names.

-i, --installed-only - Shows only packages that are already installed.

-u, --uninstalled-only - Shows only packages that are not currently installed.

-c, --catalog - Shows only the packages from the catalog you specify.

--sort-by-name - Sorts packages by name (default).

--sort-by-catalog - Sorts packages by catalog, not by name.

--show-nevra - Shows the NEVRA details of the packages.

--show-duplicates - Shows the duplicate packages available in all catalogs.

If the --show-nevra option is not specified, the output for this command is presented in Status, Catalog, Bundle, Name, Version, and Arch columns. These provide the details of every package that is part of the given bundle. Catalog, Bundle, Name, Version, and Arch represent the catalog name, bundle name, package name, package version, and package architecture respectively. The Status field is empty if the package is not installed, and displays "i" if the package is installed, or "v" if the package is installed but is of a different version compared to the one displayed in the list.

The description of these columns is the same with other package commands.

If the --show-nevra option is specified, the output for this command is presented in the Status, Catalog, Bundle, Name, Epoch, Version, Release, and Arch columns.

summary (sum)

Shows a summary of available updates for each catalog.

update (up) [catalog] [...]

Downloads and installs updates. With no arguments, this installs updates for all subscribed catalogs. Provide the catalog name to keep the updates specific to the mentioned catalogs. For single bundles or packages, use `rug install`. If you are not subscribed to a catalog, there are no updates available, even if you list the catalog as an argument; you must subscribe to install updates. Accepts the following option flags:

-d, --download-only - Only downloads packages.

-t, --type - Specifies type of updates.

--skip-interactive - Skips interactive updates.

-g, --category - Specifies the category of patches to update.

-N, --dry-run - Tests and displays, but does not actually perform the requested actions.

-i, --confirm - Prompts for confirmation.

-y, --no-confirm - Does not prompt for confirmation.

--agree-to-third-party-licences - Automatically agree to third party licences.

verify (ve) [options]

Verifies system dependencies. If system dependencies are not satisfied, rug suggests removal or installation of packages necessary to resolve conflicts. Accepts the following option flags:

-N, --dry-run - Tests and displays, but does not actually perform the requested actions.

-i, --confirm - Prompts for confirmation.

-y, --no-confirm - Does not prompt for confirmation.

what-conflicts (wc) [package-dep]

Lists packages that conflict with the item you specify.

what-provides (wp) [querystring]

Displays packages that provide the library, program, or package that you specify as `[querystring]`.

what-requires (wr) [querystring]

Lists packages that require the library, program, or package you specify as `[querystring]`.

Patch Management Commands

patches (pch) [options] [catalog] [catalog] [...]

Shows the patches in a given catalog. Accepts the following option flags:

-i, --installed-only - Shows only installed patches.
-u, --uninstalled-only - Shows only uninstalled patches.

patch-info [patch]

Shows detailed information for a patch.

Pattern Management Commands

pattern-info [pattern]

Shows detailed information for a pattern.

patterns (pt) [options] [catalog] [catalog] [...]

Shows the patterns in a given catalog. Accepts the following option flags:

-i, --installed-only - Shows only installed patterns.
-u, --uninstalled-only - Shows only uninstalled patterns.

Policy Management Commands

policy-list (pl) [options]

Lists the effective policies assigned to the devices along with their schedule details.

Preference Management Commands

get-prefs (get) [token]

Displays the value of the specified preference token. If no token is provided, all preferences are displayed. Accepts the following option flag:

-d, --no-descriptions - Does not show descriptions of the preferences.

set-prefs (set) [token] [value]

Sets a preference variable.

Use `rug get` to display the preferences and current values.

Product Management Commands

product-info [product]

Shows detailed information for a product.

```
products (pd) [options] [catalog] [catalog] [...]
```
Shows the products in a given catalog. Accepts the following option flags:

-i, --installed-only - Shows only installed products.
-u, --uninstalled-only - Shows only uninstalled products.

Security Management Commands

```
key-add (ka) [keyname] [keyid]
```
Adds to the list of whitelisted keys for a service.

```
key-delete (kd) [keyid]
```
Removes from the list of whitelisted keys for a service.

```
key-list (kl) [...]
```
Displays whitelisted keys for a service.

Service Management Commands

```
mount [options] [path]
```
Mounts a directory as a catalog, adding all packages within the directory to the catalog. The platform for the catalog is assumed to be the same as the platform of the server. Accepts the following option flags:

-r, --recurse - Recurse into the directory.
-a, --alias - Alias for the new channel.
-n, --name - Name for the new channel.

```
refresh (ref) [uri | number | name]
```
Refreshes the specified services. If no service is specified, all services are refreshed. You must add a service by using the `rug service-add` command before you can refresh. Use `rug service-list` to view the current list of services. The service argument can be the service number from the service-list output.

```
register (reg) [uri | number | name] [key]
```
Registers the client against the specified server.

```
service-add (sa) [options] [uri]
```
Adds the specified server as a service. In most cases, the URI is the URL of your ZENworks Linux Management server, for example `https://zlmserver`. Accepts the following option flags:

-t, --type - Type of service. The default is zenworks. Use `rug service-types` to view the available services.
-d, --device-type - The type of device you are registering.
-k, --key - Registration key.
-f, --ignore-failure - Retries the service if it fails. By default, the retry interval is 5 minutes and the number of retry attempts is 3. If you do not use the -f option, the service is not added if the ZENworks Management Daemon (ZMD) cannot resolve the service and register it.

-r, --rebuild - Registers a managed device with the ZENworks server by performing a point-in-time replacement of the old agent. The point-in-time replacement of the managed device lets you replace the older device object on the ZENworks Server with the current device object that is requesting the rebuild. The rebuild operation ensures that all the bundle and policy associations are retained. The replacement of the device object is based on the alias name (display name) and the primary IP address of the managed device. This option is not supported for ZENworks Primary Server and ZENworks Secondary Server.

-o, --option - Set an option. Accepts the following options:

--normal-output - Normal output (default)

--terse - Terse output

--no-abbrev - No abbreviation

--debug - Debug output, prints full exception traces

--quiet - Quiet output, prints only error messages

`service-delete (sd) [uri | number | name] [...]`

Deletes the specified services. Accepts the following option flag:

--all - Deletes all the services.

-y, --no-confirm - Does not prompt for confirmation.

`service-list (sl)`

Lists the available services.

`service-types (st)`

Lists the available service types.

System Commands

`clean-cache (cc) [...]`

Cleans the HTTP cache.

`load-modules (lm) [...]`

Loads ZENworks Management Daemon (zmd) modules.

`ping`

Pings the ZMD deamon running on the client.

`restart`

Restarts the ZLM daemon. Accepts the following option flags:

-f, --force - Forces the shutdown.

-n, --no-wait - Does not wait for confirmation that the daemon has restarted.

--clean - Cleans up at restart

`schedule (sch)`

Shows scheduled items.

`shutdown [options] [...]`

Halts the ZLM daemon. Accepts the following option flags:

-f, --force - Force the shutdown.

-n, --no-wait - Don't wait for confirmation that the daemon was shut down.

`sleep [options] [...]`

Put the daemon to sleep. Accept the following option flags:

-f, --force - Force the restart.

`you-clean-cache (yc) [options]`

Cleans the YOU cache directory, `/var/lib/YaST2/mnt` on SLES 9, Novell Linux Desktop, and OES.

User Management Commands

`user-add (ua) [username] [privilege] [...]`

Adds a new user with the specified username and privileges. The following privileges can be granted: install, lock, remove, subscribe, trusted, upgrade, view, superuser. If you do not provide arguments, you are prompted for them. After the user is added, `rug user-update` is launched automatically. Use this tool to grant additional privileges. Accept the following option flags:

-r, --replace - Replaces the user if that user already exists.

`user-delete (ud) [username] [...]`

Deletes the specified users.

`user-edit (ue) [username]`

Edits an existing user. This command is interactive: it first lists privileges, then offers you a prompt. Enter the plus (+) or minus (-) symbol and then the name of the privilege, then press Enter. For example, to permit the user to install software, you would type +install. To save and quit, press Enter on a blank line. The following privileges can be granted or revoked: install, lock, remove, subscribe, trusted, upgrade, view, superuser.

`user-list (ul)`

Lists users. To view the list of users, you need to have either the readonly or the superuser privilege. The readonly privilege can be enabled by using either the `user-add` or `user-edit` command.

Global Options

The following options can be applied to any rug transaction:

`--normal-output`

Normal output (the default mode). This is somewhere between debug output and terse output.

`--terse`

Terse output.

`--no-abbrev`

No abbreviation.

`--quiet`

Quiet output; prints only error messages.

`--debug`

Debug output, prints full exception traces.

`--version`

Prints the rug version and exits.

Authors

Copyright 2005-2010, Novell, Inc. (http://www.novell.com). All rights reserved.

See Also

zlman (1), zmd (8), zrmservice (1), zlm-debug (1), zlmmirror (1)

To report problems with this software or its documentation, visit Novell Bugzilla (http://bugzilla.novell.com).

Bundle and Policy Schedules

B

Using Novell® ZENworks® Linux Management, you can schedule when bundles are deployed to or installed on assigned devices. You can also schedule when policies are applied to assigned devices.

The following scheduling options are available:

- Section B.1, "Date Specific," on page 601
- Section B.2, "Day of the Week Specific," on page 602
- Section B.3, "Event," on page 603
- Section B.4, "Monthly," on page 603
- Section B.5, "Relative to Refresh," on page 604

B.1 Date Specific

Select one or more dates on which to run the scheduled event and set other restrictions that might apply.

NOTE: If you schedule an event in the past, the scheduled event occurs when the assigned device refreshes.

Start Dates(s): Click the plus (+) symbol to display a calendar from which you can select dates to run the event on. Click the arrows next to the month to display the previous or next month's calendar; click the arrows next to the year to display the previous or next year's calendar.

Run Event Every Year: Select this option to run the event every year on the dates that you selected in the *Start date(s)* field.

Select When Schedule Execution Should Start: Select one of the following options:

- **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.
- **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the scheduled event does not run at the same time on multiple devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.

StartTime\End Time: Use the down-arrows to select the start and end times of the scheduled event.

IMPORTANT: Be aware that ZENworks Linux Management uses the *End Time* as the "expiration time." If a bundle or policy is in the middle of being executed, execution stops at the specified time.

Use Greenwich Mean Time (GMT): Usually, a schedule is based on the device's local time zone. If your network spans different time zones and you schedule an application to run at 13:00 (1:00 p.m.), it runs at 13:00 in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

B.2 Day of the Week Specific

Select one or more days of the week to run the scheduled event on and set other restrictions that might apply.

The Day of the Week Specific schedule applies to policies only; you cannot configure a bundle with the Day of the Week Specific schedule.

Select the Days of the Week to Run the Scheduled Event: Select one or more days, Sunday to Saturday, on which you want to run the scheduled event. By default, no days are selected; a day is selected when the check box is checked.

Restrict Schedule Execution to the Following Date Range: Use the *Start date* and *End date* fields to restrict the scheduled event to the dates between the start and end dates. Click the *Calendar* icon to display a calendar from which you can select the respective dates.

Select When Schedule Execution Should Start: Select one of the following options:

- **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.

- **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the scheduled event does not run at the same time on all devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.

- **Start Immediately at Start Time, and then Repeat until End Time Every:** Use the *Hours* and *Minutes* fields to specify how often you want the scheduled event repeated until deployment or installment of the bundle is successful.

Start Time\End Time: Use the down-arrows to select the start and end times of the scheduled event.

IMPORTANT: Be aware that ZENworks Linux Management uses the *End Time* as the "expiration time." If a bundle or policy is in the middle of being executed, execution will stop at the specified time.

Use Greenwich Mean Time (GMT): Usually, a schedule is based on the device's local time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

Set the "Black Out" Time Ranges when Execution Should Not Occur: Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.

B.3 Event

The *User login* option lets you trigger the event schedule when the user logs in to the device.

B.4 Monthly

Select the day of the month to run the scheduled event on and set other restrictions that might apply.

The Monthly schedule applies to policies only; you cannot configure a bundle with the Monthly schedule.

Day of the Month: Select one of the following options:

- **Start the Scheduled Event on a Specific Day of the Month:** Specify the day of the month on which to run the scheduled event.
- **Start the Scheduled Event on the Last Day of the Month:** Select this option to run the scheduled event on the last day of the month. For example, for the month of February, the event runs on the 28th (except for leap years, in which case it runs on the 29th); for the month of December, the event runs on the 31st.

Select When Schedule Execution Should Start: Select one of the following options:

- **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.
- **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the event is not run at the same time on all devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.

Start Time\End Time: Use the down-arrows to select the start and end times of the scheduled event.

IMPORTANT: Be aware that ZENworks Linux Management uses the *End Time* as the "expiration time." If a bundle or policy is in the middle of being executed, execution stops at the specified time.

Use Greenwich Mean Time (GMT): Usually, a schedule is based on the device's local time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

Set the "Black Out" Time Ranges when Execution Should Not Occur: Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.

B.5 Relative to Refresh

Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that might apply.

Schedule Execution: Select one of the following options:

- **Start Immediately on Refresh:** Select this option to run the scheduled event when the device refreshes (looks for new bundles, policies, and so forth). The event runs on the first device refresh only and does not run on subsequent refreshes. By default, the system global refresh schedule is every two hours.

  To change the default refresh schedule, click the *Configuration* tab > *Device Refresh Schedule*.

  If the user performs a manual refresh on the device by running the `rug ref` command, the scheduled action runs on the first manual refresh only and not on subsequent refreshes (manual refreshes or global refreshes).

- **Delay Execution after Refresh:** Select this option to run the scheduled event for a specified number of days, hours, or minutes after the device refreshes (looks for new bundles, policies, and so forth).

After Executing, Repeat Every: Select this option and specify the number of days, hours, and minutes after which you want to repeat execution of the scheduled event after a successful execution.

Set the "Black Out" Time Ranges when Execution Should Not Occur: Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.

Naming Conventions in the ZENworks Control Center

C

When you name an object in the ZENworks Control Center (folders, bundles, bundle groups, catalogs, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.
- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. Leading and trailing underscores are also removed. For example, Bundle_1, BUNDLE 1, and _bundle_1_ are all considered identical.
- If you use spaces, you must enclose the name in quotes when entering it on the command line. You must enclose bundle 1 in quotes ("bundle 1") when entering it in the zlman utility, for example.

Imaging Utilities and Components

D

The following sections provide reference information on Novell® ZENworks® Linux Management imaging utilities, commands, and configuration settings.

D.1 Image Explorer (imgexp.exe)

Use the Image Explorer utility at a Windows workstation to view or modify workstation images, create add-on images, compress image files, and split images.

Although ZENworks Imaging Explorer looks and functions like Microsoft Windows Explorer in most situations, some functionality differences exist between the two programs. The following describes the key differences between how ZENworks Image Explorer and Microsoft Windows Explorer function:

- **Replacing Files in an Image:** During the life cycle of an image, files might be deleted or updated using Image Explorer. When you replace an existing file in an image by using Image Explorer, the original file is not deleted from the image. Image Explorer purges only deleted files; it does not purge files that have been updated.

  When files are added to an image where the file already exists, Image Explorer appends the entry to the end of the image. When images are restored, all files that have been previously updated are sequentially restored.

  To avoid performance problems, you should manually delete and purge each instance of a duplicate file in order to have the duplicates purged from the image. In Windows Explorer, replaced files are automatically deleted.

- **Dragging Files from Image Explorer:** You cannot drag files from Image Explorer in order to extract them, which you can do in Windows Explorer. However, you can drag and drop files and folders into an image using Image Explorer.

IMPORTANT: When editing a base image, do not exclude BPB files from it or the device won't be able to boot the new operating system after receiving the image.

The following sections describe the tasks that you can perform using the Image Explorer:

D.1.1 Starting Image Explorer (imgexp.exe)

The Image Explorer utility must be run on a Windows device. You need Samba running on the Linux imaging server where the utility file is located in order for the Windows device to have access to it.

There are no command line parameters for the Image Explorer utility.

1 To start Image Explorer, run the following file:

```
/opt/novell/zenworks/zdm/imaging/winutils/imgexp.exe
```

D.1.2 Opening an Image

1 Start Image Explorer.

2 Click 🖱 on the toolbar, browse for and select the image (`.zmg`) file, then click *Open*.

Large image files might take a few moments to open.

D.1.3 Adding a File or Folder to an Open Image

1 Start Image Explorer.

2 In the left pane, browse to the partition or directory where you want to add the file or folder.

3 Click 📄 or 📁 on the toolbar, browse to the file or folder, then click *Add* or *OK*.

D.1.4 Creating a Folder in an Open Image

1 Start Image Explorer.

2 In the left pane, browse to the partition or folder where you want to create the folder, click ⬚, type the name of the folder, then click *OK*.

D.1.5 Excluding a File or Folder from a File Set in the Open Image

1 Start Image Explorer.

2 Select the file or folder, click *Edit*, click *File sets*, then select the file sets that you want the file or folder to be excluded from.

This image has 10 possible file sets, labeled Set 1, Set 2, and so on. The files and/or folders that you selected in the main window is excluded only from the file sets that you select in this dialog box.

D.1.6 Marking a File or Folder for Deletion in the Open Image

1 Start Image Explorer.

2 Select the file or folder, click *Image*, then click *Delete*.

> **IMPORTANT:** Deleting a file in the Image Explorer merely marks it for deletion; it can still be retrieved. A file marked as deleted is not removed from the image until the image is purged; files and folders marked as deleted are not restored during imaging.

D.1.7 Purging Files and Folders Marked for Deletion from the Open Image

1 Start Image Explorer.

2 Ensure that the open image has been saved, click *File*, then click *Purge deleted files*.

3 Browse to the image filename or specify a new image filename, then click *Save*.

D.1.8 Extracting a File or Directory from the Open Image to a Folder

1 Start Image Explorer.

2 Click the file or directory, click *File > Extract > As files*, browse to and select a folder, then click *OK*.

D.1.9 Extracting a File or Directory from the Open Image As an Add-On Image

1 Start Image Explorer.

2 Click the file or directory, click *File > Extract > As add-on image*, type the name of the new add-on image, then click *OK*.

D.1.10 Viewing a File from the Open Image in its Associated Application

1 Start Image Explorer.

2 Click the file, then click *File > Extract and view*.

D.1.11 Saving Your Changes to the Open Image

1 Start Image Explorer.

2 Click ▣ on the toolbar.

D.1.12 Creating an Add-On Image

1 Start Image Explorer.

2 Click ▢ on the toolbar, open Windows Explorer, browse to the files and folders you want the add-on image to contain, drag the files and folders into the right pane from Windows Explorer, then click *Save*.

D.1.13 Adding a Partition to a New Add-On Image

1 Start Image Explorer.

2 Click ▢ on the toolbar, click the root of the image, click *Image*, then click *Create partition*.

You cannot add a partition to an existing add-on image or to any base image.

D.1.14 Compressing an Image

You can set compression options so that it takes less time to restore the image file and less space to store the file on your imaging server. You can compress an uncompressed image (including images created by previous versions of ZENworks) by 40 to 60 percent of the original file size.

The ZENworks Linux Management Image Explorer provides the following types of image compression:

- "Compressing an Open Image" on page 610
- "Compressing Any Image without Waiting for the File to Fully Load into Image Explorer" on page 611

Compressing an Open Image

1 Start Image Explorer.

2 Browse for the image (`.zmg`) file, then click *Open*.

Large image files might take a few moments to open.

3 Click *File > Compress image*.

4 Browse to a folder, specify a new image filename, then select a compression option:

Optimize for Speed: Takes the least amount of time to compress, but creates the largest compressed image file.

Balanced (Recommended): Represents a compromise between compression time and image file size. This option is used by default when an image is created.

Optimize for Space: Creates the smallest image file, but takes longer to compress.

5 Click *Compress*.

Files marked for deletion in the image are removed during the compression operation.

Compressing Any Image without Waiting for the File to Fully Load into Image Explorer

You can set compression options to quickly compress an image file without waiting for the file to fully load into Image Explorer.

To use QuickCompress:

1 Start Image Explorer.

2 Click *Tools* > click *QuickCompress*.

3 Browse to the image file, browse to a folder, specify a new image filename, then select a compression option:

Optimize for Speed: Takes the least amount of time to compress, but creates the largest compressed image file.

Balanced (Recommended): Represents a compromise between compression time and image file size. This option is used by default when an image is created.

Optimize for Space: Creates the smallest image file, but takes longer to compress.

4 Click *Compress*.

Files marked for deletion in the image are removed during the compression operation.

D.1.15 Splitting an Image

You can split an image file into separate files so that you can span the entire image across several CDs or DVDs.

When you split a device image and span it across several CDs or DVDs, you are essentially creating a base image on the first CD or DVD. The remaining CDs or DVDs are add-on images.

To restore a device image that has been spanned across several CDs or DVDs you should restore the first CD or DVD before restoring the remaining CDs or DVDs containing the add-on images. For more information, see "Manually Putting an Image on a Device" on page 420.

Restoring split Images is a manual task and can only be automated using scripted imaging. For more information, see "Imaging a Device Using a Script" on page 414.

To split an image:

1 Start Image Explorer.

2 Click *Tools* > *Image split*.

3 Specify an existing base image file to split, specify the directory in which to store the split images, then specify the maximum file size of each split-image file.

Because images are split by placing individual files into different images, an image cannot be split if it contains any single file that is larger than the specified maximum file size.

4 Click *Split*.

D.1.16 Resizing a Partition in an Image

For base images, you can edit the value in the *Original size* field to allow you to change how big the ZENworks Imaging Engine makes the partition when the image is restored.

For example, suppose you create a base image of a device with a 20 GB hard drive and you want to then put that image on a new device with a 60 GB hard drive. If you do not increase the size of the partition, the partition will be 20 GB, thus making the remaining 40 GB unusable.

However, if you increase the number in the *Original size* field to match the size of the new hard drive, the ZENworks Imaging Engine expands the partition when the image is restored so that you can use the entire drive.

To resize a partition:

1 Start Image Explorer.

2 Right-click a partition in the left frame, then click *Properties*.

3 Increase or decrease the value in the *Original size* field.

You cannot decrease the number in the *Original size* field to a smaller value that what is in the *Minimum size* field.

The *Original size* field is not applicable for add-on images and cannot be modified for them.

D.2 Novell ZENworks Linux Management Imaging Agent (novell-zislnx)

The Novell ZENworks Linux Management client (which includes novell-zislnx) should be installed on devices where you want to apply images. For information on installing the client on your devices, see "Setting Up Managed Devices" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

Installing the Linux Management client automatically installs the Novell ZENworks Linux Management Imaging Agent (novell-zislnx). The Imaging Agent's purpose is to save certain device-unique data (such as IP addresses and host names) to an area on the hard disk that is safe from imaging. The Imaging Agent records this information when you install it on the device. Then the agent restores this information from the image-safe area after the device has been imaged. This allows the device to use the same network identity as before.

IMPORTANT: To read or write the image-safe data from or to the hard disk, you must set the `Mode` to `Enable` in the `/etc/opt/novell/zenworks/preboot/novell-zislnx.conf` file.

The Imaging Agent is installed on your imaging server by default when you install ZENworks Linux Management.

If a device is new and does not contain a unique network identity, the default settings that you have configured for the ZENworks Management Zone are applied when you image the device using a Preboot Services Imaging bundle.

The data that the Imaging Agent saves to (or restores from) the image-safe area includes the following:

- Whether a static IP address or DHCP is used
- If a static IP address is used:
    - IP address
    - Subnet mask
    - Default gateway (router)
- DNS settings
    - DNS suffix
    - DNS hostname
    - DNS servers

The novell-zislnx daemon is generally run automatically. However, if you want to run it manually, for the command line arguments that can be used with the Imaging Agent, see "Understanding Script Arguments" on page 629.

D.3 Image-Safe Data Viewer and Editor (zisview and zisedit)

After booting a device from an imaging boot media (PXE, CD, DVD, or ZENworks partition), you can enter `zisedit` and `zisview` at the Linux bash prompt to edit and view the image-safe data for that device.

The following sections contain additional information:

- Section D.3.1, "Information Displayed by the Image-Safe Data Viewer," on page 613
- Section D.3.2, "Using the Image-Safe Data Viewer," on page 615
- Section D.3.3, "Using the Image-Safe Data Editor," on page 616

D.3.1 Information Displayed by the Image-Safe Data Viewer

After booting a device from an imaging boot media, enter `zisview` at the Linux bash prompt to view the image-safe data for that device.

The image-safe data viewer (`zisview`) displays the following information about the device:

Table D-1 *zisview Information*

Category	Information
Image-safe Data	◆ **Version:** The version number of the Novell ZENworks Linux Management Imaging Agent (novell-zislnx). ◆ **Just Imaged Flag:** If this is set to False, the Imaging Agent reads data from Linux and writes it to the image-safe data store. If this is set to True, the Imaging Agent reads data from the image-safe data store and writes it to Linux. ◆ **Scripted Image Flag:** If this option is set to True, the last imaging operation was a scripted image. If this option is set to False, the last imaging operation was not a scripted image. ◆ **Last Base Image:** The last base image that was restored to the device. ◆ **Last Base Image Time:** The time stamp of the last base image that was restored to the device. ◆ **Last Base Image Size:** The size of the last base image that was restored to the device. ◆ **Last Base Image Address:** The IP address of the last base image that was restored to the device. ◆ **Script Checksum:** Displays the checksum value representing the last script run. The ZENworks Imaging Engine uses the checksum to prevent the same script from re-running on the device unless you specify in the ZENworks Control Center that you want to rerun the same script.
Device Identity Information	◆ **Zone GUID:** The ZENworks Management Zone that contains the device, if it has been imported. ◆ **Device GUID:** The Globally Unique Identifier of this computer's device. ◆ **Device Index:** The device identification number. ◆ **Win 9x Computer Name:** The computer name for the device. [1] ◆ **Windows Workgroup:** The Microsoft network workgroup of the device. [1] ◆ **Windows SID:** The Windows Security ID of the device, a unique number that identifies this device in Windows. [1]

Category	Information
Network Information	◆ **DHCP:** Displays whether this device uses DHCP to obtain its IP address.
	◆ **IP Address:** Displays the static IP address that this device uses.
	◆ **Gateway:** Displays the gateway that this device uses.
	◆ **Subnet Mask:** Displays the subnet mask that this device uses.
	◆ **DNS Servers:** The number of DNS nameservers used for DNS name resolution.
	◆ **DNS Server [0]:** The IP address of the DNS server. This line is repeated, numbering from 0, 1, 2, 3, and so on for each DNS name server. For example, if the DNS Servers number is 3, there will be three of these lines, numbered from 0 through 2.
	◆ **DNS Suffix:** The DNS context of the device.
	◆ **DNS Hostname:** The DNS local hostname of the device. Use this field to change the computer name of Linux devices.

[1] The *Win 9x Computer Name*, *Windows Workgroup*, and *Windows SID* device identity information fields are present for imaging compatibility with ZENworks Desktop Management. These fields are not relevant to Linux devices.

D.3.2 Using the Image-Safe Data Viewer

To use `zisview`, enter any of the following commands at the Linux bash prompt:

Table D-2 *Data Viewer Commands*

Command	Explanation
zisview	Displays all image-safe data.

Command	Explanation
`zisview -z field`	Displays information about a specific field or fields. *field* is one or more field names separated by a space. *field* is not case-sensitive.
	All of the following are valid field names (the corresponding minimum names that can also be entered on the command line follow each field name in parenthesis):
	JustImaged (J) ScriptedImage (SC) LastBaseImage (L) Zone GUID (T) Device GUID (ObjectDN) Device Index (N) Windows WorkGroup (WorkG) Windows SID (SI) WorkstationID (Works) DHCP (DH) IP (I) Gateway (Gateway) Mask (M) DNSServerCount (DNSServerC) DNSServer (DNSServer) DNSSuffix (DNSSu) DNSHostName (DNSH)
`zisview -s`	Creates a script that can be used to generate environment variables that contain all of the image-safe data fields.
`zisview -h`	Displays help for `zisview`.

D.3.3 Using the Image-Safe Data Editor

After booting a device from an imaging boot media, you can enter `zisedit` at the Linux bash prompt to change, clear, or remove information the image-safe data for that device.

To use `zisedit`, enter any of the following commands at the Linux bash prompt:

Table D-3   zisedit Commands

Command	Explanation
`zisedit`	Displays a screen showing all of the image-safe data fields. You can add or change any of the information in the fields.

Command	Explanation
zisedit field=new_information	You can change the information for one field using this syntax, where *field* is any valid field name and *new_information* is the information you want this field to contain. *field* is not case sensitive.
	For example, enter zisedit Mask=255.255.252.0 to enter this information in the *subnet mask* field.
	All of the following are valid field names (the corresponding minimum names that can also be entered on the command line are shown in parenthesis after each field name):
	JustImaged (J) ScriptedImage (SC) LastBaseImage (L) Zone GUID (T) Device GUID (ObjectDN) Device Index (N) Windows WorkGroup (WorkG) Windows SID (SI) WorkstationID (Works) DHCP (DH) IP (I) Gateway (Gateway) Mask (M) DNSServerCount (DNSServerC) DNSServer1 (DNSServer1) DNSSuffix (DNSSu) DNSHostName (DNSH) PXEWorkRevision (PXEWorkR) PXEWorkObject (PXEWorkO) PXETaskID (PXETaskI) PXETaskState (PXETaskS) PXETaskRetCode (PXETaskR)
zisedit -c	Clears all image-safe data fields.
zisedit -r	Removes the image-safe data store.
zisedit -h	Displays help for zisedit.

D.4 ZENworks Imaging Floppy Boot Disk Creator (zmediacreator.exe)

You can use this utility to do the following:

- Create a floppy boot diskette to help devices that cannot boot from their CD or DVD to do so
- Manage the settings.txt file
- Create a Preboot Bootable Image (PBI)

The ZENworks Imaging Media Creator utility must be run on a Windows device. You need Samba running on the Linux imaging server in order for the Windows device to have access to the utility.

The `zmediacreator.exe` file is located at `/opt/novell/zenworks/zdm/imaging/winutils/zmediacreator.exe` on your ZENworks Linux Management imaging server.

For instructions on using the utility, see Section 29.2.3, "Using the ZENworks Imaging Media Creator," on page 356.

D.5 Imaging Configuration Parameters (settings.txt)

The `settings.txt` file contains parameters that control how the imaging boot process occurs. A copy is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed. You should maintain the working copy of `settings.txt` at the root of the imaging boot device (CD or DVD, or ZENworks partition).

`Settings.txt` is a plain text file that contains various parameters, each on a separate line. Each parameter has the general format of PARAMETER=value. Lines that begin with a pound sign (#) signify comments and are ignored during the imaging boot process.

You can edit this file manually in a text editor, or by making configuration changes in the `zimgboot.exe` utility (see Section D.4, "ZENworks Imaging Floppy Boot Disk Creator (zmediacreator.exe)," on page 617).

IMPORTANT: If you manually edit the `settings.txt` file to provide any paths to executables, make sure that you provide the full path, or the executable might not run.

The format and function of each parameter in the `settings.txt` file are described in Table D-4:

Table D-4 *Settings.txt File Parameters*

Parameter	Specifies
PROMPT	Specifies whether to prompt for each configuration setting when you boot a device from the imaging boot media.
	If you leave this parameter commented out or set it to No, the device boots using the configuration settings specified in `settings.txt` and you can't override the settings when booting, unless you type `config` at the boot prompt before the Linux operating system begins to load.
	If you set this parameter to Yes, you are automatically prompted for each configuration setting when booting.

Parameter	Specifies
MANUALREBOOT	Specifies whether you must reboot a device manually after it was booted from the imaging boot media in automatic mode. If the device was booted from the imaging boot media in manual mode, you must always reboot the device manually. If you boot a device from the imaging boot media and you let the boot process proceed in automatic mode, the ZENworks Imaging Engine starts and checks the imaging server to see if an imaging operation should be performed on the device. If so, it performs the imaging operation and quits. If not, it quits without doing anything. What happens next depends on how you set this parameter: ◆ If you leave it commented out or set it to No, you are prompted to remove the imaging boot media (if necessary) and press any key to reboot the device to the native operating system. ◆ If you set this parameter to Yes, the device doesn't reboot automatically, but instead displays the Linux bash prompt, allowing you to perform additional imaging-related tasks using the Linux menu or at the command line. This is helpful if you want to do things such as check the current partition information or the image-safe data before booting to the native operating system. Example: MANUALREBOOT=YES
PARTITIONSIZE	Specifies the number of megabytes to allocate to the ZENworks partition if you choose to create one locally on a device when you boot the device from the imaging boot media. The default size is 150 MB. The minimum partition size is 50 MB. The maximum size allowed is 2048 MB (2 GB). If you plan to store an image in the ZENworks partition, such as to enable the device to be restored to a certain state without connecting to the network, you might want to specify a larger size on this parameter. Example: PARTITIONSIZE=500
netsetup	If you are using DHCP, keep this option enabled. If you are using a specific IP address, replace "dhcp" with "1" and uncomment and configure the other three IP address lines (HostIP, NETMASK, and GATEWAY). Example: netsetup=dhcp
HostIP	The IP address used by a device to communicate on the network when you boot the device from the imaging boot media, if a static IP address is needed. Example: HostIP=137.65.95.126 If you want DHCP to be used, leave this and the next two parameters commented out.
NETMASK	Specifies the subnet mask to be used by the device, if the device is using a static IP address. Example: NETMASK=255.255.252.0 If DHCP is being used, leave this parameter commented out.

Parameter	Specifies
GATEWAY	Specifies the IP address of the gateway (router) to be used by the device, if the device is using a static IP address. Example: GATEWAY=137.65.95.254 If DHCP is being used, leave this parameter commented out.
NAMESERVER	Specifies the list of DNS name servers, by IP address, to use for resolving DNS domain names used on this device. Use a space to separate entries. Example: NAMESERVER=123.45.6.7 123.45.6.9 If DHCP is being used, leave this parameter commented out.
DOMAIN	Specifies the list of DNS domain suffixes to be used to identify connections used by this device. Use a space to separate entries. For example: DOMAIN=example.novell.com example.xyz.org If DHCP is being used, leave this parameter commented out.
PROXYADDR	Specifies the IP address or full DNS name of the imaging (proxy) server to connect to when you boot a device from the imaging boot media in auto-imaging mode. Examples: PROXYADDR=137.65.95.127 PROXYADDR=imaging.xyz.com This parameter is used to set the PROXYADDR environment variable in Linux when the device is booted from an imaging boot media (other than PXE). The ZENworks Imaging Engine then reads this variable to determine which server to contact if it is running in automatic mode. Whether it is running in automatic or manual mode, the ZENworks Imaging Engine attempts to log the imaging results to the server specified in this variable. **IMPORTANT:** This parameter is set automatically when booting PXE and normally should not be specified in `/srv/tftp/boot/settings.txt`, which is the copy of settings.txt that is used by PXE.
/bin/setleds -D +num < /dev/tty1	Turns on NUMLOCK upon booting.
export PS1="\`pwd \`#"	Configures the string used by the bash shell. You can change the string by editing the text after the = symbol. The ' character is not a single quote mark, but is from the ~ key.
export IMGCMD	Use to alter the behavior of automated imaging. If this variable is defined as a script (or a series of commands), then that script (or those commands) are executed instead of the usual `img auto` command (see `/bin/imaging.s`).

Parameter	Specifies
export ENTERPISE_NAME=*name*	This feature is not supported in Novell ZENworks Linux Management.
	This should be a valid Enterprise Name for an AMT device, such as entZENworks. It allows imaging utilities to access image-safe data in AMT NVRAM when AMT devices are disconnected from the ZENworks Management Zone.
	If you do not use this parameter for disconnected AMT devices, the imaging utilities might not be able to keep the image-safe data up to date.
netdevice=eth0	Selects a specific network adapter. If necessary, replace `eth0` with the correct interface.
noshell=1	Suppresses a secondary terminal program from displaying.

D.6 Imaging Boot Parameter for PCMCIA Cards

When performing imaging work using CDs or DVDs, some computers (particularly laptops) with PCMCIA cards can hang during the boot process. By default, ZENworks Linux Management allows the loading of a PCMCIA driver when a device boots for imaging work. Although loading this driver does not normally cause problems, you can use a command line parameter to prevent it from loading.

To prevent the PCMCIA card manager from starting, enter the following at the bash prompt when booting from a CD or DVD:

```
manual NoPCMCIA=1
```

D.7 Imaging Server

The imaging server is a software component of the Linux Management server. It enables imaging clients to connect with the network to receive imaging services, including:

- Storage or retrieval of an image on a server
- Automatic imaging based on settings created in the ZENworks Control Center
- Logging of the results of an imaging operation
- A multicast imaging session

Use the imaging server software to do the following:

D.7.1 Initiating the Imaging Processes

An imaging server daemon is initiated by running the script at the Linux terminal program command line, which in turn calls the executable and uses the configuration set in the corresponding `.conf` file. Because the scripts do not normally accept parameters, but only arguments (such as `start`), you can configure parameters in their corresponding `.conf` files.

The following Linux daemons run the imaging server processes:

-
-
-
-
-

novell-pbserv

The novell-pbserv daemon provides imaging services to devices.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

-
-

Understanding the novell-pbserv Components

To initiate the novell-pbserv daemon, enter the following command on the Linux command line in a terminal program:

```
/etc/init.d/novell-pbserv
```

Table D-5 lists the arguments for this command, the executable it starts, and the configuration file it uses:

Table D-5 *Novell-pbserv Command Details*

Script Arguments:	start, stop, restart, force-reload, status, showpid (for descriptions of these arguments, see "Understanding Script Arguments" on page 629)
Executable:	`/opt/novell/zenworks/preboot/bin/novell-pbservd`
Configuration File:	`/etc/opt/novell/zenworks/preboot/novell-pbserv.conf`

Configuring novell-pbserv

The novell-pbserv configuration file (`novell-pbserv.conf`), contains the following parameters:

Table D-6 *Novell-pbserv Parameters*

Parameter	Description
EnableLogging=YES	If YES, a log file is created for debug messages. This is the default.
	If NO, no log file is created for debug messages.
	The `novell-pbserv.log` file is created in the `/var/opt/novell/log/zenworks/preboot` directory.

Parameter	Description
IPAddress=	The IP address to be used by imaging for all communications. If nothing is entered, novell-pbserv attempts to detect an IP address.
	Can be used in a clustering environment to specify the IP address of the virtual server.
	Can also be used in a multiple-NIC environment to bind the imaging server to a specific IP address.
	By default, this is commented out.
LIBRARY_NAME=	Full path of the library to be loaded by the ZENWorks Imaging Service. If the library name is not specified, then by default `libzenimgweb.so` is loaded from the `/opt/novell/zenworks/preboot/lib` directory.
	By default, this is commented out.

novell-proxydhcp

The novell-proxydhcp daemon provides PXE devices with the information that they require to be able to connect to the ZENworks Preboot Services system.

This daemon is not started automatically when installing ZENworks Linux Management.

- "Understanding the novell-proxydhcp Components" on page 623
- "Configuring novell-proxydhcp" on page 623

Understanding the novell-proxydhcp Components

To initiate the novell-proxydhcp daemon, enter the following command listed for Script Location on the Linux command line in a terminal program:

`/etc/init.d/novell-proxydhcp`

Table D-7 lists the arguments for this command, the executable it starts, and the configuration file it uses:

Table D-7   *Novell-proxydhcp Command Details*

Script Arguments:	start, stop, restart, force-reload, status, showpid, install (for descriptions of these arguments, see "Understanding Script Arguments" on page 629)
Executable:	`/opt/novell/bin/novell-proxydhcpd`
Configuration File:	`/etc/opt/novell/novell-proxydhcp.conf`

Configuring novell-proxydhcp

The novell-proxydhcp configuration file (`novell-proxydhcp.conf`), contains the following parameters:

Table D-8   *Novell-proxydhcp Parameters*

Parameter	Description
LocalDHCPFlag = 0	Indicates whether the DHCP server for this subnet resides on the same server as novell-proxydhcp. 0 (the default) means novell-proxydhcp is not running on the same server as the DHCP service. 1 means they are running on the same server. The Proxy DHCP server needs to behave slightly differently if it is loaded on the same server as the DHCP service.
LocalInterface = 10.0.0.1	Indicates the IP address to be used by the Proxy DHCP server. This setting is intended only for use on servers with multiple LAN interfaces. The IP address must be valid on the server. By default, this parameter is commented out.
NovellPolicyEngine = 10.0.0.1	The IP address of the server where a Novell Preboot policy engine is running. Most often, this is a ZENworks imaging daemon. If no value is specified, the Proxy DHCP assumes that the daemon is running on the same server. By default, this parameter is commented out.
NBPx86 = nvlnbp.sys	The name of the boot file this service will suggest for all x86 computers, such as `nvlnbp.sys`.
MenuTimeout = 2	The number of seconds the F8 menu is displayed before automatically choosing the first option, which is always this server and its default NBP. The default is 2 seconds.
ProxyLogLevel = 2	The value assigned here determines which events are entered in `novell-proxydhcp.log`. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2. Each message from the Proxy DHCP server is assigned a priority level. If *ProxyLogLevel* is set to a value equal to or greater than a message's priority level, that message is entered in `novell-proxydhcp.log`. All other messages are ignored. Priority meaning: **0:** Critical information. Service start, stop, and critical events are logged. **1:** Warning information. Additionally, warning information is logged. **2:** Transaction information. All completed client transactions are logged. **3:** Request information. All client requests and Proxy DHCP requests received are logged, including ignored requests. If a request is ignored, the reason for ignoring it is also logged. **4:** Debugging information. All DHCP packets received and accepted are decoded and logged.
ProxyLogFile = /var/opt/ novell/log/novell-proxydhcp.log	The file where all log file entries are placed. It is located at `/var/opt/ novell/log/novell-proxydhcp.log`. By default, this parameter is commented out.

Parameter	Description
ProxyLogFileSize = 15	The size of the *ProxyLogFile* file is controlled by the value of *ProxyLogFileSize*, where 15 is the default (in MB).
	When the log file exceeds the *ProxyLogFileSize* value, it is deleted and restarted.

Parameters that are not commented out, but contain no values, are given a default value.

The novell-proxydhcp daemon is compliant with the following RFCs:

RFC 2131 - Dynamic Host Configuration Protocol

RFC 2132 - DHCP Options and BOOTP Vendor Extensions

The novell-proxydhcp daemon is compliant with the Preboot eXecution Environment (PXE) Specification v2.1 industry specification, published by Intel.

novell-tftp

The novell-tftp daemon provides TFTP services to imaging clients.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

Understanding the novell-tftp Components

To initiate the novell-tftp daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

```
/etc/init.d/novell-tftp
```

Table D-9 lists the arguments for this command, the executable it starts, and the configuration file it uses:

Table D-9 *Novell-tftp Command Details*

Script Arguments:	start, stop, restart, force-reload, status, showpid (for descriptions of these arguments, see "Understanding Script Arguments" on page 629)
Executable:	/opt/novell/bin/novell-tftpd
Configuration File:	/etc/opt/novell/novell-tftp.conf

Configuring novell-tftp

The novell-tftp configuration file (`novell-tftp.conf`), contains the following parameters for the Novell TFTP server:

Table D-10 *Novell-tftp Parameters*

Parameter	Description
TFTPInterface = 10.0.0.1	The IP address that is used for all TFTP communications. If a value is not given here, the service tries to detect one.
	This value is most useful for multihomed servers.
	By default, this parameter is commented out.
TransferBlockSize = 1428	This value determines the size of the data block used by the TFTP server to transmit and receive data to and from a client. Valid values are between 512 and 4428.
	For ethernet networks, this value should be 1428.
	For token ring networks, this value can be 4428, but only if you are sure there are no ethernet segments; otherwise, use 1428.
	Older TFTP clients might be restricted to 512 bytes, the original transfer block size before the adoption of RFC 2348. The Novell TFTP server is compatible with these clients.
	By default, this parameter is commented out.
TimeoutInterval = 1	This is the amount of time (in seconds) that the TFTP server waits for a client to acknowledge before resending a packet. However, because the TFTP server uses an adaptive algorithm to calculate the actual timeout interval, this value is only used as an initial value. It may increase or decrease, depending on the performance of the network.
	This value is only a default. It can be changed at the request of a client. See RFC 2349.
	Valid values are 1 through 60.
	By default, this parameter is commented out.
Linux -- TFTPDirectory = /srv/tftp	*TFTPDirectory* is the directory where the TFTP server can store and retrieve files. All paths submitted to the TFTP server by clients are assumed to be relative to this directory.
	Because TFTP has no security, it is suggested that you not place files with sensitive information in this directory, and that you place a space quota on it.
	The TFTP server does not load if this directory does not exist.
	By default, this parameter is commented out.
TFTPAllowWrites = 0	This tells the TFTP server whether to allow users to place new files on the server. Setting this variable to 0 (the default) makes the TFTP server more secure by not allowing users to place new files on the server. The other option is 1, which allows users to place new files on the server.
AllowOverwrites = 0	This tells the TFTP server whether to allow users to overwrite existing files on the server. Setting this variable to 0 (the default) makes the TFTP server more secure by not allowing users to overwrite files on the server. The other option is 1, which allows users to overwrite files on the server.
	TFTPAllowWrites must be set to 1 in order for the AllowOverwrites parameter to be recognized.

Parameter	Description
TFTPLogLevel = 2	The value assigned here determines which events are entered in `novell-tftp.log`. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2.
	Each message from the TFTP server is assigned a priority level. If *TFTPLogLevel* is set to a value equal to or greater than a message's priority level, that message is entered in `novell-tftp.log`. All other messages are ignored.
	Priority meaning:
	0: Critical information. Service start, stop, and critical events are logged.
	1: Warning information. Only failed client transactions are logged.
	2: Transaction information. All completed client transactions are logged.
	3: Request information. All client requests and TFTP options are logged.
	4: Debugging information. All server events, including each packet received, are logged.
	By default, this parameter is commented out.
TFTPLogFile = /var/opt/ novell/log/novell-tftp.log	The file where all log file entries are placed.
	By default, this parameter is commented out.
TFTPLogFileSize = 15	The size of the log file is controlled by the value of *TFTPLogFileSize*, where 15 is the default (in MB).
	When the log file exceeds the *TFTPLogFileSize* value, it is deleted and restarted.
	By default, this parameter is commented out.

Parameters that are not commented out, but contain no values, are given a default value.

The novell-tftp daemon is compliant with the following RFCs:

  RFC 1350 -- THE TFTP PROTOCOL (REVISION2)

  RFC 2347 - TFTP Option Extension

  RFC 2348 - TFTP Blocksize Option

  RFC 2349 - TFTP Timeout Interval and Transfer Size Options

novell-zmgprebootpolicy

The novell-zmgprebootpolicy daemon allows PXE devices to query the ZENworks Linux Management system for work to do and for Preboot Menu policies.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- ◆ "Understanding the novell-zmgprebootpolicy Components" on page 628
- ◆ "Configuring novell-zmgprebootpolicy" on page 628

Understanding the novell-zmgprebootpolicy Components

To initiate the novell-zmgprebootpolicy daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

`/etc/init.d/novell-zmgprebootpolicy`

Table D-11 lists the arguments for this command, the executable it starts, and the configuration file it uses:

Table D-11 Novell-zmgprebootpolicy Command Details

Script Arguments:	start, stop, restart, force-reload, status, showpid (for descriptions of these arguments, see "Understanding Script Arguments" on page 629)
Executable:	`/opt/novell/zenworks/preboot/bin/novell-zmgprebootpolicyd`
Configuration File:	`/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf`

Configuring novell-zmgprebootpolicy

The novell-zmgprebootpolicy configuration file (`novell-zmgprebootpolicy.conf`), contains the following parameters:

Table D-12 Novell-zmgprebootpolicy Parameters

Parameter	Description
LocalInterface = 10.0.0.1	The IP address that is used by the Policy server.
	This setting is intended only for use on servers with multiple LAN interfaces. The address must be valid on the server.
	By default, this parameter is commented out.
PolicyLogLevel = 1	The value assigned here determines which events are entered in `novell-zenprebootpolicy.log`. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2.
	Each message from the novell-zmgprebootpolicy server is assigned a priority level. If *PolicyLogLevel* is set to a value equal to or greater than a message's priority level, that message is entered in `novell-zenprebootpolicy.log`. All other messages are ignored.
	Priority meaning:
	0: Critical information. Service start, stop, and critical events are logged.
	1: Warning information. Only failed client transactions are logged.
	2: Transaction information. All completed client transactions are logged.
	3: Request information. All client requests are logged.
	4: Debugging information. All server events, including each packet received, are logged.
	By default, this parameter is commented out.

Parameter	Description
PolicyLogFile = /var/opt/novell/log/zenworks/preboot/novell-zenprebootpolicy.log	The file where all log file entries are placed. By default, this parameter is commented out.
PolicyLogFileSize = 15	The size of the log file is controlled by the value of *PolicyLogFileSize*, where 15 is the default (in MB). When the log file exceeds the *PolicyLogFileSize* value, it is deleted and restarted.
PrebootServer = 10.0.0.5	This field contains the address of the imaging server that should be used to resolve policies. By default, this parameter is commented out.
EnableAMTSupport = Yes	This feature is not currently supported in Novell ZENworks Linux Management. This field enables or disables support for Intel's AMT technology. By default, this support is disabled by commenting out the parameter.

Parameters that are not commented out, but contain no values, are given a default value.

Understanding Script Arguments

The following arguments are available for each of the Preboot Services daemons described above:

Table D-13 *Script Arguments*

Argument	Function
start	Starts the daemon. Because novell-proxydhcp is optional, use this argument to start this daemon. However, this daemon does not automatically start when the server reboots. (See install below.)
start setjustimagedflag	For novell-zislnx only, it sets the Just Imaged flag so that a device can be imaged using its existing Image Safe Data.
stop	Stops the daemon.
restart	Stops and restarts the daemon if it is already running.
force-reload	Causes the daemon's configuration file to be reloaded.
status	Displays the current status of the daemon. For example, if you enter `/etc/inid.d/novell-pbserv status`, information similar to the following is returned: `Novell ZENworks Imaging Service running`

Argument	Function
showpid	Displays the daemon's process ID.
	For example, if you enter `/etc/inid.d/novell-pbserv showpid`, information similar to the following is returned:
	``` Novell ZENworks Imaging Service running 10211 ```
install	For novell-proxydhcp only, causes the daemon to be automatically loaded when the server boots.

D.7.2 Viewing Information About Imaging Requests

After the imaging server has started, you can view information about the status and results of the imaging requests that it has received from imaging clients. A statistical summary of these requests is shown on the server's command line. The statistics shown on this screen are explained below. All statistics are reset to zero if you restart the imaging server.

To view the multicast imaging information, at the server's command line enter:

`/opt/novell/zenworks/preboot/bin/novell-zmgcast -status`

The information in Table D-14 explains what is displayed:

Table D-14 *Imaging Request Statistics*

Statistic	Specifies
PXE Requests	The number of imaging requests of any kind that have been received by the Imaging Server since it was last started. This includes requests that failed, were denied, or were referred to other Imaging Servers. Information about each of these requests, such as the source, type, date/time, and results, is logged on the Imaging Server.
Images Sent	The number of images that the imaging server has sent to imaging clients since the imaging server was started. This includes only images that were retrieved from this imaging server.
Images Received	The number of new images that have been received and stored on the imaging server since it was started. This includes images that were received through client referrals.

D.7.3 Starting a Manual Multicast Session

At the bash prompt, you can start a manual multicast session, see any sessions in progress, and delete sessions. For more information, see "Initiating a Multicast Session from Each Client" on page 437.

ZENworks Imaging Engine Commands

E
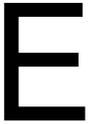
After booting a device from an imaging boot media, you can use the img command at the Linux bash prompt or the ZENworks® Imaging Engine menu to do any of the following:

- ◆ Take an image of the device's hard disks
- ◆ Put down an image on the device's hard disks
- ◆ View or manipulate the device's hard disk partitions
- ◆ View the device's hardware configuration or image-safe data
- ◆ Display a menu from which you can also perform all of these tasks

The ZENworks Imaging Engine is installed to the /bin directory on the imaging boot device. If the imaging boot device is a diskette, a CD, or DVD, the /bin directory is actually archived in the root file, which is expanded during the imaging boot process. If the imaging boot method is Preboot Services, the ZENworks Imaging Engine is downloaded to the device when booting.

Because the ZENworks Imaging Engine is a Linux application, the command syntax is case sensitive. The overall syntax is:

```
img [mode]
```

where *mode* is any of the modes described in the following sections:

Each mode can be abbreviated to the first letter of its name. For example, img dump can be abbreviated as img d.

To access the ZENworks Imaging Engine menu and perform all of these tasks, enter img with no parameters.

E.1 Help Mode (img help)

Use Help mode to get information about the img command if you don't have this documentation available.

To use the Help mode:

1 Do the one of following:

◆ Enter:

```
img [help [mode]]
```

where *mode* is the mode whose command syntax you want help with.

Examples:

Example	Explanation
img help	Displays a short description of each mode.
img help m	Displays information on how to use the Make mode.
img help p	Displays information on how to use the Partition mode.

◆ Enter `img` to display the ZENworks Imaging Engine menu, click *Help*, then select a mode name.

E.2 Automatic Mode (img auto)

Use automatic mode to image the device automatically, based on any applicable Preboot Services default settings. The ZENworks Imaging Engine runs in this mode if you let the imaging boot process proceed without interruption, or if you type the command below at the Linux prompt.

To use the automatic mode, do any of the following at the bash prompt:

◆ Enter:

```
img auto
```

◆ To display the ZENworks Imaging Engine menu, enter:

```
img
```

and on the menu bar, click *Imaging*, then click *Query for work*.

◆ To display the ZENworks Imaging Engine menu, enter:

```
img
```

then click *F9 Query for work* on the task bar.

◆ To display the ZENworks Imaging Engine menu, enter:

```
img
```

then press *F9*.

In this mode, the ZENworks Imaging Engine queries the imaging server specified in the PROXYADDR environment variable for any work to do. The imaging server checks the relevant Preboot Services default settings to determine what imaging tasks should be performed (if any), such as taking or putting down an image. It then instructs the ZENworks Imaging Engine to perform those tasks. If any tasks involve storing or retrieving images on other imaging servers, the imaging server refers the ZENworks Imaging Engine to those servers to complete those tasks. After the ZENworks Imaging Engine has completed its work, it communicates the results to the original imaging server, and the results are logged on that server.

For information on configuring the settings that control what happens in this mode, see Section 29.4, "Configuring Preboot Services Defaults," on page 379.

E.3 Make Mode (img make)

Use the Make mode to take an image of the device and store it in a specified location. Normally, all partitions on the local hard disks are included in the image, but there are some exceptions noted in Table E-1 on page 633.

You can take an image of a device using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see "Manually Taking an Image of a Device" on page 415. You can also use the Make Locally mode to take an image of the device and store it in a partition on a local hard disk. For step-by-step instructions, see Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424.

The image size corresponds to about half the size of the data in all of the device's partitions, except that the ZENworks partition and Compaq or Dell configuration partitions are always excluded. Devices with logical volumes (LVMs) are not supported for imaging.

The syntax of this mode depends on whether you store the image locally or on an imaging (proxy) server.

The following sections contain additional information:

- Section E.3.1, "Make Locally (img makel)," on page 633
- Section E.3.2, "Make to Proxy (img makep)," on page 634

E.3.1 Make Locally (img makel)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `makel` "make locally" parameter:

```
img makel[pNumber] filepath [comp=comp level] [xpartition]
```

Commands

Table E-1 *makel Commands*

Parameter	Specifies
makel[*pNumber*]	The partition number (as displayed by `img dump`) of the local partition for where to store the image. It must be a primary partition. This partition is excluded from the image that is created.
	If you omit the partition number from this parameter, the image is stored in the local ZENworks partition.
filepath	The image filename, including a `.zmg` extension (case sensitive) and the complete path from the root of the partition. The directories in the path must exist. If the file already exists, it is overwritten. However, you are prompted to verify whether to overwrite.

Parameter	Specifies
[comp=*comp level*]	*comp level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for Speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for Space*.
xpartition	The partition number (as displayed by `img dump`) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions. If you omit this parameter, all partitions are included in the image except the one where the image is stored.

Examples

Table E-2 *makel Examples*

Example	Explanation
`img makel8 /imgs/dellnt.zmg`	Takes an image of all partitions except the one in slot 8 and saves the image to `imgs/dellnt.zmg` in the partition in slot 8. (Assumes that slot 8 contains a primary partition.)
`img makel /imgs/dellnt.zmg`	Takes an image of all partitions and saves it to `imgs/dellnt.zmg` in the ZENworks partition. (Assumes that the partitions have been installed.)
`img makel /imgs/dellnt.zmg x2 x3`	Takes an image of all partitions except those in slots 2 and 3 and saves the image to `imgs/dellnt.zmg` in the ZENworks partition. (Assumes that the partitions have been installed.)

E.3.2 Make to Proxy (img makep)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `makep` "make to proxy" parameter:

`img makep` *address filepath* `[comp=`*comp level*`]` `[`*xpartition*`]`

Commands

Table E-3 *makep Commands*

Parameter	Specifies
address	The IP address or DNS name of the imaging server to store the image on.

Parameter	Specifies
filepath	The image filename, including a `.zmg` extension (case sensitive) and the complete path in UNC style. The directories in the path must exist. If the file already exists, the imaging server won't overwrite it unless you enable this behavior in the ZENworks Control Center. If no folders are specified in the path, the image is created at the root of the volume or drive where the ZENworks Linux Management imaging server software is installed. **IMPORTANT:** Because Linux doesn't recognize backslashes, you must use forward slashes in the UNC path, or enclose the entire path in quotes.
[comp=*comp level*]	*comp level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for Speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for Space*.
xpartition	The partition number (as displayed by `img dump`) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions. If you omit this parameter, all partitions are included in the image.

Examples

Table E-4   *makep Examples*

Example	Explanation
`img makep 123.45.67.890 //xyz_server/sys/imgs/dellnt.zmg`	Takes an image of all partitions and saves it to `sys/imgs/dellnt.zmg` on `xyz_server`. (Assumes that 123.45.67.890 is the IP address of `xyz_server`.)
`img makep img.xyz.com //xyz_server/sys/imgs/dellnt.zmg x2 x3`	Takes an image of all partitions except those in slots 2 and 3 and saves the image to `sys/imgs/dellnt.zmg` on `xyz_server`. (Assumes that `img.xyz.com` is the DNS name of `xyz_server`.)

E.4 Restore Mode (img restore)

Use the Restore mode to retrieve an image from a specified location and put it down on a device.

You can restore an image of a device using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see "Manually Taking an Image of a Device" on page 415. You can also use the Restore mode to restore an image from a partition on a local hard disk. For step-by-step instructions, see Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424.

Normally, if the image to be put down is a base image (one created previously by the ZENworks Imaging Engine), all existing partitions except the ZENworks partition and Dell or Compaq configuration partitions are removed from all local hard disks before the new image is put down. When the image is put down, the sizes of the original partitions from which the image was taken are preserved, if possible. If there is insufficient space, the last partition is shrunk to fit, unless this

would result in data loss, in which case the ZENworks Imaging Engine denies the requested operation. If there is extra space left after all partitions in the image have been restored to their original sizes, that space is left unpartitioned.

If the image to be put down is an add-on image, or if it's a base image and you specify the a*partition*:p*partition* parameter, none of the existing physical partitions are removed. Instead, the appropriate partitions are merely updated with the files from the image, overwriting any existing file of the same name and location.

Restoring add-on images over 4 GB in size is not supported by Linux Management imaging.

The syntax of this mode depends on whether you will retrieve the image from a local device or from an imaging (proxy) server, as explained in the subsections below:

- Section E.4.1, "Restore from Local (img restorel)," on page 636
- Section E.4.2, "Restore from Proxy (img restorep)," on page 638

E.4.1 Restore from Local (img restorel)

Use the Restore from Local mode to retrieve an image from a local device and put it down on the device. For more information, see Section 30.1.3, "Setting Up Disconnected Imaging Operations," on page 424.

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `restorel` "restore from local" parameter:

```
img restorel[pNumber] filepath [sfileset] [apartition:ppartition]
```

Commands

Table E-5   *restorel Commands*

Parameter	Specifies
restorel[*pNumber*]	The partition number (as displayed by `img dump`) of the local partition to retrieve the image from. It must be a primary partition. This partition is not changed by the imaging operation.
	If you omit the partition number from this parameter, the image is retrieved from the local ZENworks partition.
filepath	The filename of the image to retrieve, including the `.zmg` extension (case-sensitive) and the complete path from the root of the partition.
s*fileset*	The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see Section 28.5.2, "Creating, Installing, and Restoring Standard Images," on page 346.
	If you omit this parameter, file set 1 is used.

Parameter	Specifies
apartition:p*partition*	A mapping between a partition in the image archive (*apartition*) and a target physical partition on the local machine (p*partition*). Use this parameter to selectively restore a specific part of the image to a specific local partition.
	IMPORTANT: If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files; however, any existing files of the same names are overwritten. If you want to remove all existing files from the target partition before updating it, first use the Partition Mode (img part) to delete and recreate the partition.
	For *apartition*, use the partition number displayed for the source partition in the Image Explorer (imgexp.exe) utility. For p*partition*, use the partition number displayed by `img dump` for the target partition. The target partition must be a partition of a supported file system. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can't apply the same part of an image to multiple local partitions in a single operation.

Examples

Table E-6   restorel Examples

Example	Explanation
`img restorel8 /imgs/dellnt.zmg`	Removes all existing local partitions except the one in slot 8, retrieves the image from `imgs/dellnt.zmg` in slot 8, and puts down the partitions and contents of that image on the available local writable devices (assuming there is sufficient local space and that slot 8 contains a primary partition).
`img restorel /imgs/dellnt.zmg`	Removes all existing local partitions, retrieves the image from `imgs/dellnt.zmg` in the ZENworks partition, and puts down the partitions and contents of that image on the available local writable devices (assuming there is sufficient space).
`img restorel /imgs/dellnt.zmg s2`	Removes all existing local partitions, retrieves the image from `imgs/dellnt.zmg` in the ZENworks partition, and puts down the partitions and contents of file set 2 of that image on the available local writable devices (assuming there is sufficient space).
`img restorel /imgs/dellnt.zmg a2:p1 a3:p1`	Retrieves the image from `imgs/dellnt.zmg` in the ZENworks partition, updates local partition 1 with the data from partitions 2 and 3 of that image, and leaves the other local partitions unchanged (assuming there is sufficient space in local partition 1).

E.4.2 Restore from Proxy (img restorep)

Use the Restore from Proxy mode to retrieve an image from an imaging (proxy) server and put it down on the device. For more information, see "Manually Putting an Image on a Device" on page 420.

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the restorep "restore from proxy" parameter:

img restorep *address filepath* [s*fileset*] [a*partition*:p*partition*]

Commands

Table E-7   restorep Commands

Parameter	Specifies
address	The IP address or DNS name of the imaging server to retrieve the image from.
filepath	The filename of the image to retrieve, including the .zmg extension (case-sensitive) and the complete path in UNC style.
	IMPORTANT: Because Linux doesn't recognize backslashes, you must use forward slashes in the UNC path or enclose the entire path in quotes.
s*fileset*	The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see Section 28.5.2, "Creating, Installing, and Restoring Standard Images," on page 346.
	If you omit this parameter, file set 1 is used.
a*partition*:p*partition*	A mapping between a partition in the image archive (*apartition*) and a target physical partition on the local machine (*ppartition*). Use this parameter to selectively restore a specific part of the image to a specific local partition.
	IMPORTANT: If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files or overwrite any existing files of the same names if they are newer. If you want to remove all existing files from the target partition before updating it, first use the Partition Mode (img part) to delete and recreate the partition.
	For a*partition*, use the partition number displayed for the source partition in the Image Explorer (imgexp.exe) utility. For p*partition*, use the partition number displayed by img dump for the target partition. The target partition must be a partition of a supported file system. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can't apply the same part of an image to multiple local partitions in a single operation.

Examples

Table E-8 *restorep Examples*

Example	Explanation
`img restorep 137.65.95.127 //` `xyz_server/sys/imgs/dellnt.zmg`	Removes all existing local partitions, retrieves the image from `sys/imgs/dellnt.zmg` on `xyz_server`, and puts down the partitions and contents of that image on the available local writable devices (assuming there is sufficient local space and that 137.65.95.127 is the IP address of `xyz_server`).

`img restorep img.xyz.com //`
`xyz_server/sys/imgs/dellnt.zmg`
`s2`
	Removes all existing local partitions, retrieves the image from `sys/imgs/dellnt.zmg` on `xyz_server`, and puts down the partitions and contents of file set 2 of that image on the available local writable devices (assuming there is sufficient local space and that `img.xyz.com` is the DNS name of `xyz_server`).

`img restorep img.xyz.com //`
`xyz_server/sys/imgs/dellnt.zmg`
`a2:p1`
	Retrieves the image from `sys/imgs/dellnt.zmg` on `xyz_server`, updates local partition 1 with the data from partition 2 of that image, and leaves the other local partitions unchanged (assuming there is sufficient space in local partition 1 and that `img.xyz.com` is the DNS name of `xyz_server`).

E.5 Session (Multicast) Mode (img session)

Use the Session (Multicast) mode to take an image of one device and put it down on multiple other devices simultaneously over the network in a single operation.

IMPORTANT: For multicasting to work properly, the routers and switches on the network must have multicast features configured. Otherwise, multicast packets might not be routed properly.

For multicasting to work, each participating device must boot from an imaging boot media and run the ZENworks Imaging Engine in this mode, as explained below. The device from which the image is taken is called the *master*, and the devices that receive the image are called *participants*.

You can start the multicast session from the imaging server. If you start the session this way, you specify an image file for multicasting rather than a device as the session master. Otherwise, if you start the session from a client device, you can specify one of the session participants as the session master. In that case, an image of the session master's hard drive is sent to the session participants. For more information, see .

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `session` parameter:

```
img session name [master|client] [clients=count [t=minutes]]
```

Commands

Table E-9   *session Commands*

Parameter	Specifies
name	The name of the multicast session. Each device joining the session uses the same value for this parameter.
	IMPORTANT: The name must be unique among concurrent multicast sessions. It is hashed by the ZENworks Imaging Engine to produce a Class D IP address for the multicast session. To facilitate troubleshooting (wire sniffing), all Linux Management imaging multicast addresses start with 231. For example, the session name `mcast01` can produce the multicast address 231.139.79.72.
master|client	Specifies that this device is the session master or a session client.
	If you omit this parameter, the ZENworks Imaging Engine waits for the user at the master device to press `m` to designate that device as the master, or it waits for another device to be declared master for the imaging session to be started from the imaging server by selecting *Manually start multicast*, providing the required information, then selecting *Yes*.
clients=*count*	The number of participating devices that must register with the master before imaging begins. This option only applies to session masters.
	If you omit this parameter, the ZENworks Imaging Engine waits for the user at the master device to press `g`. After imaging has begun, any participating devices attempting to register are denied.
time=*minutes*	The number of minutes the master device waits for the next participant to register before starting the imaging process without reaching *count* registered participants. This option only applies to session masters.
	If you omit this parameter, the imaging process does not start until *count* is reached, or the user at the master device presses `g`. After that, any participants attempting to register are denied and queued for the next multicast session.

Examples

Table E-10   *session Examples*

Example	Explanation
`img session mcast01`	Starts a multicast session named `mcast01`. Each successive device that issues this same command before the imaging begins joins the session. Imaging doesn't start until one of the users presses `m` to designate himself as master and presses `g` to start the imaging, or the imaging session is started from the imaging server by selecting *Manually start multicast*, providing the required information, then selecting *Yes*.

Example	Explanation
`img session mcast01 m`	Starts a multicast session named `mcast01` and designates this device as the master. Each successive device that issues `img session mcast01` before the imaging begins joins the session as a participant. Imaging doesn't start until the master user presses `g`.
`img session mcast01 master clients=5`	Starts a multicast session named `mcast01`. Each successive device that issues `img session mcast01` before the imaging begins joins the session. Imaging doesn't start until one of the users presses `m` to designate himself as master, or until the imaging session is started from the imaging server by selecting *Manually Start Multicast*, providing the required information, then selecting *Yes*. Five other devices must also register as participants before the session begins.
`img session mcast01 master clients=5 time=20`	Starts a multicast session named `mcast01`. Each successive device that issues `img session mcast01` before the imaging begins joins the session. Imaging doesn't start until one of the users presses `m` to designate himself as master, or until the imaging session is started from the imaging server by selecting *Manually Start Multicast*, providing the required information, then selecting *Yes*. Either five other devices must register as participants or more than 20 minutes must elapse between any consecutive participant registrations, whichever occurs first, and then the session begins.

E.6 Partition Mode (img part)

Use the Partition mode to activate (make bootable), add, or delete a partition on the device.

You can activate, add, or delete a partition using either ZENworks Imaging Engine menu or the bash prompt.

The Partition mode can be used in two ways:

- Section E.6.1, "Using the ZENworks Imaging Engine Menu," on page 641
- Section E.6.2, "Using the Bash Prompt," on page 642

E.6.1 Using the ZENworks Imaging Engine Menu

1 Enter `img` to display the ZENworks Imaging Engine menu, then click *Partitioning*.

2 Click *Modify partitions*, then click an option:

Active: Select a partition that you want to activate (make bootable), then click *Active*.

Add: Opens the Create New Partition window. Click a partition type, partition size, and cluster size, then click *OK*.

Delete: Select a partition, then click *Delete*.

For more information, see the table in Section E.6.2, "Using the Bash Prompt," on page 642.

E.6.2 Using the Bash Prompt

1 From the bash prompt, enter:

`img p`*operation*

where *operation* is one of the following:

Operation	Action
pc*pNumber type* [*size*] [cluster=*clusterSize*]	Creates a new partition, where: • *pNumber* is the number of the partition slot (as displayed by `img dump`) in which to create the partition • *type* is a keyword, a partition name, Extended, or a numerical value for the partition type, for example 0x0C (hexadecimal) or 11 (decimal) If you are creating an extended partition, you can create a logical drive inside of the extended partition. (See the next table for an example.) • *size* is a valid size for the partition type in MB or a percentage If you omit this parameter, the largest valid size for the partition type is used, given the available unpartitioned space on the drive. If you give a percentage, include the % symbol; otherwise, the value is considered the size in MB. The new partition is recognizable by other operating systems, but must be formatted or have a base image restored to it before you can store files in it.
pd*pNumber*	Deletes the partition from slot number *pNumber*. Use `img dump` to get the slot number.
pd-all	Deletes all non-protected partitions.
pa*pNumber*	Activates (make bootable) the partition in slot number *pNumber*. Use `img dump` to get the slot number.

The following are examples:

Example	Explanation
`img pc1 ext2`	Creates the ext2 partition in slot 1 using all of the available unpartitioned space on the drive.
`img pc5 reiser 5671`	Creates a Reiser partition in slot 5 using 5,671 MB on the drive.
`img pd3`	Deletes the partition from slot 3.
`img pc2 extended 2500` `img pc2 reiser 500`	Creates an extended partition with a 2500 ext2 logical drive and a 500 MB Reiser logical drive.

E.7 ZENworks Partition Mode (img zenPartition)

Use the ZENPartition mode to enable, disable, or remove the installed ZENworks partition.

1 Do one of the following:

   • From the bash prompt, enter the following:

```
img zenPartition operation
```

where *operation* is enable, disable, or remove.

- Enter `img` to display the ZENworks Imaging Engine menu, click *Partitioning*, then click one of the following:

  Disable ZENworks partition

  Enable ZENworks partition

  Remove ZENworks partition

2 Enter `lilo.s` to make this change effective.

IMPORTANT: If you remove an installed ZENworks partition, you must immediately restore a base image with a valid non-LILO MBR (Master Boot Record). If you do not, the device cannot boot properly.

E.8 Dump Mode (img dump)

Use the Dump mode to view information about the hard drives and partitions on the device.

1 Do one of the following:

- Enter `img` to display the ZENworks Imaging Engine menu, click *System information*, then click *Drive information*.

- Enter the following:

  ```
  img dump [geo]
  ```

  where:

Parameter	Action
dump	Lists the existing partitions on all local hard drives. For each partition, the type, size, and slot number of the partition are given.
	The ZENworks partition and Dell or Compaq configuration partitions are not listed.
geo	Displays additional information about the geometry (cylinders, heads, and sectors) and capacity of each hard drive.

Examples:

Example	Explanation
img dump	Lists the current partitions on all local writable devices.
img dump geo	Lists all hard drives, their geometry and capacity, and the current partitions on the writable devices.

E.9 Information Mode (img info)

Use the Information mode to view the following:

- The data currently stored in the image-safe area on the device

This data is saved by the Novell ZENworks Linux Management Imaging Agent (novell-zislnx) during each device's session to ensure that it can be restored after the device is reimaged. If the device is new and doesn't have an operating system yet, an initial set of data is supplied from the default configuration for the ZENworks Management Zone, such as IP addresses.

- ◆ Information about the hardware devices on the device

  This information is detected during the imaging boot process. If the ZENworks Imaging Engine runs in auto-imaging mode, this information is sent to the imaging server to help determine which image to put on the device, if necessary.

- ◆ Name of the base image that was last put down on the device

To use the Information mode:

1 Enter `img` to display the ZENworks Imaging Engine menu, click *System information*, then click *Image-safe data* or *Detected hardware*. (See Table E-11 for details.)

or

Enter the following from the bash prompt:

```
img info [zisd]
```

Commands

Table E-11   *Information Mode Parameters*

Menu item or parameter	Action
System Information > Detected Hardware *or* info *(from the bash prompt)*	Lists the detected hardware devices on the device, including: ◆ CPU chipset ◆ BIOS asset tag ◆ BIOS serial number ◆ Video adapter ◆ Network adapter ◆ MAC address ◆ Sound card ◆ Hard drive controller ◆ Hard disk capacity ◆ Detected RAM ◆ Boot media
System Information > Image Safe Data *or* img info zisd *(from the bash prompt)*	Lists the data currently stored in the image-safe area on the device. The items that comprise this data are listed in Section D.3, "Image-Safe Data Viewer and Editor (zisview and zisedit)," on page 613. In addition to the image-safe data, the last base image that was put down on the device is also listed.

Examples

Table E-12 *Examples*

Example	Explanation
img info	Lists the detected hardware devices on the device.
img info zisd	Lists the Linux Management image-safe data currently stored on the device and the last base image that was put down.

Updating ZENworks Imaging Resource Files

F

In Novell® ZENworks® 7 Linux Management, you can manually update ZENworks imaging resource files.

The following sections provide concepts on how the boot process works with ZENworks imaging, and instructions for updating imaging resource files:

F.1 The Linux Distribution for Imaging

ZENworks Imaging uses a small Linux distribution on the client device to perform imaging operations. The distribution shipping with ZENworks 7 is based on the SUSE® installation system, where SUSE Linux or SUSE Linux Enterprise Server (SLES) boot to a small distribution to perform a YaST installation. ZENworks Imaging uses the same installation system found in SLES, but instead of starting a YaST installation, it starts a ZENworks Imaging session.

In ZENworks 6.5 SP1 and earlier, Linux kernel 2.4.x is used in the customized distribution. In ZENworks 6.5 SP2, the kernel is updated to 2.6 and is a SLES-based distribution.

Using a stable Linux distribution based on SLES gives customers a distribution with the broadest range of stable drivers available. The hardware industry is continually introducing new and updated network and disk drivers, so it's not always possible to provide the latest drivers in its software releases.

This section covers how to update Linux drivers using the new distribution. It deals with the imaging resource files that are based on the SLES distribution and ZENworks Preboot Services processing.

F.2 Understanding Device Boot Processes in a ZENworks Imaging Environment

The following provides a high-level overview of a Linux boot process and how ZENworks 7 imaging affects it:

1. A boot loader program loads the Linux kernel and initrd (initial RAM drive) into memory.

   The SLES-based imaging distribution uses `isolinux` as the boot loader for imaging CDs, a modified `pxelinux` for booting using PXE, or `linld.com` when using a single diskette with the CD. If you have a ZENworks partition installed, it uses the lilo program to boot alternately between the ZENworks partition and the installed operating system.

   Following are the filenames and paths:

Files	When booting from a CD	When booting from PXE
Preboot Loader	`isolinux`	`linld.com`
Linux Kernel Name	`/boot/loader/linux`	`/srv/tftp/boot/linux`
Initrd Filename	`/boot/loader/initrd`	`/srv/tftp/boot/initrd`

2. The Linux kernel starts running, does some device driver setup, then mounts the `initrd` file system.

   Regardless of which boot loader method is used, the main purpose is to set up the `initrd` file as a RAM drive, load the Linux kernel into memory, then turn control over to it with an indication to the Linux kernel of where to find `initrd`.

3. The Linux kernel turns control over to linuxrc, for performing initial hardware detection. When finished, control is returned to the Linux kernel.

4. The Linux kernel starts a background process (`/sbin/init`).

   After control is passed to the linuxrc program, control is never returned to the Linux kernel or passed on to the init process.

For more information on `linuxrc` and `zenworks.s`, review the following sections:

F.2.1 linuxrc

When control is turned over to linuxrc, there are several processes it performs to get the system ready for the imaging process. Linuxrc is initially configured from the `/linuxrc.config` file, which is located in the `initrd` file system. Additional configuration information for linuxrc can be placed in the `/info` file (located in the `initrd` file system), but ZENworks does not normally use this information.

Linuxrc also loads a `root` file system, which is combined with the `initrd` file system that is set up by the boot loader. The `root` file system is located on an imaging CD as the file `/boot/root`. For PXE booting, the `root` file system is stored on the ZENworks imaging server as `/srv/tftp/boot/root`.

Linuxrc attempts to locate and load the `settings.txt` file, either on the root of the imaging CD, or on the ZENworks imaging server in the `/srv/tftp/boot` directory. From `settings.txt`, linuxrc reads and processes any parameters that pertain to itself, then copies `settings.txt` to the root (`/`) of the file system.

Linuxrc then also attempts to locate and load a file named `driverupdate`. It is usually located in the same directory as `root`. This file is used to update drivers and other files in the imaging distribution.

The `driverupdate` file is based on standard SUSE technology during a PXE boot. Because the network must be operating normally in order to obtain `driverupdate`, this file cannot update drivers for the active network device. However, other files and drivers can be updated by using the `driverupdate` file. For more information, see Section F.4.3, "Using the Driverupdate File Method," on page 654.

F.2.2 zenworks.s

A normal SUSE installation for SUSE Linux or SLES boots to a small distribution to perform a YaST installation. ZENworks Imaging boots with the same installation system, but instead of starting a YaST installation, it starts the ZENworks Imaging process. Control is turned over to the ZENworks script `/bin/zenworks.s`, which is the main script file for ZENworks imaging processing. The script performs a certain number of setup tasks, then gives control to the appropriate script for the selected imaging process. For more information on the imaging process, see Chapter 28, "Understanding Preboot Services in ZENworks Linux Management," on page 329.

One of the setup tasks is to apply any update files. When booting from a CD, `zenworks.s` copies the `/addfiles` directory structure to the Linux file system. For more information, see Section F.4.1, "Adding Files to an Imaging Boot CD," on page 651.

F.3 Understanding ZENworks Partitions and Command Line Parameters

The following sections provide an understanding of the ZENworks partition and imaging commands that are used when updating Linux drivers:

- Section F.3.1, "The ZENworks Partition," on page 649
- Section F.3.2, "Command Line Parameters and Variables," on page 650

F.3.1 The ZENworks Partition

The ZENworks partition is used to store the files required to load Linux into RAM, making the result similar to using a CD or PXE boot method. The ZENworks partition has a similar boot media layout as an imaging CD. It has a minimum size of 150 MB.

The files stored on the ZENworks partition are `/boot/loader/linux`, `/boot/loader/initrd`, and `/boot/root`, which are the same directories as on the imaging CD. In ZENworks 7, the boot loader continues to be lilo, which loads Linux as described under Section F.2, "Understanding Device Boot Processes in a ZENworks Imaging Environment," on page 648. The `driverupdate` and `settings.txt` files are searched for and loaded from the ZENworks partition.

If you need to modify the Linux files, you must modify the initrd or root file sets the same way as you would for other boot methods. For information, see Section F.4.2, "Adding Files to the Initrd or Root File Systems," on page 651.

F.3.2 Command Line Parameters and Variables

There are four types of command line parameters that can be used with the ZENworks imaging process. They are entered manually on the command line when booting from a CD or they can be placed in the `isolinux.cfg` file located in the `/boot/loader` directory. The commands are also located in the `*.cfg` files for PXE and are located in the `/srv/tftp` directory on the ZENworks imaging server.

- **Kernel parameters:** The valid parameters for the Linux kernel are found in the `/Documentation/kernel-parameters.txt` file that is installed with the kernel source.

  Some devices have a faulty BIOS, where you must turn off ACPI processing for the kernel to load properly. To do this, use the kernel parameter acpi=off. For more information, see Novell Support (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=10099330&sliceId=&dialogID=1284337&stateId=1%200%20548668).

- **Linuxrc parameters:** These parameters affect the way linuxrc detects hardware or sets hardware settings. They are described briefly in the `/usr/share/doc/packages/linuxrc/linuxrc.html` file in a Linux system.

  Linuxrc parameters can be found in the `/linuxrc.config` or `/info` files that reside in the `initrd` file system. Some parameters can be placed in the `settings.txt` file that is located on the root of the imaging CD or ZENworks partition, or in the `/srv/tftp/boot` file for PXE booting.

  Parameters that can be placed in the `settings.txt` file (the easiest file to edit) are limited. During PXE booting, parameters that affect the network are not processed from `settings.txt`, because by the time linuxrc loads the `settings.txt` file, the network is already set up. Network settings can be placed in the `settings.txt` file when booting from an imaging CD, because it is loaded early enough in the process to take effect.

- **ZENworks variables:** Some environment variables affect the way imaging performs. They can be configured in any file, but should normally be configured in the `settings.txt` file.

  If you add variables to the `settings.txt` file that were not originally defined there, you must export the variable. For example, in the `settings.txt` file, enter:

  `export IMGCMD="myscript"`

  A list of all image engine or script variables is listed under Section F.7, "Variables and Parameters," on page 659.

- **Other variables:** Environment variables that you might want in your script can be added in the same manner as described for the ZENworks variables.

F.4 Modifying ZENworks Imaging Resource Files

From time to time you might want to modify an imaging distribution by adding your own files. These can be additional programs, scripts, data files, or updated Linux drivers.

You can use the following methods to update imaging resource files:

- The easiest method is to edit the `settings.txt` file, which is located on the root of the imaging CD or in `/srv/tftp/boot` on the ZENworks Imaging Server for PXE booting.

- Where you are using a ZENworks partition, you can boot to the manual or maintenance mode, mount the ZENworks partition, then copy the modified `settings.txt` and the files in `initrd` or `root` to the mounted ZENworks partition.

- Another easy method is to edit the `.cfg` files located in `/srv/tftp` on the ZENworks Imaging Server for PXE booting. This method is only available for Linux Imaging Servers, because the configuration files are provided by Novell's version of PXE.

- You can modify files in the `initrd` or `root` file systems, but you need a Linux environment for performing the modification process. Files required during the initial setup (during linuxrc processing time), such as LAN drivers, must be placed in the `initrd` file system. Other files that are not needed until the `zenworks.s` script file takes control can be placed in the `root` file system (for example, an imaging script), or you can use the `driverupdate` file.

  This method is discussed in this section.

- Section F.4.1, "Adding Files to an Imaging Boot CD," on page 651
- Section F.4.2, "Adding Files to the Initrd or Root File Systems," on page 651
- Section F.4.3, "Using the Driverupdate File Method," on page 654

F.4.1 Adding Files to an Imaging Boot CD

If you have files to add to an imaging boot CD so they can be available for use when you get to the actual imaging process (such as scripts, but normally not driver modules), you can copy the files to the `/addfiles` directory on the imaging CD. This is an easy way to insert your script or other files into the distribution without modifying the initrd or root file systems. However, these files are not available during the boot and module loading phases.

The imaging boot CD has a directory named `/addfiles` where you can add files. They should be placed below this directory in their proper directory names. They are then available in this directory structure during the imaging process.

An example of how you can add files:

1 If you want to execute your own script instead of the normal imaging process, create a script file named `myscript.s` and place it on the boot CD. For example, `/addfiles/bin/myscript.s`.

IMPORTANT: The script file must have proper LF line terminators that Linux requires, not the DOS CR and LF end-of-line characters. In other words, you cannot use `Notepad.exe` to create the script; you must use a text editor compatible with Linux, such as TextPad.

---

2 To place the following line in the `settings.txt` file, enter:

`export IMGCMD="/bin/myscript.s"`

When imaging is run, it runs `/bin/myscript.s` instead of using the normal `img -auto` command.

F.4.2 Adding Files to the Initrd or Root File Systems

This is the preferred method for updating imaging resource files, and must be performed in a Linux environment.

Before performing the procedures given below, make sure you have created backup copies of any files you plan to change, specifically the `/srv/tftp/boot/initrd` file. If you want to change the files on an imaging CD, you need an ISO editor or some other process for extracting and replacing the file in the `bootcd.iso` image file.

IMPORTANT: When updating or adding files and Linux drivers in the `initrd` or `root` file systems, document the changes you make. When you receive updated resource files from Novell, they do not contain your customized changes. If the kernel version has changed with the newer resource files from Novell, previously added drivers must be updated either by obtaining a new version from the manufacturer or recompiling the driver using the correct Linux kernel version source.

- "Adding to Initrd" on page 652
- "Adding to Root" on page 653

To add files to the `root` file system, you can also use the `driverupdate` file method described in Section F.4.3, "Using the Driverupdate File Method," on page 654.

Adding to Initrd

To modify the `initrd` file system:

1 Using a Linux device, create a working directory and change to that directory.

2 To copy initrd from the PXE server or the boot CD to the new working directory:

- For PXE, copy `/tftp/boot/initrd` to the Linux workstation's working directory.
- For the CD, extract `initrd` from the `/boot/i386/loader` directory on the boot CD, then copy the extracted `initrd` to the Linux workstation's working directory.

3 To rename `initrd` to `initrd.gz`, enter:

```
mv initrd initrd.gz
```

4 To unzip the `initrd.gz` file, enter:

```
gunzip initrd.gz
```

5 To create another working directory for use as a mount point in the subsequent steps, enter:

```
mkdir work
cd work
```

6 To extract `initrd` into the `/work` directory, enter:

```
cpio -idmuv ../initrd >/dev/null 2>&1
```

7 To copy your files or updated driver to the extracted `initrd` file system, enter:

```
cp /your_path/module.ko work/lib/modules/2.6.5-override-default/initrd
```

where *your_path* is the path to the *module*.ko file and *module* is the name of the module.

Other files to be included in the `initrd` file system should be copied to the appropriate directory.

8 To re-package the `initrd` file system, enter:

```
cd work
find . | cpio -quiet -o -H newc > ../initrd
cd ..
```

9 To zip the new `initrd` file, enter:

```
gzip -v9c initrd > initrd.gz
```

10 To rename `initrd.gz` back to `initrd`, enter:

```
mv initrd.gz initrd
```

11 To copy the file back:

- For PXE, copy the updated `initrd` file to the `/tftp/boot` directory on the PXE server.
- For the CD, copy the updated `initrd` file to the `/boot/i386/loader` directory on the boot CD.

Adding to Root

To modify the `root` file system:

1 Using a Linux device, create a working directory and change to that directory.

2 To copy `initrd` from the PXE server or the boot CD to the new working directory:

- For PXE, copy `/tftp/boot/initrd` to the Linux workstation's working directory.
- For the CD, extract `root` from the `/boot/i386/` directory on the boot CD, then copy the extracted `root` to the Linux workstation's working directory.

3 To rename `root` to `root.gz`, enter:

```
mv root root.gz
```

4 To unzip the `root.gz` file, enter:

```
gunzip root.gz
```

5 To create another working directory for use as a mount point in the subsequent steps, enter:

```
mkdir work
```

6 To mount the `initrd` file system to the `/work` directory, enter:

```
mount -o loop root work
```

7 To copy your files or updated driver to the mounted `root` file system, enter:

```
cp /your_path/module.ko work/lib/modules/2.6.5-override-default/initrd
```

where *your_path* is the path to the *module*.ko file and *module* is the name of the module.

Other files to be included in the `initrd` file system should be copied to the appropriate directory.

8 To unmount the `root` file system, enter:

```
umount work
```

9 To zip the new `rrot` file, enter:

```
gzip -v9c root > root.gz
```

10 To rename `root.gz` back to `root`, enter:

```
mv root.gz root
```

11 To copy the file back:

- For PXE, copy the updated `root` file to the `/tftp/boot` directory on the PXE server.
- For the CD, copy the updated `root` file to the `/boot/i386/` directory on the boot CD.

F.4.3 Using the Driverupdate File Method

Another way to customize the Novell imaging distribution is to utilize the driver update mechanism that is built into all SUSE distributions. This entails modifying a file named `driverupdate` that is located in the `/srv/tftp/boot` directory on your Imaging Server or on the root (/) of an imaging boot CD.

This method is a little less intrusive than modifying the `initrd` or `root` file systems. You simply create an additional file that is incorporated into the imaging operating system during boot time.

There are three types of driver update operations that can be performed:

- Install the kernel modules or hardware drivers
- Install files and execute a script
- Simply place files into the operating system

This section describes how to install files and execute a script. For information on the other two methods, see "Tech Talk #3 - Spittin' Image" (http://www.novell.com/connectionmagazine/2005/11/tech_talk_3.html) in the *Novell Connection Magazine*. Specifically, see the "SUSE Linux Driver Updates" and "Adding files to the distro "root" file" sections in the article.

The example in this section takes the program "tree" that is not currently available in the imaging distribution and installs it at boot time.

The driver update mechanism seeks the `driverupdate` file, which contains a directory structure that mimics the directory structure in the operating system after a device has booted with the ZENworks distribution. If it is present, linuxrc downloads it during booting and incorporates it into the operating system dynamically.

The `driverupdate` file is a file system file that can be of any file system type, such as EXT3 or REISER. For simplicity, we'll use the CRAMFS file system in our example.

To place the tree program into the `driverupdate` file:

1 Create a working directory on your Imaging Server, such as `/work`.

2 If you are using the `driverupdate` file, download the `driverupdate.tgz` file into the `/work` directory, then untar it by entering:

```
mkdir work
cd work
wget http://www.novell.com/connectionmagazine/2005/11/download/
driverupdate.tgz
tar -xzvf driverupdate.tgz
```

The `driverupdate.tgz` file contains the same directory structure as is created in Step 3.

3 If you are manually creating the directories, create the following structure under the `/work` directory:

```
`-- linux
    `-- suse
        |-- i386-sles10
            |-- dud.config
            |-- inst-sys
                `-- lib
                `-- bin
            |-- adddir.s
```

The contents of the `dud.config` file should contain lines similar to those listed below. You should maintain the keywords by supplying your own data. However, you can use the listed values:

```
UpdateName:     ZENworks 10 Patch 1
UpdateID:       a37f92556e4dd99e
UpdatePriority: 100
```

The `adddir.s` file should be an executable script that contains the following lines:

```
echo "Processing: adddir.s" > /dev/tty3 2>&1
# driver update: add files to inst-sys
for i in /update/[0-9]*/inst-sys ; do
    [ -d "$i" ] && adddir "$i" /
done
# driver update: run update.pre scripts
for i in /update/[0?9]*/install/update.pre ; do
    echo "Processing: $i" > /dev/tty3 2>&1
    [ -x "$i" ] && "$i"
done
```

4 To copy the tree program into the `/bin` directory, enter:

```
cp /usr/bin/tree dirstruct/linux/suse/i386-9.2/inst-sys/bin/
```

5 To create the CRAMFS file, enter:

```
mkfs.cramfs work/ driverupdate
```

The CRAMFS file is required by the SUSE distribution.

6 To copy the `driverupdate` file into `/srv/tftp/boot`, enter:

```
cp driverupdate /srv/tftp/boot
```

7 Add the following lines to the end of the `/srv/tftp/boot/settings.txt` file:

```
# SUSE driver update
for i in /update/[0?9]*/install/adddir.s ; do
    [ -x "$i" ] && "$i"
    rm $i
done
```

This causes the `adddir.s` script to run, which creates soft links to all of the new files being copied.

These lines might already be present in the `settings.txt` file.

8 Reboot the PXE-enabled device.

You should see the text "ZENworks 10 Patch 1" at the imaging maintenance mode prompt after the operating system has booted.

9 Execute the tree program.

All of the files you put into the `driverupdate` file are now located under the `/update` directory in the operating system after booting. Then, the `adddir.s` script (or the code that you added to the `settings.txt` file in Step 7) creates soft links under the `root` file system that point to the corresponding files under the `/update` directory structure. You can verify this by running:

```
/# which tree
/bin/tree
/# ll /bin/tree
lrwxrwxrwx  1 root root 29 Aug 31 21:45 /bin/tree -> /update/000/inst-sys/bin/
tree
```

If you want to simply include a new hardware driver or kernel module in the imaging operating system, an easier process might be to copy the `.ko` file into the `/dirstruct/linux/suse/i386-9.2/modules/` directory. Then, the imaging operating system automatically loads any `.ko` files that are in this directory.

F.5 Adding or Updating LAN Drivers

As LAN card manufacturers develop and release new LAN adapters, they usually release new or updated drivers as well. Sometimes the new LAN card functions properly with an earlier driver, and sometimes the earlier driver does not recognize the new LAN card and refuses to load. Occasionally, the older driver does load, but the LAN card exhibits serious performance problems. To obtain the full performance capabilities of a new LAN card, you should use the new driver.

The following sections explain how to obtain or compile drivers:

- Section F.5.1, "Obtaining Drivers," on page 656
- Section F.5.2, "Building Drivers," on page 656

If you need to load your drivers with specific parameters, see Section F.5.3, "Loading Drivers with Parameters," on page 658.

F.5.1 Obtaining Drivers

New LAN drivers should be obtained from the manufacturer. Most LAN card manufacturers have drivers available for free downloading from their Web site. Some drivers are available from www.scyld.com/network, and the source to the Broadcom BCM5700 driver can be downloaded from http://www.broadcom.com/drivers/downloaddrivers.php.

If a manufacturer has a binary driver compiled specifically for the kernel version used by ZENworks, you can obtain the driver and use one of the update methods to add the driver. If the driver is not for this specific version, you must obtain the source and compile it for this version. For more information, see Section F.5.2, "Building Drivers," on page 656.

F.5.2 Building Drivers

Nearly all Linux drivers are distributed in source code form and need to be compiled before they can be used. Follow the manufacturer's instructions included with the new driver to build the driver module. Many drivers can be built in such a way that they are built into the kernel itself; however, we recommend that LAN drivers be built as external kernel modules.

When building your LAN drivers, make sure that your build machine uses the same kernel as the imaging environment. If you have a LAN driver that doesn't load in your imaging environment, it usually means that you have a mismatch between your build environment and the imaging environment.

You can find the current kernel version of your Linux environment using the following command:

```
uname -r
```

However, you might need to modify the results from the `uname` command to get your kernel versions to match. For more information, see Section F.6, "Using Uname," on page 658.

To build your drivers:

- "Obtaining the Linux Source Code Tree" on page 657
- "Compiling the Module" on page 658

Obtaining the Linux Source Code Tree

To compile a module, you need the Linux source code tree that contains the configuration matching the ZENworks kernel. To obtain the necessary source code, do the following:

To use the Linux source code tree:

1 Obtain the current kernel version of the Imaging distro:

  1a Boot any device in the Management Zone into the ZENworks Imaging Maintenance mode.

  1b Run the `uname -r` command.

    This displays the kernel version of the Imaging distro.

2 From the Novell Downloads Web site (http://download.novell.com/patch/finder/?familyId=7261&productId=8162&yearValue=2009&keywords=kernel), download the kernel source RPM for the kernel version obtained in Step 1b.

  The kernel source RPM filename is in the following format:

  `kernel-source-kernel_version.i586.rpm`

  For example, `kernel-source-2.6.27.29-0.1.i586.rpm` is the souce code for the kernel version `2.6.27.29-0.1-default`.

3 Install the downloaded kernel source RPM.

  The RPM is installed to the `/usr/src` directory, and the following subdirectories are created:

  - `/usr/src/linux-Kernel_source_version`

  - `/usr/src/linux-Kernel_source_version-obj`

  For example, the following directories are created when you install `kernel-source-2.6.27.29-0.1.i586.rpm`:

  - `/usr/src/linux-2.6.27.29-0.1`

  - `/usr/src/linux-2.6.27.29-0.1-obj`

4 To create a link to the source tree:

  4a To change to the `/usr/src` directory, enter:

    `cd /usr/src`

  4b If there is a Linux soft link in the directory, delete it.

  4c Create the new Linux soft link, such as:

    `ln -s linux-2.6.27.29-0.1 linux`

You now have the Linux kernel source tree and soft link ready for compiling the module. Continue with "Compiling the Module" on page 658.

Compiling the Module

To manually compile the module:

1 Install the source.

Follow the manufacturer's instructions to install the source.

Normally, the module source is in a directory under `/usr/src`. Module source files usually come in the form of a gzipped tar file (`.tar.gz` or `.tgz`). The file might also be a bzipped file (`.bz2`).

2 To compile the source:

  2a Change directories to the source.

  2b If you modified `uname` to change to the proper kernel version, issue a `make` command.

3 When you have your module compiled for ZENworks, take the generated `.ko` module file (make sure you select the proper module name and not a work `.ko` file) and install it by using the driver update method or placing it in the `initrd` file system.

F.5.3 Loading Drivers with Parameters

If there is a module that you want to load during the linuxrc processing time, and if linuxrc does not recognize that it needs to be loaded or you want to specify the load parameters, you can enter a line in the `linuxrc.config` or `/info` file. This file then needs to be updated in the `initrd` file system.

You might need to load a LAN driver module with specific parameters. You can do this with a line like:

```
insmod="moduleName parm=xxx"
```

This type of line is most commonly used to load a LAN driver with specific parameters, such as full duplex or specific speed.

F.6 Using Uname

The `uname` command enables you to find the current kernel version of your Linux environment. However, you might need to modify the results from the `uname` command to get your kernel versions to match.

The following steps modify the `uname` command to provide the value you need:

1 To obtain your current kernel version, enter:

```
uname -r
```

Write down the version number so you can use it in Step 4. This example uses version 2.6.13-15-smp from a SLES 9 SP2 installation.

2 To create a new directory, enter:

```
mkdir /bin/orig
```

3 To move the `uname` binary to the `/bin/orig` directory that you just created, enter:

```
mv /bin/uname /bin/orig/uname
```

4 Use a Linux editor (such as vi) to create the `/bin/uname` file that contains the following lines:

```
#!/bin/sh
#uname
if [ $KRNLVERSION"a" = "a" ] ; then
  if [ $(/bin/orig/uname -r) = "2.6.13-15-smp" ] ; then
        export KRNLVERSION=2.6.13-15-smp
    else
        export KRNLVERSION=2.4.31
    fi
fi
if [ $1"a" = "-ra" ] ; then
    echo $KRNLVERSION
else
    /bin/orig/uname $*
fi
```

IMPORTANT: Replace the strings "2.6.13-15-smp" with the version you found in Step 1.

5 To make the new `uname` command script executable, enter:

```
chmod +x /bin/uname
```

6 Enter the following to cause the `uname -r` command to return a specific version, such as when compiling a module:

```
export KRNLVERSION="2.6.5-7.191"
```

7 Following the manufacturer's directions, compile the module using the appropriate `make` command.

8 Reset `uname` so that it returns actual values:

```
unset KRNLVERSION
```

F.7 Variables and Parameters

The following sections describe the variables and parameters used in updating resource files:

- Section F.7.1, "Imaging Script Variables," on page 659
- Section F.7.2, "Linuxrc Parameters Specified in Settings.txt," on page 660
- Section F.7.3, "Image Engine Variables," on page 660

F.7.1 Imaging Script Variables

The following environment variables are used in imaging scripts and must not be modified:

Table F-1 *Imaging Script Variables*

Variable	Definition
ACTIVEPARTITION	Device of the active OS partition.
CDBOOT	YES = Booted from a CD.
DISABLEZEN	1 = Disable the ZENworks partition.
ENABLEZEN	1 = Re-enable the ZENworks partition.
ZENDEVICE	Device name of the ZENworks partition.

Variable	Definition
ZENPARTBOOT	YES = Booted from ZENworks partition.

The following environment variables can be modified or set in the `settings.txt` file:

Table F-2 *Environment Variables*

Variable	Definition
HDPARM	NO = Do not set hdparm parameters.
IMGCMD	Imaging command to run instead of the `img a` command.
MANUALREBOOT	YES = Do not automatically reboot.
PARTITIONSIZE	Size in MB to create the ZENworks partition.
PROXYADDR	IP/DNS address of the Imaging server.
PROMPT	Go to the bash prompt after imaging is complete.

F.7.2 Linuxrc Parameters Specified in Settings.txt

Table F-3 *Linuxrc Parameters*

Variable	Definition
netsetup	dhcp = Use DHCP.
	1 = Static IP.
HostIP	Static IP address to use.
NetMask	Network mask.
Gateway	Network gateway.
HostName	Host name to assign.
Nameserver	DNS name server.
Domain	Domain suffix.
NetDevice	ethx = Define which network device to configure.

F.7.3 Image Engine Variables

Table F-4 *Image Engine Variables*

Variable	Definition
DEVELOPER_LOG	"A" creates a verbose `imglog` debug file.
ZENIMGLOG	"A" creates a less verbose `imglog` debug file.

Variable	Definition
ZEN_IGNORE_GEO_MISMATCH	Ignore geometry device mismatches when restoring raw image formats.
NOABORTBUTTON	If defined, do not display the Abort button during imaging.

F.8 Troubleshooting Linux Driver Problems

- Section F.8.1, "Troubleshooting During the Boot Process," on page 661
- Section F.8.2, "Troubleshooting at the Bash Prompt," on page 661

F.8.1 Troubleshooting During the Boot Process

While booting ZENworks imaging, there are several things that you can do to help troubleshoot if there is a problem:

- Press Esc to see the kernel messages. Usually, messages are shown for failures.
- Screen 3 (press Alt+F3) is used to show the progress of the linuxrc process. It lists progress results, what linuxrc is doing, which modules are loaded, and so on.
- Screen 4 (press Alt+F4) is used to show output from the modules during the linuxrc process.
- Screens 1 (press Alt+F1), 3, and 4 can be used to help determine which part of the process is failing or causing a problem.
- Screens 3 and 4 indicate which drivers are loaded.
- If a drive is loaded properly but fails in some way, view screen 4 to see if there is an outdated driver.

If the boot process fails, the first command line parameter to use is acpi=off.

F.8.2 Troubleshooting at the Bash Prompt

When the bash prompt is displayed, there are a few tools that you can use to gather information about the hardware:

- **hwinfo:** This utility is used by linuxrc to load hardware. You can use `hwinfo -pci` to determine exactly what hardware was recognized.

  Pipe to "less," because `hwinfo` can create a lot of output. For example, `hwinfo -pci | less`.

  If you need to contact Novell Support for help, you should capture the output from `hwinfo -pci` to a file for their use. You can gather the most information with this command:

  `hwinfo -pci -log /logfilename`

  where `logfilename` is the name of the file that you should send.

  You can then mount a device, such as a Thumb drive or other USB device, and save the output file for later use. You might also be able to use FTP to save the file where it can be available.

- **ethtool:** This is a valuable tool (contained in a ZENworks distribution) that can be used to change the configuration on most Ethernet network devices.

Upgrading the Dell DTK

G

Novell® ZENworks® 7 Linux Management ships with the latest available version of the Dell OpenManage Deployment Toolkit (DTK). The DTK is integrated with ZENworks. However, when new versions of the DTK become available, you can upgrade to a newer version.

To obtain the current Dell DTK build from Dell:

1 Make sure the novell-proxydhcp daemon is running on a server in your network.

This service must be available so that the device's PXE can access files from the ZENworks server, such as the Preboot Services Menu file and the Dell DTK (Maintenance Mode) files.

2 Boot a Dell device that is PXE-enabled and press the Ctrl-Alt keys during booting.

This boots the device into the Preboot Services Menu. These keys must be pressed by the time a string starting with "Novell ..." is displayed during the boot process.

3 Select the Dell DTK (Maintenance Mode) option.

4 When the bash (#) prompt is displayed, view the content of the /BUILD file.

This shows the version of the Dell DTK currently used by ZENworks.

5 Make a note of the build version of your current DTK.

6 Obtain the latest Linux-based Dell DTK from www.dell.com.

This is normally available as an ISO file.

7 Create a CD using the downloaded ISO file.

8 Insert the newly created CD into the drive of any Linux workstation or server.

9 To update the Linux resource files:

   9a Using a file manager or a terminal on the server or workstation, copy the SA.1 and SA.2 files from the /isolinux directory on the CD to the /srv/tftp/dell-dtk directory on your ZENworks server.

   This replaces files of the same name.

   You might need drives mapped to your servers from the device where you inserted the CD. Otherwise, you need to place the CD into the drive of each device in order to copy the files locally to replace them.

   9b Repeat for each ZENworks server to replace these files on them.

10 If necessary, to modify the configuration files:

   10a Mount the Dell DTK CD's ISO file, then open /isolinux/isolinux.cfg using any editor, text-viewing command, or utility.

   10b Look for the ramdisk_size parameter and note its assigned value.

   This parameter occurs many times in the file, but each instance is generally set to the same value. If different values are assigned in different instances of the parameter, use the value displayed in the default configuration section. For example, the file might contain

default 1 on a line, indicating the default section's name is "1," which is displayed immediately after "label" on a line, such as label 1 under which the ramdisk_size parameter is listed.

10c On the ZENworks server, open the /srv/tftp/dell-dtk.cfg and /srv/tftp/dell-dtk_maint.cfg files and modify all ramdisk_size parameter values to be the same as what you obtained in step Step 10b.

11 To ensure that the Dell DTK has been properly updated on the ZENworks server, reboot the device into PXE and select the Dell DTK (Maintenance Mode) option.

12 To verify that the build number has increased from the number you noted in Step 5, when the bash (#) prompt is displayed, view the content of the /BUILD file:

If the build number has not incremented, either it really isn't an update, or the copy operations failed.

Supported Ethernet Cards

H

Novell® ZENworks® Linux Management provides the Ethernet card drivers contained in the Linux kernel (2.6) that ships with ZENworks 7.

To determine which Linux kernel you are using, enter `uname -r` at the bash prompt.

If your device or laptop computer uses a different card that is not supported, you must supply your own Ethernet driver.

Using a Specific Network Card for Devices Running Dual NICs

You can chose to use a specific network card for a device running dual NICs by using one of the following ways:

 ◆ Modify the `/srv/tftp/z_auto.cfg` or the `/srv/tftp/z_maint.cfg` file (or both) by adding the following line at the end of the *Append* command:

    netdevice=eth0

◆ In ZENworks Control Center, add `netdevice=eth0` as an additional kernel parameter while creating the AutoYaST bundle. For more information on how to create and configure the AutoYaST bundle, see Section 30.3.1, "Configuring an AutoYaST Bundle," on page 440.

Bundles > Create New Bundle

Create New Bundle	AutoYaST 1	?

🔧 **Step 4: Set AutoInstall Attributes**

Describe how to access the Linux boot files. These files should have been copied to the Preboot TFTP server from the CD.

Linux Kernel File:

(Path should be relative to the default directory of the TFTP daemon. e.g.: suse/pro9.1/linux)

Initial RAM Drive:

(Path should be relative to the default directory of the TFTP daemon. e.g.: suse/pro9.1/initrd)

Additional Kernel Parameters:

Protocol and IP address (or DNS name) required to access the network install directory:

NFS

Path to network install directory (relative to protocol):

(Path should be relative to the default directory of the selected protocol daemon. e.g.: suse/pro9.1)

Protocol and IP address (or DNS name) required to access the script:

NFS

AutoYaST Script name and path (Relative to protocol default directory):

(e.g.: /installs/suse9.3/autoyast.xml)

☐ Use IP Address from the preboot bundle rather than from Image Safe Data
☐ Use Identity Information from the preboot bundle rather than from Image Safe Data

[<< Back] [Next >>] [Cancel]

This eliminates the need to select a NIC's IP address manually.

Establishing SSH Tunneling

J

If you are using Remote Management over a network that is not secure, the data between the Remote Management Viewer running on the management console and the Remote Management Agent on the managed device is unencrypted and could be viewed by someone with access to the intervening network. You should tunnel your Remote Management sessions through a secure channel such as SSH.

J.1 SSH Tunneling between a Linux Management Console and a Linux Managed Device

If you are using Linux, SSH clients and servers are freely available on the internet. The SSH client and server RPMs can be downloaded from the OpenSSH site. (http://www.openssh.com).

J.1.1 Basic Use

SSH provides you with a "Secure SHell" to the remote device. All traffic is encrypted between the two devices using public key encryption techniques, making it very difficult for anyone else to spy on it. When SSH is installed, you could connect to a managed device from elsewhere simply by running the SSH client. For example, if you want to connect to a managed device called "work." you use the following command:

```
ssh work
```

You are then prompted for the password of your account on the managed device and you are logged in, just like a telnet session, but safer. You can also request that it listens on a particular port on your local management console and forwards that down the secure connection to a port on a managed device at the other end. To do this, use the following command:

```
ssh -L x:work:y work
```

This starts an SSH connection to a device named "work" and also listen on port x on the local management console, and forwards any connections there to port y on "work."

Remote Management uses two ports on the managed device. By default, the Remote Control service listens on port 5950 and the Remote Login service listens on port 5951. If you want to enable SSH tunneling for Remote Control, you need to forward Remote Management data from a port on your local management console to 5950 of managed device.

Similarly, you should forward data to 5951 if you want to tunnel Remote Login:

- If you are running Remote Control service on "work" on 5950 and you want a secure connection to it from your local management console, you can start the SSH session using:

```
ssh -L 5952:work:5950 work
```

◆ Any connections to port 5952 on your local management console would actually connect to 5950 on "work," so instead of running a vnc viewer as:

```
vncviewer work:50
```

run it as follows:

```
vncviewer localhost :52
```

Figure J-1   *Linux Console to Linux Managed Device with Tunneling*
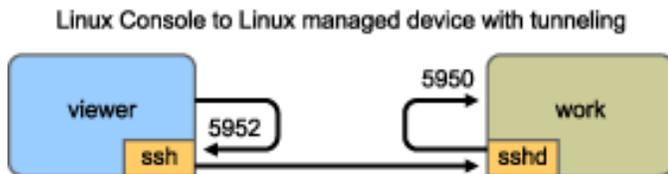
NOTE: If you are using the Linux VNC viewer to connect via SSH, when the viewer connects to a server on the local management console, by default it uses VNC's pixel encoding because this generally gives better performance for local access. If this server is actually an SSHD redirecting the data for another workstation, you can override this using the -tight option to the viewer or you can send a lot more data over the network.

J.2 SSH Tunneling between a Windows Management Console and a Linux Managed Device

SSH clients are also available for Windows, Macintosh, and other platforms, but if you want servers on these platforms you might need to use a commercial version or route your connection via a Linux device.

There are several scenarios for using SSH tunneling between a Windows management console and a Linux managed device. For the sake of simplicity, the following procedure uses a scenario in which you are using a Windows laptop "viewer" in a non-secure Wide Area Network to remotely control your Linux managed device "work" installed inside your secure Local Area Network. Another Linux device called "gateway" is in your secure local area network and runs the SSH daemon. The following steps explain how you can use the PuTTY SSH client to configure an SSH tunnel so that the Remote Management data is encrypted when it travels between "viewer" and "gateway" and is then forwarded to "work" inside the secure network.

NOTE: The PuTTY SSH client is available at the PuTTY site (http://www.chiark.greenend.org.uk/~sgtatham/putty). If you are using other SSH client software, use the appropriate commands for that software.

1 Enter the following command in the shell prompt:

```
putty -L 5952:work:5950 gateway
```

The first argument is the local forwarding option, which says that the local fake port 5952 should be created and connected to the genuine port work:5950. The second argument is the main non-option parameter to SSH, which tells it to connect to the device that runs the SSH daemon.

2 In the PuTTY Security Alert dialog box, verify that the key matches with that of the "gateway" device, then click *Yes*.

3 To establish the SSH tunnel between "viewer" and "gateway," you need to require authentication to "gateway." Specify a valid username and password of the "gateway" device in the PuTTY dialog box, then click *Yes*.

4 Any connections to port 5952 on your local management console would actually connect to 5950 on "work," so instead of running a vnc viewer as

```
vncviewer work:50
```

run it as follows

```
vncviewer localhost :52
```


Windows Console to Linux managed device with tunneling

NOTE: If you are using the Linux VNC viewer to connect via SSH, when the viewer connects to a server on the local management console, by default it uses VNC's pixel encoding because this generally gives better performance for local access. If this server is actually an SSHD redirecting the data for another workstation, you can override this using the -tight option to the viewer or you can send more data over the network.

J.3 Compression

SSH can also compress the data. This is particularly useful if the link between your management console and the managed device is a slow one, such as a modem, but even on a faster network it can be helpful, because encryption takes a certain amount of time and can slow the link down a little. To add simple compression, use the -C option. For more control, set it up in your SSH configuration files. To see how much your data is being compressed, use the -v option.

License Agreement for libacl and libgconf

K

The following is the license agreement for the libacl and libgconf library that is used in the ZENworks® 7 Linux Management Policy Handler/Enforcer software:

K.1 Library GNU Public License

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you."

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification.")

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

◆ You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

◆ You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   ◆ The modified work must itself be a software library.

   ◆ You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

- You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

- If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

  (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

  These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

  Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

  In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

- You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

  Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

  This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

- You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

  If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

- A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library." Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library." The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

- As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library," as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

- For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

- It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

- You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

  - Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

  - Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

- You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

- You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

- Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

- If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

  If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

◆ If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

◆ The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version," you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

◆ If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

◆ NO WARRANTY

◆ BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

◆ IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Documentation Updates

L

This section contains information on documentation content changes that were made in this *Administration Guide* after the initial release of Novell® ZENworks® 7.3 Linux Management. The information can help you to keep current on updates to the documentation.

All changes that are noted in this section are also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes are published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the guide.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains its publish date on the front title page.

The documentation was updated on the following dates:

L.1 February 12, 2010 (Interim Release 2)

Updates were made to the following sections. The changes are explained below.

L.1.1 Package and Content Management

The following changes were made in this section:

Location	Change
Section 25.6, "Mirroring Bundles Between ZENworks Linux Management Servers Located in Different Management Zones," on page 312	Updated the Note in this section with information on mriroring YaST patches on SLES 9 platform from the YOU repository and OES 1 platforms from the RCE repository
Section 25.8, "Mirroring Dell Updates from the OpenManage Server Administrator Repository by Using a YUM Subscription," on page 316	Added this section for this release.

L.1.2 Appendix

The following changes were made in this section:

Loation	Change
"Obtaining the Linux Source Code Tree" on page 657	Updated this section.

L.1.3 ZENworks System Management

The following changes were made in this section:

Location	Change
Section 9.1.1, "Backing Up the ZENworks Object Store," on page 85	Updated this section.
Section 9.1.2, "Restoring the ZENworks Object Store," on page 86	Updated this section.

L.2 December 24, 2009

Updates were made to the following sections. The changes are explained below.

- Section L.2.1, "ZENworks System Management," on page 680
- Section L.2.2, "Package and Content Management," on page 680
- Section L.2.3, "Appendix," on page 681

L.2.1 ZENworks System Management

The following changes were made in this section:

Location	Change
Section 9.2.3, "Backing Up the ZENworks Data Store," on page 88	Updated this section to provide information about the hostname in the `.pgpass` file.

L.2.2 Package and Content Management

The following changes were made in this section:

Location	Change
Chapter 25, "Mirroring Software," on page 293	Added the following important note in this chapter: - Mirroring YaST online updates for a SLES 9 platform with ia64, ppc, or s390 architectures is not supported in ZENworks 7.2 Linux Management or later.

L.2.3 Appendix

The following changes were made in this section:

Loation	Change
rug (1) (page 586)	Added the list of options in the service-add (sa) [options] [uri] command.

L.3 November 4, 2009

Updates were made to the following sections. The changes are explained below.

- Section L.3.1, "ZENworks System Management," on page 681

L.3.1 ZENworks System Management

The following changes were made in this section:

Location	Change
Section 9.1.3, "Deleting the Dangling Objects from ZENworks Object Store," on page 87	Changed the `<TreeName></TreeName>` tag to `<ZoneName></ZoneName>` in the XML file content in Step 2.

L.4 October 12, 2009 (Interim Release 1)

Updates were made to the following sections. The changes are explained below.

- Section L.4.1, "ZENworks System Management," on page 681
- Section L.4.2, "Policy Management," on page 682
- Section L.4.3, "Package and Content Management," on page 682
- Section L.4.4, "Event Monitoring," on page 682

L.4.1 ZENworks System Management

The following changes were made in this section:

Location	Change
Section 5.3.2, "Uninstalling a Secondary ZENworks Server By Using zlm-config," on page 51	Updated this section.
Section 9.3.8, "User-managed Backup and Recovery," on page 97	Added this section.
Section 7.4, "Configuring Local Device Logging," on page 73	Updated the following options in this section: ◆ *Log message to a local file if severity is* ◆ *Number of backup files per day*

L.4.2 Policy Management

The following changes were made in this section:

Loation	Change
Section 14.2, "Creating Policies," on page 125	Updated this section for the following policies: ◆ Firefox Policy ◆ Novell Linux Desktop Policy

L.4.3 Package and Content Management

The following changes were made in this section:

Location	Change
Section 25.7, "Mirroring Red Hat Updates from the NU Repository by Using a YUM Subscription," on page 314	Added this section.

L.4.4 Event Monitoring

The following changes were made in this section:

Location	Change
Section 40.2.1, "Configuring Local Log Settings," on page 528	Updated this section for the *Number of backup files per day* field.

L.5 May 26, 2009 (Hot Patch 1)

Updates were made to the following sections. The changes are explained below.

- Section L.5.1, "ZENworks System Management," on page 682
- Section L.5.2, "Policy Management," on page 683
- Section L.5.3, "Package and Content Management," on page 683
- Section L.5.4, "Appendix," on page 683

L.5.1 ZENworks System Management

The following changes were made in this section:

Loation	Change
Section 3.3, "Accessing the ZENworks Control Center through Novell iManager," on page 42	Updated this section.

Loation	Change
Section 9.1.3, "Deleting the Dangling Objects from ZENworks Object Store," on page 87	Added the following note:
	NOTE: If you have installed ZENworks 7.3 Linux Management HP1, you must replace the `<TreeName></TreeName>` tag with `<ZoneName></ZoneName>`.
Section 9.2.4, "Restoring the ZENworks Data Store," on page 89	Updated this section.

L.5.2 Policy Management

The following changes were made in this section:

Loation	Change
Section 16.3, "Firefox Policy," on page 145	Updated this section.

L.5.3 Package and Content Management

The following changes were made in this section:

Loation	Change
Section 25.3.1, "Creating the Configuration Files by using the Command Line Utility," on page 295	Updated this section.

L.5.4 Appendix

The following changes were made in this section:

Loation	Change
zlman (1) (page 562)	Changed the title from ~/.ZLMANRC to RC File.
zlmmirror (1) (page 554)	Updated this section.