System Administration Reference

Novell®
ZENworks® 10 Asset Management SP2

10.2

August 17, 2009

www.novell.com

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

About This Guide

This *System Administration Reference* provides information about general administrative tasks required to manage your Novell® ZENworks® 10 Asset Management SP2 (10.2) system. The information in this guide is organized as follows:

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

Additional Documentation

ZENworks 10 Asset Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 10 Assset Management documentation (http://www.novell.com/documentation/beta/zam10/index.html).

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*, should use forward slashes as required by your software.

ZENworks Control Center

This section contains information about using ZENworks® Control Center (ZCC) to configure system settings and perform management tasks in your Management Zone.

ZENworks Control Center

1

You use ZENworks® Control Center to configure system settings and perform management tasks in your Management Zone.

ZENworks Control Center is installed on all ZENworks Servers in the Management Zone. You can perform all management tasks on any ZENworks Server.

1.1 Accessing ZENworks Control Center

1 Using a Web browser that meets the requirements listed in "Administration Browser Requirements" in the *ZENworks 10 Asset Management Installation Guide,* enter the following URL:

```
https://ZENworks_Server_Address:port
```

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server. You only need to specify the *port* if you are not using one of the default ports (80 or 443). ZENworks Control Center requires an HTTPS connection; HTTP requests are redirected to HTTPS.

The login dialog box is displayed.

2 In the *Username* field, type `Administrator` (the default) or an administrator name that you previously created in ZENworks Control Center.

3 In the *Password* field, do one of the following:

- ◆ If you are logging in through the default Administrator account, specify the Administrator password that you created during installation.

- ◆ Specify the password for the administrator name that you created in ZENworks Control Center.

To prevent unauthorized users from gaining access to ZENworks Control Center, the administrator account is disabled after three unsuccessful login attempts, and a 60-second timeout is enforced before you can attempt another login. To change these default values, see Section 1.4, "Changing the Default Login Disable Values," on page 19.

4 Click *Login* to display ZENworks Control Center.

To log in again as a different administrator, click the *Logout* option in the upper right corner of the ZENworks Control Center window, then when the login dialog box is displayed, log in as a different administrator.

The *Logout* option includes the name of the administrator who is logged in as part of the option. For example, *Logout John*.

1.2 Accessing ZENworks Control Center through Novell iManager

ZENworks 10 Asset Management includes a Novell® plug-in module (`.npm`) that you can use to access ZENworks Control Center from Novell iManager, which is a management console used by many Novell products.

The ZENworks Control Center plug-in supports iManager 2.7 only. It does not support iManager 2.6 or 2.5; it will install to these versions but does not work.

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

1 On the server where iManager is located (or on a device that has access to the iManager server), open a Web browser to the ZENworks download page:

https://*server*/zenworks-setup

where *server* is the DNS name or IP address of a ZENworks Server.

2 In the left navigation pane, click *Administrative Tools*.

3 Click *zcc.npm* and save the file to a location on the iManager server.

4 Follow the instructions in the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_27/data/b8qrsg0.html) to install and configure the plug-in module.

5 Log into iManager.

6 Click the ZENworks icon at the top of the page.

7 Enter the ZENworks Control Center URL:

```
https://ZENworks_Server_Address:port
```

Replace *ZENworks_Server_Address* with the IP address or DNS name of the ZENworks Server. You only need to specify the *port* if the ZENworks server is not using the default port (80 or 443).

8 Click the ZENworks icon to launch ZENworks Control Center.

1.3 Navigating ZENworks Control Center

The following Servers page represents a standard view in ZENworks Control Center:

Figure 1-1 *ZENworks Control Center*
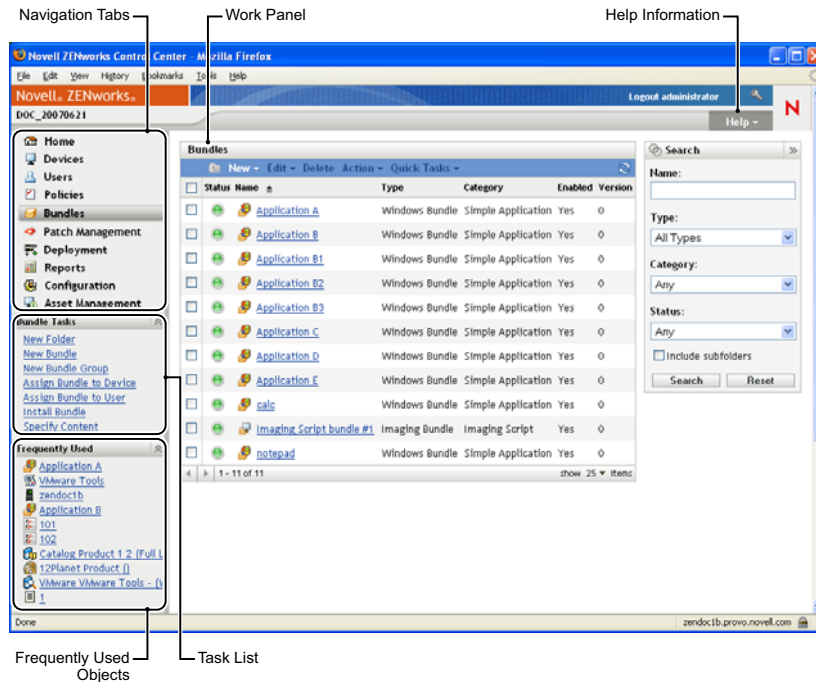
Navigation Tabs: The tabs in the left pane let you navigate among the functional areas of ZENworks. For example, the Servers page shown above lets you manage tasks associated with servers.

Task List: The task list in the left pane provides quick access to the most commonly performed tasks for the current page. The task list changes for each page.

Frequently Used Objects: The Frequently Used list in the left pane displays the 10 objects that you have accessed most often, from most used to least used. Clicking an object takes you directly to the details page for the object.

Work Panel: The work panels are where you monitor and manage your ZENworks system. The panels change depending on the current page. In the above example, there are two work panels: Devices and Search. The Devices panel lists the servers, folders, server groups, and dynamic server groups that have been created; you use this panel to manage the servers. The Search panel lets you filter the Devices panel based on criteria such as a device's name, operating system, or status.

Help Information: The *Help* button links to Help topics that provide information about the current page. The *Help* button links change depending on the current page.

1.4 Changing the Default Login Disable Values

By default, an administrator's account is disabled for 60 seconds after he or she unsuccessfully attempts to log in three times. You can change the number of login tries and the timeout length by editing a configuration file. The changes are only applied to the instance of ZENworks Control

Center being run from the server where you open and modify the configuration file. To make the change applicable to all ZENworks Primary Servers, you must make the same change in each server's copy of this file.

IMPORTANT: Login attempts per administrator account are maintained in the ZENworks database, and there is only one ZENworks database per Management Zone. Therefore, if a particular administrator unsuccessfully attempts to log in to one Primary Server, that administrator is locked out of all Primary Servers in the zone. The lockout period is determined by the configuration on the server where the login attempts failed.

To modify the login tries and timeout values:

1 In a text editor, open the following file:

Windows: *installation_location*\novell\zenworks\conf\datamodel\zdm.xml

Linux: /etc/opt/novell/zenworks/datamodel/zdm.xml

2 Add the following lines to the file:

```
<entry key="allowedLoginAttempts">5</entry>
<entry key="lockedOutTime">300</entry>
```

The 5 in this example represents the number of retries before disabling login, and 300 represents the number of seconds (the default is 60 seconds, or 1 minute).

Keep in mind that the longer the delay before allowing a re-login after the configured number of failures (such as 5), the longer your authorized administrators must wait to access ZENworks Control Center.

IMPORTANT: If you enter 0 as the login attempts value, the lockout functionality is disabled, allowing unlimited attempts at logging in.

---

3 Save the file, then restart the zenloader and zenserver services on the Primary Server to make the changes effective.

For instructions on restarting the services, see Section 5.2.4, "Restarting a ZENworks Service," on page 66.

1.5 Changing the Timeout Value for ZENworks Control Center

By default, ZENworks Control Center has a 30-minute timeout value, so if you leave ZENworks Control Center idle on your computer for more than 30 minutes, you are prompted to log in again to continue.

The purpose of the timeout is to clear memory resources. The larger the timeout value, the longer ZENworks Control Center retains the memory resources, which might have a negative impact on the long-term performance of the device from which you have launched ZENworks Control Center, including the ZENworks Server if you have it running locally on it.

To increase or decrease the timeout value, you modify two XML files on the ZENworks Server. The change applies only to that server's ZENworks Control Center. Therefore, any devices that launch ZENworks Control Center from that server experience the same timeout value.

You can make the ZENworks Control Center timeout value different on each ZENworks Server in the Management Zone.

To change the ZENworks Control Center timeout value on a ZENworks Server:

1 On the ZENworks Server, open the `config.xml` file in a text editor.

- ◆ **Windows:** `\Novell\ZENworks\share\tomcat\webapps\zenworks\WEB-INF\config.xml`

- ◆ **Linux:** `/opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/config.xml`

2 Locate the `<setting id="timeout">` entry.

3 Increase or decrease the timeout value, as needed.

Specify the timeout value in minutes.

4 Save the `config.xml` file.

5 Open the `custom-config.xml` file in a text editor.

This file allows you to maintain customizations of ZENworks Control Center because information contained in this file overrides any corresponding information in the `config.xml` file. Therefore, changes made in this file are not lost when the `config.xml` file is overwritten during software updates or upgrades.

The `custom-config.xml` file is located in the same directory as the `config.xml` file:

- ◆ **Windows:** `\Novell\ZENworks\share\tomcat\webapps\zenworks\WEB-INF\custom-config.xml`

- ◆ **Linux:** `/opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/custom-config.xml`

6 Locate the `<setting id="timeout">` entry.

7 Set the timeout value to the same number as you entered in the `config.xml` file.

8 Remove the comments surrounding the `<setting id="timeout">` entry (`<!--` and `-->`).

9 Save the `custom-config.xml` file.

10 Restart the ZENworks Server by restarting the zen-server service.

For instructions, see .

1.6 Using the Config.xml File to Modify ZENworks Control Center Settings

In addition to enabling you to configure the timeout value for the ZENworks Control Center (see), the `config.xml` file lets you control several additional configuration settings. However, with the exception of the timeout value, you should not need to modify the `config.xml` settings.

1 On the ZENworks Server, open the `config.xml` file in a text editor.

- ◆ **Windows server path:** `\Novell\ZENworks\share\tomcat\webapps\zenworks\WEB-INF\config.xml`

- ◆ **Linux server path:** `opt/novell/zenworks/share/tomcat/webapps/zenworks/WEB-INF/config.xml`

2 Modify the desired setting. All settings begin with `<setting id=`.

timeout: Specify the timeout value in minutes. The larger the timeout value, the longer ZENworks Control Center retains the memory resources, which might have a negative impact on the long-term performance of the device where you have launched ZENworks Control Center. If you change this value, you must also change the timeout entry in the `custom-config.xml` file. See Section 1.5, "Changing the Timeout Value for ZENworks Control Center," on page 20).

debug.enabled: Change the value to *false* if you do not want any messages written to the ZENworks Control Center log files. The default value, *true*, causes messages to be written to the log files.

debug.tags: These settings control debug information. You should not change them unless instructed by Novell Support.

debug.log.viewstate: This setting controls debug information. You should not change it unless instructed by Novell Support.

hideGettingStarted: Suppresses the Getting Started page. This setting is not functional at this time. To manually suppress the page, open the ZENworks Control Center, display the Getting Started page, then select *Do not show me this again*.

noQuickTaskAutoRefresh: This setting disables automatic refreshing of the QuickTask status dialog box. It is used to discover issues with QuickTask status updates. You should not change this setting unless instructed by Novell Support.

3 Save the `config.xml` file.

4 Restart the ZENworks Server by restarting the zen-server service. See Chapter 5, "ZENworks Server," on page 63 for instructions.

1.7 Bookmarking ZENworks Control Center Locations

The Bookmark feature allows you to use your Web browser to manage direct access to the various locations in ZENworks Control Center, instead of performing the usual navigation clicks. You can also use this feature to bookmark hard-to-find locations.

You can create bookmarks for your Web browser to locations within the following sections of ZENworks Control Center:

 ◆ *Managed* tab on the *Devices* tab
 ◆ *Management Zone Settings* on the *Configuration* tab

The locations you can bookmark include such items as lists, details of objects, and configuration settings.

Wherever the Link icon (⬚⬚ ▾) is displayed, you can create a bookmark. The icon is located in the upper right of the page. If it is not displayed, a bookmark cannot be created for that location.

If you are logged in to ZENworks Control Center when you click a bookmark, the location is immediately displayed.

If you are not logged in to ZCC when you click a bookmark, the Login dialog box is displayed. After you enter valid credentials, the location is immediately displayed.

To create bookmarks:

1 In ZENworks Control Center, navigate to a location where you want to create a bookmark.

2 Click 🔗 ▾.

This opens the following dialog box, where the URL to the current location is already selected:
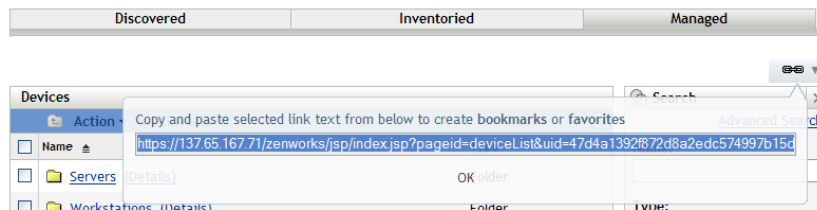
3 Press Ctrl+C to copy the URL, then click *OK* to close the dialog box.

4 Paste the URL as a new bookmark in your Web browser.

Administrators

2

During installation, a default ZENworks® administrator account (named Administrator) is created. This account, called a Super Administrator account, provides full administrative rights to the Management Zone.

Typically, you should create administrator accounts for each person who will perform administrative tasks. You can define these accounts as Super Administrator accounts, or you can define them as administrator accounts with restricted rights. For example, you could give a user an administrator account that only enables him or her to discover and register devices in the Management Zone. limit the user to performing asset management tasks such as contract, license, and document management.

IMPORTANT: In addition to the default Administrator account, you should make sure that you have at least one other Super Administrator account. This provides redundancy in case the password for the Administrator account is forgotten or lost. For information on how to create a Super Administrator account, see Section 2.2.1, "Assigning Super Administrator Rights," on page 28. If you need any further help, contact Novell® Support (http://www.novell.com/support).

In some cases, you might have multiple administrator accounts that require the same administrative rights. Rather than assign rights to each account individually, you can create an administrator role, assign the administrative rights to the role, and then add the accounts to the role. For example, you might have a Help Desk role that provides administrative rights required by several of your administrators.

You can use ZENworks Control Center (ZCC) or the zman command line utility to create and modify administrator accounts and assign roles. The following procedures explain how to perform these tasks by using ZCC. If you prefer the zman command line utility, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

- Section 2.1, "Managing Administrator Accounts," on page 25
- Section 2.2, "Managing Administrator Rights," on page 28
- Section 2.3, "Rights Descriptions," on page 29
- Section 2.4, "Managing Administrator Roles," on page 37

2.1 Managing Administrator Accounts

The following sections help you create and manage administrator accounts:

- Section 2.1.1, "Creating Administrators," on page 26
- Section 2.1.2, "Deleting Administrators," on page 27
- Section 2.1.3, "Renaming Administrators," on page 27
- Section 2.1.4, "Changing Administrator Passwords," on page 27

2.1.1 Creating Administrators

To create an administrator account:

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

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

The Add New Administrator dialog box lets you create a new administrator account by providing a name and password, or you can create a new administrator based on an existing user in the user source. Optionally, you can give the new administrator the same rights that the logged-in administrator has.

3 Fill in the fields:

Create a New Administrator by Providing Name, Password: Select this option if you want to create a new administrator account by manually specifying the name and password.

Administrator login names with Unicode* characters are case-sensitive. Make sure that you use the correct case for each character in the login name when it contains Unicode characters.

The new 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 ZENworks Control Center.

Based on User(s) in a User Source: Select this option if you want to create a new administrator account based on information from your user source. To do so, click *Add*, then browse for and select the user you want.

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.

Give this Administrator the Same Rights as I Have: Select this option if you want to assign the new administrator the same rights that you have as the currently-logged in administrator.

4 When you have finished filling in the fields, click *OK* to add the new administrator.

You can also use the `admin-create` command in zman to create an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2.1.2 Deleting Administrators

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

2 In the Administrators panel, select the check box next to the administrator's name, then click *Delete*.

You can also use the `admin-delete` command in zman to delete an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2.1.3 Renaming Administrators

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

2 In the Administrators panel, select the check box next to the administrator's name, click *Edit*, then click *Rename*.

3 Specify the new name, then click *OK*.

You can also use the `admin-rename` command in zman to rename an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2.1.4 Changing Administrator Passwords

To change the password for any administrator account other than the default Administrator account:

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

2 In the Administrators panel, select the check box next to the administrator, click *Edit*, then click *Set Password* to display the Change Administrator Password Dialog box.

3 Fill in the fields, then click *OK*.

To change the password for the currently logged-in administrator:

1 In ZENworks Control Center, click the 🔍 icon located next to the *Logout Administrator* option in the top right corner.

The Change Administrator Password dialog box is displayed.

2 Fill in the fields, then click *OK*.

To change the password for the default Administrator account:

1 Log in using the Administrator account.

2 Click the 🔍 icon located next to the *Logout Administrator* option in the top right corner.

The Change Administrator Password dialog box is displayed.

3 Fill in the fields, then click *OK*.

2.2 Managing Administrator Rights

The following sections help you manage existing administrator accounts and their assigned rights:

- Section 2.2.1, "Assigning Super Administrator Rights," on page 28
- Section 2.2.2, "Assigning Additional Rights," on page 28
- Section 2.2.3, "Modifying Assigned Rights," on page 29
- Section 2.2.4, "Removing Assigned Rights," on page 29

2.2.1 Assigning Super Administrator Rights

A Super Administrator has all rights to perform all actions in ZENworks Control Center. For more information about all of the rights that a Super Administrator has, see Section 2.3, "Rights Descriptions," on page 29. If you grant an administrator Super Administrator rights, any assigned rights that have been allowed, denied, or not set are overridden.

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

2 In the Administrators panel, click the administrator's name.

3 Select the *Super Administrator* check box.

4 Click *Apply*.

2.2.2 Assigning Additional Rights

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

2 Click the administrator in the *Name* column of the Administrators panel.

3 In the Assigned Roles panel, click *Add*, then select the rights you want to assign.

4 Fill in the fields.

For more information, see Section 2.3, "Rights Descriptions," on page 29.

5 Click *OK*.

You can also use the `admin-rights-set` command in zman to assign additional rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2.2.3 Modifying Assigned Rights

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

2 Click the administrator in the *Name* column of the Administrators panel.

3 In the Assigned Rights panel, select the check box next to the assigned right.

4 Click *Edit*, then modify the settings.

For more information, see Section 2.3, "Rights Descriptions," on page 29.

5 Click *OK*.

2.2.4 Removing Assigned Rights

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

2 Click the administrator in the *Name* column of the Administrators pane.

3 Select the check box next to the assigned right.

4 Click *Delete*.

You can also use the `admin-rights-delete` command in zman to delete assigned rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2.3 Rights Descriptions

When you create additional administrator accounts you can provide full access to your zone or you can create accounts with limited rights. For example, you could create an administrator account that allows access to all management tasks except those pertaining to Management Zone configuration (user sources, registration, configuration settings, and so forth). For information about creating additional administrators, see "Creating Administrators" on page 26.

For Administrator roles only, a third column of rights options is added to each rights assignment dialog box: *Unset*, which allows rights set elsewhere in ZENworks to to be used for the role.

The most restrictive right set in ZENworks prevails. Therefore, if you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

You can also add, modify, or remove the assigned rights for an existing administrator. For more information, see Section 2.2.2, "Assigning Additional Rights," on page 28, Section 2.2.3, "Modifying Assigned Rights," on page 29, or Section 2.2.4, "Removing Assigned Rights," on page 29.

The following sections contain additional information about the various rights that you can assign:

- Section 2.3.1, "Administrator Rights," on page 30
- Section 2.3.2, "Contract Management Rights," on page 30

2.3.1 Administrator Rights

The Administrator Rights dialog box lets you allow the selected administrator to grant rights to other administrators and to create or delete administrator accounts for your Management Zone.

The following rights are available:

- **Grant Rights:** Allow or deny the administrator the rights necessary to grant rights to other administrators.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete administrator accounts.

2.3.2 Contract Management Rights

The Contract Management Rights dialog box lets you select folders containing contracts, then modify the rights associated with contracts and folders.

- "Contexts" on page 30
- "Privileges" on page 30

Contexts

To select the folder that contains the contracts for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- **Modify:** Allow or deny the administrator the rights necessary to modify the existing contracts.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete contracts.

- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.3 Credential Rights

The Credential Rights dialog box lets you select folders containing credentials, then modify the rights associated with those folders.

- "Contexts" on page 31
- "Privileges" on page 31

Contexts

Click *Add* to select the folder that contains the credentials for which you want to assign rights.

Privileges

The Privileges section lets you grant the selected administrator rights to create or modify credentials, create or modify groups, and create or modify folders.

The following rights are available:

- **Modify:** Allow or deny the administrator the rights necessary to modify existing credentials.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete credentials.
- **Modify Folders:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

For more information about the tasks you can perform on credentials, see Chapter 4, "Credential Vault," on page 57.

2.3.4 Deployment Rights

The Deployment Rights dialog box lets you allow or deny the administrator the rights necessary to perform deployment operations.

Deployment lets you discover network devices and deploy the ZENworks Adaptive Agent to them so that they become managed devices in your Management Zone. For more information, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 10 Discovery, Deployment, and Retirement Reference*.

2.3.5 Device Rights

The Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

- "Contexts" on page 32
- "Privileges" on page 32

Contexts

To select the folder that contains the devices for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders.

The following rights are available:

- **Modify:** Allow or deny the administrator the rights necessary to modify the existing device objects.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete device objects.
- **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.
- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- **Modify Settings:** Allow or deny the administrator the rights necessary to modify device settings.

2.3.6 Discovery Rights

The Discovery Rights dialog box lets you allow or deny the administrator the rights necessary to perform discovery operations.

The following rights are available:

- **Discovery:** Allow or deny the administrator the right necessary to perform discovery.
- **Edit Discovered Device:** Allow or deny the administrator the rights necessary to edit a discovered device.

2.3.7 Document Rights

The Document Rights dialog box lets you select folders containing documents, then modify the rights associated with documents and folders.

-
-

Contexts

To select the folder that contains the documents for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- **Modify:** Allow or deny the administrator the rights necessary to reassign existing documents.
- **Create/Delete:** Allow or deny the administrator the rights necessary to import or delete documents.
- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.8 LDAP Import Rights

The LDAP Import Rights dialog box lets you allow or deny importing of LDAP information.

2.3.9 Inventoried Device Rights

The Inventoried Device Rights dialog box lets you select folders containing devices, then modify the rights associated with those folders.

Contexts

To select the folder that contains the inventoried devices for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

The *Privileges* section lets you grant the selected administrator rights to work with inventoried devices, including device groups and folders.

The following rights are available:

- **Modify:** Allow or deny the administrator the rights necessary to modify existing inventoried device objects.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete inventoried device objects.
- **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- **Modify Group Membership:** Allow or deny the administrator the rights necessary to modify the list of devices contained in device groups.

- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.
- **Modify Settings:** Allow or deny the administrator the rights necessary to modify inventoried device settings.

2.3.10 License Management Rights

The License Management Rights dialog box lets you select folders containing licenses, then modify the rights associated with licenses and folders.

- "Contexts" on page 34
- "Privileges" on page 34

Contexts

To select the folder that contains the licenses for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

- **Modify:** Allow or deny the administrator the rights necessary to modify the existing licenses.
- **Create/Delete:** Allow or deny the administrator the rights necessary to create or delete licenses.
- **Modify Folder:** Allow or deny the administrator the rights necessary to modify folders.
- **Create/Delete Folders:** Allow or deny the administrator the rights necessary to create or delete folders.

2.3.11 Patch Management Rights

The Patch Management Rights dialog box lets you determine which patch management functions an administrator can have.

The following rights are available:

- **Patch Deploy:** Allow or deny the administrator the rights necessary to deploy patches.
- **Patch Enable:** Allow or deny the administrator the rights necessary to enable a disabled patch.
- **Patch Disable:** Allow or deny the administrator the rights necessary to disable a patch.
- **Patch Update Cache:** Allow or deny the administrator the rights necessary to cache patches.
- **Assign to Baseline:** Allow or deny the administrator the rights necessary to assign a patch to the baseline.
- **Remove from Baseline:** Allow or deny the administrator the rights necessary to remove a patch that was assigned to the baseline.
- **View Patch Details:** Allow or deny the administrator the rights necessary to view patch details.
- **Export Patch:** Allow or deny the administrator the rights necessary to export patches.

- **Scan Now:** Allow or deny the administrator the rights necessary to start a scan.
- **Remove Patch:** Allow or deny the administrator the rights necessary to remove a patch.
- **Recalculate Baseline:** Allow or deny the administrator the rights necessary to recalculate the baseline.
- **Configure:** Allow or deny the administrator the rights necessary to configure the patch.

2.3.12 Quick Task Rights

The Quick Tasks Rights dialog box lets you select folders containing devices, then modify the Quick Task rights associated with those folders.

Quick Tasks are tasks that appear in ZENworks Control Center task lists (for example, Server Tasks, Workstation Tasks, and so forth). When you click a task, either a wizard launches to step you through the task or a dialog box appears in which you enter information to complete the task.

You can use the Quick Tasks Rights dialog box to allow or deny the selected administrator the rights to perform certain tasks by using Quick Tasks.

- "Contexts" on page 35
- "Privileges" on page 35

Contexts

To select the folder that contains the device for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

The following rights are available:

- **Shutdown/Reboot/Wake Up Devices:** Specify whether the administrator can shut down, reboot, or wake up the devices in the folders you selected in the list.
- **Execute Processes:** Allow or deny the administrator the rights necessary to execute processes on the devices.
- **Refresh ZENworks Adaptive Agent:** Allow or deny the administrator the rights necessary to refresh the ZENworks Adaptive Agent on devices.
- **Inventory:** Allow or deny the administrator the rights necessary to inventory devices.

2.3.13 Reporting Rights

The Reporting Rights dialog box lets you allow or deny the administrator the rights to create, delete, execute, or publish reports.

2.3.14 User Rights

The User Rights dialog box lets you select folders containing users, then modify the rights associated with those folders.

- "Contexts" on page 36
- "Privileges" on page 36

Contexts

To select the folder that contains the users for which you want to assign rights, click *Add* to display the Contexts dialog box, then browse for and select the folders for which you want to assign rights.

Privileges

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders.

The following rights are available:

- **Modify ZENworks Group Membership:** Allow or deny the rights necessary to modify ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *ZENworks User Group Rights*.

2.3.15 ZENworks User Group Rights

The ZENworks User Group Rights dialog box lets you allow or deny the administrator the rights to create, delete, or modify groups and to modify group membership.

The following rights are available:

- **Modify Groups:** Allow or deny the administrator the rights necessary to modify existing groups.
- **Create/Delete Groups:** Allow or deny the administrator the rights necessary to create or delete groups.
- **Modify ZENworks Group Membership:** Allow or deny the administrator the rights necessary to modify the ZENworks group membership. If you select this option, you must also grant rights to *Modify ZENworks Group Membership* under *User Rights*.

2.3.16 Zone Rights

The Zone Rights dialog box lets you modify the administrator's rights to administer settings in your ZENworks Management Zone.

The following rights are available:

- **Modify User Sources:** Allow or deny the administrator the rights necessary to modify user sources.

  A user source is an LDAP directory that contains users that you want to reference in your ZENworks Management Zone. When you define a user source, you also define the source containers from which you want to read users and user groups.

- **Create/Delete User Sources:** Allow or deny the administrator the rights necessary to create or delete user sources.
- **Modify Settings:** Allow or deny the administrator the rights necessary to modify your Management Zone settings.

  The Management Zone settings let you manage the global configuration settings for your Management Zone. These global configuration settings are inherited by other objects (devices, users, and folders) within your Management Zone and remain in effect unless they are overridden on those objects.

- **Modify Zone Infrastructure:** Allow or deny the administrator the rights necessary to modify Zone infrastructure. This right includes the rights to perform the following actions in the Server Hierarchy section of the *Configuration* tab:

    - Specify content for a device

    - Move the device in the hierarchy

    - Configure a Satellite

    - Add a Satellite

    - Remove a Satellite

    Other actions can be taken in the Server Hierarchy section. However, rights for those actions must be specified individually. They are not automatically included in the Modify Zone Infrastructure right. These are:

    - Delete ZENworks Server

    - Refresh Device

- **Configure Registration:** Allow or deny the administrator the rights necessary to configure device registration.

    Registration lets you manage the various configuration settings for registering devices as managed devices in the Management Zone. It also lets you create registration keys or registration rules to help you register devices. A registration key lets you apply group and folder assignments to devices as they register. A registration rule lets you apply group and folder assignments to folders if the device meets the rule criteria.

- **Delete News Alerts:** Allow or deny the administrator the rights necessary to delete the news alerts.

- **Update News Alerts:** Allow or deny the administrator the rights necessary to update the news alerts.

2.4 Managing Administrator Roles

Perform the following tasks to manage administrator roles in the Management Zone:

- Section 2.4.1, "Understanding Administrator Roles," on page 37
- Section 2.4.2, "Creating a Role," on page 40
- Section 2.4.3, "Assigning Roles," on page 42
- Section 2.4.4, "Editing a Role," on page 46
- Section 2.4.5, "Renaming a Role," on page 49
- Section 2.4.6, "Deleting a Role," on page 49

2.4.1 Understanding Administrator Roles

The roles feature allows you to specify rights that can be assigned as roles for ZENworks administrators. You can create a specialized role, then assign administrators to that role to allow or deny them the ZENworks Control Center rights that you specify for that role. For example, you could create a Help Desk role with the ZENworks Control Center rights that you want help desk operators to have.
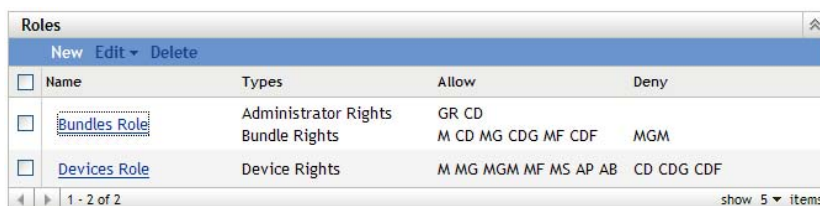
The following sections explain the different locations in ZENworks Control Center where you can manage roles:

Roles Panel

The Roles panel displays the following information:

Figure 2-1 *Roles Panel*

- **Name:** You specified this when you created the role. You can rename the role here. You can also click a role name to edit its rights configuration.
- **Types:** Lists each ZENworks Control Center rights type that is configured for the role.
- **Allow:** For each type listed, abbreviations are displayed to indicate the rights that are allowed for that role.
- **Deny:** For each type listed, abbreviations are displayed to indicate the rights that are denied for that role.

If a right is configured as *Unset*, its abbreviation is not listed in either the *Allow* or *Deny* column.

In the Roles panel, you can add, assign, edit, rename, and delete a role.

Role Settings Page

If you click a role in the *Name* column on the Roles panel, the Role Settings page is displayed with the following information:

Figure 2-2 *Role Settings Page*

- ◆ **General panel:** Displays the ZENworks Control Center object type (Role), its GUID, and a description that you can edit here.

- ◆ **Rights panel:** Displays the ZENworks Control Center rights configured for the role. You can add, edit, and delete the rights in this panel.

- ◆ **Assigned Administrators panel:** Lists the administrators assigned to this role. You can add, edit, or delete the administrators in this panel.

Administrator Settings Page

If you click an administrator in the *Administrator* column on the Roles Settings page, the Administrator Settings page is displayed with the following information:

Figure 2-3 *Administrator Settings Page*

- ◆ **General panel:** Displays the administrator's full name and provides the option to specify the administrator as a Super Administrator, which grants all ZENworks Control Center rights to that administrator, regardless of what is configured for the role.

- ◆ **Rights panel:** Lists the rights that are assigned to the administrator, independent of rights granted or denied by any roles assigned to the administrator. The rights listed in this panel override any rights assigned by a role. You can add, edit, and delete rights in this panel.

- ◆ **Assigned Roles panel:** Lists the roles assigned to this administrator. You can add, edit, and delete roles in this panel.

2.4.2 Creating a Role

A role can include one or more rights types. You can configure as many roles as you need. To configure the role's function:

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, click *New* to open the Add New Role dialog box:
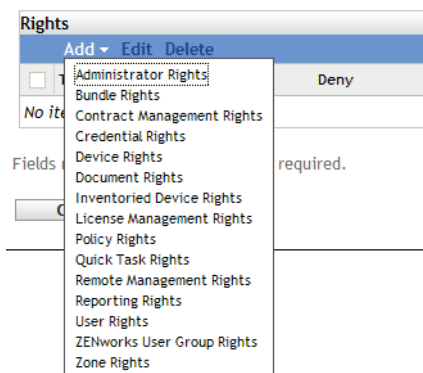
2 Specify a name and description for the role.

3 To configure the rights for the role, click *Add* and select a rights type from the drop-down list:

4 In the following dialog box, select whether each privilege should be allowed, denied, or left unset.

The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

5 Click *OK* to continue.

6 To add another rights type to the role, repeat Step 3 through Step 5.

7 Click *OK* to exit the Add New Role dialog box.

The role is now displayed in the Roles panel. To assign it to administrators, see Section 2.4.3, "Assigning Roles," on page 42.

2.4.3 Assigning Roles

You can assign roles to administrators, or administrators to roles:

- "Assigning Roles to Administrators" on page 42
- "Assigning Administrators to Roles" on page 44

Assigning Roles to Administrators

Rights can be set in multiple locations in ZENworks Control Center, including for administrators. Administrators can be assigned to multiple roles.

If an administrator has rights conflicts because different conditions are set for a particular right in ZENworks Control Center, the *Deny* option is used if it is set anywhere for the administrator. In other words, *Deny* always supersedes *Allow* when there are rights conflicts.

To assign roles to an administrator:

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Administrators panel, click an administrator name in the *Name* column to open the administrator's settings page:

2 In the Assigned Roles panel, click *Add* to display the Select Role dialog box.

3 Browse for and select the roles for the administrator, then click *OK* to display the Add Role Assignment dialog box:

The Add Role Assignment dialog box is displayed so that you can define the contexts for the role types included in the role. A context allows you to limit where granted rights can be used. For example, you can specify that the administrator's Quick Task Rights role is limited to the Devices folder in ZENworks Control Center.

Contexts are not required. However, if you do not specify a context, the right is not granted because it has no information about where it can be applied.

Rights that are global automatically display `Zone` as the context.

4 If necessary, assign contexts to role types where they are missing:

    4a In the *Types* column, click a role type.

        Role types that are designated with the Zone context are not clickable because they are generally available.

    4b In the subsequent Select Context dialog box, click *Add* and browse for a ZENworks Control Center context.

        While browsing, you can select multiple contexts in the Browse dialog box.

    4c When you are finished selecting the contexts for a particular role, click *OK* to close the Select Contexts dialog box.

    4d Repeat Step 4a through Step 4c as necessary to assign contexts to the roles.

    4e When you are finished, click *OK* to close the Add Role Assignment dialog box.

5 To add another administrator, repeat Step 2 and Step 4.

6 Click *Apply* to save the changes.

Assigning Administrators to Roles

Rights can be set in multiple locations in ZENworks Control Center. Administrators can be assigned to multiple roles.

If an administrator has rights conflicts because different conditions are set for a particular right in ZENworks Control Center, the *Deny* option is used if it is set anywhere for the administrator. In other words, *Deny* always supersedes *Allow* when there are rights conflicts.

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, click a role name in the *Name* column to open the role's settings page:

2 In the Assigned Administrators panel, click *Add* to display the Select Administrator dialog box:

3 Browse for and select the administrators for the role, then click *OK* to display the Add Role Assignment dialog box:

The Add Role Assignment dialog box is displayed so that you can define the contexts for the role types included in the role. A context allows you to limit where granted rights can be used. For example, you can specify that the administrator's Quick Task Rights role is limited to the Devices folder in ZENworks Control Center.

Contexts are not required. However, if you do not specify a context, the right is not granted because it has no information about where it can be applied.

Rights that are global automatically display `Zone` as the context.

4 If necessary, assign contexts to role types where they are missing:

    4a In the *Types* column, click a role type.

        Role types that are designated with the Zone context are not clickable because they are generally available.

    4b In the subsequent Select Context dialog box, click *Add* and browse for a ZENworks Control Center context.

        While browsing, you can select multiple contexts in the Browse dialog box.

    4c When you are finished selecting the contexts for a particular role, click *OK* to close the Select Contexts dialog box.

    4d Repeat Step 4a through Step 4c as necessary to assign contexts to the roles.

    4e When you are finished, click *OK* to close the Add Role Assignment dialog box.

5 To add another role, repeat Step 2 and Step 4.

6 Click *Apply* to save the changes.

2.4.4 Editing a Role

You can edit a role's configuration at any time. After you apply the edited role, its changes are then effective for any assigned administrator.

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, click *Edit* to open the Edit Role dialog box:

2 To edit the description, make the changes directly in the *Description* field.

3 To edit existing rights, do the following:

3a In the Rights panel, select the check box for a rights type, then click *Edit* to open the following dialog box:

3b For each privilege, select whether it should be allowed, denied, or left unset.

The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

3c Click *OK* to continue.

3d To edit another existing role, repeat Step 3a through Step 3c.

4 (Optional) To add new rights:

4a In the Rights panel, click *Add*, then select one of the rights types from the drop-down list:
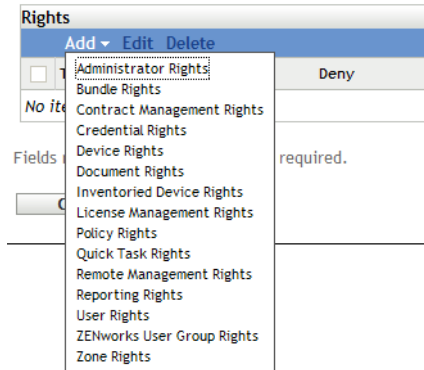
4b In the Rights dialog box, select whether each privilege should be allowed, denied, or left unset.
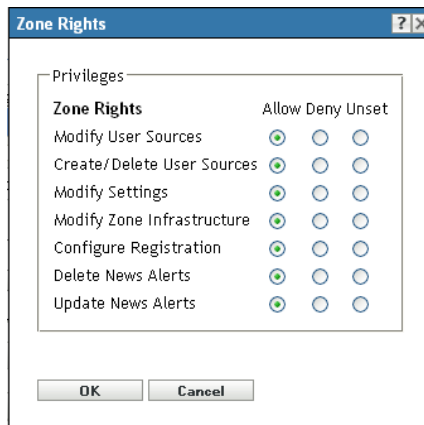
The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Allow* option and the right has not been denied elsewhere in ZENworks, the administrator has that right for the role.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

4c Click *OK* to continue.
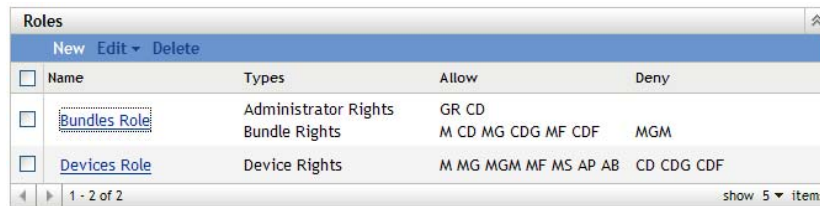
4d To add another rights type to the role, repeat Step 4a through Step 4c.

5 To exit the dialog box and save your changes to the role, click *OK*.

2.4.5 Renaming a Role

Role names can be changed at any time. The changed role name is automatically replicated wherever it is displayed in ZENworks Control Center.

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, select the check box for the role to be renamed.
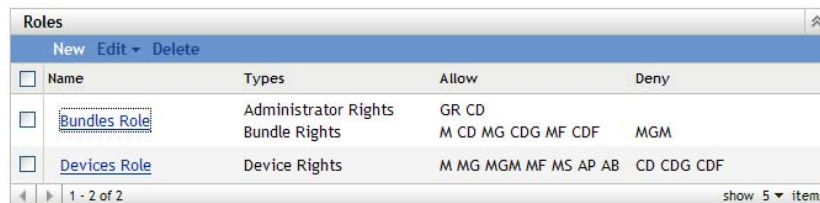
2 Click *Edit > Rename* to open the Rename Role dialog box:

3 Specify the new role name, then click *OK*.

2.4.6 Deleting a Role

When you delete a role, its rights configurations are no longer applicable to any administrator that was assigned to the role.

Deleted roles cannot be recovered. You must re-create them.

1 In ZENworks Control Center, click *Configuration* in the left pane, click the *Configuration* tab, then in the Roles panel, select the check box for the role to be deleted.

2 Click *Delete*, then confirm that you want to delete the role.
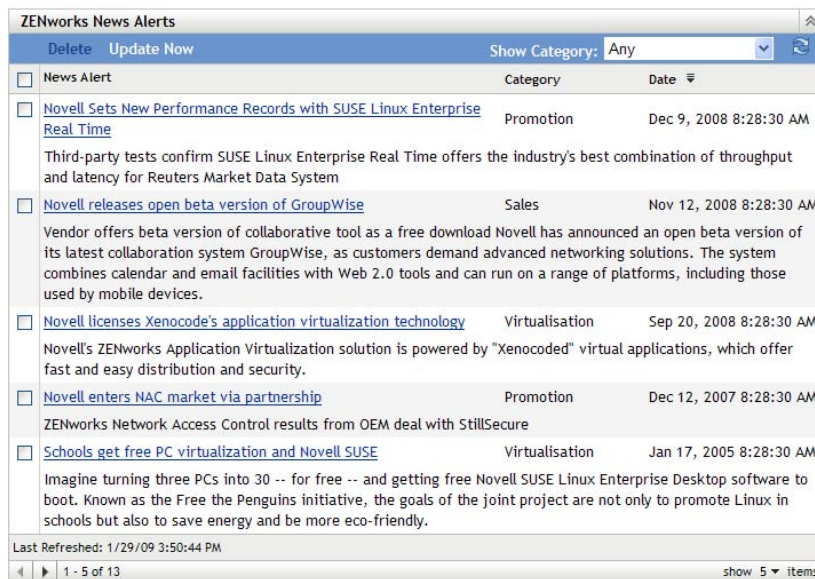
ZENworks News

Novell® ZENworks® 10 Asset Management displays information from Novell about current top issues, news updates, promotions, and so forth on the home page of ZENworks Control Center.

The following sections provide information on deleting, updating, and sorting the news alerts, and on viewing the news. You can also configure the server and the schedule for downloading the news.

- Section 3.1, "Managing ZENworks News Alerts," on page 51
- Section 3.2, "Configuring ZENworks News Settings," on page 52

3.1 Managing ZENworks News Alerts

Figure 3-1 *ZENworks News Alerts*

Review the following sections to manage the ZENworks News Alerts:

- Section 3.1.1, "Deleting the News Alerts," on page 51
- Section 3.1.2, "Updating the News Alerts," on page 52
- Section 3.1.3, "Displaying the News Alerts Based on the Selected Category," on page 52
- Section 3.1.4, "Viewing the News," on page 52
- Section 3.1.5, "Sorting the News Alerts," on page 52

3.1.1 Deleting the News Alerts

1 In ZENworks Control Center, click *Home*.

2 In ZENworks News Alerts panel, select the check box next to the news alerts you want to delete.

3 Click *Delete*.

3.1.2 Updating the News Alerts

1 In ZENworks Control Center, click *Home*.

2 In ZENworks News Alerts panel, click *Update Now*.

The latest ZENworks news updates downloaded by the Primary Server are displayed in the ZENworks News Alerts panel. This might take some time.

3.1.3 Displaying the News Alerts Based on the Selected Category

1 In ZENworks Control Center, click *Home*.

2 In ZENworks News Alerts panel, select a category in the drop-down list next to *Show Category* to display all the news alerts based on the selected category.

3.1.4 Viewing the News

1 In ZENworks Control Center, click *Home*.

2 In ZENworks News Alerts panel, click the news alert to display the news in a new browser window.

3.1.5 Sorting the News Alerts

By default, the news alerts are sorted by the publication date. You can also sort the news alerts alphabetically by the title or category.

1 In ZENworks Control Center, click *Home*.

2 In ZENworks News Alerts panel, click *News Alert* to sort the news alerts alphabetically.

or

Click *Category* to sort the news alerts by category.

or

Click *Date* to sort the news alerts by date.

3.2 Configuring ZENworks News Settings

The ZENworks News Settings page lets you configure a dedicated news server and a schedule to download the ZENworks news. By default, the news is downloaded at midnight by the Primary Server of the Management Zone.

Figure 3-2   *News Download Schedule*

Review the following sections to configure the settings to download the news:

- Section 3.2.1, "Dedicated News Server," on page 53
- Section 3.2.2, "Schedule Type," on page 54

3.2.1 Dedicated News Server

By default, any available server in the Management Zone can be used to download the news updates. However, you can specify one ZENworks Server to be dedicated to handle the news downloads. The server that you select should have access to the Internet, either directly or through a proxy server.

The following sections contain more information:

- "Specifying a Dedicated News Server" on page 53
- "Clearing a Dedicated News Server" on page 54

Specifying a Dedicated News Server

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *ZENworks News Settings* to display the News Download Schedule panel.

3 In the *Dedicated News Server* field, browse for and select a server, then click *OK*.

The server's identification is displayed in the *Dedicated News Server* field.

4 (Conditional) If you need to revert to the last saved dedicated server setting, click *Reset*.

This resets the dedicated server to the last saved setting, such as when you last clicked *Apply* or *OK*.

5 Click *Apply* to make the changes effective.

6 Either click *OK* to close the page, or continue with configuring the schedule type.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

Clearing a Dedicated News Server

Clearing a dedicated update server causes the news updates to be retrieved randomly from any server in the Management Zone.

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *ZENworks News Settings* to display the News Download Schedule panel.

3 Click ✖ to remove the dedicated server from the *Dedicated News Server* field.

4 (Conditional) If you need to revert to the last saved dedicated server setting, click *Reset*.

This resets the dedicated server to the last saved setting, such as when you last clicked *Apply* or *OK*.

5 Click *Apply* to make the change effective.

3.2.2 Schedule Type

You can configure the schedule for downloading the news:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *Configuration* tab.

2 Click *Management Zone Settings* to expand its options, click *Infrastructure Management* to expand its options, then select *ZENworks News Settings*.

3 (Conditional) To exclude scheduled checking for news updates, click the down-arrow in the *Schedule Type* field, select *No Schedule*, click *Apply* to save the schedule change, then skip to Step 6.

With this option selected, you must download the news updates manually. For more information, see "Updating the News Alerts" on page 52.

4 (Conditional) To set a recurring schedule for checking for the news updates, click the down-arrow in the *Schedule Type* field, then select *Recurring*.

5 Fill in the fields:

   5a Select one or more check boxes for the days of the week when you want to check for news updates.

   5b Use the *Start Time* box to specify the time of day for checking to occur.

   5c (Optional) Click *More Options*, then select the following options as necessary:

      ◆ **Process Immediately if Device Unable to Execute on Schedule:** Causes checking for news updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for news updates occurs immediately after the server comes back online.

      ◆ **Use Coordinated Universal Time:** Causes the schedule to interpret the times you specify as UTC instead of local time.

      ◆ **Start at a Random Time Between Start and End Times:** Allows checking for news updates to occur at a random time between the time you specify here and the time you specified in Step 5b. Fill in the *End Time* fields.

      ◆ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify a date range to check for the news updates.

5d (Conditional) If you need to revert to the last saved schedule, click *Reset* at the bottom of the page.

This resets all data to the last saved state, such as when you last clicked *Apply* or *OK*.

5e When you have finished configuring the recurring schedule, click *Apply* to save the schedule change.

6 To exit this page, click *OK* when you are finished configuring the schedule.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

Credential Vault

<div style="text-align: right; font-size: large;">4</div>

The Credential Vault stores the credentials used by Novell® ZENworks® 10 Asset Management actions and tasks that require authentication to access a particular resource.

You can use ZENworks Control Center or the zman command line utility to manage credentials. The procedures in this section explain how to manage credentials by using ZENworks Control Center. If you prefer the zman command line utility, see "Credential Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

Currently, third-party imaging uses credentials stored in the credential vault.

The following sections contain information to help you manage credentials:

4.1 Adding a Credential

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

2 In the *Credential Vault* panel, click *New > Credential* to display the Add Credential dialog box.
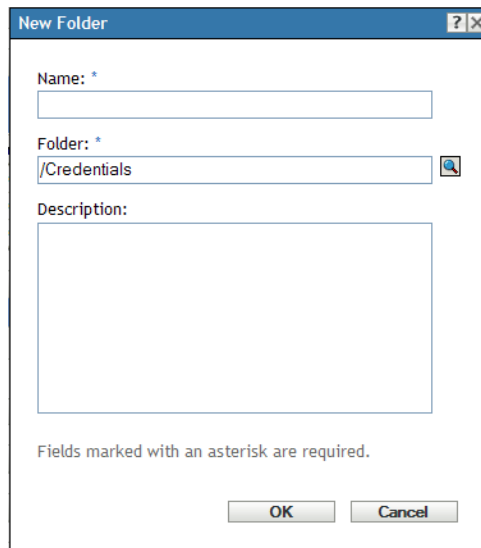
3 Fill in the fields.

If you need help, click the *Help* button.

4.2 Creating a Folder for Credentials

1 In ZENworks Control Center, click the *Configuration* tab.
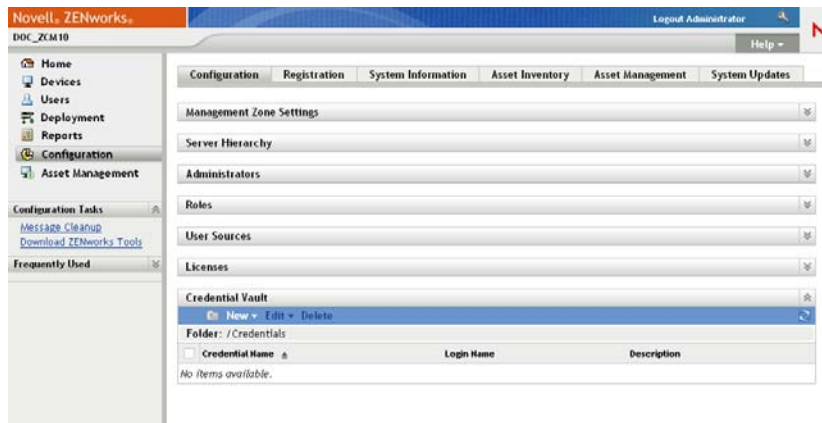
2 In the Credential Vault panel, click *New > Folder* to display the New Folder dialog box.

3 In the *Name* field, specify a unique name for the folder.

The folder cannot have the same name as any folders or credentials that already exist in the folder where you are creating it.

4 In the *Folder* field, click 🔍 to browse for and select the folder where you want the new folder created.

5 Type a description for the new folder, if desired.

6 Click *OK* to create the folder.

4.3 Assigning Credential Rights

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

2 In the *Administrators* section, click the underlined link for the administrator for which you want to change rights.

3 In the *Assigned Rights* section, click *Add > Credential Rights*.

4 Click *Add* to select folders containing credentials, then modify the rights associated with those folders.

If you need help, click the *Help* button.

4.4 Editing a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click *Edit*.

4 Edit the fields.

If you need help, click the *Help* button.

5 Click *OK*.

4.5 Renaming a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click *Edit > Rename*.

4 Type the new name for the credential.

5 Click *OK*.

4.6 Moving a Credential to Another Folder

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click *Edit > Move*.

4 In the *Folder* field, click to browse for and select the folder where you want the credential moved.

5 Click *OK*.

4.7 Removing a Credential

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

2 In the Credential Vault panel, select the check box next to the credential.

3 Click *Delete*.

ZENworks Server and Adaptive Agent
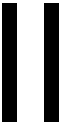
This section contains information about configuring the ZENworks® Servers and the ZENworks Adaptive Agent.

ZENworks Server

5

The ZENworks® Server is the backbone of the ZENworks system. It communicates with the ZENworks Adaptive Agent on managed devices to perform management tasks. It communicates with other ZENworks Servers and ZENworks Satellites to replicate or receive software and hardware inventory and messages throughout the Management Zone.

The following sections provide additional information about the ZENworks Server:

5.1 ZENworks Services on a Windows Server

When it is running on a Windows* server, a ZENworks Server includes the services listed in the following table. All services are always installed regardless of the ZENworks 10 products (Configuration Management, Asset Management, and Patch Management) you have licensed and activated. If a service is not required for your product, it is disabled.

Table 5-1 *ZENworks Services on Windows*

Service	Service Name	Description
Proxy DHCP Service	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell® TFTP server.
TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
ZENworks Agent Service	zenworkswindowsservice novell-zmd	Used to enable the server as a managed device.
ZENworks Datastore	dbsrv10	Embedded database used for storing ZENworks objects and resources.
ZENworks Loader	zenloader	Used for loading and controlling the Java* services that perform ZENworks Server tasks.
ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.

Service	Service Name	Description
ZENworks Preboot 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 Remote Management	nzrwinvnc	Used to enable remote management of the server.
ZENworks Server	zenserver	Used for communicating with the ZENworks Agent.
ZENworks Services Monitor	zenwatch	Used to monitor the status of the ZENworks services.
ZENworks Imaging Agent	ziswin	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 `\novell\zenworks\bin` directory on a 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

1 On the server, click *Start*, select *Administrative Tools > Services*, then review the status of the services listed in Table 5-1 on page 63.

5.1.2 Starting a ZENworks Service

1 On the server, click *Start*, select *Administrative Tools > Services*.

2 Select the service you want to start (see Table 5-1 on page 63), then click *Start the service*.

The ZENworks services start when the ZENworks Server is booted and should not normally need to be restarted. If you need to frequently restart the services, ensure that your server hardware meets the ZENworks minimum requirements. If the server does not have adequate RAM, ZENworks services might not continue running. For more information, see "Primary Server Requirements" in the *ZENworks 10 Asset Management Installation Guide*.

5.1.3 Stopping a ZENworks Service

1 On the server, click *Start*, then select *Administrative Tools > Services*.

2 Select the service you want to stop (see Table 5-1 on page 63), then click *Stop the service*.

5.2 ZENworks Services on a Linux Server

When it is running on a Linux server, the ZENworks Server includes the services listed in the following table. All services are always installed regardless of the ZENworks 10 products (Configuration Management, Asset Management, and Patch Management) you have licensed and activated. If a service is not required for your product, it is disabled

Table 5-2 *ZENworks Services on Linux*

Service	Service Name	Description
Proxy DHCP Service	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell TFTP server.
TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
ZENworks Agent Service	novell-zmd	Used to enable the server as a managed device.
ZENworks Datastore	sybase-asa	Used to run the embedded SQL Anywhere* database.
ZENworks Loader	novell-zenloader	Used for loading and controlling the Java services that perform ZENworks Server tasks.
ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
ZENworks Preboot 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 Server	novell-zenserver	Used for communicating with the ZENworks Agent.
ZENworks Services Monitor	novell-zenmntr	Used to monitor the status of the ZENworks services.
ZENworks Imaging Agent	novell-zenagent	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. Refer to the following sections for instructions to help you control the ZENworks services:

-
-

5.2.1 Checking the Status of a ZENworks Service

1 At the server command prompt, enter the following command:

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

Replace *servicename* with the name of the service as listed in Table 5-2 on page 65.

5.2.2 Starting a ZENworks Service

1 At the server command prompt, enter the following command:

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

Replace *servicename* with the name of the service as listed in Table 5-2 on page 65.

2 To start all services, use the following command:

```
/opt/novell/zenworks/bin/novell-zenworks-configure Start
```

The ZENworks services start when the ZENworks Server is booted and should not normally need to be restarted. If you need to frequently restart the services, ensure that your server hardware meets the minimum ZENworks requirements. If the server does not have adequate RAM, ZENworks services might not continue running. For more information, see "Primary Server Requirements" in the *ZENworks 10 Asset Management Installation Guide*.

5.2.3 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 5-2 on page 65.

5.2.4 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 5-2 on page 65.

5.3 Configuring Additional Access to a ZENworks Server

If you have managed devices that are unable to authenticate to the IP address or DNS name of a ZENworks Server, such as devices outside the firewall or devices using a proxy server, you can specify additional IP addresses or DNS names for the ZENworks Server that can be used by the devices for access to the server.

5.3.1 Addressing Non-Detectable IP Address Conditions

The Non-Detectable IP Addresses panel lets you specify the addresses that can be used to access the ZENworks Server when the server's IP address cannot be found by a device.

1 In ZENworks Control Center, click *Devices* in the left pane, select *Servers* in the Devices panel, select a server object, click the *Settings* tab, click *Infrastructure Management*, then select *Non-detectable IP Addresses*.

2 Fill in the field:

IP Address: Standard dotted-decimal notation. For example, `123.45.167.100.`

3 Click *Add* to add the address to the list.

4 Repeat Step 1 to Step 3 to add additional IP addresses.

5 If necessary, use the *Move Up* and *Move Down* buttons to reorder the list.

The IP addresses are used in the order listed, from top to bottom.

6 When you are finished adding addresses, click *Apply* or *OK* to save the addresses.

5.3.2 Addressing Non-Detectable DNS Name Conditions

The Additional DNS Names panel lets you specify additional names that can be used to access the ZENworks Server when the server's DNS name cannot be found by a device.

The DNS names added in this panel are distributed to all managed devices for them to use in connecting to the server.

To add a DNS name:

1 In ZENworks Control Center, click *Devices* in the left pane, select *Servers* in the Devices panel, select a server object, click the *Settings* tab, click *Infrastructure Management*, then select *Additional DNS Names*.

2 In the *List of Server DNS Names* field, specify the DNS name for the IP address of the server (such as a proxy server) that the devices can access.

3 Click *Add* to add the DNS name to the list.

4 If necessary, use the *Move Up* and *Move Down* buttons to reorder the list.

The DNS names are used in the order listed, from top to bottom.

5 When you are finished adding addresses, click *Apply* or *OK* to save the addresses.

5.4 Determining the ZENworks Software Version Installed on Servers

For upgrading and troubleshooting purposes, you use ZENworks Control Center to determine which versions of ZENworks Configuration Management (ZCM), ZENworks Asset Management (ZAM), and ZENworks Patch Management (ZPM) are running on ZENworks Primary Servers in your Management Zone.

To see ZENworks version information for a specific Primary Server in your Management Zone:

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

2 Click *Servers*, then click the desired Primary Server.

3 View the version number in the *ZENworks Configuration Management Version*, *ZENworks Asset Management Version*, and *ZENworks Patch Management Version* rows.

4 (Optional) Click the underlined version number next to *ZENworks Configuration Management Version* to see a list of installed packages.

To see ZENworks version information for all Primary Servers in your Management Zone:

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

2 In the Server Hierarchy panel, view the version information in the *ZCM Version*, *ZAM Version*, and *ZPM Version* columns for each server.

5.5 Uninstalling a ZENworks Server

Instructions for uninstalling a ZENworks Server are provided in "Uninstalling ZENworks 10 Asset Management SP2" in the *ZENworks 10 Asset Management Installation Guide*.

5.6 Deleting a ZENworks Primary Server

If you cannot run the uninstallation program to uninstall a ZENworks Primary Server, you can delete it from the Server Hierarchy panel.

WARNING: Use extreme caution when deleting a ZENworks Primary Server from your ZENworks system.

Deleting a ZENworks Primary Server is irreversible. The preferred way to decommission a Primary Server is to run the uninstallation program from the Server. Deleting a Primary Server should only be used if the uninstallation program cannot be run (for example, if the Primary Server experiences a hard drive failure). For more information about running the uninstallation program, see "Uninstalling ZENworks 10 Asset Management SP2" in the *ZENworks 10 Asset Management Installation Guide*.

If you remove a Primary Server that hosts an internal ZENworks Sybase database, your entire ZENworks Management Zone becomes inoperable.

Deleting a ZENworks Server completely removes the ZENworks Server from the Management Zone. There is no recovery.

You can delete managed server and workstation devices by using the options on the *Devices* tab, as explained in "Deleting Devices from Your ZENworks System" in the *ZENworks 10 Discovery, Deployment, and Retirement Reference*.

To remove a ZENworks Primary Server from your Management Zone:

1 In ZCC, click the *Configuration* tab.

2 In the Server Hierarchy section, select the check box next to the Primary Server (you can select multiple devices).

3 Click *Action > Delete ZENworks Server*.

5.7 ZENworks Server Reports

You must have installed ZENworks Reporting Server to view the predefined reports. For more information on how to install ZENworks Reporting Server, see the *ZENworks 10 Asset Management Reporting Server Installation Guide*.

To view a predefined report for the ZENworks Server:

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

2 In the ZENworks Reporting Server panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView.

3 Navigate to the *Novell ZENworks Reports* folder > *Predefined Reports > ZENworks System* folder.

The following predefined report is included for the ZENworks Server:

ZENworks Server Statistics: Displays server statistics such as database, disk space, CPU usage, and various connection details that include total connections per day and average connections per day.

For more information on creating and managing reports, see the *ZENworks 10 Asset Management System Reporting Reference* documentation.

Satellites

6

A Satellite is a managed device that can perform certain roles that a ZENworks® Primary Server normally performs. A Satellite can be any managed Windows device (server or workstation), but not a Primary Server. A Satellite can also be an unmanaged Linux device (server or workstation) that has the ZENworks Agent for Linux installed. For more information, see "Satellite Requirements" in the *ZENworks 10 Asset Management Installation Guide* and "Deploying the Agent to a Linux Satellite" in the *ZENworks 10 Discovery, Deployment, and Retirement Reference*.

When you configure a Satellite, you specify which roles it performs (Collection or Content). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks 10 Asset Management framework.

You might, for example, create a Satellite in a location across a slow WAN link and create Closest Server rules to offload one or more roles from the Primary Server to the newly created Satellite to improve the performance of your ZENworks system.

The following sections contain more information:

- Section 6.1, "Understanding the Satellite Roles," on page 71
- Section 6.2, "Adding Satellites into the Server Hierarchy," on page 72
- Section 6.3, "Removing Satellites from the Server Hierarchy," on page 74
- Section 6.4, "Configuring Satellites from the Server Hierarchy," on page 75
- Section 6.5, "Configuring Satellites from the Device View," on page 76
- Section 6.6, "Moving a Satellite from One Primary Server to Another Primary Server," on page 78
- Section 6.7, "Specifying a Different Repository for the Content Role Satellite (Windows Only)," on page 79
- Section 6.8, "Deleting a ZENworks Server," on page 80
- Section 6.9, "Refreshing a Satellite," on page 80

6.1 Understanding the Satellite Roles

- Section 6.1.1, "Understanding the Collection Role," on page 71
- Section 6.1.2, "Understanding the Content Role," on page 72

6.1.1 Understanding the Collection Role

If you want to improve information roll-up access for a group of devices to minimize traffic to the ZENworks Primary Server that is hosting the ZENworks database, you can enable the Collection role on a device. For example, if you have devices that are rolling up information to a Primary Server outside of their network segment, you can minimize network traffic by enabling the Collection role on a device within the network segment to accept the information from the other devices in that segment. That Collection role device is then the only device from that segment that is rolling up information to the Primary Server.

You can enable the Collection role on any managed device. The Collection role requires only the Collection role module that is installed with the ZENworks Adaptive Agent. The module is inactive until you enable the Collection role on the managed device.

When you enable a Collection role on a device, you can assign any ZENworks Primary Server as its parent server. The Collection role device uploads information to its parent Primary Server only. If the parent Primary Server is not a child of another Primary Server, it then writes the information directly to the database. If the parent Primary Server is a child of another Primary Server, it passes the information up to its parent Primary Server, which writes the information to the database.

The information that is rolled up includes device inventory information and messages (errors, warning, informational, and so forth). There is a roll-up schedule that you can edit.

6.1.2 Understanding the Content Role

Content consists ofsystem updates (ZENworks Server and Adaptive Agent).

If you want to improve content access for a group of devices without creating another Primary Server, you can create the Content role on a device. For example, if you have devices that are accessing a Primary Server outside of their network segment, you can create the Content role on a device within the network segment to service those devices.

The Content role provides the same content delivery service as a Primary Server but requires only the Content role module that is installed with the ZENworks Adaptive Agent. The module is inactive until you enable it on the managed device.

When you enable the Content role on a device, you assign a Primary Server as its parent content server. The Content role Satellite downloads content from its parent Primary Server only. Therefore, any content you want hosted on a Content role Satellite must also be hosted on its parent Primary Server.

6.2 Adding Satellites into the Server Hierarchy

Complete the following steps to add devices into the Server Hierarchy listing and configure them with Satellite roles.

NOTE: Before you can create Linux Satellites, you must install the ZENworks Agent on the devices, add them into the Server Hierarchy listing, and then configure them with Satellite roles. For more information, see "Deploying the Agent to a Linux Satellite" in the *ZENworks 10 Discovery, Deployment, and Retirement Reference*. After the ZENworks Agent is installed on the Linux device, continue with the steps in this section.

---

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

2 In the Server Hierarchy panel, select the check box next to the desired Primary Server.

You can add a Satellite under any Primary Server displayed in the listing, at any nested depth. You cannot add a Satellite to be a child of another Satellite. Only a Primary Server can be a parent of a Satellite.

3 Click *Action > Add Satellite Server*.

4 In the *Device to Promote* field, browse for and select a device (server or workstation) to be made a Satellite.

5 In the *Satellite Server Roles* section, configure the desired roles.

If the *Configure* link is disabled for any role, that role is disabled for this device. For example, if the Satellite's parent Primary Server does not have the Collection role, the Satellite's Collection role is disabled and cannot be configured. Non-configurable roles that a managed device performs are also listed in the dialog box but cannot be edited.

5a (Optional) Select the check box next to *Collection*, then click *Configure*.

This role causes the device to collect inventory information and messages (errors, warning, informational, and so forth), then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information to its parent Primary Server, which does the database writing.

The Collection Roll-Up schedule determines how often the collected inventory information is rolled up to the parent Primary Server for inclusion in the ZENworks database. When the information is in the database, it is viewable in ZENworks Control Center.

To specify the devices that use the Collection Roll-Up role, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Collection Roll-Up Schedule: Specify the number of days, hours, and minutes for how often you want the collected inventory data to be rolled up from the devices that use it as a collection server.

5b (Optional) Select the check box next to *Content*, then fill in the *Content Replication Schedule*.

This role enables the managed device to distribute content (system updates) to other devices.

When you set up a device to function with a Content role, you must specify a Primary Server as its parent. The device with the Content role receives all content from its parent Primary Server. Any content you want hosted on a Satellite with the Content role must also be hosted on its parent Primary Server. If the content is not hosted on the new Primary Server, it is added.

To specify the devices that need content from this Satellite, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Content Replication Schedule: Specify the number of days, hours, and minutes for how often you want the Satellite's content to be updated from the parent Primary Server.

6 (Optional) In the *Port for Content and/or Collection HTTP Requests* field, specify the port number.

The default port is 80. Content and Collection servers share the same Web server and the same port. Make sure that the specified port is not in use.

7 Click *OK*.

6.3 Removing Satellites from the Server Hierarchy

You can remove a Satellite from the Server Hierarchy listing when that device is no longer needed to perform Satellite functions. The device's object isn't removed from ZENworks; it is just removed from the Server Hierarchy listing. However, removing a Satellite from the hierarchy listing does cause the content, or collection roll-up information to be removed from the device.

When you remove a Satellite, the managed devices that used it must be reconfigured to use another server for content and collection purposes.

You cannot use this option to remove a Primary Server from the listing.

To remove a Satellite:

1 For the Satellite that you want to remove, make a note of all devices that are using it for their content and collection information roll-up.

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

3 In the Server Hierarchy panel, select the check box next to the Satellite that you want to remove from the zone.

4 Click *Action > Remove Satellite Server*.

Server Hierarchy					
Move Action ▾ Dev Tab ▾					
Name			Folder	Roles	Write to Database
☐ └─ 🏢 kn	Specify Content...		/Devices/Servers	All	🗄
☐ ⊟─ 🏢 Pr	Configure Satellite Server...		/Devices/Servers	All	🗄
	Add Satellite Server...				
☑ ├─ 🗗	Remove Satellite Server...		/Devices/Servers	🖥📄📁	
☐ ├─ 🗗 Satellite Server 2	Refresh Device...		/Devices/Servers	📁	
☐ ├─ 🗗 DP 1			/Devices/Servers	🖥📄📁	
☐ ├─ 🗗 DP 2			/Devices/Servers	🖥📄📁	
☐ └─ 🗗 RP 1			/Devices/Servers	📄	
☐ ⊞─ 🏢 Primary Server 2			/Devices/Servers	All	🗄

5 To confirm the removal, click *OK*.

6 As necessary, reconfigure the managed devices that used the Satellite so that they can continue to receive content and roll up collection information.

6.4 Configuring Satellites from the Server Hierarchy

You can configure a Satellite with the Content and Collection roles, change its default port, and adjust the schedules for the roles.

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

2 In the Server Hierarchy panel, select the check box next to the device that you want to configure.

You can only configure one Satellite at a time.

3 Click *Action > Configure Satellite Server*.

4 In the *Satellite Server Roles* section, configure the desired roles.

If the *Configure* link is disabled for any role, that role is disabled for this device. For example, if the Satellite's parent Primary Server does not have the Collection role, the Satellite's Collection role is disabled and cannot be configured. Non-configurable roles that a managed device performs are also listed in the dialog box but cannot be edited.

4a (Optional) Select the check box next to *Collection*, then click *Configure*.

This role causes the device to collect inventory information and messages (errors, warning, informational, and so forth), then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information to its parent Primary Server, which does the database writing.

The Collection Roll-Up schedule determines how often the collected inventory information is rolled up to the parent Primary Server for inclusion in the ZENworks database. When the information is in the database, it is viewable in ZENworks Control Center.

To specify the devices that use the Collection Roll-Up role, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Collection Roll-Up Schedule: Specify the number of days, hours, and minutes for how often you want the collected inventory data to be rolled up from the devices that use it as a collection server.

4b (Optional) Select the check box next to *Content,* then click *Configure.*

This role enables the managed device to distribute content (system updates) to other devices.

When you set up a device to function with a Content role, you must specify a Primary Server as its parent. The device with the Content role receives all content from its parent Primary Server. Any content you want hosted on a Satellite with the Content role must also be hosted on its parent Primary Server. If the content is not hosted on the new Primary Server, it is added.

To specify the devices that need content from this Satellite, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Content Replication Schedule: Specify the number of days, hours, and minutes for how often you want the Satellite's content to be updated from the parent Primary Server.

5 (Optional) In the *Port for Content and/or Collection HTTP Requests* field, specify the port number.

The default port is 80. Content and Collection servers share the same Web server and the same port. Make sure that the specified port is not in use.

6 Click *OK* to save your changes and exit the dialog box.

7 Repeat the previous steps to configure other Satellites.

6.5 Configuring Satellites from the Device View

1 In ZENworks Control Center, click the *Devices* tab, then on the *Managed* tab, click either *Servers* or *Workstations*.

2 In the Servers or Workstations panel, select the check box for the Satellite that you want to configure.

You can only configure one Satellite at a time.

3 Click *Action > Configure Satellite Server*.

4 In the Satellite Server Roles section, configure the desired roles.

If the *Configure* link is disabled for any role, that role is disabled for this device. For example, if the Satellite's parent Primary Server does not have the Collection role, the Satellite's Collection role is disabled and cannot be configured. Non-configurable roles that a managed device performs are also listed in the dialog box but cannot be edited.

4a (Optional) Select the check box next to *Collection*, then click *Configure*.

This role causes the device to collect inventory information and messages (errors, warning, informational, and so forth), then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information to its parent Primary Server, which does the database writing.

The Collection Roll-Up schedule determines how often the collected inventory information is rolled up to the parent Primary Server for inclusion in the ZENworks database. When the information is in the database, it is viewable in ZENworks Control Center.

To specify the devices that use the Collection Roll-Up role, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Collection Roll-Up Schedule: Specify the number of days, hours, and minutes for how often you want the collected inventory data to be rolled up from the devices that use it as a collection server.

4b (Optional) Select the check box next to *Content*, then click *Configure*.

This role enables the managed device to distribute content (system updates) to other devices.

When you set up a device to function with a Content role, you must specify a Primary Server as its parent. The device with the Content role receives all content from its parent Primary Server. Any content you want hosted on a Satellite with the Content role must also be hosted on its parent Primary Server. If the content is not hosted on the new Primary Server, it is added.

After you enable the Content role, the Satellite receives content that it can send to other devices in its network segment.

To specify the devices that need content from this Satellite, configure the *Closest Server Rules* setting in the *Management Zone* settings on the *Configuration* page.

Fill in the field:

Content Replication Schedule: Specify the number of days, hours, and minutes for how often you want the Satellite's content to be updated from the parent Primary Server.

5 (Optional) In the *Port for Content and/or Collection HTTP Requests* field, specify the port number.

The default port is 80. Content and Collection servers share the same Web server and the same port. Make sure that the specified port is not in use.

6 Click *OK* to confirm the changes.

If you enabled one or more roles, the Satellite's role icon is added to the Server Hierarchy panel in the *Roles* column.

Name	Folder	Roles	Write to Database
krobinson2	/Devices/Servers	All	
Primary Server 1	/Devices/Servers	All	
Satellite Server 1	/Devices/Servers		
Satellite Server 2	/Devices/Servers		
DP 1	/Devices/Servers		
DP 2	/Devices/Servers		
RP 1	/Devices/Servers		
Primary Server 2	/Devices/Servers	All	

Icon	Description
	Indicates a Satellite with the Collection role. With this role, the device collects inventory information and messages (errors, warning, informational, and so forth), then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information to its parent Primary Server, which does the database writing.
	Indicates a Satellite with the Content role. With this role, the device can distribute system updates to other devices. When you set up a device to function with a Content role, you must specify a Primary Server as its parent. The device with the Content role receives all content from its parent Primary Server.

If you disabled a role, the Satellite's role icon is removed from the Server Hierarchy panel. If the Satellite had only one role and you removed it, that device is no longer listed in the Hierarchy panel. Its Satellite functionality is no longer available, and its content, imaging, or collection roll-up information is removed from the device.

7 (Optional) If you disabled all of the Satellite's roles, reconfigure the devices that were dependent on its roles to recognize a different server with those functions.

6.6 Moving a Satellite from One Primary Server to Another Primary Server

You can move a Satellite from its parent Primary Server to another Primary Server.

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

2 In the Server Hierarchy panel, select the check box next to the Satellite that you want to move, then click *Move*.

3 Select the Primary Server you want to be the Satellite's new parent, then click *OK*.

6.7 Specifying a Different Repository for the Content Role Satellite (Windows Only)

The content repository is located in the following default path on Windows Satellites:

installation_path\zenworks\work\content-repo

To change the default path to another location accessible to the server:

1 Make sure that the disk drive you want to use is attached to the Satellite and is properly formatted.

You do not need to specify a drive letter, but the server must recognize the hardware.

2 Make sure that there is no content in the default location (*installation_path*\zenworks\work\content-repo) by doing one of the following:

- ◆ If the content-repo directory is not present in the path given above, create the content-repo directory in that path.

- ◆ If you need to save the content that is now in this directory, rename the existing directory and create a new empty directory named content-repo.

 You can later copy the content from the renamed directory to the new content repository location (see Step 9).

- ◆ If you do not need any of the content in the existing content-repo directory, delete the directory and re-create the content-repo directory.

An empty content-repo directory must exist to act as the pointer to the new content repository location for the Satellite.

3 Click *Start*, right-click the *My Computer* icon, then select *Manage*.

You can also click *Start*, then enter compmgmt.msc at the *Run* command line.

4 Select *Disk Management* under the *Storage* section in the left pane.

The disk drive you selected in Step 1 should be displayed.

5 Right-click the partition of the disk drive that you want to use as your content repository on the Satellite, then select *Change Driver Letter and Paths*.

This is the disk drive (see Step 1) that you will mount to the content-repo directory.

6 Click *Add*.

This displays the Add Drive Letter or Path dialog box.

7 Select *Mount in the Following Empty NTFS Folder*, then browse for and select the content-repo directory:

installation_path\zenworks\work\content-repo

8 Click *OK* as necessary to exit and save the configuration change.

9 If necessary (see Step 2), move the files from the old renamed content-repo directory to the new content-repo directory.

This copies the files to the hard drive that you have selected for your new content repository.

6.8 Deleting a ZENworks Server

You can completely remove any ZENworks Server from the Management Zone that is listed in the Server Hierarchy panel. This includes removing the server from the listing, deactivating it from the zone, and changing the server's status to `Retired` in the Deleted Servers folder in ZCC. This action cannot be recovered. You would need to reinstall the ZENworks Server.

For more information about deleting a Primary Server, see .

1 In ZCC, click the Configuration tab, in the Server Hierarchy section, select the check box in front of the ZENworks Server that you want to delete.

2 Click *Action > Delete ZENworks Server*.

3 Confirm that you want to completely delete the server, then click *OK*.

6.9 Refreshing a Satellite

You can refresh a device so that any pending actions immediately take place.

1 Select the check box in front of the Satellite Server that you want to refresh.

2 Click *Action > Refresh Device*.

The QuickTask Status box is displayed while the action is in progress.

3 (Optional) To close the status dialog box, click *Hide*.

The refresh action continues in the background.

4 (Optional) To cancel the refresh action, click the check box for the device, click *Stop*, then click *Hide* to close the dialog box.

Server Hierarchy

7

Your Management Zone's server hierarchy determines the relationships among the ZENworks® Primary Servers and Satellites. These relationships control the flow of content and information within the zone. Proper configuration can help you to minimize network traffic between network segments connected by slow links.

7.1 Primary Servers: Peer Versus Parent/Child Relationships

By default, each Primary Server that you add to the system is created as a peer to all other Primary Servers. Being in a peer relationship enables a Primary Server to:

- Have direct write access to the ZENworks database so that it can add information (inventory, messages, and status).
- Retrieve device configuration information directly from the database.
- Pull content (system updates) from any Primary Server.

Direct write access to the ZENworks database requires a JDBC*/ODBC connection. If a Primary Server is located on the network so that it cannot effectively access the ZENworks database via a JDBC/ODBC connection, you can configure the Primary Server to be a child of another Primary Server that does have direct write access to the database. However, you should try to maintain peer relationships between your Primary Servers unless your network connections do not allow it.

Being in a child relationship instructs a Primary Server to use HTTP to roll up inventory, message, and status information to its parent Primary Server, which then writes the information to the database. However, the child Primary Server still retrieves configuration information from the database and passes configuration information back up to the database. For this reason, the child Primary Server must have a direct connection to the ZENworks database.

We do not recommend having a Primary Server across a WAN link from the ZENworks database because this causes increased traffic across the network. We recommend that you use a Satellite device across a WAN link. For more information, see Section 7.2, "Satellite Role Relationships," on page 81.

7.2 Satellite Role Relationships

A Satellite is a device that can perform certain roles that a ZENworks Primary Server normally performs. A Satellite can be any managed Windows device (server or workstation), but not a Primary Server. A Satellite can also be an unmanaged Linux device (server or workstation). When you configure a Satellite, you specify which roles it performs (Collection or Content). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks 10 Asset Management framework. For more information about the tasks you can perform on Satellites, see Chapter 6, "Satellites," on page 71.

The following sections contain more information:

7.2.1 Content Role Server Relationships

A Content role identifies a managed device that is able to distribute content (system updates) to other devices. When you set up a device to function with a Content role, you must specify a Primary Server as its parent. The device with the Content role receives all content from its parent Primary Server.

7.2.2 Collection Role Server Relationships

A Collection role causes a managed device to collect inventory information and messages (errors, warning, informational, and so forth), then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information on to its parent Primary Server, which does the database writing.

7.3 Changing the Parent-Child Relationships of Primary Servers

You can move a Primary Server to be a peer or child of other Primary Servers:

7.3.1 Making a Primary Server a Child

You can place a Primary Server as a child of another Primary Server. This child Primary Server no longer writes collection data directly to the ZENworks database; instead, it passes its information on to its parent Primary Server, which does the database writing. However, the child Primary Server still retrieves configuration information from the database and passes configuration information back up to the database. For this reason, the child Primary Server must have a direct connection to the ZENworks database

To make a Primary Server a child of another server:

1 In ZENworks Control Center, click the *Configuration* tab.
2 In the Server Hierarchy panel, select the check box next to the Primary Server you want to make a child.
3 Click *Move* to display the *Move Device* dialog box.
4 Select the Primary Server that you want to be its parent server.
5 Click *OK*.

7.3.2 Making a Primary Server a Peer

This places the Primary Server back to the first level of the hierarchy, or moves it to be a child of another Primary Server if it is nested more than one level deep.

If you move a Primary Server back to the first level, it writes directly to the ZENworks database.

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

2 In the Server Hierarchy panel, select the check box next to the Primary Server you want to make a peer.

3 Click *Move* to display the *Move Device* dialog box.

4 Do one of the following:

   ◆ Select *None* to move it up to the first level of servers in the listing.

   ◆ Select another Primary Server to be the parent server.

5 Click *OK*.

Closest Server Rules

<div align="right" style="font-size:4em">8</div>

When you have multiple ZENworks Servers (Primary Servers and Satellites) in your environment, you can use Closest Server rules to determine which ZENworks Server a managed device contacts to perform the following functions:

- Collection
- Content
- Configuration

Closest Server rules help you improve load balancing between ZENworks Servers, perform failover, and improve performance when there is a slow link between the managed devices and Servers.

The Closest Server rules let you map devices to ZENworks Servers based on network addresses (DNS names and IP addresses).

For example, you can create a rule that maps all devices to Server1 that fall within the IP address range of 123.45.67.1 to 123.45.67.100.

The following sections provide information and instructions for setting up Closest Server rules:

8.1 Understanding Closest Server Rules

When your ZENworks Management Zone includes more than one server (Primary Servers and Satellites), devices need to know which server to contact. The Closest Server Rules panel lets you create rules to determine which servers a device contacts.

With respect to Closest Server rules, devices that are configured as Satellites are considered as servers and can be listed for selection in the *Collection Servers* and *Content Servers* lists.

The following sections provide information you should understand before you start creating Closest Server rules:

8.1.1 ZENworks Server Functions

There following are basic functions for which devices contact a server:

- **Collection:** Inventory and message log information is collected from each device, to be viewed in ZENworks Control Center and output to reports. Each ZENworks Primary Server and any Satellite can act as a collection server.

- **Content:** Content is provided to managed devices. Each ZENworks Primary Server and any Satellite can act as a content server.
- **Configuration:** Configuration settings and registration information are applied to devices. Only ZENworks Primary Servers can act as configuration servers.

A device can contact the same server for all functions, or it can contact different servers for each function.

8.1.2 Mapping Devices to Servers

A Closest Server rule maps devices with specific network addresses to the following lists:

- *Collection Server* list
- *Content Server* list
- *Configuration Server* list

For example, assume that you want to create a rule for devices that fall within the IP address range of 123.45.678.1 to 123.45.678.100. You specify the IP address range, then create the following lists:

Collection Server List	Content Server List	Configuration Server List
Server 1	Server 3	Server 1
Server 2	Server 1	Server 3
Server 3		Server 2

Based on the lists, any device whose IP address falls within the range contacts Server 1 for collection, Server 3 for content, and Server 1 for configuration. If any of these servers are unavailable, the device contacts the next server in the list.

8.1.3 Effective Rules

You can configure Closest Server rules at three levels:

- **Management Zone:** The rules are inherited by all device folders and devices.
- **Device Folder:** The rules are inherited by all devices contained within the folder or its subfolders. They override the Management Zone settings.
- **Device:** The rules apply only to the device for which they are configured. They override the settings set at the Management Zone and folder levels.

Each device can have only one Closest Server rule applied to it. A device's effective rule is determined as follows:

1. **Device Settings:** Evaluate all rules that are set on the device. If the device meets a rule's criteria, that rule becomes the device's effective rule.
2. **Folder settings:** If no device rule applies, evaluate all rules that are set on the device's parent folder. If the device meets a rule's criteria, that rule becomes the device's effective rule. If not, evaluate the rules on the next folder up in the hierarchy.

3. **Management Zone:** If no folder rule applies, evaluate all rules that are set in the Management Zone. If the device meets a rule's criteria, that rule becomes the device's effective rule. If not, apply the Default rule to the device.

4. **Default Rule:** If no device, folder, or Management Zone rule applies, apply the default rule to the device. The Default rule is simply a listing of all content servers in the order you want devices to contact them.

8.2 Configuring the Closest Server Default Rule

The Closest Server Default rule lets you define the rule that is used by a device to determine the closest collection, content, and configuration servers when no Closest Server rules have been defined or when none apply. This rule is simply a listing of the servers in the order you want devices to contact them. You cannot add or remove servers from the lists.

For Closest Server Default rules, devices that are Satellites are considered as servers and can be listed for selection in the appropriate lists.

By default, all ZENworks Servers function as collection, content, and configuration servers and are displayed in the appropriate lists. In addition, any devices that are defined with the Content or Imaging roles are also displayed in the Content Servers list, and any devices that are defined with the Collection role are also displayed in the Collection Servers list.

To configure a Closest Server Default rule:

1 In ZENworks Control Center, click the *Configuration* tab, click *Infrastructure Management* (in the Management Zone Settings panel), then click *Closest Server Default Rule*.

Configuration > Closest Server Default Rule

Closest Server Default Rule	✕
Configure the setting for how managed devices determine their closest server using the default rule.	

Collection Servers:

Move Up Move Down Groups ▾ L4 Switch ▾

Name
☐ ∟ /Devices/Servers/msorensen5

Content Servers:

Move Up Move Down Groups ▾ L4 Switch ▾

Name
☐ ∟ /Devices/Servers/msorensen5

Configuration Servers:

Move Up Move Down Groups ▾ L4 Switch ▾

Name
☐ ∟ /Devices/Servers/msorensen5

OK   Apply   Reset   Cancel

2 To configure the servers listed in the any section, do any of the following:

Task	Steps	Additional Details
Copy an existing group	1. In one of the role section listings, click *Groups > Copy Existing Group*. 2. Select a group from the drop-down list, then click *OK*. 3. Click *Apply* to make the change effective.	When you copy an existing group, it retains its group name and some of its members. For a member to be retained in the copied group, it must already have the role assigned to it that matches the role for the copied group's new section.
Create an empty group	1. In one of the role section listings, click *Groups > Create Empty Group*. You can add members to it later by using the *Groups > Add to Group* option. 2. Specify a name, click *OK*. 3. Click *Apply* to make the change effective.	The created group displays only in the role section where it is created.
Create a group from the selected servers	1. In one of the role section listings, select the check boxes for one or more servers. 2. Click *Groups > Create Group from Selection*. 3. Specify a group name, then click *OK*. 4. Click *Apply* to make the change effective.	Servers can be members of multiple groups and L4 switch definitions. Servers that are members of a group or L4 switch definition are no longer listed at the top level of the server listing.
Remove a group	1. In one of the role section listings, select the check boxes for one or more groups. 2. Click *Groups > Remove Group*, then click *OK*. 3. Click *Apply* to make the change effective.	When you remove a group, servers that were previously added to a role section's listing are retained. This is automatically done by moving members that are not members of another group or L4 switch definition in the role section listing to the top level of the listing.

Task	Steps	Additional Details
Add servers to a group	1. In one of the role section listings, select the check boxes for one or more servers. 2. Click *Groups > Add to Group*. 3. Do one of the following: ◆ To add the selected servers to a new group, select *Create New* and specify a group name, then click *OK*. ◆ To add the selected servers to an existing group, select a group from the drop-down list in the *Select Existing* field, then click *OK*. 4. Click *Apply* to make the change effective.	Servers can be members of multiple groups and L4 switch definitions. Servers that are members of a group are no longer listed at the top level of the server listing.
Remove servers from a group	1. In one of the role section listings, select the check boxes for one or more servers that are listed under the group. 2. Click *Groups > Remove from Group*, then click *OK*. 3. Click *Apply* to make the change effective.	In order to retain servers that were previously added to a role section's listing, this places the removed servers back at the top level of the listing, unless they are a member of another group or L4 switch definition in that listing.
Create an empty L4 switch definition	1. In one of the role section listings, click *L4 Switch > Create Empty L4 Switch Definition*. 2. Specify an L4 switch definition name, then click *OK*. **IMPORTANT:** The L4 switch definition name must be either the DNS name or IP address of the L4 switch itself. 3. Click *Apply* to make the change effective.	The L4 switch definition is displayed in each of the listings, no matter where it is created.

Task	Steps	Additional Details
Create an L4 switch definition from selected servers	1. In one of the role section listings, select the check boxes for one or more servers. 2. Click *L4 Switch > Create L4 Switch Definition from Selection*. 3. Specify an L4 switch definition name, then click *OK*. **IMPORTANT:** The L4 switch definition name must be either the DNS name or IP address of the L4 switch itself. 4. Click *Apply* to make the change effective.	The created L4 switch definition is displayed in each of the listings, no matter where it is created, with the selected servers listed under each instance of the L4 switch definition. Servers can be members of multiple groups and L4 switch definitions. Servers that are members of an L4 switch definition or group are no longer listed at the top level of the server listing.
Remove an L4 switch definition	1. In one of the role section listings, click *L4 Switch > Remove L4 Switch Definition*, then click *OK*. 2. Click *Apply* to make the change effective.	Removing an L4 switch definition from one role section removes it from the other role sections. When you remove an L4 switch definition, servers that were previously added to a role section's listing are retained. This is automatically done by moving members that are not members of another group or L4 switch definition in the role section listing to the top level of the listing.

Task	Steps	Additional Details

Add servers to an L4 switch definition	1. In one of the role section listings, select the check boxes for one or more servers.
	
	2. Click *L4 Switch > Add to L4 Switch Definition*.
	
	3. Do one of the following:
	
	   ◆ To add the selected servers to a new L4 switch definition, select *Create New* and specify an L4 switch definition name, then click *OK*.
	
	   IMPORTANT: The L4 switch definition name must be either the DNS name or IP address of the L4 switch itself.
	
	   ◆ To add the selected servers to an existing L4 switch definition, select an L4 switch definition from the drop-down list in the *Select Existing* field, then click *OK*.
	
	4. Click *Apply* to make the change effective.
		Servers can be members of multiple groups and L4 switch definitions.
		
		Servers that are members of an L4 switch definition are no longer listed at the top level of the server listing.

Remove servers from an L4 switch definition	1. In one of the role section listings, select the check boxes for one or more servers that are listed under the L4 switch definition. 2. Click *L4 Switch > Remove from L4 Switch Definition*, then click *OK*. 3. Click *Apply* to make the change effective.	In order to retain servers that were previously added to a role section's listing, this places the removed servers back at the top level of the listing, unless they are a member of another group or L4 switch definition in that listing.

3 Use the *Move Up* and *Move Down* buttons to determine the order devices should use to contact the servers.

4 When you are finished reordering the servers, click *OK* or *Apply* to save the changes.

8.3 Creating Closest Server Rules
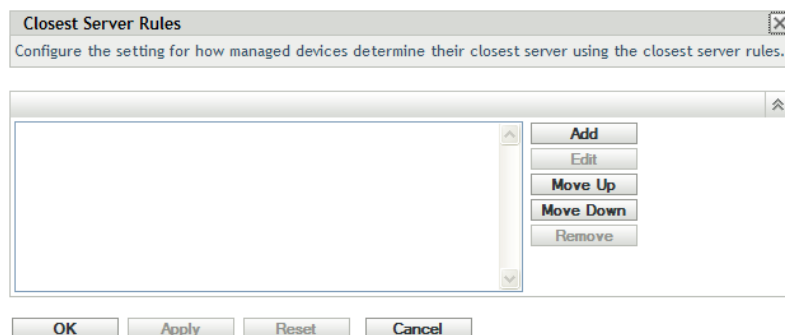
1 Launch ZENworks Control Center.

2 Do one of the following:

   ◆ To create a Closest Server rule for your Management Zone, click the *Configuration* tab, then click *Infrastructure Management* (in the Management Zone Settings panel) > *Closest Server Rules*.

- To create a Closest Server rule for a device folder, open the folder's details page, then click *Settings > Infrastructure Management* (in the Settings panel) > *Closest Server Rules*.
- To create a Closest Server rule for a device, open the device's details page, then click *Settings > Infrastructure Management* (in the Settings panel) > *Closest Server Rules*.

Configuration > Closest Server Rules

Closest Server Rules ⊠
Configure the setting for how managed devices determine their closest server using the closest server rules.

Add
Edit
Move Up
Move Down
Remove

OK   Apply   Reset   Cancel

3 Conditional: If you are creating Closest Server rules on a device or device folder, click *Override settings* to activate the Closest Server Rules panel.

The *Override* option (not depicted) displays only at the device and device folder levels.

4 Click *Add* to display the Rule Construction dialog box:

Rule Construction ? ⊠

Rule Name:* [   ]   ☐ Exclude the Closest Server Default Rule
Rule Logic:

Add Filter   Insert Filter ▾   Delete

☐ [▾] [--Select-- ▾]

Collection Servers:
Move Up Move Down Add Remove Groups ▾ L4 Switch ▾
Name

Content Servers:
Move Up Move Down Add Remove Groups ▾ L4 Switch ▾
Name

Configuration Servers:
Move Up Move Down Add Remove Groups ▾ L4 Switch ▾
Name

Fields marked with an asterisk are required.
OK   Cancel

5 In the *Rule Name* field, specify a name for the rule.

The name displays in the Closest Server Rules listing in ZENworks Control Center. To access this listing, click *Configuration* in the left pane, click the *Configuration* tab, click the *Management Zone Settings* panel to open it, click the *Infrastructure Management* section to open it, then click *Closest Server Rules*. All defined rules for the current level are displayed there.

6 If you do not want to append the Closest Server Default rule to the servers you are listing in this Closest Server rule, select the *Exclude the Closest Server Default Rule* check box.

The Closest Server rules feature first uses the servers specified in the rule, then proceeds to any other servers listed in the Closest Server Default rule if the specified servers are not available to the managed device. Therefore, to obtain content only from the servers specified in the rule, select this check box to exclude all other servers.

7 Use the *Rule Logic* fields to create the rule expression.

An expression consists of a criteria option, operator, and value. For example:

```
DNS Name Filter equal to *.novell.com
```

`DNS Name Filter` is the criteria option, `equal to` is the operator, and `*.novell.com` is the value. In the above example, the Closest Server rule is applied only to devices whose DNS name ends with `.novell.com`.

If necessary, you can use NOT to perform a logical negation of the expression. For example:

```
NOT DNS Name Filter equal to *.novell.com
```

In the above example, the Closest Server rule is applied only to devices whose DNS name does not end with `.novell.com`.

You can use more than one expression for the rule. For example:

```
DNS Name Filter equal to provo.novell.com or IP Address equal to
123.45.678.12/24
```

You can use the following criteria:

Option	Explanation
DNS Name Filter	Matches DNS names that meet the filter criteria. You can specify an exact filter or use a question mark (?) or an asterisk (*) as a wildcard to match one or more characters in the DNS name. A ? matches one character and an * matches one or more characters. Examples: provo.novell.com: Matches all devices in the provo subdomain of the novell.com top-level domain. *.novell.com: Matches all devices in the novell.com top-level domain, including any devices in subdomains. provo?.novell.com: Matches all devices in the provo1 and provo 2 subdomains of the novell.com top-level domain; does not match devices in the provo12 subdomain.

Option	Explanation
IP Address /n	Matches IP addresses that fall within the specified CIDR (Classless Inter-Domain Routing) block. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. Examples: 123.45.678.12/16: Matches all IP addresses that start with 123.45. 123.45.678.12/24: Matches all IP addresses that start with 123.45.678.

8 To configure the servers listed in any section, do any of the following:

Task	Steps	Additional Details
Add members to a servers list	1. In one of the role section listings, click *Add*. 2. Browse for and select one or more servers. You can add Primary Servers and Satellites. 3. Click *OK* to add the selected servers to the list.	The selected servers are added only into the list where you clicked *Add*. You can have different servers in each list. Primary Servers and Satellites with the assigned role are automatically included in the lists for the Closest Server Default rule.

Reorder the servers	1. In one of the role section listings, select the check box for one of the servers.
	
	2. Click *Move Up* or *Move Down* as necessary to change its order in the list.
	
	3. Repeat as necessary for the other servers listed.
		Determines the order devices should use to contact the servers.
		
		You can order the servers differently in the lists. This allows you to spread the workload by placing different servers higher in one list than in the other two lists. For example:
		
		◆ **Collection Servers:**
		   Server1, Server2, Server3
		
		◆ **Content Servers:**
		   Server2, Server3, Server1
		
		◆ **Configuration Servers:**
		   Server3, Server1, Server2

Copy an existing group	1. In one of the role section listings, click *Groups > Copy Existing Group*. 2. Select a group from the drop-down list, then click *OK*. 3. Click *Apply* to make the change effective.	When you copy an existing group, it retains its group name and some of its members. For a member to be retained in the copied group, it must already have the role assigned to it that matches the role for the copied group's new section.

Task	Steps	Additional Details
Create an empty group	1. In one of the role section listings, click *Groups > Create Empty Group*. You can add members to it later by using the *Groups > Add to Group* option. 2. Click *Apply* to make the change effective.	The created group displays only in the role section where it is created.
Create a group from the selected servers	1. In one of the role section listings, select the check boxes for one or more servers. 2. Click *Groups > Create Group from Selection*. 3. Specify a group name, then click *OK*. 4. Click *Apply* to make the change effective.	Servers can be members of multiple groups and L4 switch definitions. Servers that are members of a group or L4 switch definition are no longer listed at the top level of the server listing.
Remove a group	1. In one of the role section listings, select the check boxes for one or more groups. 2. Click *Groups > Remove Group*, then click *OK*. 3. Click *Apply* to make the change effective.	When you remove a group, servers that were previously added to a role section's listing are retained. This is automatically done by moving members that are not members of another group or L4 switch definition in the role section listing to the top level of the listing.
Add servers to a group	1. In one of the role section listings, select the check boxes for one or more servers. 2. Click *Groups > Add to Group*. 3. Do one of the following: ◆ To add the selected servers to a new group, select *Create New* and specify a group name, then click *OK*. ◆ To add the selected servers to an existing group, select a group from the drop-down list in the *Select Existing* field, then click *OK*. 4. Click *Apply* to make the change effective.	Servers can be members of multiple groups and L4 switch definitions. Servers that are members of a group are no longer listed at the top level of the server listing.

Task	Steps	Additional Details
Remove servers from a group	1. In one of the role section listings, select the check boxes for one or more servers that are listed under the group. 2. Click *Groups > Remove from Group*, then click *OK*. 3. Click *Apply* to make the change effective.	In order to retain servers that were previously added to a role section's listing, this places the removed servers back at the top level of the listing, unless they are a member of another group or L4 switch definition in that listing.
Create an L4 switch definition		This option is not used in the Rule Construction dialog box.
Remove an L4 switch	1. In one of the role section listings, click *L4 Switch > Remove L4 Switch*, then click *OK*. 2. Click *Apply* to make the change effective.	Removing an L4 switch definition from one role section removes it from the other role sections on the dialog box. Removing an L4 switch definition in the Rule Construction dialog box does not remove the definition from the Closest Servers Default Rule page. When you remove an L4 switch definition, servers that were previously added to a role section's listing are retained. This is automatically done by moving members that are not members of another group or L4 switch definition in the role section listing to the top level of the listing.
Add an L4 switch	1. In one of the role section listings, click *L4 Switch > Add L4 Switch*, select an existing switch from the drop-down list, then click *OK*. 2. Click *Apply* to make the change effective.	Allows you to select an existing L4 switch definition from those displayed on the Closest Server Default Rule page.

9 Use the *Move Up* and *Move Down* buttons to determine the order devices should use to contact the servers.

The order in which the ZENworks Servers are listed is the order in which a device contacts them. If the first ZENworks Server is not available, the second server is contacted, and so on.

10 When you are finished, click *OK* to add the rule to the *Closest Server Rules* list.

11 Repeat Step 2 through Step 10 to create additional rules.

12 If necessary, when you are finished creating rules, use the *Move Up* and *Move Down* buttons to reorder the rules in the *Closest Server Rules* list.

The rules are evaluated in the order they are listed. You should place the rules in the order you want them evaluated.

8.4 Backing Up Closest Server Rules

If your ZENworks Management Zone has complex Closest Server rules configured, you might want to export these rules as part of your backup procedure.

The following zman commands are useful when backing up Closest Server rules:

- **location-copy-rules (loccp):** Copies Closest Server rules data from a source device or device folder to one or more destination devices or device folders.

- **location-export-rules-to-file (loctf):** Exports Closest Server rules data (in XML format) to a file. The XML file can be used as input for creating or appending to the Closest Server rules.

- **location-import-rules-from-file (locff):** Imports Closest Server rules data (in XML format) from a file.

For more information about these commands and their usage, see "Location Rules Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

ZENworks Adaptive Agent

9

The ZENworks® Adaptive Agent is part of the Novell® ZENworks 10 Asset Management software that lets you manage devices over the network. The ZENworks Adaptive Agent, commonly referred to as the Adaptive Agent, provides services that do the following without requiring you to visit individual devices:

- Deliver system updates to devices.
- Take inventory of device hardware and software.
- Act as a Satellite to help distribute content and collect inventory and device messages.

Each of these services is provided through the use of modules that plug in to the Adaptive Agent. Using ZENworks Control Center, you can configure which modules are active on devices, thus controlling which services are available on those devices. You can also configure a variety of other Adaptive Agent settings.

The following sections contain more information:

- Section 9.1, "Viewing the Version of the Adaptive Agent Software and Modules on a Device," on page 99
- Section 9.2, "Searching for Devices that Have a Specified Version of the Adaptive Agent," on page 100
- Section 9.3, "Configuring Adaptive Agent Settings after Deployment," on page 100
- Section 9.4, "Troubleshooting the Adaptive Agent," on page 104

9.1 Viewing the Version of the Adaptive Agent Software and Modules on a Device

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

2. Click *Servers* to view the Adaptive Agent software version on a server.

   or

   Click *Workstations* to view the Adaptive Agent software version on a workstation.

3. Click the underlined link for the desired device.

4. In the General section, view the version in the *ZENworks Agent Version* row.

5. (Optional) Click the underlined version number to display a list of the ZENworks Agent modules that are installed on the device, along with their version numbers.

   You can uninstall, enable, or disable the ZENworks modules by using the ZENworks Agent settings on the device's Settings page. For more information, see "Agent Features" on page 103.

9.2 Searching for Devices that Have a Specified Version of the Adaptive Agent

For upgrading or troubleshooting purposes, you can use the Advanced Search feature to display a list of devices in your ZENworks Management Zone that have a specified version of the Adaptive Agent software installed.

1 Depending on whether you want to search for all devices (servers and workstations), for servers, or for workstations that have the specified version of the Adaptive Agent installed, do one of the following in ZENworks Control Center:

  ◆ To search for all devices, click the *Devices* tab.

  ◆ To search for all servers, click the *Devices* tab > *Servers*.

  ◆ To search for all workstations, click the *Devices* tab > *Workstations*.

2 In the Search section, click *Advanced Search*.

3 Click *Add* to display the Search Criteria dialog box.

4 Click *Add Filter*, click *Device/AgentVersion* from the drop-down list, then click *OK*.

9.3 Configuring Adaptive Agent Settings after Deployment

By default, the ZENworks Adaptive Agent is deployed with the features selected at the Management Zone level in the Agent Features panel of ZENworks Control Center. For more information on how to customize the agent features during deployment, see "Customizing Features before Deployment". After the deployment, you can choose to uninstall, enable or disable the Adaptive Agent features, configure the agent's cache, set retry settings, and select whether to let users uninstall the agent.

You can configure settings at three levels:

  ◆ **Management Zone:** The setting applies to all devices in the Management Zone.

  ◆ **Device Folder:** The setting applies to all devices contained within the folder or its subfolders. It overrides the Management Zone setting.

  ◆ **Device:** The setting applies only to the device for which it is configured. It overrides the settings established at the Management Zone and folder levels.

The following sections contain more information:

9.3.1 Configuring Agent Settings on the Management Zone Level

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

2 In the *Management Zone Settings* panel, click *Device Management*.

| Configuration | Registration | System Information | Asset Inventory | Asset Management | System Updates |

Management Zone Settings

Device Management

Category	Description
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.
Device Refresh Schedule	Configure the device refresh interval.
ZENworks Agent	ZENworks Agent Configuration.
Registration	Configure registration settings.
System Variables	Configure system variables.
Primary User	Configure the setting for how the primary user is determined.
Primary Workstation	Configure the setting for how the primary workstation is determined.
Dynamic Group Refresh Schedule	Configure dynamic group refresh schedule.
Wake-on-LAN	Configure the Wake-on-LAN settings

Discovery and Deployment

Event and Messaging

Infrastructure Management

Inventory

Reporting Services

Asset Management

3 Click *ZENworks Agent*.

4 Fill in the fields. For more information, see Section 9.3.4, "ZENworks Agent Settings," on page 101.

5 Click *OK* to apply the changes.

9.3.2 Configuring Agent Settings on the Device Folder Level

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

2 Click the *Servers* or *Workstations* folder.

3 Click *Details* next to the folder for which you want to configure settings.

4 Click the *Settings* tab, click *Device Management*, then click *ZENworks Agent*.

5 Fill in the fields. For more information, see Section 9.3.4, "ZENworks Agent Settings," on page 101.

6 Click *OK* to apply the changes.

9.3.3 Configuring Agent Settings on the Device Level

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

2 Click the *Servers* or *Workstations* folder.

3 Click the device for which you want to configure settings.

4 Click the *Settings* tab, click *Device Management*, then click *ZENworks Agent*.

5 Fill in the fields. For more information, see Section 9.3.4, "ZENworks Agent Settings," on page 101.

6 Click *OK* to apply the changes.

9.3.4 ZENworks Agent Settings

- "General" on page 102
- "Agent Features" on page 103

General

You can configure the ZENworks Adaptive Agent's cache, whether or not users can uninstall the Adaptive Agent, and set retry settings.

If you are configuring the ZENworks Agent settings on a device folder or a device, click *Override settings*.

The following settings can be configured:

- **Allow Users to Uninstall Agent:** Enable this option if you want users to be able to uninstall the ZENworks Adaptive Agent. This option is applicable only for the local uninstallation.

- **Cache Life:** The ZENworks Adaptive Agent's cache directory contains content data used by the agent. Each piece of data, referred to as a cache entry, is stored in the cache database.

  When a cache entry is added to the cache database, it is assigned a creation time and an expiration time. The creation time is simply the time it was added to the database. The expiration time is the creation time plus the number of hours specified by the *Cache Life* setting (by default, 336 hours or 14 days). For example, suppose that a cache entry is added on June 10 at 3:00 p.m. With the default *Cache Life* setting, the expiration time is set to June 24 at 3:00 p.m.

  The agent does not attempt to update a cache entry until after the entry's expiration time. At that point, the agent updates the cache entry the next time it contacts the ZENworks Server to refresh its information.

  NOTE: Updates to expired cache entries occur only for cache entries that are content-related. Updates to cache entries that are event-related only occur at the time the event takes place on the device.

  A higher *Cache Life* setting reduces the traffic load on your network because cache entries are refreshed less frequently. A lower setting provides newer information but increases the traffic load.

  This setting affects only how often the agent requests updates to a cache entry. Cache entries can also be updated before their expiration time if information is changed in ZENworks Control Center that causes the information to be pushed from the ZENworks Server to the agent.

- **Cache Orphaning Threshold:** Over a period of time, it is possible for entries to be inserted in the cache database but not removed. This can cause the cache to grow unnecessarily.

  An orphan is an entry that is inserted into the cache but not accessed within the number of days specified by the *Cache Orphaning Threshold* setting. For example, suppose that a cache entry is accessed on July 1 at 10:00 a.m. Without the default *Cache Orphaning Threshold* setting (30 days), the entry becomes an orphan if it is not accessed again before July 31 at 10:00 a.m.

  A higher *Cache Orphaning Threshold* setting ensures that infrequently accessed information is not removed from the cache database. A lower setting can reduce the cache size.

- **Times to Retry Requests to a Busy Server:** Lets you specify the number of times that the agent retries a request to a busy server before considering the server as bad instead of busy.

  The default value is 15. The maximum value that you can specify is 20.

◆ **Initial Retry Request Wait:** The *Initial Retry Request Wait* setting lets you specify the initial amount of time that the agent waits before retrying a Web service request after receiving a busy response from the server. The wait time increases by one second with every busy response. The default setting is four seconds. The maximum value that you can set is ten seconds. Each subsequent request is incremented by one second.

For example, suppose that you leave this setting at the default (four seconds). After receiving a busy response from the server, the agent waits four seconds for the first retry attempt. If the server is still busy, the agent waits five additional seconds (4 + 1) before making the second retry attempt. The third retry attempt is 15 seconds after the initial retry attempt (4 + 5 + 6). The time increments until the value specified in the *Maximum Retry Request Wait* setting is reached. The retry attempts stop when the value specified in the *Times to Retry Requests to a Busy Server* setting is reached.

◆ **Maximum Retry Request Wait:** Lets you specify the maximum amount of time to wait before retrying a Web service request after receiving a busy response from the server.

The default setting is 16 seconds. The maximum value that you can specify is 20 seconds.

Agent Features

The ZENworks Adaptive Agent uses modules to perform the following functions on managed devices:

◆ Asset Management

◆ User Management

If you are viewing the properties of a Windows 2000 device, the User Management options are disabled because user management cannot be disabled or uninstalled from Windows 2000 devices. If you are viewing the properties of the Management Zone or a folder, user management settings are ignored for Windows 2000 devices.

NOTE: You can use ZENworks 10 Asset Management with ZENworks 7 Desktop Management installed in your environment.

If you enable any Agent feature besides Asset Management, and you are running ZENworks 7 Desktop Management in your environment, you are prompted that the ZENworks 7 Desktop Management Agent will be uninstalled.

Ensure that you enable only the Asset Management feature if you want to use ZENworks 10 Asset Management and you want to continue using ZENworks 7 Desktop Management in your environment.

By default, all modules are installed on a device. However, you can uninstall any of the modules. You can also disable (or enable) any of the installed modules.

You can install, uninstall, enable or disable the modules at three levels:

◆ **Management Zone:** The setting applies to all devices in the Management Zone.

◆ **Device Folder:** The setting applies to all devices contained within the folder or its subfolders. It overrides the Management Zone setting.

◆ **Device:** The setting applies only to the device for which it is configured. It overrides the settings established at the Management Zone and folder levels.

To modify a module's state:

1 (Conditional) If you are configuring the ZENworks Agent settings on a device folder or a device, click *Override settings*.

2 To install a module, select the *Installed* check box.

or

To uninstall a module, deselect the *Installed* check box.

By default, the *Installed* check boxes for all modules are selected, meaning that all modules are installed on devices when they register to your ZENworks Management Zone. If you deselect a module's *Installed* check box, that module is uninstalled from the device the next time it refreshes.

3 To enable an installed module, click the *Enabled* button.

or

To disable an installed module, click the *Disabled* button.

By default, the *Enabled* option for all installed modules is selected, meaning that all modules are enabled on devices. Disabling a module does not cause that module to be uninstalled from currently managed devices. The module remains installed on the device, but it is disabled.

4 Specify the reboot behavior if a reboot is required.

This option applies only when installing or uninstalling a module. In some cases, Windows Installer might require a reboot of the device when installing or uninstalling the module. If a reboot is required during install, the module does not function until the reboot occurs. If a reboot is required during uninstall, the module's files are not completely removed until a reboot occurs, but the module stops functioning.

◆ *Prompt user to reboot (Default)*: The user is prompted to reboot the device. The user can reboot immediately or wait until later.

◆ *Do not reboot device*: No reboot occurs. The user must initiate a reboot.

◆ *Force device to reboot*: The device is automatically rebooted. The user is notified that the device will reboot in 5 minutes.

5 Click *Apply* to save the changes.

9.4 Troubleshooting the Adaptive Agent

The following section provides solutions to the problems you might encounter while working with the ZENworks Adaptive Agent:

◆ "Satellite menu is not displayed in the left navigation pane of the ZENworks Adaptive Agent page" on page 104

◆ "Unable to use rights-based authentication to remotely manage a device" on page 105

◆ "Unable to launch a terminal session with a Citrix Server that has ZENworks Adaptive Agent installed" on page 105

Satellite menu is not displayed in the left navigation pane of the ZENworks Adaptive Agent page

> Source: ZENworks 10 Asset Management; ZENworks Adaptive Agent.

Explanation: When you promote a device to Satellite through ZENworks Control Center, the configured Satellite role is added to the device. However, when you double-click the ◪ icon, the Satellite menu is not displayed in the left navigation pane of the ZENworks Adaptive Agent page.

Action: Refresh the managed device (In the notification area of the device, right-click the ◪ icon, then click *Refresh*).

Unable to use rights-based authentication to remotely manage a device

Source: ZENworks 10 Management; ZENworks Adaptive Agent.

Explanation: When you use rights-based authentication to remotely manage a device, the following error is logged on the device:

```
Rights Authentication failed. An internal error occurred
while communicating to ZENworks Management Daemon. Contact
Novell Technical Services.
```

Possible Cause: ZENworks Adaptive Agent is not installed on the device. Only Remote Management service is installed on the device.

Action: Install ZENworks Adaptive Agent on the device. For more information on installing the ZENworks Adaptive Agent, see "Installing the ZENworks Adaptive Agent" in *ZENworks 10 Asset Management Administration Quick Start*.

Unable to launch a terminal session with a Citrix Server that has ZENworks Adaptive Agent installed

Source: ZENworks 10 Management; ZENworks Adaptive Agent.

Explanation: After deploying the ZENworks Adaptive Agent on a Citrix* server, you might encounter any of the following ICA login session issues:

- The ICA login session that is launched from Citrix agent terminates after some time.
- The ICA login session displays the following exception:

  ```
  winlogon.exe ..Application Error
  ```

  If you try to close the exception window, the session hangs displaying the following message:

  ```
  Running login scripts
  ```

Action: Before launching a terminal session with the Citrix server, do any of the following on the server:

- Rename `NWGina.dll`.
    1. In the `c:\windows\system32` directory, rename `NWGina.dll`.
    2. In the Registry Editor, go to `HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon`, and change the value of the `CtxGinaDLL` key to the new name for `NWGina.dll`.
    3. Reboot the server.
- Install Novell Client.

NOTE: This needs to be done only once.

Backing Up and Restoring the ZENworks Server and Certificate Authority

<div align="right">

10

</div>

The following sections provide more information about backing up and restoring a ZENworks Server and Certificate Authority:

10.1 Backing Up a ZENworks Server

Novell® ZENworks® 10 Asset Management allows you to back up and restore the configuration files for a ZENworks Primary Server. This enables you to maintain a ZENworks Server's identity and configuration if a server fails or if you need to upgrade to new server hardware.

A ZENworks Server only needs to be backed up once. The backup saves only the configuration files. The following items must be backed up separately:

- The content repository . You should do a separate backup for the content repository if you only have one Primary Server in the Management Zone. If you have two or more Primary Servers and you've replicated all content to both servers, they serve as backup copies to each other.
- The ZENworks database (if it resides on the ZENworks Server). Backing up the ZENworks Server and backing up the ZENworks database are two separate processes. If your ZENworks database resides on the same server as one of your ZENworks Servers, first back up the database and then back up the ZENworks Server. Because the ZENworks database changes frequently, you should back up the database on a regular schedule. For information about backing up the database, see Part VI, "Database Management," on page 195.

When you back up a ZENworks Server using a zman command, all files in the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks/` directory on a Linux server are stored in an encrypted backup file in a location that you specify.

1 (Conditional) If the server you are backing up hosts the ZENworks database, manually back up the database file to a safe location.

   For information about backing up the database, see Part VI, "Database Management," on page 195.

2 At a command prompt on the ZENworks Server, enter the following command:

   `zman zenserver-backup` *path_to_backup_file_to_create*

   For example:

   `zman zenserver-backup c:\zcm_backups\zone_backup.bak`

   or

```
zman zenserver-backup /root/zcm_backups/zone_backup.bak
```

3 When prompted, enter a ZENworks administrator name and password.

4 When prompted, enter a passphrase (at least 10 characters) to be used for encrypting the backup file.

Make sure you remember this passphrase. You must enter it if you ever need to restore the server.

5 (Conditional) If this is your only Primary Server, or if this is the only Primary Server that contains all content defined in your Management Zone, manually back up your content repository to a safe location.

IMPORTANT: If this is the only Primary Server that contains all of your defined content for the Management Zone and you do not back up the content repository, you are not prepared for a full disaster recovery.

6 Repeat Step 1 and Step 5 on a regular basis.

The zman command documented in Step 2 through Step 4 only needs to be run once.

10.2 Restoring a ZENworks Server

This procedure assumes the following:

◆ You have a backup of the ZENworks Server's configuration information. See Section 10.1, "Backing Up a ZENworks Server," on page 107.

◆ If the ZENworks database resides on the ZENworks Server, you have a backup of the database. See Section 22.3, "Backing Up the Embedded Sybase SQL Anywhere Database," on page 199.

IMPORTANT: When you restore the ZENworks Server and the database, you must first restore the ZENworks Server, then continue with restoring the latest backed-up ZENworks database.

To restore a ZENworks server:

1 Reinstall the ZENworks Server, using the same IP address and DNS name.

If you do not use the same IP address and DNS name, any devices that connect to the server need to reregister.

If you have only one Primary Server connected to an external database in a zone, reinstall the Primary server and create a dummy database during the installation. You do not need to create an internal database.

If you have more than one Primary server connected to an external database in a zone, reinstall the failed Primary server as a second Primary Server. You are not prompted to configure the database during the installation.

2 Ensure that you have read/write rights to the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks` directory on a Linux server.

3 At a command prompt on the ZENworks Server, enter the following command:

```
zman zenserver-restore path_to_backup_file_to_restore
```

For example:

```
zman zenserver-restore c:\zcm_backups\zone_backup.bak
```

or

```
zman zenserver-restore /root/zcm_backups/zone_backup.bak
```

4 When prompted, enter a ZENworks administrator name and password.

5 When prompted, enter the passphrase (at least 10 characters) to be used for decrypting the backup file.

This is the same passphrase that was entered to encrypt the file when backing up the server.

6 (Conditional) If the database is located on the server, restore the database after the ZENworks Server information has been restored. For instructions, see Section 22.4, "Restoring the Embedded Sybase SQL Anywhere Database," on page 204.

7 Restart the ZENworks Server.

10.3 Backing Up the Certificate Authority

To back up the Certificate Authority files on the Primary Server that is configured to be the ZENworks internal Certificate Authority:

1 At the command prompt of the ZENworks Server, enter the following command:

```
zman certificate-authority-export (certificate-authority-export/cae)
[options] (file path)
```

This command exports the key-pair credentials of the zone Certificate Authority to a file. For more information about zman Certificate Authority commands, see "zman(1)"in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2 Enter the username and password of the administrator of the Management Zone.

3 Enter a passphrase for the file encryption.

Make sure you remember this passphrase. You must enter it if you ever need to restore the server.

10.4 Restoring the Certificate Authority

To restore the Certificate Authority files on the Primary Server that is configured to be the ZENworks internal Certificate Authority:

1 At the command prompt of the ZENworks Server, enter the following zman command:

```
zman certificate-authority-import (certificate-authority-import/cai) (file
path)
```

This command imports the key-pair credentials of the zone certificate authority from a file. For more information about zman Certificate Authority commands, see "zman(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2 Enter the username and password of the administrator of the Management Zone.

3 Enter the file encryption passphrase you specified when you backed up the Certificate Authority files (Step 3 in Section 10.3, "Backing Up the Certificate Authority," on page 109).

Disaster Recovery

11

The following sections explain the disaster recovery mechanisms available in Novell® ZENworks® 10 Asset Management that help you protect the first Primary Server of a Management Zone if an organizational risk assessment identifies a need for such steps:

11.1 Replacing the First Primary Server with the Second Primary Server

You can replace the first Primary Server in your Management Zone with an existing second Primary Server or with a new server. If you choose to replace the first Primary Server with a new server that has a different hostname and IP address, you must install ZENworks 10 Asset Management on the new server in the same Management Zone. Consequently, the new server becomes the second Primary Server.

The first Primary Server and the second Primary Server must have the same version of the ZENworks 10 Asset Management installed.

NOTE: This scenario has been tested on the following platform combinations:

◆ Windows Server* 2003 (32-bit) to Windows Server 2008 (32-bit)
◆ SUSE® Linux Enterprise Server (SLES) 10 (32-bit) to SLES 10 (32-bit)

It has not been tested with ZENworks Reporting Server.

This scenario is not supported on Windows to Linux and vice-versa platform combinations.

To replace the first Primary Server with the second Primary Server:

1 Make sure that all the contents of the `content-repo` directory of the first Primary Server are replicated to the second Primary Server.

The `content-repo` directory is located in the `ZENworks_installation_directory\work\` directory on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

2 Export the Certificate Authority role.

  2a Take a reliable backup of the Certificate Authority of the first Primary Server.

   For detailed information on how to take a backup of the Certificate Authority, see Section 10.3, "Backing Up the Certificate Authority," on page 109.

IMPORTANT: You must use the `-d` option with the `zman certificate-authority-export` command to remove the Certificate Authority role of the local server.

    2b Restore the backed-up Certificate Authority on the second Primary Server.

    For detailed information on how to restore a backed-up Certificate Authority, see Section 10.4, "Restoring the Certificate Authority," on page 109.

3 In the default closest server rule at the Management Zone level, move the first Primary Server as the last entry in the servers list.

    3a In ZENworks Control Center, click the *Configuration* tab.

    3b In the Management Zone Settings panel, click *Infrastructure Management > Closest Server Default Rule*.

    3c In the *Collection Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    3d In the *Content Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    3e In the *Configuration Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    3f Click *OK*.

4 (Conditional) If you have any additional closest server rules configured, remove the first Primary Server from the rules.

    4a In ZENworks Control Center, click the *Configuration* tab.

    4b In the Management Zone Settings panel, click *Infrastructure Management > Closest Server Rules*.

    4c Select a closest server rule, then click Edit.

    The Rule Construction dialog box is displayed.

    4d In the *Collection Servers* list, select the check box next to the first Primary Server, then click *Remove*.

    4e In the *Content Servers* list, select the check box next to the first Primary Server, then click *Remove*.

    4f In the *Configuration Servers* list, select the check box next to the first Primary Server, then click *Remove*.

    4g Click *OK* twice.

5 Refresh all the devices (Primary Serves, Satellites, and managed devices) in the Management Zone so that they get the new closest server rules.

6 (Conditional) Move the database to another device in any of the following scenarios:

- You are using an internal ZENworks database (embedded Sybase SQL* Anywhere).
- You are using an external database installed on the device hosting the first Primary Server and you do not plan to use the device after uninstalling the Primary Server.

To move the database to another device:

    6a (Conditional) If you are using an external database, ensure that you have a reliable backup of the database.

    6b Obtain the credentials of the database.

To procure the credentials of the internal database, use one of the following commands:

```
zman dgc -U administrator_name -P administrator_password
```

or

```
zman database-get-credentials -U administrator_name -P
administrator_password
```

To obtain the credentials of the external database, contact the database administrator.

6c Remove the database role from the first Primary Server:

6c1 Log into the database.

6c2 In the SQL editor, execute the following SQL query to remove the database role entry for the first Primary Server from the zZENServerRoles table:

```
delete from zZENServerRoles where Roles='Database';
```

6c3 In the SQL editor, execute the following SQL command:

```
commit;
```

6d If the database is installed on the same device as that of the first Primary Server, move the database.

Internal Sybase: For detailed information on how to move the data from an internal Sybase database to an external Sybase database, see Section 22.5, "Moving the Data from an Embedded Sybase Database to an External Sybase Database," on page 205.

External Sybase: For detailed information on how to move the data from one external Sybase database to another external Sybase database, see Section 23.1, "Moving the Data from One External Sybase Database to another External Sybase Database," on page 219.

MS SQL: For detailed information on how to move the data to a new MS SQL database, see the MS SQL documentation. Later on, perform the steps described in Section 23.2, "Configuring the ZENworks Server to Point to the New MS SQL Database Containing Data Moved from Another MS SQL Database," on page 220.

Oracle: For detailed information on how to move the data from one Oracle database to another Oracle database, see the Oracle documentation. Later on, perform the steps described in Section 23.3, "Configuring the ZENworks Server to Point to the New Oracle Database Containing Data Moved from Another Oracle Database," on page 222.

7 Remove all Satellites under the first Primary Server from the Server Hierarchy.

For more information on how to remove the Satellites from the Server Hierarchy listing in ZENworks Control Center, see Section 6.3, "Removing Satellites from the Server Hierarchy," on page 74.

8 Retire the first Primary Server by entering one of the following commands at the server prompt:

```
zman zsd primary_server_object_name
```

or

```
zman zenserver-delete primary_server_object_name
```

For more information about zman, view the zman man page (man zman) on the server or see "zman(1)"in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

9 After ensuring that all the operations in the Management Zone are working as expected, uninstall ZENworks 10 Asset Management on the first Primary Server.

For detailed information on how to uninstall ZENworks 10 Asset Management, see "Uninstalling ZENworks 10 Asset Management SP2" in the *ZENworks 10 Asset Management Installation Guide*.

11.2 Replacing an Existing Primary Server with a New Primary Server

If you have only one Primary Server in the Management Zone and if you want to replace the device hosting the Primary Server with a new device that has the same hostname and IP address as the old device, you must move the Primary Server to the new device.

The existing Primary Server and the new Primary Server must have the same version of the ZENworks 10 Asset Management installed.

NOTE: This scenario has been tested on the following platform combinations:

- Windows Server* 2003 (32-bit) to Windows Server 2008 (32-bit)
- SUSE® Linux Enterprise Server (SLES) 10 (32-bit) to SLES 10 (32-bit)

It has not been tested with ZENworks Reporting Server.

This scenario is not supported on Windows to Linux and vice-versa platform combinations.

1 Take a reliable backup of the existing ZENworks Server.

For detail information on how to take a backup of the ZENworks Server, see Section 10.1, "Backing Up a ZENworks Server," on page 107.

2 Take a reliable backup of the Certificate Authority of the Primary Server.

For detail information on how to take a backup of the Certificate Authority, see Section 10.3, "Backing Up the Certificate Authority," on page 109.

3 (Conditional) Take a reliable backup of database in any of the following scenarios:

- You are using an internal ZENworks database (embedded Sybase SQL Anywhere).
- You are using an external database installed on the device hosting the Primary Server and you do not plan to use the device after uninstalling the Primary Server.

For detailed information on how to take a backup of an internal database, see Section 22.3, "Backing Up the Embedded Sybase SQL Anywhere Database," on page 199.

To take a backup of an external database, see the documentation for the database.

4 Stop all the ZENworks services on the Primary Server.

For detailed information on how to stop the ZENworks services on Windows, see Section 5.1.3, "Stopping a ZENworks Service," on page 64. For detailed information on how to stop the ZENworks services on Linux, see Section 5.2.3, "Stopping a ZENworks Service," on page 66

5 Take a reliable backup of the `content-repo` directory of the Primary Server.

The `content-repo` directory is located in the *ZENworks_installation_directory*\work\ directory on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

6 Disconnect the device from the network.

7 Ensure that the hostname and the IP address of the new server are same as those of the old Primary Server.

8 Install ZENworks 10 Asset Management on the new server with the same Management Zone name and ports as that of the old Primary Server.

For detailed information on how to install ZENworks 10 Asset Management, see "Installing ZENworks 10 Asset Management SP2 Server" in the *ZENworks 10 Asset Management Installation Guide*.

9 Do the following on the new Primary Server:

9a Restore the backed-up ZENworks Server.

For detailed information on how to restore the ZENworks Server, see Section 10.2, "Restoring a ZENworks Server," on page 108.

9b Restore the backed-up Certificate Authority.

For detailed information on how to restore the Certificate Authority, see Section 10.4, "Restoring the Certificate Authority," on page 109.

9c (Conditional) Restore the backed-up database.

For detailed information on how to restore the internal ZENworks database, see Section 22.4, "Restoring the Embedded Sybase SQL Anywhere Database," on page 204.

9d Copy the backed-up `content-repo` directory to the `ZENworks_installation_directory`\work\ directory on Windows or to the `/var/opt/novell/zenworks/` directory on Linux.

10 Ensure that the new server is running correctly. Subsequently, uninstall ZENworks Asset Management from the old device.

For detailed information on how to uninstall ZENworks 10 Asset Management see "Uninstalling ZENworks 10 Asset Management SP2" in the *ZENworks 10 Asset Management Installation Guide*.

11.3 Changing the Internal Certificate to an External Certificate on a Primary Server

To change the internal certificate to an external certificate on a Windows or Linux Primary Server:

1 Create a Certificate Signing Request (CSR) by providing the hostname of the Primary Server as the subject.

For more information on how to create a CSR, see "Creating an External Certificate Authority" in the *ZENworks 10 Asset Management Installation Guide*.

2 Perform the following steps on the Primary Server whose certificate you want to change:

2a At the console prompt, run the following command:

```
novell-zenworks-configure -c SSL -Z
```

2b Provide the information of the external certificate created in Step 1.

2c Restart all the ZENworks services by running the following command:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

2d In a Web browser, enter the following URL to ensure that the new certificate is displayed:

```
https://ZENworks_Server_IP_address
```

2e Edit the `initial-web-service` file, which is located in the `ZENworks_installation_directory\Novell\ZENworks\conf` directory on Windows and in the `/etc/opt/novell/zenworks/` directory on Linux, to replace the content of the server certificate section with the pem format available in the `server.cert` file. The `server.cert` file is located in the `ZENworks_installation_directory\novell\zenworks\conf\security` directory on Windows and in the `/etc/opt/novell/zenworks/security/` directory on Linux.

2f Rebuild the agent packages by running the following commands:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
novell-zenworks-configure -c RebuildCustomPacks -Z
```

3 Perform the following steps at the command prompt of each managed device and Satellite registered to the Primary Server whose certificate you changed:

3a Run the following command to force the device to be unregistered locally:

```
zac unr -f
```

For more information about zac, view the zac man page (`man zac`) on the device or see "zac(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

3b Clear the cache.

On Windows: Run the following command:

```
delete c:\program files\novell\zenworks\cache\zmd /s
```

On Linux: Run the following command:

```
rm -rf /var/opt/novell/zenworks/zmd/cache
```

3c Run the following command to register the device in the Management Zone:

```
zac reg https://ZENworks_Server_DNS_name
```

For more information about zac, view the zac man page (`man zac`) on the device or see "zac(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

This replaces the server certificate in the local cache.

11.4 Tasks to Be Performed after Changing the DNS Name of a Primary Server

If you change only the DNS name of a Primary Server, you must perform the following tasks:

1 Ensure that the DNS entry of the Primary Server has been updated with the new DNS name.

2 Take a reliable backup of the existing certificate on the Primary Server. The certificate is located in the `\novell\zenworks\conf\security` directory on Windows and in the `/etc/opt/novell/zenworks/security` directory on Linux.

3 (Conditional) If the Primary Server whose DNS you changed hosts the database and the database server IP address or DNS has been changed, do the following on all the Primary Servers:

3a Ensure that the database server IP address or DNS name has been configured correctly in the `zdm.xml`. The `zdm.xml` file is located in the `ZENworks_Installation_Directory\Novell\ZENworks\conf\datamodel\` directory on Windows, and in the `/etc/opt/novell/zenworks/datamodel/` directory on Linux.

3b Restart the following services:

- Novell ZENworks Server
- Novell ZENworks Loader
- Novell ZENworks Agent Service

4 Recreate the certificate on the Primary Server:

- Tasks to be performed on the Primary Server
- Tasks to be performed on the managed devices and Satellites

4a Perform the following steps on the Primary Server:

4a1 At the console prompt, run the following command:

```
novell-zenworks-configure -c SSL -Z
```

Follow the prompts.

4a2 Restart all the ZENworks services by running the following command:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

4a3 In a Web browser, enter the following URL to ensure that the new certificate is displayed:

```
https://ZENworks_Server_IP_address
```

4a4 Edit the `initial-web-service` file, which is located in the `ZENworks_installation_directory\Novell\ZENworks\conf` directory on Windows and in the `/etc/opt/novell/zenworks/` directory on Linux, to replace the content of the server certificate section with the pem format available in the `server.cert` file. The `server.cert` file is located in the `ZENworks_installation_directory\novell\zenworks\conf\security` directory on Windows and in the `/etc/opt/novell/zenworks/security/` directory on Linux.

4a5 Rebuild the agent packages by running the following commands:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
novell-zenworks-configure -c RebuildCustomPacks -Z
```

4b Perform the following steps at the command prompt of each managed device and Satellite registered to the Primary Server whose certificate you changed:

4b1 Run the following command to force the device to be unregistered locally:

```
zac unr -f
```

For more information about zac, view the zac man page (`man zac`) on the device or see "zac(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

4b2 Clear the cache.

    On Windows: Run the following command:

    `delete c:\program files\novell\zenworks\cache\zmd /s`

    On Linux: Run the following command:

    `rm -rf /var/opt/novell/zenworks/zmd/cache`

4b3 Run the following command to register the device in the Management Zone:

    `zac reg https://ZENworks_Server_DNS_name`

    For more information about zac, view the zac man page (`man zac`) on the device or see "zac(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

    This replaces the server certificate in the local cache.

ZENworks System Updates

III

The System Updates feature allows you to obtain updates to the Novell® ZENworks® 10 Asset Management software on a timely basis, and also allows you to schedule automatic downloads of the updates.

Introduction to ZENworks System Updates

<div style="text-align: right">**12**</div>

The System Updates feature allows you to obtain updates to the Novell® ZENworks® 10 Asset Management software on a timely basis, and also allows you to schedule automatic downloads of the updates.

Software updates are provided periodically and you can choose whether to deploy each update after viewing its content.

You can also download the latest Product Recognition Update (PRU) to update your knowledgebase so that Inventory can recognize newer software.

When you select to update your ZENworks software, you can update globally in one step or in stages. You can also select to update specific devices, groups of devices, or all devices in the Management Zone that have the ZENworks software installed. You can use ZENworks Control Center to track the successes and failures per device for each software update.

The following figure illustrates the System Updates page:

Figure 12-1 *System Updates Panels (Available System Updates, Deploying System Updates, and Deployment Stages)*
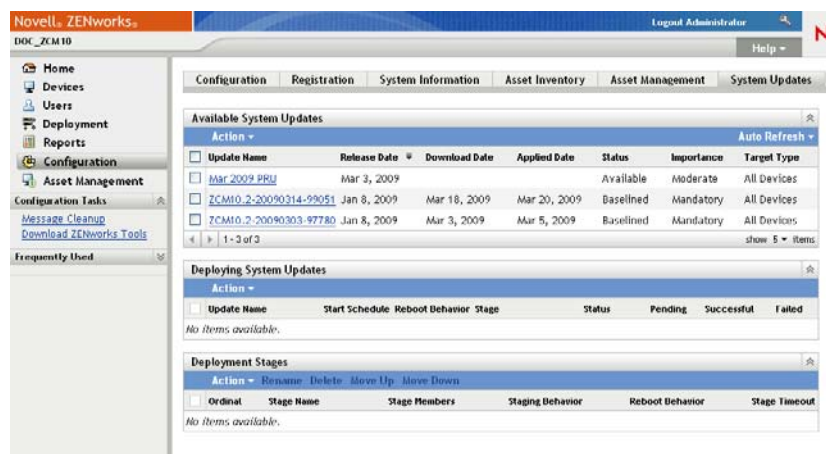
Review the following sections to set up and manage updates for your ZENworks software:

- Chapter 13, "Configuring Updates," on page 123
- Chapter 14, "Managing Update Downloads," on page 141
- Chapter 15, "Deploying Updates," on page 147
- Chapter 16, "Deleting Updates," on page 163
- Chapter 17, "Reviewing the Content of an Update," on page 165
- Chapter 18, "Update Statuses," on page 169

Configuring Updates

13

Perform the following tasks to configure your update process:

13.1 Configuring System Update Settings

You should configure System Update before attempting to use it. Configure as many of the following settings as necessary for your system:

13.1.1 Check for Updates Schedule

The default is to not schedule update checking (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can check for software updates is to do so manually in the Available System Updates panel on the *System Updates* tab.

You can specify how often you want to check for updates. When you do this, information on available updates is automatically downloaded from Novell® to the Available System Updates panel on the *System Updates* tab when the schedule fires. This does not download the update content itself. Downloading can be scheduled in the Download Schedule panel (see "Download Schedule" on page 125).

To schedule checking for the ZENworks software updates:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *Configuration* tab.

2 Click *Management Zone Settings* to expand its options, click *Infrastructure Management* to expand its options, then select *System Update Settings*.

In the Check for Updates panel, there are two scheduling options for updates:

- **No Schedule:** The default is to not schedule update checking. With this scheduling option selected, the only way you can check for software updates is to do so manually in the Available System Updates panel on the *System Updates* tab. To specify the *No Schedule* option, continue with Step 3.

◆ **Recurring:** Lets you specify how often you want to check for updates. When you set this option, information on available updates is automatically downloaded from Novell to the Available System Updates panel on the *System Updates* tab when the schedule fires. This does not download the update content itself. To set a recurring schedule, skip to Step 4.

3 (Conditional) To exclude scheduled checking for software updates (the default), click the down-arrow in the *Schedule Type* field, select *No Schedule*, click *Apply* to save the schedule change, then skip to Step 6.

With this option selected, you must check for updates manually. For more information, see "Manually Downloading Updates" on page 143.

4 (Conditional) To set a recurring schedule for checking for updates to your ZENworks software, click the down-arrow in the *Schedule Type* field, then select *Recurring*.

Configuration > System Update Settings

System Update Settings   ☒
Configure the server for downloading System Updates, proxy server settings, and scheduling updates

Check For Updates Schedule   ⌃
This setting allows the administrator to configure a schedule to check for available updates from Novell.

Schedule Type:
[Recurring   ▼]

◉ Days of the week
   Sun Mon Tue Wed Thu Fri Sat
    ☐   ☐   ☐   ☐   ☐   ☐   ☐
   Start Time: [1 ▼] : [00 ▼] [am ▼]
   Hide Options
      ☐ Process immediately if device unable to execute on schedule
      ☐ Use Coordinated Universal Time (Current UTC 7:50 PM)
      ☐ Start at a random time between Start and End Times
          End Time: [1 ▼] : [00 ▼] [am ▼]
      ☐ Restrict schedule execution to the following date range:
          Start Date: [2/5/08   ] 📅
          End Date: [2/5/08   ] 📅

5 Fill in the fields:

5a Select one or more check boxes for the days of the week.

5b To set the time of day for checking to occur, use the *Start Time* box to specify the time.

5c (Optional) For additional scheduling options, click *More Options*, then select the following options as necessary:

◆ **Process Immediately if Device Unable to Execute on Schedule:** Causes checking for updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for updates occurs immediately after the server comes back online.

◆ **Use Coordinated Universal Time:** Causes the schedule to interpret the times you specify as UTC instead of local time.

◆ **Start at a Random Time Between Start and End Times:** Allows checking for updates to occur at a random time between the time you specify here and the time you specified in Step 5b. Fill in the *End Time* fields.

◆ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify a date range for when the checking can occur.

5d When you have finished configuring the recurring schedule, click *Apply* to save the schedule change.

6 To exit this page, click *OK* when you are finished configuring the schedule.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.1.2 Download Schedule

The default is to not schedule downloading of updates (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can download updates is to do so manually in the Available System Updates panel on the *System Updates* tab.

If you do specify how often you want to download updates, you should set this schedule in conjunction with the schedule to check for updates (see "Check for Updates Schedule" on page 123).

After an update has been checked for and its information displayed in the Available System Updates panel on the *System Updates* tab, you can schedule the download from Novell to automatically occur when the schedule fires.

To schedule ZENworks software updates:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *Configuration* tab.

2 Click *Management Zone Settings* to expand its options, click *Infrastructure Management* to expand its options, then select *System Update Settings*.

In the Download Schedule panel, there are two scheduling options for downloading updates:

- ◆ **No Schedule:** The default is to not schedule downloading of updates (*No Schedule* is displayed in the *Schedule Type* field). With this scheduling option selected, the only way you can download updates is to do so manually in the Available System Updates panel on the *System Updates* tab. To specify the *No Schedule* option, continue with Step 3.

- ◆ **Recurring:** You can specify how often you want to download updates. After an update has been checked for and its information displayed in the Available System Updates panel on the *System Updates* tab, you can schedule the download from Novell to automatically occur when the schedule fires. To set a recurring schedule, skip to Step 4.

3 (Conditional) To exclude scheduled downloading of software updates (the default), click the down-arrow in the *Schedule Type* field, select *No Schedule*, click *Apply* to save the schedule change, then skip to Step 6.

With this option selected, you must download updates manually. For more information, see Section 14.2, "Downloading Updates," on page 142.

4 (Conditional) To set a recurring schedule for downloading updates to your ZENworks software, click the down-arrow in the *Schedule Type* field, then select *Recurring*.

System Update Settings ☒
Configure the server for downloading System Updates, proxy server settings, and scheduling updates

Check For Updates Schedule ☒

Download Schedule ☒
This setting allows the administrator to configure a download schedule for updates.

Schedule Type:
| Recurring ▾ |

⊙ Days of the week

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Start Time: 1 ▾ : 00 ▾ am ▾
Hide Options
☐ Process immediately if device unable to execute on schedule
☐ Use Coordinated Universal Time (Current UTC 7:52 PM)
☐ Start at a random time between Start and End Times
    End Time: 1 ▾ : 00 ▾ am ▾
☐ Restrict schedule execution to the following date range:
    Start Date: 2/5/08 📅
    End Date: 2/5/08 📅

5 Fill in the fields:

  5a Select one or more check boxes for the days of the week.

  5b To set the time of day for downloading to occur, use the *Start Time* field to specify the time.

  5c (Optional) For additional scheduling options, click *More Options*, then select the following options as necessary:

    ◆ **Process Immediately if Device Unable to Execute on Schedule:** Causes checking for updates to occur as soon as possible if the checking cannot be done according to schedule. For example, if a server is down at the scheduled time, checking for updates occurs immediately after the server comes back online.

    ◆ **Use Coordinated Universal Time:** Causes the schedule to interpret the times you specify as UTC instead of local time.

    ◆ **Start at a Random Time Between Start and End Times:** Allows downloading of updates to occur at a random time between the time you specify here and the time you specified in Step 5b. Fill in the *End Time* fields.

    ◆ **Restrict Schedule Execution to the Following Date Range:** In addition to the other options, you can specify the days when downloading can occur.

  5d When you have finished configuring the recurring schedule, click *Apply* to save the schedule change.

6 To exit this page, click *OK* when you are finished configuring the schedule.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.1.3 E-Mail Notification

In conjunction with using stages, you can set up e-mail notifications to indicate when each stage has completed. When you deploy an update, you can specify to use the e-mail notifications.

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *Configuration* tab.

2 Click *Management Zone Settings* to expand its options, click *Events and Messaging*, then select *SMTP Settings* to display the E-mail Notification panel:

Configuration > SMTP Settings

SMTP Settings	[x]
Configuration of settings related to SMTP Server	

E-mail Notification ⟰

SMTP Server Address _____

SMTP Port _____

☐ SMTP Server requires authentication

User _____

Password _____

[OK] [Apply] [Reset] [Cancel]

Staging must be used to receive notifications, and the stage behavior must be set to one of the following:
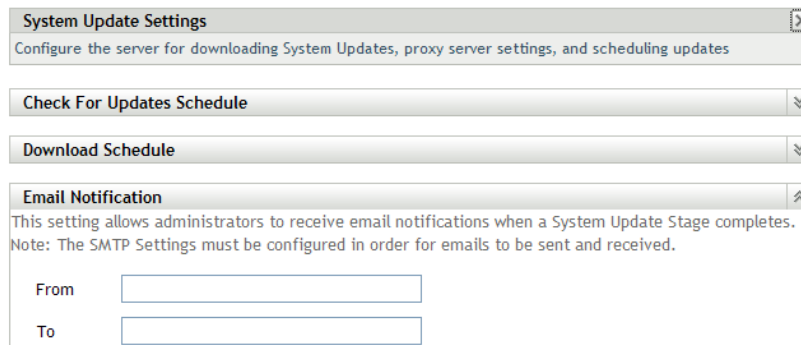
- *Advance Through Stage Automatically With Notification*
- *Advance To Next Stage and Notify When Complete*

SMTP must be configured in order for the staging e-mail configuration to work.

3 (Conditional) If you do not have SMTP configured:

3a To access the SMTP Settings page, click *Configuration* in the left pane, click the arrows in the *Management Zone Settings* heading to expand its options, click *Event and Messaging*, then select *SMTP Settings*.

3b In the *E-mail Notification* section, fill in the fields:

SMTP Server Address: Specify the DNS name or IP address of the SMTP server.

SMTP Port: Specify the SMTP server's communication port.

Use SSL: To use an encrypted SSL channel for sending e-mails. By default this option is disabled.

SMTP Server Requires Authentication: If authentication is required, select this check box, then specify the *User* and *Password* information.

3c Click *OK* to save the changes.

3d Click *Management Zone Settings* to expand its options, click *Infrastructure Management*, then select *System Update Settings* to display the E-mail Notification panel:

Configuration > System Update Settings

System Update Settings	☒
Configure the server for downloading System Updates, proxy server settings, and scheduling updates	

Check For Updates Schedule	☒

Download Schedule	☒

Email Notification

This setting allows administrators to receive email notifications when a System Update Stage completes.
Note: The SMTP Settings must be configured in order for emails to be sent and received.

From

To

4 Fill in the fields:

From: Either specify your administrator e-mail address, or type something descriptive, such as `System-Update-Stage-Notice`. Do not use spaces between words.

To: Specify your administrator's e-mail address.

This is the person you want to be notified when the stage ends.

5 Click *Apply* to make the changes effective.

6 Either click *OK* to close the page, or continue with another configuration task.
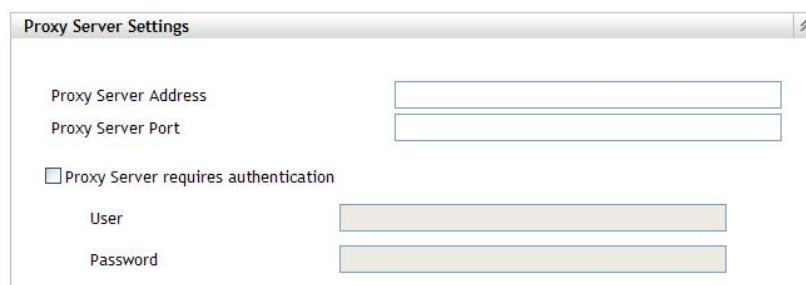
If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.1.4 Proxy Server Settings

This option is useful for restrictive environments where you do not want all of your production servers to have Internet access. This is used in conjunction with the Dedicated Server Settings panel.

To specify a proxy server:

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the Proxy Server Settings panel.

Proxy Server Settings

Proxy Server Address

Proxy Server Port

☐ Proxy Server requires authentication

User

Password

3 Fill in the fields:

Proxy Server Address: Specify the DNS name or IP address of the proxy server.

Proxy Server Port: Specify the proxy server's communication port.

Proxy Server Requires Authentication: When you select this check box, the *User* and *Password* fields become editable. If authentication is required, select this check box and specify the username and password for access to the proxy server.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.1.5 Dedicated Server Settings

By default, any available Primary Server in the Management Zone can be used randomly to download the updates. However, you can specify one ZENworks Server to be dedicated to handling your update downloads. The server that you select should have access to the Internet, directly or through a proxy server.
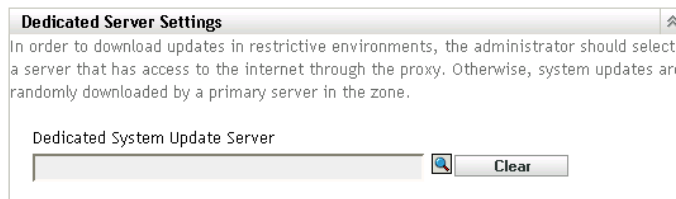
The following sections contain more information:

* "Specifying a Dedicated Update Server" on page 129
* "Clearing a Dedicated Update Server" on page 130

Specifying a Dedicated Update Server

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the Dedicated Server Settings panel:

3 Browse for and select a ZENworks Primary Server.

The server's identification is displayed in the *Dedicated System Update Server* field.

This ZENworks Server must be a member of the Management Zone.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

Clearing a Dedicated Update Server

Clearing a dedicated update server causes your updates to be retrieved randomly from any Primary Server in the Management Zone.

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* section (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the Dedicated Server Settings panel:
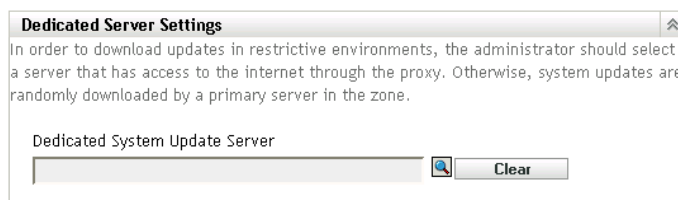
3 Click *Clear* to remove the dedicated server from the *Dedicated System Update Server* field.

4 (Conditional) If you need to revert to the last saved dedicated server setting, click *Reset*.

This resets the dedicated server to the last saved setting, such as when you last clicked *Apply* or *OK*.

5 Click *Apply* to make the change effective.

IMPORTANT: Previous settings cannot be restored after you click *Apply*.

13.1.6 Stage Timeout Settings

Deployment stages are optional; however, stages allow you to deploy an update one step at a time, such as to a test group first, then to your managed devices. If a failure occurs during the update process, the process is halted. E-mail notifications can let you know when each stage has completed.

The global default timeout setting is 3 days. This provides the same timeout length for each stage. For information about setting the timeout for individual stages, see "Modifying the Stage Timeout" on page 135.

Set this value to be long enough to accommodate updating all of the devices you plan to update.

When the timeout value is reached, the stage's deployment stops and an e-mail message is sent , if e-mail notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).

You can use E-mail notification to know when a stage has completed.

To configure global stage timeout settings:

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* panel (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the Stage Timeout Settings panel:

3 Select the *Stage Timeout* check box, then specify the days, hours, and minutes desired.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

If you did not click *Apply* to make your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.1.7 Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To configure the reboot behavior:

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 On the *Configuration* tab, expand the *Management Zone Settings* panel (if necessary), click *Infrastructure Management*, then click *System Update Settings* to display the Reboot Behavior panel:

3 Select one of the following options:

- **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.

- **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention if a reboot is required by the update.

4 Click *Apply* to make the changes effective.

5 Either click *OK* to close the page, or continue with another configuration task.

If you did not click *Apply* to make some of your changes effective, clicking *OK* does so. Clicking *Cancel* also closes the page, but loses your unapplied changes.

13.2 Creating Deployment Stages

Deployment stages are optional; however, stages allow you to deploy an update one step at a time, such as to a test group first, then to your managed devices. If a failure occurs during the update process, the process is halted. E-mail notifications can let you know when each stage has completed.

The following sections contain more information:

13.2.1 Understanding Stages

You can do the following with stages:

- Set them up for different devices or groups, such as for a test group, specific devices or device groups, or all managed devices in the zone.
- Modify an existing stage's membership.
- Change the order in which the stages run.
- Rename and delete stages.
- Specify the default timeout for a stage. When the timeout value is reached, the stage's deployment stops and an e-mail message is sent , if e-mail notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).
- Specify the reboot behavior when devices complete the update: prompt a reboot, force a reboot, or suppress rebooting.
- Specify how the update process is to advance through the stages:
  - Automatically, with or without notification
  - One stage at a time with notification when each stage is completed
  - Bypass the configured stages and immediately apply the update to all devices

There are many reasons for creating deployment stages:

- Testing the update on certain devices before deploying it to your production environment
- Including all Primary Servers in one stage so they can be updated at the same time.

◆ Grouping your servers in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.

◆ Grouping the workstations in several stages so that the update process isn't too intensive for the Primary Server being used to perform the updates.

Any managed devices that are not part of a stage are automatically updated after the last deployment stage has been processed.

You cannot configure stages when an update is in progress.

The following figure illustrates the Deployment Stages panel on the System Updates page:

Figure 13-1 *The Deployment Stages Panel*

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 13-1 *Deployment Stages column descriptions.*

Column Heading	Explanation
Ordinal	Displays the order in which the stages run. You can rearrange the staging order by using the *Move Up* and *Move Down* options. For more information, see "Rearranging the Order in Which Stages Start" on page 139.
	The first stage listed always displays ordinal 1, the second, ordinal 2, and so on. Therefore, you do not need to include a sequence number in your stage names.
Stage Name	Name of the stage, which you specify when creating the stage by using the *Action > Add Stage* option.
	Make this name descriptive enough to indicate its purpose.
Stage Members	This column contains the *View/Modify Members* option, which opens the Modify Stage Members dialog box that lists all of the members of the stage. You can use the dialog box to add or remove members from the stage.
	Stage membership can include individual devices and groups that contain devices.
	For more information, see "Modifying the Membership of a Deployment Stage" on page 137.
Staging Behavior	Displays the current behavior for each stage, which you can change by using the *Action > Modify Staging Behavior* option. For more information, see "Modifying Staging Behavior" on page 136.

Column Heading	Explanation
Reboot Behavior	Displays the reboot behavior of devices after the update is deployed.
	Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.
	You have the following reboot options:
	◆ **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.
	◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
	◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.
	For more information, see "Modifying Reboot Behavior" on page 137.
Stage Timeout	Displays the stage timeout, listed in minutes, which you can change by using the *Action > Modify Stage Timeout* option. The default is 3 days, 0 hours, and 0 minutes, which is the global timeout value that can be changed in "Stage Timeout Settings" on page 130. Changing the value here only changes it for the selected deployment stage.
	When the timeout value is reached, the stage's deployment stops and an e-mail message is sent, if e-mail notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).
	For more information, see "Modifying the Stage Timeout" on page 135.

13.2.2 Creating and Populating a Deployment Stage

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, click *Action*, then select *Add Stage*.

You cannot add a stage while a deployment is in process.

3 Specify a deployment stage name, then click *OK*.

Deployment stages appear as device folders on the *Devices* tab, so you should specify names that help you to know a folder's purpose.

You might want to include something like "Deployment Stage" at the beginning of the name to sort the groups in the devices listing in ZENworks Control Center.

For information about naming in ZENworks Control Center, see Appendix A, "Naming Conventions in ZENworks Control Center," on page 255.

A newly created stage does not have any members. You must modify the stage's membership to add them.

4 Add devices to a deployment stage:

4a In the *Stage Members* column, click *View/Modify Members* for the stage for which you want to add members.

4b Click *Add*, browse for and select the devices, then click *OK*.

You can add individual devices or device groups, or any combination of them.

You can have both managed servers and workstations in the same deployment stage or in different stages, or you can split your servers and workstations into separate deployment stages.

IMPORTANT: Some of your network servers will be Primary Servers for use in ZENworks management, while other servers on your network might only be managed devices with the ZENworks Adaptive Agent installed on them.

You must update your Primary Servers before updating any of the other managed servers and especially before updating any managed workstations.

4c Repeat Step 4b until you are finished adding members to the stage.

4d To add members to another stage, repeat Step 4a through Step 4c.

5 Repeat Step 2 through Step 4 until you have created all of your deployment stages.

6 If you need to reorder the sequence of the deployment stages, select a stage, then click *Move Up* or *Move Down*.

If you are using one of the stages for test purposes, make sure that it is first in the listing.

13.2.3 Modifying the Stage Timeout

A stage timeout sets the length of time before a stage terminates. The default timeout is 3 days. You set the value for individual stage timeouts by using the procedure in this section. The global stage timeout value is established by following the steps in "Stage Timeout Settings" on page 130.

You cannot modify a stage if an update is in progress.

To set the timeout value for a selected stage:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, select the check box for a stage, click *Action*, then select *Modify Stage Timeout* to display the following dialog box:
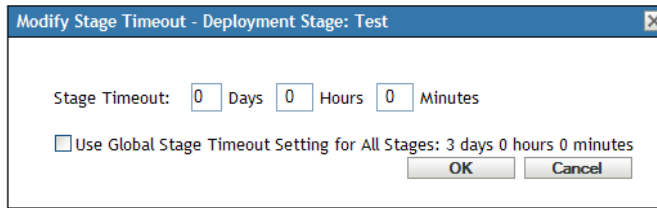
3 Specify the timeout value.

This change in timeout value only applies to the selected stage. If you specify a timeout value for this stage, set its value to be long enough to accommodate updating all of the devices in the stage.

When the timeout value is reached, the stage's deployment stops and an e-mail message is sent, if e-mail notification is configured. You can cancel the deployment, or you can clear the error to restart the stage and reset the timeout. Or, you can ignore all pending devices to trigger a stage progression (either automatic, or wait for administrator action based on the setting).

4 (Optional) Select the *Use Global Stage Timeout Setting for All Stages* check box to specify using the global timeout value (default of 3 days, 0 hours, and 0 minutes).

For more information, see "Stage Timeout Settings" on page 130.

5 Click *OK*.

13.2.4 Modifying Staging Behavior

The default stage behavior is to automatically advance through the configured stages. You can change this default behavior. If you change the staging behavior for one stage, the change becomes effective for all stages.

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, select the check box next to any stage, click *Action*, then select *Modify Stage Behavior* to display the following dialog box:
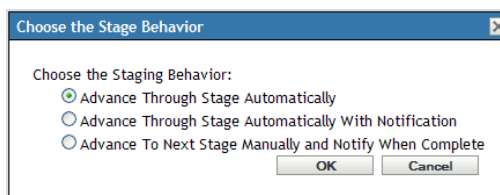
3 Select one of the following stage behaviors:

Advance Through Stages Automatically: As soon as one stage has completed its updates, the next stage begins. This is the default behavior (its check box is enabled).

After the last stage has completed, all applicable devices that are not members of a stage are then processed.

Advance Through Stages Automatically with Notification: Starts the first stage, sends an e-mail notification when it has completed, then automatically starts the next stage, and so on.

To use this option, a notification method must be set up on the System Update Download Settings page in the *E-mail Notification* section.

Advance to Next Stage Manually and Notify When Complete: Use this method for user action between the stages, such as reviewing the results of an update to a test group.

This option automatically starts the first stage. After any stage has completed, e-mail notification is sent, then the system waits for you to manually start the next stage.

To use this option, a notification method must be set up on the System Update Download Settings page in the *E-mail Notification* section.

4 Click *OK*.

13.2.5 Modifying Reboot Behavior

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

To modify the reboot behavior:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, select the check box for one or more the deployment stages, click *Action*, then click *Modify Reboot Behavior*.
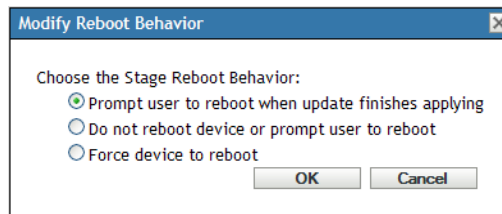
3 Select one of the following options:

- **Prompt User to Reboot When Update Finishes Applying (Default):** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted.

- **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

4 Click *OK*.

13.2.6 Modifying the Membership of a Deployment Stage

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 (Optional) Add devices to a deployment stage:

   2a In the *Stage Members* column, click *View/Modify Members* for the stage for which you want to add members.

2b Click *Add*, browse for and select the devices, then click *OK*.

You can add individual devices or device groups, or any combination of them.

You can have both managed servers and workstations in the same deployment stage or in different stages, or you can split your servers and workstations into separate deployment stages.

IMPORTANT: Some of your network servers will be Primary Servers for use in ZENworks management, while other servers on your network might only be managed devices with the ZENworks Adaptive Agent installed on them.

You must update your Primary Servers before updating any of the other managed servers and especially before updating any managed workstations.

2c Repeat Step 2b until you are finished adding members to the stage.

2d To add members to another stage, repeat Step 2a through Step 2c.

3 (Optional) Remove devices from a deployment stage:

3a In the *Stage Members* column, click *View/Modify Members* for the stage for which you want to remove members.
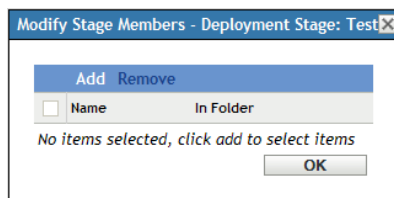
3b Select the check box next one or more devices that you want to remove, then click *Remove*.

4 Click *OK* when you have finished configuring the stage's membership.

13.2.7 Renaming a Deployment Stage

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, click the check box for the deployment stage to be renamed.

3 Click *Rename*.

4 In the Rename dialog box, specify the new name, then click *OK*.

For information about naming in ZENworks Control Center, see Appendix A, "Naming Conventions in ZENworks Control Center," on page 255.

13.2.8 Deleting a Deployment Stage

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, click the check box for one or more of the deployment stages to be deleted.

3 Click *Delete.*

Deleted stages cannot be recovered.

13.2.9 Rearranging the Order in Which Stages Start

All updates that use stages deploy to the devices that are members of the stages according to the currently listed staging order.

To rearrange the staging order:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deployment Stages panel, click the check box for the deployment stage to be moved.

3 Click *Move Up* or *Move Down* as necessary to rearrange the staging order.

4 Repeat Step 2 and Step 3 as necessary for each stage.

Managing Update Downloads

14

The Available System Updates panel on the System Updates page displays the updates that are available after you have checked for them. This includes the Product Recognition Update (PRU), which Novell® provides to update your knowledgebase so that ZENworks® Inventory can recognize newer software. The display refreshed according to the schedule you set in "Check for Updates Schedule" on page 123.

The following sections contain more information:

- Section 14.1, "Understanding Available Updates," on page 141
- Section 14.2, "Downloading Updates," on page 142
- Section 14.3, "Downloading and Installing the PRU," on page 144
- Section 14.4, "Canceling or Deleting a System Update," on page 145

14.1 Understanding Available Updates

The following figure illustrates the Available System Updates panel:

Figure 14-1 *Available System Updates Panel*

The Available System Updates panel displays all available updates. If an update is cumulative, meaning that it supersedes previous updates and includes new features and fixes from previous updates, those previous updates are not listed in the Available System Updates panel.

However, if a previous update is currently being deployed, it is listed in the Available System Updates panel, but it is greyed out and cannot be deployed to new devices. Because it is being deployed to devices, it displays in the Deploying System Updates panel.

If you need to deploy a previous update that is not listed (or is greyed out) in the Available System Updates panel, you must delete the cumulative update that superceded it and then download the manual import update file for that update from the Novell Downloads Web site (http://download.novell.com) and then import it.

The following table explains the column information and the *Auto Refresh* drop-down list (on the right side of the panel, above *Target Type*). For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 14-1 *Available System Updates column descriptions.*

Column Heading or List	Explanation
Update Name	Displays the name of the update, which is created by Novell. Click the name to access the Release Details page. For more information, see Chapter 17, "Reviewing the Content of an Update," on page 165.
Release Date	Displays the date that Novell created the update.
Download Date	Displays the date that you downloaded the update.
Applied Date	Displays the date that you applied the update.
Status	Displays the current status of the update, which is automatically updated every 15 seconds. For more information on the individual statuses, see Chapter 18, "Update Statuses," on page 169.
Importance	Displays the relative importance of the update's content to your ZENworks installation. Some possible entries include: **OPTIONAL:** Not required for normal operation of ZENworks. **MANDATORY:** A required update that must be applied.
Target Type	Displays the type of update, such as: **ZENworks Servers:** The update applies only to ZENworks Servers. **All Devices:** The update applies to all managed devices, including ZENworks Servers.
Auto Refresh	Click *Auto Refresh* (the menu item on the right side of the panel, above *Target Type*), then select one of the following: ❖ No Auto Refresh ❖ 15-second Refresh ❖ 30-second Refresh ❖ 60-second Refresh By default the panel view is not automatically refreshed. However, you can manually refresh the view by clicking the *System Updates* tab.

14.2 Downloading Updates

You can schedule the downloads, or download them manually:

❖ Section 14.2.1, "Scheduling Update Downloads," on page 143
❖ Section 14.2.2, "Manually Checking for Updates," on page 143
❖ Section 14.2.3, "Manually Downloading Updates," on page 143
❖ Section 14.2.4, "Manually Importing Updates to Servers without Internet Connectivity," on page 144

14.2.1 Scheduling Update Downloads

You can schedule both checking for updates and downloading them:

- "Check for Updates Schedule" on page 123
- "Download Schedule" on page 125

14.2.2 Manually Checking for Updates

If the most recent updates are not being displayed in the Available System Updates panel on the System Updates page, you can manually refresh the display.

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Available System Updates panel, click *Action > Check for Updates*.

Any available updates are displayed with a status of *Available*.

3 To re-sort the listed updates, click the heading for any of the columns in the Available System Updates panel.

Click the heading a second time to reverse the sorting order.

14.2.3 Manually Downloading Updates

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Available System Updates panel, select the check box next to one or more updates, click *Action*, then click *Download Update*.

The update is downloaded and its status is eventually set to `Downloaded`.

Depending on the size of the update, the downloading process can take some time.

3 To refresh the view of the download progress (*Status* column), click the *System Updates* tab or use the Auto Refresh option.

4 If you want to use deployment stages to apply the selected updates, go to Chapter 15, "Deploying Updates," on page 147 to configure the stages and deploy the updates.

or

To immediately apply the downloaded updates to all applicable devices in the Management Zone, select the check box for the downloaded update that you want to deploy, then click *Action > Deploy Update to Devices*. The Create System Update Deployment Wizard steps you through the deployment process. For more information, see Chapter 15, "Deploying Updates," on page 147.

14.2.4 Manually Importing Updates to Servers without Internet Connectivity

If you have servers in your environment that do not have Internet access, you can obtain the update or Product Recognition Update (PRU) files from the Novell Downloads page (http://download.novell.com), copy the files onto a CD or other media, and then use the CD to import the files to a ZENworks Primary Server by using the `zman system-update-import` command. For more information, see "System Update/Product Recognition Update Commands" in the "ZENworks Command Line Utilities" guide.

After the files are on a ZENworks Primary Server, the update or PRU displays in the Available System Updates panel on the *System Updates* tab in ZENworks Control Center (*Configuration > System Updates*). You can then follow the instructions in Chapter 15, "Deploying Updates," on page 147 to deploy the update to managed devices.

14.3 Downloading and Installing the PRU

Novell provides a Product Recognition Update (PRU) to update your knowledgebase so that ZENworks Inventory can recognize newer software.

This action deploys the PRU to your database and sets its deployment to your managed devices to be scheduled. Deployment is then done by the ZENworks Adaptive Agent on the devices.

If the PRU is not up-to-date, Inventory might return some software as unrecognized. However, you can use the Local Software Products utility to take a fingerprint of the unrecognized software to update your knowledgebase.

To download and install the PRU:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 If a PRU is not displayed in the Available System Updates panel, click *Action > Check for Updates*.

Information for the latest PRU is displayed, if it is available.

3 To download a listed PRU, go to the Available System Updates panel, select the check box for a listed PRU, then click *Action > Download Update*.

4 To install a downloaded PRU, go to the Available System Updates panel, then click *Action > Deploy PRU Now*.

The PRU is now listed in the Deploying System Updates panel, where its progress is displayed.

14.4 Canceling or Deleting a System Update

You can cancel the downloading of an update, or you can delete the update from the Available System Updates list.

To cancel an update:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 Select the check box for a system update that is being downloaded, then click *Action > Cancel Download*.

Cancelling an update cancels the downloading of an update. Already downloaded files are not automatically removed, but if you delete the update, any downloaded files are removed.

If a server's connection to the ZENworks database is lost while downloading an update, the download does not resume after reconnecting. Attempting to use the *Cancel Download* action results in the update hanging in the Cancel state. Use the `zman sudu --force` command to delete the update.

To delete an update:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.
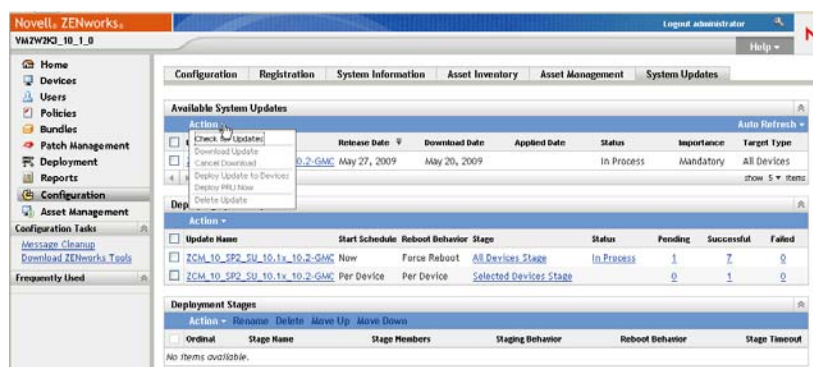
2 Select the check box for the system update that you want to delete, then click *Action > Delete Update*.

Deleting an update removes it from the list and all downloaded files are removed. However, if the deleted update is still available on the update server the next time that you check for updates, it is displayed in the list again for possible downloading.

3 Click *OK* to confirm the deletion.

Deploying Updates

<div style="text-align: right; font-size: 3em; font-weight: bold;">15</div>

15.1 Understanding Deploying Updates

You have the following options for deploying an update:

- Deploy the update to all devices without using deployment stages. You can schedule the deployment.

- Deploy the update by using deployment stages where one stage automatically starts after the previous one has completed, unless you have configured stages to pause the deployment and send e-mail notifications to the administrator. You can schedule the deployment.

- Deploy the update by using deployment stages with e-mail notification to allow manual control for starting the next stage. You can use this option to test the update before deploying it to all devices in your production environment. You can schedule the deployment.

- Deploy the update to specific devices (selected individually and by device groups) without using deployment stages. You can use this option to test the update before deploying it to all devices in your production environment. You can schedule the deployment.

IMPORTANT: After an update has been deployed, it cannot be removed without assistance from Novell Support (http://www.novell.com/support).

If you choose to retire a managed device in ZENworks Control Center before deploying an update to all the devices in the Management Zone, you must first ensure that the device has retired and subsequently apply the update. The device is retired only when the ZENworks Adaptive Agent installed on the device is refreshed. If you deploy the update before the agent is refreshed, the update is also applied to the retired device. The agent is automatically refreshed during the next device refresh schedule (the default device refresh interval is set to 12 hours). If you want to deploy the update before the next device refresh schedule, you must manually refresh the agent.

The Deploying System Updates panel displays the progress and results of deploying an update.

Updates are removed from this panel when the entire update process completes. You can view the Deployment History panel on the Release Details page for information on deployed updates.

The following figure illustrates the Deploying System Updates panel:

Figure 15-1 *Deploying System Updates Panel*

The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order.

Table 15-1 *Deploying System Updates column descriptions*

Column Heading	Explanation
Update Name	Displays the name of the update, which is created by Novell.
	Click the name to access the Status by Device page. You can also click the underlined number in the *Pending*, *Successful*, or *Failed* columns to view the appropriate Status by Device page, filtered to display devices with that status.
Start Schedule	Displays the current schedule, if any has been set. Use the Reschedule Deployment action to reschedule the update. For more information, see Section 15.4, "Rescheduling a Deployment," on page 156.
	Each device can have its own schedule.
Reboot Behavior	Displays the reboot behavior of devices after the update is deployed.
	Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.
	You have the following reboot options:
	◆ **Prompt User to Reboot When Update Finishes Applying:** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. This is the default.
	◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.
	◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

Column Heading	Explanation
Stage	Indicates the deployment state. The possible entries are:
	stage_name: The update is being deployed to the managed devices that are members of the current stage that is listed.
	Selected Devices Stage: The update is being deployed to selected managed devices without the use of stages.
	All Devices Stage: The update is being deployed to all managed devices in the Management Zone without the use of stages.
	All Devices Stage is displayed after the last stage has completed, which means any devices left in the Management Zone that were not part of a completed stage are then receiving the update. In other words, managed devices cannot skip an update.
	If stages are being used, click a stage name to view the device status for each stage member. For more information, see Section 15.8, "Viewing Status by Device," on page 158.
Status	Indicates the status of the update being deployed (for the current stage, if stages are being used). For information on the possible statuses, see Chapter 18, "Update Statuses," on page 169.
	Click an item in the *Status* column to view a message explaining the current status.
	When the status for an update reaches either the APPLIED or BASELINE status, the update deployment item is no longer displayed in this panel, but is displayed in the Deployment History panel. For more information, see Section 15.8, "Viewing Status by Device," on page 158.
Pending	Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes.
	Click the number to view the Status by Device page, which displays the devices that have a pending deployment of the update. For more information, see Section 15.8, "Viewing Status by Device," on page 158.
Successful	Displays the number of devices for which the update deployment process is complete.
	Click the number to view the Status by Device page, which displays the devices that successfully received the update. For more information, see Section 15.8, "Viewing Status by Device," on page 158.
Failed	Number of devices for which the update deployment process has failed.
	Click the number to view the Status by Device page, which displays the devices that failed to receive the update. For more information, see Section 15.8, "Viewing Status by Device," on page 158.
	For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.

15.2 Deploying Updates

1 (Optional) If you want to use deployment stages, set them up if you have not previously done so.

For more information, see Section 13.2, "Creating Deployment Stages," on page 132.

2 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab to display the Available System Updates panel:

3 (Conditional) If new updates are not being displayed, click *Action > Check for Updates*.

The following illustrates available updates:

4 (Optional) To view the content of an available update, click the name of the update (in the *Update Name* column) to display the Release Details page:
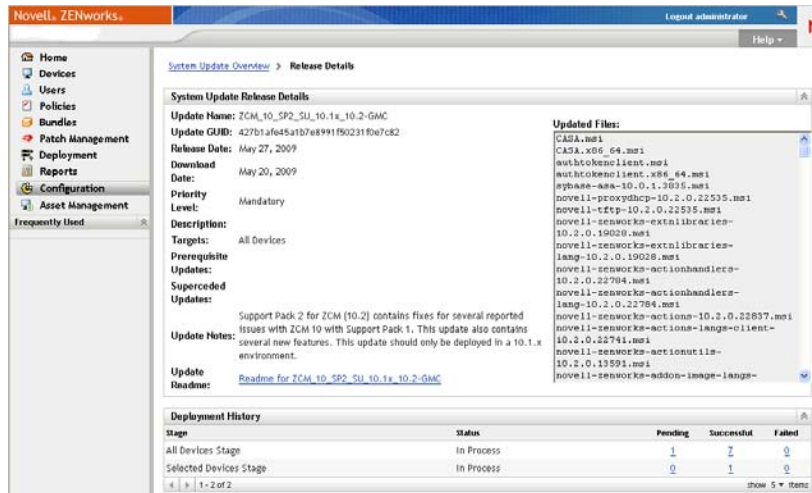
For more information, see Chapter 17, "Reviewing the Content of an Update," on page 165.

5 To download an update, select the check box for it, click *Action* > then click *Download Updates*.

After an update has completed downloading, its status is automatically changed to `Downloaded`. The length of time to download an update depends on its size and your hardware configuration.

You can download multiple updates at a time, but you can only deploy one at a time. Because these steps are repeated for each update, you only need to download the update you plan to deploy at this time.

The following illustrates downloaded updates:

6 Determine whether to deploy the downloaded update, then select its check box.

You can deploy only one update at a time.

If you want to review the content of the update that you downloaded, see Chapter 17, "Reviewing the Content of an Update," on page 165 for instructions about reviewing the content of a downloaded update.

If you want to download a different update for deployment, return to Step 4.

7 Click *Action* > *Deploy Update to Devices*.

This starts the Create System Update Deployment Wizard for deploying the update to all applicable devices. If deployment stages are enabled, they can be used.

The Deployment Wizard provides you with many options, including scheduling the deployment.

Create System Update Deployment
Step 1: Choose the Reboot Behavior for the Deployment

Update Name: Update for ZCM 10.0.7
Release Date: Apr 7, 2008
Download Date: Apr 12, 2008
Priority Level: OPTIONAL
Description:
Targets:
Product Version: 0
Update Notes:
Update Readme:

Updated Files:

Choose the Deployment Option for the Management Zone:
○ Deploy System Updates to Selected Devices in the Management Zone
◉ Deploy System Updates to All Devices in the Management Zone
○ Deploy System Updates using Stages to Devices in the Management Zone

[<< Back] [Next >>] [Cancel]

8 In the Deployment Wizard, complete the following steps:

    8a On the Choose the System Update and Deployment Option page, select a deployment option (all of them can be scheduled in a subsequent wizard page).

    Depending on the size of your ZENworks system, we recommend as a best practice to deploy the selected update to all ZENworks Servers before deploying the update to the managed devices that contact those servers. In a production environment, we recommend that you use the *Deploy System Updates to Selected Devices in the Management Zone* option to update the servers first and then update the managed devices, or you should use the *Deploy System Updates Using Stages to Devices in the Management Zone* option to deploy the update to a stage containing servers before deploying the update to another stage containing managed devices.

        ◆ **Deploy System Updates to Selected Devices in the Management Zone:** Deploys the selected update to only the devices that you select in Step 8e. Stages are not used. If you choose this option, the next page of the wizard lets you select the reboot behavior for the devices included in the deployment.

        ◆ **Deploy System Updates to All Devices in the Management Zone:** Deploys the selected update to all devices in the Management Zone. Stages are not used. If you choose this option, the next page of the wizard lets you select the reboot behavior for the devices included in the deployment.

        This option does not guarantee that ZENworks Servers are updated before managed devices. In a large ZENworks system or in a production environment, we recommend that you use one of the other options.

        ◆ **Deploy System Updates Using Stages to Devices in the Management Zone:** The selected update is deployed to only the devices that have membership in one of the stages. The stages are executed one after the other; that is, a stage does not start until the previous stage completes. After all stages complete, the *All Devices* stage is run. If you choose this option, and because the reboot behavior is set per stage, the next page of the wizard lets you select the reboot behavior for the All Devices Stage, which runs automatically after all other stages.

        For more information on stages, see the Section 13.2, "Creating Deployment Stages," on page 132.

8b Click *Next* to display the following page:

8c Select one of the following options:

- ◆ **Prompt User to Reboot When Update Finishes Applying:** After the update has been applied, a request to reboot is immediately displayed. If the user initially rejects rebooting, the user is periodically requested to reboot the device, until the device is rebooted. This is the default.

- ◆ **Do Not Reboot Device:** The device does not reboot; however, the user is periodically requested to reboot the device, until the device is rebooted.

- ◆ **Force Device to Reboot:** After the update has been applied, the device is automatically rebooted without user intervention, if a reboot is required by the update.

Some updates do not require a device to be rebooted after they have been deployed to a device. However, if a reboot is required to complete the update process, the deployment is not completed until the device is rebooted.

8d Click *Next*.

8e (Conditional) If you selected *Deploy System Updates to Selected Devices* in the Management Zone in Step 8a, the following wizard page displays:

8f To add devices or groups to the deployment configuration, click *Add*, browse for and select the devices or device groups to include in the update deployment, then click *OK*.

8g Click *Next* to display the Choose the Deployment Schedule page.

8h Fill in the fields:

Schedule Type: Select one of the schedule options:

- ◆ **Now:** Immediately deploys the update when you finish the wizard.

- **Date Specific:** Deploys the update according to the schedule that you set. The following options are displayed for the *Date Specific* option:

Fill in the fields:

- **Start Date:** Select the deployment date from the calendar.

- **Run Event Every Year:** Select this option to deploy the update every year on the start date.

- **Process Immediately if Device Unable to Execute on Schedule:** Do not use this option for updates. It does not apply to updates.

- **Start Immediately at Start Time:** Lets you deploy updates at the start time you specify.

- **Start at a Random Time Between Start and End Times:** Lets you deploy updates at a random time between the times you specify. Fill in the *End Time* fields.

8i Click *Next* to display the Review Deployment Options page, then review the information.

```
Create System Update Deployment
   Step 5: Review Deployment Options

Update Name:                ZCM Update 10.0.2
Deployment Type:            Deploy System Updates to Selected Devices in the Management Zone
Deployment Reboot Behavior: Prompt user to reboot when update finishes applying
Deployment Schedule:        Schedule Type:
                               Date Specific

                            Dates scheduled event will be performed
                            on:
                               4/12/08

                            Start time:
                               1:00 AM

                            End time:

                                    << Back      Finish       Cancel
```

9 If you are satisfied, click *Finish* to start the update's deployment; otherwise, click *Back* to make changes.

10 (Conditional) If you chose the deployment schedule type as *Now* in Step 8h, the update is deployed only during the next device refresh schedule. However, if you want to immediately apply the update to the device, you must manually refresh the managed device in one of the following ways:

 ◆ Click the *Devices* tab > the *Managed* tab > *Servers* or *Workstations*, then select the check box next to the devices you want to refresh, click *Quick Tasks* > *Refresh Device*.

 ◆ On the managed device, right-click the ▣ icon, then click *Refresh*.

 ◆ On the Linux unmanaged device, open a terminal, change your current working directory to `/opt/novell/zenworks/bin/`, and execute `./zac ref`.

11 To observe the progress of the update deployment, do any of the following:

 ◆ In ZENworks Control Center, observe the panels on the System Updates page:

   ◆ The Available System Updates panel automatically displays `Baselined` in the *Status* column when the deployment has completed.

   ◆ The Deployed System Updates panel displays the update in its listing when the deployment has completed.

 ◆ On a Windows device where the update is being deployed, right-click the ZENworks icon, then select *Show Progress* to open the ZENworks Progress dialog box.

   You cannot view the download progress on a Linux device because these devices are not ZENworks managed devices and do not have the ZENworks icon.

   The progress of downloading the update MSI files is displayed. When it has finished, the dialog box automatically closes and the *Show Progress* option is dimmed.

   After a 5-minute wait, all ZENworks services are closed on the device. Then the MSIs (for Windows) or RPMs (for Linux) are installed and the services are restarted.

12 To verify that the update was successfully deployed:

12a To verify that the MSIs or RPMs have been installed and the update process is complete, review the following log files:

Windows: *installation_path*\novell\zenworks\logs\systemupdate.log

Linux: `/var/opt/novell/log/zenworks/SystemUpdate.log`

You can also look for the existence of the following file (the same path for both Windows and Linux):

`installation_path\novell\zenworks\work\system-update\systemupdate.ini.timestamp`

12b Test the ZENworks software on the device to ensure that it is working properly.

12c To ensure that the update has been deployed, do one of the following to determine whether the version number has been incremented (for example, the first update for ZENworks should change the value from 10.0.*x* to 10.0.2):

- ◆ Open the Windows Registry and browse to the following:

  `HKEY_LOCAL_MACHINE/Software/Novell`

  For the *ZENworks* key, the update process should have incremented the *version* value.

- ◆ On a Windows device, review the following file:

  `Installation_path\Novell\ZENworks\version.txt`

- ◆ On a Linux device, review the following file:

  `/etc/opt/novell/zenworks/version.txt`

12d Repeat Step 12a through Step 12c for each test device.

13 (Conditional) If you are receiving e-mail notifications at the completion of the deployment stages and are ready to begin the next stage, go to the Deployed System Updates panel, then click *Action > Advance to Next Stage*.

14 To deploy another update, repeat from Step 4.

15.3 Starting a Pending Stage

The default stage behavior is to automatically advance through the configured stages. However, you can configure stage behavior for individual stages or for all stages.

The *Start Pending Stage* option is only available if you used the *Advance to Next Stage Manually and Notify When Complete* option to stop each stage for manual input before continuing, instead of having the stages complete automatically.

To start a pending stage:

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, select the check boxes for an update.

3 Click *Action > Start Pending Stage*.

15.4 Rescheduling a Deployment

You cannot reschedule a deployment after it starts:

- ◆ Section 15.4.1, "Rescheduling a Deployment for the All Stages Status," on page 157
- ◆ Section 15.4.2, "Rescheduling a Deployment for the Other Statuses," on page 157

15.4.1 Rescheduling a Deployment for the All Stages Status

1 Select the check box for an update.

Because all devices do not need to have the update deployed at the same time, you can set individual deployment schedules for the devices.

2 Click *Action > Reschedule Deployment* to open the Redeployment Schedule dialog box.

3 Either click *OK* to accept the default schedule of *Now*, or select *Date Specific* in the *Schedule Type* field, specify the new date, then click *OK*.

15.4.2 Rescheduling a Deployment for the Other Statuses

1 Select the check box for an update.

2 Click *Action > Reschedule Deployment*.

3 In the Status by Device page, select the check box for an update, then click *Reschedule Deployment*.

4 On the Status by Device page, select one or more devices that are listed in the *Device* column.

5 Click *Reschedule Devices* to open the Redeployment Schedule dialog box.

6 Either click *OK* to accept the default schedule of *Now*, or select *Date Specific* in the *Schedule Type* field and specify the new date, then click *OK*.

15.5 Bypassing Staging

You can bypass the stages at any time and immediately deploy the update to all managed devices in the Management Zone.

1 Select the check box for an update.

2 Click *Action > Bypass Stages and Apply to All Devices*.

15.6 Canceling a Deployment

This option is mainly for canceling a deployment that has not yet started.

If you select to apply the update only through stages, and if you cancel the update deployment, the status in the Available System Updates panel is changed to *Aborted*.

However, for an update, you can select to deploy to individual devices, as well as through stages for the other devices. Therefore, the status in the Available System Updates panel is changed to:

◆ *Ready* if you cancel only the staged deployment.

◆ *Aborted* if you cancel both the staged deployment and the deployment for individually selected devices.

To cancel a deployment:

1 Select the check box for an update.

2 Click *Action > Cancel Deployment*.

WARNING: If you cancel a deployment that is currently running (not just scheduled), all deployment actions performed up to that point cannot be reversed. There currently is no rollback option.

3 Click *OK* to confirm canceling the deployment.

15.7 Clearing an Error to Retry a Deployment

To continue with the deployment after determining that an error is not serious enough to stop the deployment:

1 Click *Action > Clear Error and Continue*.

15.8 Viewing Status by Device

The following sections contain more information:

- Section 15.8.1, "Understanding Device Statuses," on page 158
- Section 15.8.2, "Viewing a Device's Properties," on page 159
- Section 15.8.3, "Viewing Information on a Device's Status," on page 159
- Section 15.8.4, "Toggling Ignored Devices," on page 160
- Section 15.8.5, "Redeploying Updates to Devices," on page 160
- Section 15.8.6, "Rescheduling Updates to Devices," on page 161
- Section 15.8.7, "Refreshing Devices," on page 161

15.8.1 Understanding Device Statuses

The following graphic illustrates the Deploying System Updates panel on the System Updates page:

Figure 15-2 *Deploying System Updates Panel*

You can click any of the underlined links to display the corresponding status of devices. For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

Figure 15-3 *Device by Status Page for Devices with Pending Status*

The possible statuses that can be viewed on this page are:

All Devices: Lists all devices that were configured to receive the selected update, regardless of status.

Pending Devices: Lists only the devices where the selected update is pending.

Successful Devices: Lists all of the devices where the selected update has been successfully deployed.

Failed Devices: Lists only the devices where the selected update failed.

Update Assigned: Lists only the devices where the selected update has been assigned.
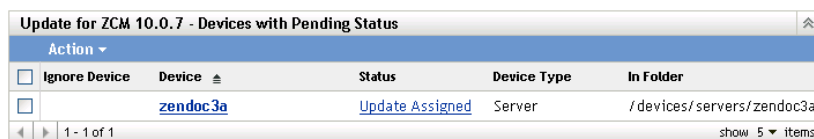
The following table explains the column information. For some columns, you can sort the listed information by clicking a column heading. Click it again to reverse the sorting order. This page refreshes automatically to allow you to work with devices as the update is applied on them.

Column Heading	Explanation
Device	The device's name. Click it to display the device's properties page in ZENworks Control Center.
Status	The current update deployment status for the device. Click the status item to view information about the status. For more information on the individual statuses, see Chapter 18, "Update Statuses," on page 169.
Device Type	Whether the device is a server or workstation.
In Folder	Displays the ZENworks Control Center folder where the device's ZENworks object resides.

15.8.2 Viewing a Device's Properties

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Click the underlined link in the *Device* column to display the device's properties.

15.8.3 Viewing Information on a Device's Status

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

Update for ZCM 10.0.7 - Devices with Pending Status				
Action ▾				
☐ Ignore Device	Device ⬆	Status	Device Type	In Folder
☐	zendoc3a	Update Assigned	Server	/devices/servers/zendoc3a
◄ ▶ 1 - 1 of 1				show 5 ▾ items

3 Click the underlined link in the *Status* column to display status information about the device.

15.8.4 Toggling Ignored Devices

Ignoring a device is helpful if an update fails on a device and you want to continue with the deployment without resolving the error. For example, if a device is offline, you might want to ignore that device so that the deployment can continue.

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

Update for ZCM 10.0.7 - Devices with Pending Status				
Action ▾				
☐ Ignore Device	Device ⬆	Status	Device Type	In Folder
☐	zendoc3a	Update Assigned	Server	/devices/servers/zendoc3a
◄ ▶ 1 - 1 of 1				show 5 ▾ items

3 Click the check box next to one or more devices.

4 Click *Action > Toggle Ignored Devices*.

The options available from the *Action* menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

15.8.5 Redeploying Updates to Devices

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

Update for ZCM 10.0.7 - Devices with Pending Status				
Action ▾				
☐ Ignore Device	Device ⬆	Status	Device Type	In Folder
☐	zendoc3a	Update Assigned	Server	/devices/servers/zendoc3a
◄ ▶ 1 - 1 of 1				show 5 ▾ items

3 Select the check box next to one or more devices.

4 Click *Action > Redeploy Update to Devices*.
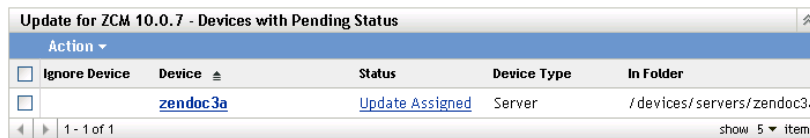
The options available from the *Action* menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

15.8.6 Rescheduling Updates to Devices

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Select the check box next to one or more devices.

4 Click *Action > Reschedule Devices*.

The options available from the *Action* menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.
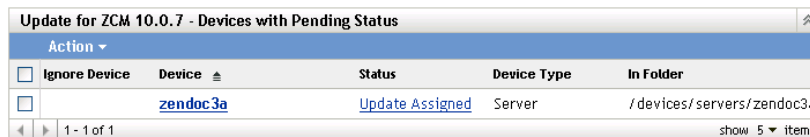
The *Reschedule Devices* option displays only when the update deployment is scheduled. If the update has a schedule of *Now*, this option is not available.

15.8.7 Refreshing Devices

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Deploying System Updates panel, click an underlined link in the *Update Name*, *Stage*, *Pending*, *Successful*, or *Failed* column to display the appropriate Status by Device page.

For example, if you click the link in the *Pending* column, you see the status of devices on which the deployment is pending, as in the following figure:

3 Select the check box next to one or more devices.

4 Click *Action > Refresh Device*.

The options available from the *Action* menu vary, depending on whether you are viewing the All Assigned Devices Status panel, the Devices with Pending Status panel, or the Devices with Failed Status panel. If you are viewing the Devices with Success Status panel, no options are available.

Deleting Updates

16

You can clear an update that fails to download, or an update that you do not want to deploy.

1 In ZENworks Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Available System Updates panel, select the check boxes for one or more updates.

3 Click *Action > Delete Update*.
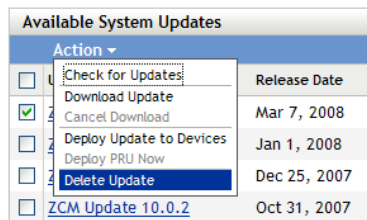
The update is deleted from the list and all downloaded files are removed. However, if the deleted update is still available on the update server, it is displayed in the list again for possible downloading the next time that you check for updates.

Reviewing the Content of an Update

<div style="text-align: right">17</div>

You might want to review the content of an update for the following reasons:

- To determine whether to download the update
- To determine whether to deploy a downloaded update
- To review what was deployed by the update
- To review the history of the update

This section contains the following information:

17.1 Viewing the Release Details Page

1 In ZENworks® Control Center, click *Configuration* in the left pane, then click the *System Updates* tab.

2 In the Available System Updates panel, click an update name in the *Update Name* column to display the Release Details page:
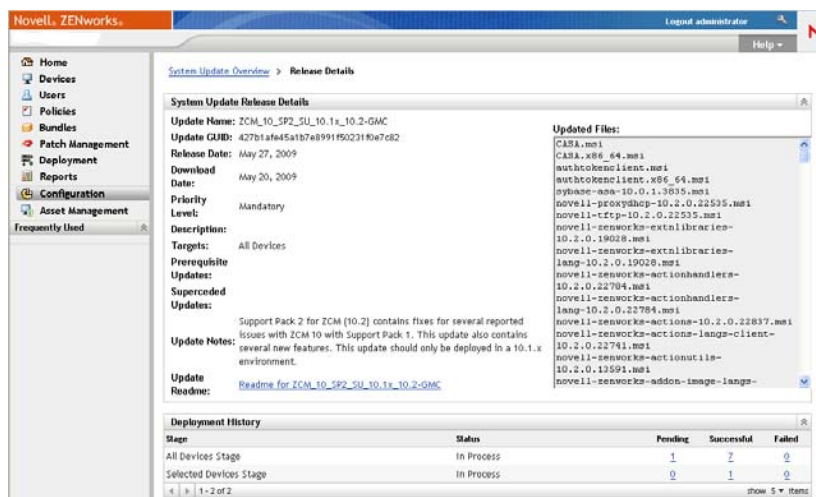
17.2 Update Release Details

Table 17-1 *Information from the System Update Release Details Panel*

Column Heading	Explanation
Update Name	The name of the update, which is created by Novell®.
Update GUID	The update's GUID.
Release Date	The date the update was released by Novell.
Download Date	The date you downloaded the content of the update, including all files necessary to install the update.
Priority Level	The relative importance of the update's content to your ZENworks installation. Some possible entries: **OPTIONAL:** Not required for normal operation of ZENworks. **MANDATORY:** A required update that must be applied.
Description	Brief information about the purpose of the update and its content.
Targets	Indicates whether the target devices are Primary Servers only, all managed devices, or servers with ZENworks roles.
Product Version	The version of ZENworks in this update.
Prerequisite Updates	Any updates that are required for this update.
Superseded Updates	Any updates that the current update supersedes.
Update Notes	Brief information about important issues related to the update.
Update Readme	Information pertinent to deploying the update, such as last-minute instructions. Click this entry to open the Readme.
Updated Files	Lists all of the files contained in the update that will be applied to update your ZENworks software.

17.3 Deployment History

This Deployment History panel displays a current snapshot of the history for the selected update. It does not automatically refresh its content.

The following sections contain more information:

17.3.1 Understanding Deployment History Details

Table 17-2 *Columns for the Deployment History Details Panel*

Column Heading	Explanation
Stage	Indicates the deployment method used. The possible entries are: **stage_name:** The update was deployed to the managed devices that are members of the stage that is listed. **Selected Devices Stage:** The update was deployed to selected managed devices in the Management Zone that are not members of a stage. **All Devices Stage:** The update was deployed to all managed devices in the Management Zone that are not members of a stage.
Status	Indicates the status of the update that was successfully deployed, such as *Applied* or *Baselined*. **In Process:** The update is currently being deployed to the members of the stage. For more information on the individual statuses, see Chapter 18, "Update Statuses," on page 169.
Pending	Displays the number of devices for which the update deployment process is pending. A device can be pending if it is a member of a stage when stages are not automatically started after another stage completes. Click the number to view the Status by Device page, which displays the devices that have the deployment of the update pending.
Successful	Displays the number of devices for which the update deployment process has completed. Click the number to view the Status by Device page, with the devices displayed that successfully received the update.
Failed	Displays the number of devices for which the update deployment process has failed. Click the number to view the Status by Device page, which displays the devices that failed to receive the update. For failed deployments, you have the option of ignoring the error and continuing, or you can redeploy the update if the error has been resolved.

17.3.2 Performing Deployment History Tasks

Table 17-3 *Tasks for Evaluating an Update's Deployment History*

Task	Steps	Additional Details
View which devices have their deployment pending	1. In the Deployment Stages panel, click the number in the *Pending* column. 2. On the Status by Device page, review the information.	Displays devices where the deployment of the update is pending.
View the devices where deployment was successful	1. In the Deployment Stages panel, click the number in the *Successful* column. 2. On the Status by Device page, review the information.	Displays devices that have had the selected update successfully applied.
View which devices had the deployment fail	1. In the Deployment Stages panel, click the number in the *Failed* column. 2. On the Status by Device page, review the information.	Displays devices where the update deployment failed. In order to consider a deployment successfully finished when there are failed devices, the failed devices should either be ignored, or the error should be fixed before you redeploy the update to those failed devices.

Update Statuses 18

The following update statuses can be displayed in the *Status* column of several System Update panels in ZENworks® Control Center:

Aborted: The deployment of the update was stopped, such as by selecting *Action > Cancel Deployment*.

Applied: The update was successfully applied to the managed devices.

Available: Updates with this status have downloaded the information about the update, which you can view by clicking the update name in the *Update ID* column.

Awaiting Reboot: The device is waiting for you to manually reboot after the update has been applied.

Baselined: The update has been assigned to the /Devices folder, meaning that all new devices added to the Management Zone automatically get the update, unless they are already at that update level. When an update is baselined, any packages (MSIs and RPMs) that were updated by the system update have been deleted and replaced with the new packages. A baselined update is considered complete; although, individual devices could have been ignored.

In previous versions of ZENworks Configuration Management, when an update was baselined, the ZENworks Agent packages on all ZENworks Servers were rebuilt with the latest software. In this version, however, the agent packages are rebuilt during the upgrade process of each individual Server.

Canceled: Displays after you select *Action > Cancel Download* and the download or deployment was successfully canceled.

Canceling: Temporarily displays after you select *Action > Cancel Download*.

Deploying: The update is currently being deployed. See Chapter 15, "Deploying Updates," on page 147 for further deployment information and for actions that you can take on an update that is being deployed.

Downloaded: You have downloaded the update's content and it is ready for deployment. See Chapter 15, "Deploying Updates," on page 147 for further deployment information and for actions that you can take on an update that has been deployed.

Downloading: Displays a percentage of completion during the downloading process. This status changes to *Downloaded* when the download is complete.

Error: The stage failed to complete because of an error with one or more of the devices being updated. You can select to ignore the error and continue, or to fix the error before continuing. This status can also indicate an error in downloading the update.

In Process: That the current stage is active.

Installing Update: The update is currently being installed on the device.

Ready: The current stage is ready to start.

Reboot in Process: Rebooting the device is in process.

Reboot Process Canceled: Rebooting the device after the update was applied was canceled.

Scheduled: The update has a schedule defined for it. See Chapter 15, "Deploying Updates," on page 147 when creating the deployment in the Create System Update Deployment Wizard. You can alter the update's schedule by using the *Action > Reschedule Deployment* option.

Stage Complete: The stage has completed.

Status Unknown: The status of updates for the device is unknown.

Superceded: Indicates that the update has been replaced by another update listed in the Available System Updates section. You should see this status only if you are in the process of deploying this update and there are pending devices. You can delete a superseded update, but you cannot deploy it.

Update Aborted: The update was canceled for the device.

Update Completed: Installation of the update has been completed on the device.

Update Completed with Errors: Installation of the update has been completed on the device, but there were errors. Check the update log for details.

Update Assigned: The update has been assigned to the device.

Zone Pre-Update Actions: Actions for the Management Zone are taking place before the server update begins.

Zone Post-Update Actions: Actions for the Management Zone are taking place after the server upgrade finishes.

Users

IV

The following sections provide information about connecting your ZENworks® Management Zone to an authoritative user source (Microsoft Active Directory* or Novell® eDirectory™) and managing how users log in to the ZENworks Management Zone:

User Sources

Novell® ZENworks® 10 Asset Management enables you to connect to one or more LDAP directories to provide authoritative user sources in ZENworks. Adding a user source lets you associate ZENworks administrator accounts with LDAP user accounts, associate devices with the users who primarily use them, and run asset inventory and management reports that include users.

NOTE: After you define a user source, the ZENworks Adaptive Agent automatically prompts device users to log in to the ZENworks Management Zone. If you do not want users to receive this prompt, you can uninstall or disable the User Management module at the ZENworks Adaptive Agent level. For more information, see Section 9.3, "Configuring Adaptive Agent Settings after Deployment," on page 100.

The following sections provide instructions to define user sources:

- Section 19.1, "Prerequisites," on page 173
- Section 19.2, "Adding a User Source," on page 173
- Section 19.3, "Deleting a User Source," on page 176
- Section 19.4, "Adding a Container from a User Source," on page 177
- Section 19.5, "Providing LDAP Load Balancing and Fault Tolerance," on page 177

19.1 Prerequisites

- **Minimum directory version:** Novell eDirectory™ 8.7.3 or Microsoft Active Directory on Windows 2000 SP4.
- **Minimum LDAP version:** LDAPv3
- **Minimum user account rights:** Read rights.

  For Active Directory, you can use a basic user account. This provides sufficient read access to the directory.

  For eDirectory, you need inheritable read rights to the following attributes: CN, O, OU, C, DC, GUID, WM:NAME DNS, and Object Class. You can assign the rights at the directory's root context or at another context you designate as the ZENworks root context.

  The username and password used to access the user source directory are stored in clear-text format on the ZENworks Primary servers in the `iaRealm.xml` file. If security is a concern, ensure that you limit access to the directory.

- **DNS name resolution:** With Active Directory, your ZENworks Servers (in particular, the DNS clients on the ZENworks Server) must be able to resolve the DNS name of each Active Directory domain defined as a user source. Otherwise, users from the Active Directory domain cannot log in to the ZENworks Management Zone.

19.2 Adding a User Source

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

2 In the User Sources panel, click *New* to launch the Create New User Source Wizard.

3 Follow the prompts to create the connection to the user source.

For information about each of the wizard pages, click the *Help* button or refer to the following table:

Wizard Page	Details
Connection Information page	Specify the information required to create a connection to the LDAP directory: ◆ **Address:** Specify the IP address or DNS hostname of the server where the LDAP directory resides. ◆ **Use SSL:** By default, this option is enabled. Disable the option if the LDAP server is not using the SSL (Secure Socket Layer) protocol. ◆ **Port:** This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the *Use SSL* option is enabled or disabled. If your LDAP server is listening on a different port, select that port number. ◆ **Root Context:** The root context establishes the point in the directory where you can begin to browse for user containers. Specifying a root context can enable you to browse less of the directory, but it is optional. If you don't specify a root context, the directory's root container becomes the entry point.

Credentials page	Specify a username and password for accessing the directory:
	
	◆ **Username:** Specify the username for a user that has read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended.
	
	For Novell eDirectory access, use standard LDAP notation. For example:
	
	`cn=admin_read_only,ou=users,o=mycompany`
	
	For Microsoft Active Directory, use standard domain notation. For example:
	
	`AdminReadOnly@mycompany.com`
	
	◆ **Password:** Specify the password for the user you specified in the *Username* field.

Wizard Page	Details
User Containers page	After you connect to an LDAP directory as a user source, you can define the containers within the directory that you want exposed. The number of user containers you define is determined by how much of the directory you want to expose. Consider the following example:

Assume that you want to expose only the user and user groups in the Accounting, Sales, and Groups containers. To gain access to those users and groups, you have two options:

- ◆ You can add MyCompany/EMEA as a user container, so all containers located below EMEA are visible in ZENworks Control Center, including the Servers and Services containers. Only users and user groups located in the EMEA containers are visible (servers and services are not), but the structure is still exposed.

- ◆ You can add MyCompany/EMEA/Accounting as one user container, MyCompany/EMEA/Sales as a second container, and MyCompany/EMEA/Groups as a third container. Only these containers become visible as folders beneath the MyCompany directory reference in ZENworks Control Center.

To add the containers where users reside:

1. Click *Add* to display the Add User Container dialog box.

2. In the *Context* field, click 🔍 to browse for and select the desired container.

3. In the *Display Name* field, specify the name you want used for the user container when it is displayed in ZENworks Control Center.

4. Click *OK* to add the container to the list.

19.3 Deleting a User Source

When you delete a source, all assignments and messages for the source's users are removed. You cannot undo a source deletion.

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

2 In the User Sources panel, select the check box next to the user source, then click *Delete*.

3 Click *OK* to confirm the deletion.

19.4 Adding a Container from a User Source

After you've defined a user source in your Management Zone, you can add containers from that source at any time.

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

2 In the User Sources panel, click the user source.

Configuration > **ZENSM1**

ZENSM1

Settings

General

Name:	ZENSM1
Directory Type:	eDirectory
Communication Status:	
Connection Details: *(Edit)*	Address: 123.65.123.65
	Port: 389
	Use SSL: No
Username and Password: *(Edit)*	cn=admin,ou=servers,o=novell
Root Context: *(Edit)*	
Description: *(Edit)*	

User Containers

Add Replace Remove Rename

Context	Name
/ ZENSM1 / Novell / Users	Novell Users

3 In the User Containers panel, click *Add* to display the Add User Container dialog box, then fill in the following fields:

Context: Click 🔍 to browse for and select the container you want to add.

Display Name: Specify the name you want used for the user container when it is displayed in ZENworks Control Center. The name cannot be the same as the name of any other user containers.

4 Click *OK* to add the user container.

The container, and its users and user groups, is now available on the *Users* page.

19.5 Providing LDAP Load Balancing and Fault Tolerance

If you have multiple LDAP servers for access to your user source (directory), you can configure your ZENworks Servers to know about each of the LDAP servers. This provides both load balancing and fault tolerance.

For example, if you have multiple ZENworks Servers, you can configure each one to access the user source through a different LDAP server. This distributes the workload more evenly among the LDAP Servers.

Likewise, for each ZENworks Server, you can list multiple LDAP servers through which it can connect to the user source. If one of the LDAP servers becomes unavailable, the ZENworks Server uses another LDAP Server.

To define additional LDAP servers for a ZENworks Server:

1 Copy the `alt-servers.properties.sample` file to a new file called `alt-servers.properties`. The file is located in the following directory on the ZENworks Server:

  ◆ Windows: `c:\program files\novell\zenworks\conf\datamodel\authsource`

  ◆ Linux: `/etc/opt/novell/zenworks/datamodel/authsource`

2 Change the `alt-servers.properties` file to include the user source name and list of LDAP servers that can be used to access it.

The file, shown below, contains instructions for formatting the entries.

```
# Sample alt-servers.properties file.
#
# The alt-servers.properties file allows you to configure how this server
will connect to a particular user source.
# When connecting to a LDAP user source, ZENworks will try to connect to
the servers in the order listed in this file.
# This allows for fail-over to other LDAP servers and for load
distribution, if different ZENworks Primary Servers are
# configured with the server addresses in a different order.
#
# * The [user-source-name] must exactly match how the user source name
appears on the configuration page in ZCC.
# * You must specify the LDAP port along with each server address.
# * SSL is configured for the entire user source, not for each individual
server. You must specify either the
#   SSL port or the clear text port for all servers, depending on how the
user source is configured in ZCC.
# * If the server-list.properties file contains an entry for a user source,
ZENworks will not try to connect to the
#   server address configured in ZCC. It only tries the addresses listed in
the properties file.
# * If you create or modify the server-list.properties file, you will need
to restart the Novell ZENworks Server and
#   Novell ZENworks Loader services for it to take effect.
# * Performance will be impacted if one or more of the servers at the top
of the list are down, as ZENworks attempts to
#   connect to the servers in order. This is particularly true of the CASA
authentication token service, which is
#   contacted when a user tries to log in to ZENworks on a workstation.
#
# Format:
#
# [user-source-name]=\
#   [host1]:[port] \
#   [host2]:[port] \
#   [host3]:[port]
#
# Example:
#
MY_EDIR_TREE=\
  edir1.novell.com:636 \
  edir2.novell.com:636 \
  edir3.novell.com:636 \
  edir4.novell.com:636
```

3 Restart the ZENworks Server.

4 Repeat Step 1 through Step 3 for each ZENworks Server for which you want to define additional LDAP servers.

User Authentication

20

The following sections provide information about authentication of users to a ZENworks®
Management Zone.

20.1 User Source Authentication

By default, a user is automatically authenticated to the Management Zone when he or she logs in to
an LDAP directory (Novell® eDirectory™ or Microsoft Active Directory) that has been defined as a
user source in the Management Zone. User authentication to ZENworks can occur only if the user's
LDAP directory (or the user's LDAP directory context) is defined as a user source in ZENworks.

The ZENworks Adaptive Agent integrates with the Windows* Login or Novell Login client to
provide a single login experience for users. When users enter their eDirectory or Active Directory
credentials in the Windows or Novell client, they are logged in to the Management Zone if the
credentials match the ones in a ZENworks user source. Otherwise, a separate ZENworks login
screen prompts the user for the correct credentials.

For example, assume that a user has accounts in two eDirectory trees: Tree1 and Tree2. Tree1 is
defined as a user source in the Management Zone, but Tree2 is not. If the user logs in to Tree1, he or
she is automatically logged in to the Management Zone. However, if the user logs in to Tree2, the
Adaptive Agent login screen appears and prompts the user for the Tree1 credentials.

On a Windows XP, Windows 2000, or Windows 2003 device, the user can choose to view the status
of the login during the process of logging in to ZENworks.

To enable the status messages to be displayed on the screen:

1 Open the Registry Editor.

2 Go to `HKEY_LOCAL_MACHINE\Software\Novell\NWGINA`

3 Create a DWORD called EnableStatusMessages and set the value to 1.

This functionality is available only with the English version of Update for ZENworks 10
Configuration Management SP2 (10.2.1).

NOTE: Authentication using a biometric device or smart card is not supported.

20.2 Credential Storage

ZENworks uses Novell CASA (Common Authentication Services Adapter) to enable single sign-on.
When the ZENworks Adaptive Agent authenticates a user to the Management Zone via the
credentials entered in the Microsoft client, Novell client, or ZENworks login screen, the username
and password is stored in the secure CASA vault on the user's device.

CASA is installed with the ZENworks Adaptive Agent. It includes the CASA Manager, which is an interface used to manage the credentials in the storage vault. The CASA Manager is available from the *Start > Program Files > Novell CASA* menu. Generally, you or the device's user should not need to use the CASA Manager. When a user's credentials change in the LDAP directory, they are updated in the CASA storage vault the next time the user logs in. If you do run the CASA Manager, you are prompted to install the GTK# Library. If you choose to install the library (which is necessary to run the CASA Manager), you are directed to a Novell Web site from which you can install it.

Do not remove CASA from the managed device. If you do not want the CASA Manager displayed to users, you can remove the Novell CASA folder from the *Start > Program Files* menu.

20.3 Disabling ZENworks User Authentication

By default, if a user source is defined in the ZENworks Management Zone, the ZENworks Adaptive Agent attempts to authenticate a user to the zone whenever he or she logs in through the Microsoft or Novell client.

If necessary, you can disable user authentication to the zone. For example, you might have some users that only receive device-assigned content, so you don't want the overhead of having them logged in to the zone.

To disable user authentication to the zone:

1 Locate the following key in the registry on the user's device:

    HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZENworks\ZenLgn

2 (Conditional) If you want to disable login, add the following DWORD value:

Value name: DisablePassiveModeLogin

Value data: Any non-zero value (for example, 1, 2, 3, 100)

With login disabled, no attempt is made to authenticate to the Management Zone when the user logs in through the Microsoft or Novell client.

3 (Conditional) If you want to disable the ZENworks login prompt that appears if login through the Microsoft client or Novell client fails, add the following DWORD value:

Value name: DisablePassiveModeLoginPrompt

Value data: Any non-zero value (for example, 1, 2, 3, 100)

Normally, the Adaptive Agent attempts to authenticate the user to the zone by using the credentials entered in the Microsoft or Novell client. If login fails, the ZENworks login prompt is displayed in order to give the user an opportunity to authenticate with different credentials. This value setting disables the ZENworks login prompt.

20.4 Troubleshooting User Authentication

This section contains explanation on some of the user authentication related problems. To troubleshoot other problems you might encounter during authentication, see TID 3273870 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

- "Incorrect username displayed in the ZENworks Login screen" on page 183
- "Unable to log in to the ZENworks Server" on page 183
- "Large number of concurrent client logins might result in login failures" on page 183

- "How do I enable debug logs on Windows 2003, Windows XP, and Windows Vista devices?" on page 184
- "How do I enable the CASA debug logs?" on page 184
- "Logging in to the user source on a ZENworks Server is slow" on page 184
- "Unable to log in to the ZENworks Server when logging in to a Windows Vista device" on page 185
- "The settings assigned to an eDirectory user are not applied on the device where the user has logged in" on page 185

Incorrect username displayed in the ZENworks Login screen

Explanation: The *Username* option in the ZENworks Login screen displays the Windows local username by default.

Possible Cause: If you changed only the full name of the user (*My Computer > Manage > System Tools > Local Users and Groups > Full Name*), the ZENworks login screen displays the old username and not the new full name.

Action: To change the local user account details, you must change both the username and the full name of the user:

1 Click the desktop *Start* menu > *Run*.

2 In the Run window, specify *control userpasswords2*, then click *OK*.

3 Double-click the username and edit both the *User Name* and *Full Name* of the user.

4 Click *OK*.

Unable to log in to the ZENworks Server

Possible Cause: A user with an account in the eDirectory that is installed on an OES 2.0 server tries to log into a non-OES 2.0 ZENworks Server.

Action: To log in to a non-OES 2.0 ZENworks Server, the user must be a Linux User Management (LUM) user. For more information on LUM users, see the *Novell Linux User Management Technology Guide (http://www.novell.com/documentation/oes2/acc_linux_svcs_lx/index.html?page=/documentation/oes2/acc_linux_svcs_lx/data/fbdecbed.html)*

Large number of concurrent client logins might result in login failures

Explanation: The maximum number of concurrent client connections that a server can support depends on the configured `Connector acceptCount`. If the number of concurrent client requests exceeds the value of `Connector acceptCount`, the client connect requests might fail because the server is not able to accept these connections.

Action: Increase the number of client connect requests that the server can support.

On a Windows server:

1 Log in as an administrator.

2 Open the
ZENworks_Install_path\share\ats\catalinabase\conf\server.
xml file.

3 In the `Define a SSL Coyote HTTP/1.1 Connector on port 2645` section, change the value of the `Connector acceptCount` to the desired value. A value of 300 is optimal.

4 Restart the Authentication Token Service:

   4a On the desktop, click *Start > Run*.

   4b In the Run window, specify *service.msc*, then click *OK*.

   4c Restart *CasaAuthTokenSvc*.

On a Linux server:

1 Log in as `root`.

2 Open the `/srv/www/casaats/conf/server.xml` file.

3 In the `Define a SSL Coyote HTTP/1.1 Connector on port 2645` section, change the value of the `Connector acceptCount` to the desired value. A value of 300 is optimal.

4 Restart the Authentication Token Service:

   4a At the server prompt, go to `/etc/init.d/`.

   4b Run the `casa_atsd restart` command.

How do I enable debug logs on Windows 2003, Windows XP, and Windows Vista devices?

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

How do I enable the CASA debug logs?

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Logging in to the user source on a ZENworks Server is slow

Explanation: Logging in to the user source on a ZENworks Server from the managed device might take some time because the login process executes the device refresh synchronously.

Action: To speed up the login process, perform the following steps to change the login process to execute the device refresh asynchronously:

1 Open the Registry Editor.

2 Go to `HKEY_LOCAL_MACHINE\Software\Novell\ZENworks`.

3 Create a String called ZENLoginUserRefreshAsync and set the value to TRUE.

4 Log in to the device again.

> **IMPORTANT:** If you change the login process to execute the device refresh asynchronously, the latest policies might not be immediately available. With this setting, the choice is login performance over the accuracy of the policies.

Unable to log in to the ZENworks Server when logging in to a Windows Vista device

Explanation: If you log in to a Windows Vista* device that has Novell SecureLogin installed and Active Directory configured as the user source, you are not automatically logged in to the ZENworks server.

Action: Do the following:

1 Open the Registry Editor.

2 Go to `HKLM\Software\Protocom\SecureLogin\`.

3 Create a DWORD called ForceHKLMandNoDPAPI, and set the value to 1.

4 Restart the device.

The settings assigned to an eDirectory user are not applied on the device where the user has logged in

Possible Cause: Two or more eDirectory users with the same username and password might exist in different contexts of the eDirectory tree.

Explanation: When an eDirectory user specifies the username and password to log in to a device, a user with the same username and password but located in a different context of the eDirectory tree might be logged in to the device and the settings of this user are applied on the device. This is because the login GINA is contextless.

For example: Assume that user1 and user2 have the same username and password:

User1: `CN = bob, OU = org1, O = Company1 (bob.org1.company1)`

User2: `CN = bob, OU = org2, O = Company1 (bob.org2.company1)`

When user2 specifies the username and password to log in to a device, user1 is logged in to the device instead of user2 because user1 appears first in the search performed by Novell CASA. The settings assigned to user1 are applied on the device.

Action: No two eDirectory users should have the same username and password. Even if the usernames are same, ensure that the passwords are different.

ZENworks 10 Product Licensing

V

This section contains information about evaluating, activating, and deactivating ZENworks® products.

- Chapter 21, "ZENworks 10 Product Licensing," on page 189

ZENworks 10 Product Licensing

<div style="text-align: right; font-size: 3em;">21</div>

The ZENworks® 10 family of products include the following:

- ZENworks 10 Configuration Management
- ZENworks 10 Asset Management
- ZENworks 10 Patch Management
- Asset Inventory for UNIX/Linux

All of the products are installed by default. This enables you to activate products by providing a license key or evaluate products for which you have not purchased a license. You can also deactivate licensed or evaluation products if you no longer intend to use them.

The following sections provide information on managing the product licenses:

- Section 21.1, "Evaluating a Product," on page 189
- Section 21.2, "Extending the Evaluation Period of a Product," on page 190
- Section 21.3, "Activating a Product," on page 190
- Section 21.4, "Deactivating a Product," on page 190
- Section 21.5, "Possible License State Changes," on page 191
- Section 21.6, "Using ZENworks 10 Asset Management with ZENworks 7 Desktop Management," on page 192
- Section 21.7, "Viewing the Predefined Reports," on page 192

For other actions that you can perform to view license information, see "License Commands" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

21.1 Evaluating a Product

1 Log in to the ZENworks Control Center.

2 Click the *Configuration* tab.

3 In the Product Licensing panel, click the product you want to evaluate.

4 In the Product Activation panel, select the *Evaluate/Activate product* option.
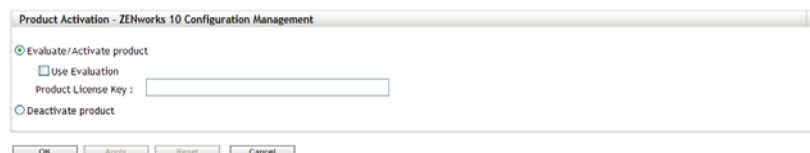
5 Select *Use Evaluation* option, then click *Apply*.

6 Click *OK*.

For more information on license state changes, see Section 21.5, "Possible License State Changes," on page 191.

21.2 Extending the Evaluation Period of a Product

1 Log in to the ZENworks Control Center.

2 Click the *Configuration* tab.

3 In the Product Licensing panel, click the product you want to evaluate.

4 In the Product Activation panel, select the *Evaluate/Activate product* option.
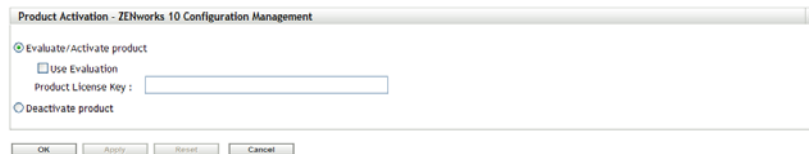
5 Specify the extended evaluation license key in *Product License Key*, then click *Apply*.

6 Click *OK*.

For more information on license state changes, see Section 21.5, "Possible License State Changes," on page 191.

21.3 Activating a Product

1 Log in to the ZENworks Control Center.

2 Click the *Configuration* tab.

3 In the Product Licensing panel, click the product you want to activate.

4 In the Product Activation panel, select the *Evaluate/Activate product* option.
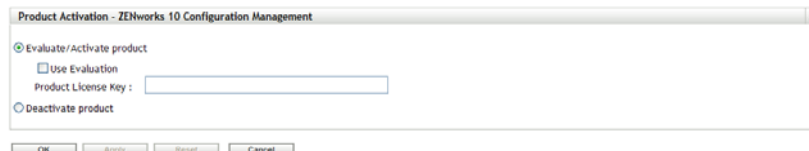
5 Specify the license key in *Product License Key*, click *Apply*.

6 Click *OK*.

For more information on license state changes, see Section 21.5, "Possible License State Changes," on page 191.

21.4 Deactivating a Product

1 Log in to the ZENworks Control Center.

2 Click the *Configuration* tab.

3 In the Product Licensing panel, click the product you want to deactivate.
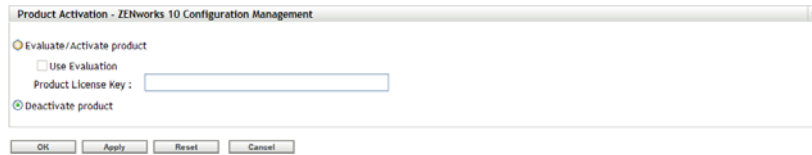
4 In the Product Activation panel, select the *Deactivate product* option.

5 Click *Apply*.

6 Click *OK*.

For more information on possible license state changes, see .

21.5 Possible License State Changes

The transition of a product to a new licence state depends on the current license state of the product and the license state of the product prior to the current license state. Accordingly, you can choose to evaluate, activate, or deactivate a product.

For example:

 ◆ A product that is currently deactivated can be moved to an evaluation, extended evaluation, or active state.

 ◆ A product that has been transitioned from an evaluation state to deactivated state can be now moved to an active, evaluation, or extended evaluation state.

Table 21-1 *Possible License State Changes for ZENworks Products*

Previous License State	Current License State	New License State	Additional Information
	Deactivated	Evaluation	You get 60 days to evaluate the product.
	Deactivated	Extended Evaluation	You get 120 days to evaluate the product.
	Deactivated	Active	
	Evaluation	Extended Evaluation	You get 60 days in addition to the remaining evaluation days.
	Evaluation	Active	
	Evaluation	Deactivated	
	Active	Deactivated	
Evaluation	Deactivated	Active	

Previous License State	Current License State	New License State	Additional Information
Evaluation	Deactivated	Evaluation	You get the remaining evaluation days. For example, if you use the product for 10 days of the evaluation period and deactivate it, then if you choose to evaluate the product again, you get 50 days of evaluation.
Evaluation	Deactivated	Extended Evaluation	You get 60 days in addition to the remaining evaluation days.
Extended Evaluation	Deactivated	Extended Evaluation	You get the remaining evaluation days.
Extended Evaluation	Deactivated	Active	
Active	Deactivated	Active	

21.6 Using ZENworks 10 Asset Management with ZENworks 7 Desktop Management

You can use ZENworks 10 Asset Management with ZENworks 7 Desktop Management installed in your environment.

If you enable ZENworks 10 Configuration Management or ZENworks Patch Management Agent features (in ZENworks Control Center, *Configuration* tab > *Device Management* > *ZENworks Agent*), you are prompted that the ZENworks 7 Desktop Management Agent will be uninstalled.

The ZENworks 10 Configuration Management Agent features include the following:

- Bundle Management
- Policy Management
- Image Management
- Patch Management
- Remote Management
- User Management

Do not enable these features if you want to continue using ZENworks 7 Desktop Management in your environment.

21.7 Viewing the Predefined Reports

You must have installed ZENworks Reporting Server to view the predefined reports. For more information on how to install ZENworks Reporting Server, see the *ZENworks 10 Asset Management Reporting Server Installation Guide*.

To view the predefined reports for Licensing:

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

2 In the ZENworks Reporting Server Reporting panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView.

3 Navigate to *Novell ZENworks Reports* > *Predefined Reports* > *ZENworks System*.

4 The following predefined report is included for Licensing:

ZENworks License Information: Displays the licensing details for the Asset Inventory for UNIX/Linux, ZENworks Configuration Management, and ZENworks Asset Management products installed on all the devices in your Management Zone. You can view information such as the license status for the products, the expiration date of the licenses, number of managed devices and inventory devices that are connected to the server holding the license, and the number of managed users.

For more information on creating and managing reports, see the *ZENworks 10 Asset Management System Reporting Reference* documentation.

Database Management

Novell® ZENworks® 10 Asset Management allows you to back up and restore the embedded Sybase SQL Anywhere database by using the zman command line utility. To back up and restore Remote Sybase SQL Anywhere, Oracle*, or Microsoft SQL Server* databases, refer to their documentation.

IMPORTANT: If you plan to back up the ZENworks Server that hosts the ZENworks database, you must ensure that the ZENworks database is backed up at least once before backing up the ZENworks Server (which only needs to be done one time). You can also back up the ZENworks database on a regular basis. However, you can back up the server and the database in any order.

When restoring the ZENworks Server and the database, you must first restore the ZENworks Server, then restore the latest backed-up ZENworks database. For more information about backing up and restoring the ZENworks Server, see Chapter 10, "Backing Up and Restoring the ZENworks Server and Certificate Authority," on page 107.

ZENworks 10 Asset Management also allows you to migrate the data from the Sybase SQL Anywhere database to an Oracle database.

Review the following sections for detailed information:

Embedded Database Maintenance

22

22.1 Retrieving and Storing the Credentials of the Embedded Sybase SQL Anywhere Database

If you have installed ZENworks® 10 Asset Management with the embedded Sybase SQL Anywhere database that is bundled with ZENworks, we recommend that you store the credentials of the database for future use.

1 Retrieve the credentials of the embedded Sybase SQL Anywhere database by entering one of the following commands at the server prompt:

```
zman database-get-credentials
```

or

```
zman dgc
```

The credentials are displayed on the console.

For more information about zman, view the zman man page (`man zman`) on the server or see "zman(1)" in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

2 Copy the credentials and save them in a file.

To retrieve and store the credentials of Remote Sybase SQL Anywhere, Oracle, or Microsoft SQL Server databases, refer to their documentation.

22.2 Changing the Ports Used by the Embedded Sybase SQL Anywhere Database

Sybase SQL Anywhere uses port 2638 by default. You can change the port on which the database runs.

1 In the `zenworks_database.conf` file, specify the new port number on which the server listens to.

The `zenworks_database.conf` file is located in `%ZENWORKS_HOME%\conf` on Windows and in `/etc/opt/novell/zenworks` on Linux.

2 In the `zdm.xml` file on all the Primary Servers, specify the new port number in the following entry:

`<entry key="Port">2638</entry>`

By default, the entry lists the default port number, 2638.

The `zdm.xml` file is located in `%ZENWORKS_HOME%\conf\datamodel` on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux.

3 (Conditional) If the ZENworks Reporting Server is installed on the Primary Server, add the new port number to the ODBC data information:

- ◆ **On a Windows server:** Do the following:

  1. From the desktop *Start* menu, click *Settings, click Control Panel*, then double-click *ODBC Data Source*.

     The ODBC Data Source Administrator window is displayed.

  2. Click the *System DSN* tab.

  3. Double-click *ZENworks Datastore*.

     The ODBC Configuration window is displayed.

  4. Click the *Networks* tab.

  5. In the *Select the Network Protocols and Options* panel, change the value of the TCP/IP port number (by default, it is 2638) to the port number specified in `zenworks_database.conf` (the new number you specified in Step 1).

- ◆ **On a Linux server:** In the `/opt/novell/zenworks/share/boe/bobje/odbc.ini` file, change the value of TCP/IP to the port number specified in `zenworks_database.conf` (the new number you specified in Step 1).

4 Restart the database service, ZENServer, and ZENLoader services on all Primary servers:

- ◆ **On Windows:** Do the following:

  1. From the Windows desktop Start menu, click *Settings > Control Panel*.

  2. Double-click *Administrative Tools > Services*.

  3. Restart the following services: *Novell ZENworks Embedded Datastore*, *Novell ZENworks Loader Service*, and *Novell ZENworks Server*.

- ◆ **On Linux:** At the console prompt, enter the following commands in the order given:

  - ◆ `/etc/init.d/novell-zenmntr stop`
  - ◆ `/etc/init.d/novell-zenserver stop`
  - ◆ `/etc/init.d/novell-zenloader stop`
  - ◆ `/etc/init.d/sybase-asa restart`
  - ◆ `/etc/init.d/novell-zenserver start`
  - ◆ `/etc/init.d/novell-zenloader start`
  - ◆ `/etc/init.d/novell-zenmntr start`

Even though the TCP and UDP ports are changed from 2638, the database server also listens on UDP port 2638. For more information, see the Sybase database documentation (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbdaen10/da-serverport-network-conparm.html).

22.3 Backing Up the Embedded Sybase SQL Anywhere Database

The embedded Sybase SQL Anywhere database can be backed up to a directory on the local machine or to a network location.

- Section 22.3.1, "Backing Up the Embedded Sybase SQL Anywhere Database on a Windows or Linux Server," on page 199
- Section 22.3.2, "Backing up the Embedded Sybase SQL Anywhere Database Running on a Windows Server to a Network Location on a Remote Windows Machine," on page 200
- Section 22.3.3, "Backing up the Embedded Sybase SQL Anywhere Database Running on a Linux Server to a Network Location on a Remote Linux Machine," on page 202

22.3.1 Backing Up the Embedded Sybase SQL Anywhere Database on a Windows or Linux Server

1 Store the ZENworks administrator name and password by entering the following command at the command prompt:

```
zman admin-store-credential administrator
```

If you do not store the credentials, you must enter the ZENworks administrator name and password for each zman command.

You can back up the embedded Sybase SQL Anywhere database immediately or schedule the backup to run at a specific time. To back up the embedded Sybase SQL Anywhere database immediately, continue with Step 2. To schedule the backup to run at a specific time, skip to Step 3.

2 To immediately back up the embedded Sybase SQL Anywhere database to a directory on the database server, enter the following command at the command prompt:

```
zman database-backup
complete_path_of_the_backup_directory_on_database_server
```

For example, to back up the database to the `c:\dbbackup` directory on a Windows database server, execute `zman database-backup c:\dbbackup`. To back up the database to the `/root/dbBackup` directory on a Linux database server, execute `zman database-backup /root/dbBackup`.

3 To schedule the backup to run at a specific time every day or on specific days of a month, you need to create a schedule file and run it.

  3a Create a schedule file, `backupschedule.sql`, with the following contents:

```
CREATE EVENT backup_schedule_name
SCHEDULE
specify_the_schedule
```

A sample schedule file to back up the database at a 11 p.m. every day is as follows:

```
CREATE EVENT ZENDBBackup

SCHEDULE

START TIME '11:00 PM' EVERY 24 HOURS
```

A sample schedule file to back up the database at 1:00 a.m. on the first, second, third and fourth days of the month is as follows:

```
CREATE EVENT ZENDBBackup1

SCHEDULE

START TIME '1:00 AM'

ON (1,2,3,4)
```

Sample schedule files are available in the `ZENworks_Installation_directory:\Novell\Zenworks\share\zman\samples\database` directory on a Windows server, and in the `/opt/novell/zenworks/share/zman/samples/database` directory on a Linux server.

3b Enter the following command at the command prompt:

```
zman database-backup complete_path_of_the_backup_directory
c:\backUpSchedule.sql -d SQL_function_call
```

For example, to back up the database to the `c:\dbbackup\day_of_the_week` directory on a Windows server, enter the following command:

```
zman database-backup c:\dbbackup c:\backUpSchedule.sql -d
"DAYNAME(now())"
```

For more information about this command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

4 Clear the credentials stored in Step 1 by entering the following command at the command prompt:

```
zman admin-clear-credential
```

According to the backup schedule, the `zenworks_zone_name.db` database file and the `zenworks_zone_name.log` transaction log file are created in the database backup directory.

22.3.2 Backing up the Embedded Sybase SQL Anywhere Database Running on a Windows Server to a Network Location on a Remote Windows Machine

To back up an embedded Sybase SQL Anywhere database that is installed and running on a Windows server to a network location on another Windows machine, you need a local machine and a remote machine. The local machine is a Windows server with the ZENworks server components and the embedded Sybase SQL Anywhere database installed. The remote machine is a Windows machine with the network location to which you want to back up the database.

1 Perform the following steps on the local machine:

1a Create an administrative user and specify a password.

For example, you could specify the administrative username as `Administrator` and the password as `novell`.

1b From the desktop *Start* menu, click *Settings*, click *Control Panel*, double-click *Administrative Tools*, then double-click *Services*.

1c Right-click the *Novell ZENworks Datastore* service, then click *Properties*.

1d Click the *Log On* tab.

1e Select *This account*, then specify the name and the password of the administrative user created in Step 1a.

For example, specify the user as `Administrator` and the password as `novell`.

1f Click *OK*.

2 Perform the following steps on the remote machine with the network location where you want to save the backup:

2a Create an account with the same credentials as the user you created in Step 1a.

For example, specify user as `Administrator` and password as `novell`.

2b Provide Read/Write permission on the network location to the user.

To immediately back up the database, continue with Step 3. To schedule the backup to run at a specific time every day or on specific days of a month, skip to Step 4.

3 To immediately back up the database to the network location on the remote machine, enter the following command at the command prompt:

```
zman database-backup
\\IP_address_of_the_remote_machine\backup_directory\custom_directory
```

Where `\\IP_address_of_the_remote_machine\backup_directory` is the network location on the remote machine and `custom_directory_name` is a name that you specify for a directory to be newly created by zman and into which the database files are backed up.

4 To schedule the backup:

4a Create a schedule file, `backupschedule.sql`, with the following contents:

```
CREATE EVENT backup_schedule_name

SCHEDULE

specify_the_schedule
```

A sample schedule file to back up the database at a 11 p.m. every day is as follows:

```
CREATE EVENT ZENDBBackup

SCHEDULE

START TIME '11:00 PM' EVERY 24 HOURS
```

A sample schedule file to back up the database at 1:00 a.m on the first, second, third, and fourth days of the month is as follows:

```
CREATE EVENT ZENDBBackup1

SCHEDULE

START TIME '1:00 AM'

ON (1,2,3,4)
```

Sample schedule files are available in the `ZENworks_Installation_directory\Novell\Zenworks\share\zman\samples\database` directory.

4b Execute the following command at the command prompt:

```
zman database-backup
\\IP_address_of_the_remote_machine\backup_directory\custom_directory
c:\backUpSchedule.sql -d SQL_function_call
```

Where `\\IP_address_of_the_remote_machine\backup_directory` is the network location on the remote machine and `custom_directory_name` is a name that you specify for a directory to be newly created by zman and into which the database files are backed up.

For more information about the command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

According to the backup schedule, `zenworks_zone_name`.db and `zenworks_zone_name`.log are created in the network location on the remote machine. The backed-up database is stored in `zenworks_zone_name`.db. The result of the database backup is logged in `zenworks_zone_name`.log.

22.3.3 Backing up the Embedded Sybase SQL Anywhere Database Running on a Linux Server to a Network Location on a Remote Linux Machine

To back up the embedded Sybase SQL Anywhere database that is installed and running on a Linux server to a network location on a Linux machine, you need a local machine and a remote machine. The local machine is a Linux server with the ZENworks server components and the embedded Sybase SQL Anywhere database installed. The remote machine is a Linux machine with the network location to which you want to back up the database.

You can back up the database on a Linux machine by using any Linux share such as Samba share or NFS share.

To back up the embedded Sybase SQL Anywhere database that is installed and running on a Linux server to a network location on a Linux machine by using Samba share:

1 Create a Samba share on the remote machine:

   1a Create a user by entering the `useradd user_name` command at the command prompt.

   1b Log in to the remote machine with the username created in Step 1a, and set the password by using the `passwd specify_the_password` command.

   1c Create a directory to save the database backup.

      For example, create a directory with the name `backup`.

   1d Open the Samba server settings by running the `yast2 samba-server` command.

   1e Click the *Shares* tab, then click *Add* to specify the share name and the path to the backup directory created in Step 1c.

      For example, specify the sharename as `dbbackup`.

   1f Select the `dbbackup` share, click *Edit*, then add the following attributes:

        ◆ create mask = 0640

        ◆ force user = *user_name_created_in_*Step 1a

        ◆ guest ok = yes

        ◆ public = yes

- ◆ wide links = no
- ◆ writeable = yes

2 Create a directory on the local machine.

For example, create a directory with the name `zenworks_dbbackup` in `/root`.

3 Mount the Samba share on the `zenworks_dbbackup` directory on the local machine by entering the following command at the command prompt:

```
mount -t smbfs //IP_address of the remote_machine/share_name -o
username=user_name_specified_in_Step1a,password=password_
specified_in_Step_1b
local_directory_name_with_complete_path_created_in_Step2
```

For example:

```
mount -t smbfs //IP_address of the remote_machine/dbbackup -o
username=user_name_specified_in_Step1a,password=password_
specified_in_Step_1b /root/zenworks_dbbackup
```

To immediately back up the database, continue with Step 4. To schedule the backup to run at a specific time every day or on specific days of a month, skip to Step 5.

4 To immediately back up the database to the network location on the remote machine, enter the following command at the command prompt:

```
 zman database-backup database_backup_directory
```

For example:

```
 zman database-backup /root/zenworks_dbbackup
```

5 To schedule the backup:

5a Create a schedule file, `backupschedule.sql`, with the following contents:

```
CREATE EVENT backup_schedule_name
SCHEDULE
specify_the_schedule
```

A sample schedule file to back up the database at a 11 p.m. every day is as follows:

```
CREATE EVENT ZENDBBackup
SCHEDULE
START TIME '11:00 PM' EVERY 24 HOURS
```

A sample schedule file to back up the database at 1:00 a.m. on the first, second, third, and fourth days of the month is as follows:

```
CREATE EVENT ZENDBBackup1
SCHEDULE
START TIME '1:00 AM'
ON (1,2,3,4)
```

Sample schedule files are available in the `ZENworks_Installation_directory:\Novell\Zenworks\ share\zman\samples\database` directory.

5b Enter the following command at the command prompt:

```
zman database-backup database_backup_directory c:\backUpSchedule.sql -
d SQL_function_call
```

For example:

```
zman database-backup /root/zenworks_dbbackup c:\backUpSchedule.sql -d
SQL_function_call
```

For more information about this command, view the zman man page (man zman) on the device, or see zman(1) in the *ZENworks 10 Asset Management Command Line Utilities Reference*.

According to the backup schedule, zenworks_*zone_name*.db and zenworks_*zone_name*.log are created in the network location on the remote machine (/root/zenworks_dbbackup). The backed-up database is stored in zenworks_*zone_name*.db. The result of the database backup is logged in zenworks_*zone_name*.log.

22.4 Restoring the Embedded Sybase SQL Anywhere Database

The following sections provide information on restoring the backed-up embedded Sybase SQL Anywhere database:

◆ Section 22.4.1, "Restoring the Embedded Sybase SQL Anywhere Database on a Windows Server," on page 204

◆ Section 22.4.2, "Restoring the Embedded Sybase SQL Anywhere Database on a Linux Server," on page 205

IMPORTANT: If the database is located on a ZENworks Server, you must first restore the ZENworks Server, then restore the ZENworks database. Ensure that you have backed up the ZENworks Server and the database (at least once). You can also back up the ZENworks database on a regular basis. However, you can back up the server and the database in any order. For more information about backing up and restoring the ZENworks Server, see Chapter 10, "Backing Up and Restoring the ZENworks Server and Certificate Authority," on page 107.

22.4.1 Restoring the Embedded Sybase SQL Anywhere Database on a Windows Server

1 At the Windows server prompt, go to *ZENworks_Installation_directory:*\novell\zenworks\bin, and enter the following command:

```
ZenworksWindowsDBRestore.bat
ZENworks_Installation_directory:\Novell\Zenworks\Database
c:\dbBackup\zenworks_zone_name.db c:\dbBackup\zenworks_zone_name.log
```

2 Press any key when the following message is displayed:

```
Before proceeding, make sure you have backed up any files in:<Installation
directory>:\Novell\ZENworks\database Press any key to continue.
```

3 Enter Y when the following message is displayed:

```
The following services are dependent on the Novell ZENworks Datastore
service. Stopping the Novell ZENworks Datastore service will also stop
these services: Novell ZENworks Loader, Novell ZENworks Agent Service,
Novell ZENworks Server. Do you want to continue this operation? (Y/N) [N]:
```

4 Press any key when the following message is displayed:

```
The Novell ZENworks Datastore service was stopped successfully. Press any
key to continue...
```

5 Enter `Yes` when the following message is displayed:

```
Overwrite <installation
directory>:\Novell\ZENworks\database\zenworks_<zone_name>.db? (Yes/No/
All)
```

6 Enter `Yes` when the following message is displayed:

```
Overwrite <installation
directory>:\Novell\ZENworks\database\zenworks_<zone_name>.log? (Yes/No/
All):
```

The `backupFile` and the `backupLogFile` are copied to
ZENworks_Installation_directory:\Novell\ZENworks\database, and the database is
restored.

7 (Conditional) If you restore the database to a location other than the one mentioned in the
zenworks_installation_directory\novell\zenworks\database\conf\zenworks_da
tabase.conf file, manually edit `zenworks_database.conf` to specify the new location of
the database.

22.4.2 Restoring the Embedded Sybase SQL Anywhere Database on a Linux Server

1 Log in to the ZENworks server as `root`.

2 Change to `/opt/novell/zenworks/bin`, and enter the following command:

```
./ZenworksLinuxDBRestore.sh -F "/root/dbBackup/zenworks_zone_name.db"
```

3 Enter `Y` when the following message is displayed:

```
The backup database file will OVERWRITE the existing database. Is that OK?
[y/n]
```

4 Enter `Y` when the following message is displayed:

```
The novell-zenloader needs to be stopped for the database restore to be
performed. Would you like to proceed [y/n]?
```

The backup file is copied to `/var/opt/novell/zenworks/database`, and the restore log file
to `/var/opt/novell/log/zenworks/dbrestore.log`. The database is restored.

22.5 Moving the Data from an Embedded Sybase Database to an External Sybase Database

ZENworks 10 Asset Management allows you move the data from a Sybase SQL Anywhere database
(embedded Sybase database) to an OEM Sybase database (external Sybase database).

22.5.1 Preparing to Move the Data

Before moving the data from an internal Sybase database to an external Sybase database, do the following:

- Make sure that ZENworks 10 Asset Management is installed with an internal Sybase database on a Windows or Linux device.

- Install the external Sybase database. For more information on how to install an external Sybase database, see "Installing an External ZENworks Database" in the *ZENworks 10 Asset Management Installation Guide*.

22.5.2 Moving the Data from the Internal Sybase to the External Sybase

1 On the device that has the external Sybase database installed, stop the Novell ZENworks Embedded Datastore service.

- **On Windows:** Do the following:

   1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

   2. Double-click *Administrative Tools > Services*.

   3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Stop*, or select the *Novell ZENworks Embedded Datastore* service, then click ∎ on the toolbar.

- **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa stop`.

2 From the device that has the internal Sybase database installed, copy `zenworks_database.conf` and all files within the `database` directory to the appropriate directories on the device that has the external Sybase database.

The `zenworks_database.conf` is located in the `ZENworks_installation_path\conf\` directory on Windows and in the `/etc/opt/novell/zenworks/` directory on Linux.

The `database` directory is located in `ZENworks_installation_path` on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

3 On the device that has the external Sybase database installed, open `zenworks_database.conf` and make sure that it contains the correct path of the database file.

4 On the device that has the internal Sybase database installed, edit `zdm.xml` (located in `ZENworks_installation_path\conf\datamodel` on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux):

- Change the value of the `Embedded` entry key to `false`. By default, it is `true`.

- Set the value of the `Server` entry key to the IP address of the device that has the external Sybase database installed.

- Make sure that the value of the `Port` entry key is the port number on which the external Sybase database is running.

5 On the device that has the external Sybase database installed, start the Novell ZENworks Embedded Datastore service.

- **On Windows:** Do the following:

   1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

2. Double-click *Administrative Tools* > *Services*.

3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Start*, or select the *Novell ZENworks Embedded Datastore* service, then click ▶ on the toolbar.

- **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa start`.

6 On the device that has the internal Sybase database installed, restart the ZENworks services:

- **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings* > *Control Panel*.

  2. Double-click *Administrative Tools* > *Services*.

  3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

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

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

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

The ZENworks Server now points to new database.

22.6 Moving the Data from an External OEM Sybase Database to an Embedded Sybase Database

ZENworks 10 Asset Management allows you move the data from an OEM Sybase database (external Sybase database) to a Embedded OEM Sybase SQL Anywhere database (embedded Sybase database) that is installed on the ZENworks Server.

- Section 22.6.1, "Preparing to Move the Data," on page 207
- Section 22.6.2, "Moving the Data from the External Sybase to the Embedded Sybase," on page 208

22.6.1 Preparing to Move the Data

Before moving the data from an external Sybase database to an embedded Sybase database, do the following:

- Make sure that ZENworks 10 Asset Management is installed with an external OEM Sybase database on a Windows or Linux device.

- Install the Embedded OEM Sybase database on the ZENworks Server. For more information on how to install the database, see "Installing an External ZENworks Database" in the *ZENworks 10 Asset Management Installation Guide*.

  During the installation of the embedded Sybase database, you must consider the following points while configuring the Sybase Access Configuration page:

  - The database name can be same as that of the external Sybase database or can be a unique name.

- Make sure that the username and password are same as that of the external Sybase database.
- Make sure that the database server name is unique.

22.6.2 Moving the Data from the External Sybase to the Embedded Sybase

1 On the ZENworks Server that has the embedded Sybase database installed, do the following: .

   1a Stop the Novell ZENworks Embedded Datastore service.

- **On Windows:** Do the following:

   1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

   2. Double-click *Administrative Tools > Services*.

   3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Stop*, or select the *Novell ZENworks Embedded Datastore* service, then click ■ on the toolbar.

- **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa stop`.

   1b Delete the contents of the `database` directory.

The `database` directory is located in *ZENworks_installation_path* on Windows and in the `/opt/novell/zenworks/` directory on Linux.

2 On the device that has the external Sybase database installed, stop the Novell ZENworks Embedded Datastore service.

- **On Windows:** Do the following:

   1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

   2. Double-click *Administrative Tools > Services*.

   3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Stop*, or select the *Novell ZENworks Embedded Datastore* service, then click ■ on the toolbar.

- **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa stop`.

3 From the device that has the external Sybase database installed, copy all files within the `database` directory to the appropriate directories on the ZENworks Server that has the embedded Sybase database.

The `database` directory is located in *ZENworks_installation_path* on Windows and in the `/opt/novell/zenworks/` directory on Linux.

4 On the ZENworks Server that has the embedded Sybase database installed, open `zenworks_database.conf` and make sure that it contains the correct path of the database file.

5 On the ZENworks Server that has the embedded Sybase database installed, edit `zdm.xml` (located in *ZENworks_installation_path*\conf\datamodel on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux):

- Add the following entry:

`<entry key="Embedded">true</entry>`

- Set the value of the `Server` entry key to 127.0.0.1 (the IP address of the ZENworks Server that has the embedded Sybase database installed).

- Make sure that the value of the `Port` entry key is the port number on which the embedded Sybase database is running.

- Set the value of the `Engine` entry key to the database server name specified during the installation of the embedded Sybase database.

- (Optional) If you've specified a unique database name during the installation of the embedded Sybase database, set the value of the `Database` entry key to the unique database name.

6 On the ZENworks Server that has the embedded Sybase database installed, restart the ZENworks services:

- **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

  2. Double-click *Administrative Tools > Services*.

  3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, *Novell ZENworks Embedded Datastore*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

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

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

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

  - `/etc/init.d/./sybase-asa restart`

The ZENworks Server now points to new database.

22.7 Migrating the Data from an Embedded Sybase SQL Anywhere to an External Oracle Database

ZENworks 10 Asset Management allows you migrate the data from an internal Embedded Sybase SQL Anywhere database or an external Sybase SQL Anywhere database running on a ZENworks Primary Server to an Oracle database installed on a device that does not have the ZENworks 10 Asset Management installed.

IMPORTANT: If the ZENworks Reporting Server is installed on the device, the Reporting Server does not work after migrating the database. For the Reporting Server to work, you must again install the ZENworks Reporting Server on a Primary Server on which you have installed the Oracle client after migrating the database. For more information, see Section 22.7.3, "Post-Migration Tasks," on page 213.

Review the following to migrate the database:

- Section 22.7.1, "Preparing to Move the Data," on page 210
- Section 22.7.2, "Migrating the Data from the Sybase SQL Anywhere Database to an Oracle Database," on page 211
- Section 22.7.3, "Post-Migration Tasks," on page 213
- Section 22.7.4, "Troubleshooting Database Migration," on page 214
- Section 22.7.5, "Reverting to the Sybase Database," on page 216

22.7.1 Preparing to Move the Data

Before migrating the data from the Sybase database to Oracle database, do the following:

- Make sure that the license state of ZENworks 10 Asset Management is Active. The product must be installed and running either in the licensed version or the evaluation version.

- Save all the reports, `rights.xml`, and `ownership.xml` by using the `report-save (rpsv) (destination folder)` command. The XML files contain rights and ownership details of all the reports.

- Make sure that the Primary Server on which the Sybase database is configured has been upgraded to ZENworks 10 Asset Management.

- Make sure that the ZENworks Primary Server has an internal or external Sybase database installed.

- Make sure that the Oracle database is installed on a device that does not have ZENworks 10 Asset Management installed.

- Make sure that the USERS tablespace has sufficient space to create and store the ZENworks database schema. The tablespace requires a minimum of 100 MB to create ZENworks database schema without any data in it and an appropriate additional space depending upon the size of the database to be migrated. The database migration utility uses only the USERS tablespace by default. You cannot manually specify any other tablespace during the migration.

- Make sure that the NLS_CHARACTERSET parameter is set to AL32UTF8 and the NLS_NCHAR_CHARACTERSET parameter to AL16UTF16 by running the following query at the database prompt:

```
select parameter, value from nls_database_parameters where parameter like
'%CHARACTERSET%';
```

- (Conditional) If you want to migrate the database by creating a new user schema, ensure that the following additional requirements are met:

  - You must be aware of the database administrator credentials.

  - A tablespace must already exist for associating to the Oracle access user

- You can choose to migrate the database by using an existing user schema that resides on a server in your network in the following scenarios:

  - The database administrator creates a user schema with the necessary rights and you get the credentials for that user schema from the database administrator. In this case, the database administrator credentials are not required to migrate the database.

  - You create a user schema in the Oracle database and choose to use it during the database migration.

If you want to migrate the database by using an existing user schema, ensure that the following additional requirements are met:

- Make sure that the user schema has the following rights to create the database.

  ```
  CREATE SESSION
  CREATE_TABLE
  CREATE_VIEW
  CREATE_PROCEDURE
  CREATE_SEQUENCE
  ```

```
CREATE_TRIGGER
```

 ◆ Make sure that the quota for the user schema is set to Unlimited on the USERS tablespace.

◆ Manually stop the ZENworks services running on all the servers in the Management Zone.

 To stop the services:

 ◆ **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings* > *Control Panel*.

  2. Double-click *Administrative Tools* > *Services*.

  3. Stop the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

 ◆ **On Linux:** At the console prompt, enter the following commands:

  ◆ `/etc/init.d/./novell-zenmntr stop`

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

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

◆ Make sure that the Novell ZENworks Embedded Datastore service on the Primary Server is running.

 ◆ **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings* > *Control Panel*.

  2. Double-click *Administrative Tools* > *Services*.

  3. The status of the *Novell ZENworks Embedded Datastore* service must be *Started*.

 ◆ **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa status`.

◆ (Optional) The status of database migration is logged into the `novell-zenworks-configure.log` file. By default, only the messages of the type Info and Severe are logged. If you want other message types (such as Finer, Finest, and Warning) to also be logged into the file, do the following in the `novell-zenworks-configure.properties` file:

 1. Set the value of `Logger.logLevel` to the appropriate message type.

  For example, if you want messages of the type Finest to be logged:

  ```
  #Logger.logLevel   = FINEST
  ```

 2. Uncomment the line by removing the "#" as follows:

  ```
  Logger.logLevel   = FINEST
  ```

 The `novell-zenworks-configure.properties` file is located in `%ZENWORKS_HOME%\conf\` on Windows and in `/etc/opt/novell/zenworks/` on Linux.

22.7.2 Migrating the Data from the Sybase SQL Anywhere Database to an Oracle Database

◆ "Migrating the Data from the Sybase SQL Anywhere Database to an Oracle Database" on page 212

◆ "Resuming the Database Migration" on page 212

Migrating the Data from the Sybase SQL Anywhere Database to an Oracle Database

1 Make sure that all the tasks listed in are completed.

2 Run the database migration utility.

   ◆ **On Windows:** At the command prompt, go to
   `ZENworks_installation_path\bin\novell-zenworks-configure.bat` file and
   enter the following command:

   `novell-zenworks-configure.bat -c DBMigrateConfigureAction`

   ◆ **On Linux:** At the console prompt, go to `/opt/novell/zenworks/bin` and enter the
   following command:

   `novell-zenworks-configure -c DBMigrateConfigureAction`

3 Enter the target database type as Oracle.

4 Enter the IP address or host name of the Oracle database server.

5 Enter the port used by the Oracle database server.

6 Enter the fully qualified net service name for the Oracle database.

7 You can choose to create a new user schema or use an existing user schema.

   If you choose to create a new schema, continue with .

   If you choose to use an existing user schema, skip to .

8 Enter the database server administrator's username and password.

9 Enter the schema name when prompted for the database username.

10 Enter the database schema password when prompted for the database user's password.

   The database migration starts.

11 When the database migration is complete, you can check the `novell-zenworks-configure.log` file to see if the migration was successful. The log file is located in
   `%ZENWORKS_HOME%\log\` on Windows and in `/var/opt/novell/log/zenworks/` on Linux.

12 After the database is successfully migrated, continue with .

Resuming the Database Migration

If the migration of the database is stopped for any reason, the ZENworks migration utility allows you to resume the migration if the `dbmigration.xml` file has been created. The file is located in the `ZENworks_installtion_path\bin` directory on Windows, and in the `/opt/ novell/ zenworks/bin` directory on Linux.

1 Run the database migration utility.

   ◆ **On Windows:** At the command prompt, go to
   `ZENworks_installation_path\bin\novell-zenworks-configure.bat` file and
   enter the following command:

   `novell-zenworks-configure.bat -c DBMigrateConfigureAction`

   ◆ **On Linux:** At the console prompt, go to `/opt/novell/zenworks/bin` and enter the
   following command:

   `novell-zenworks-configure -c DBMigrateConfigureAction`

2 Enter the target database type as Oracle.

3 Enter the IP address or host name of the Oracle database server.

You must specify the IP address or host name of the Oracle database server used while migrating the database. For example, if you had specified the IP address of the database server while migrating the database, then you must specify the same IP address while resuming the database migration. You cannot specify the host name of the database server.

4 Enter the port used by the Oracle database server.

5 Enter the fully qualified net service name for the Oracle database.

6 Choose to use an existing schema.

7 Enter the schema name when prompted for the database username specified before stopping the database migration.

8 Enter the database schema password when prompted for the database user's password specified before stopping the database migration.

9 Choose to resume the database migration.

The database migration starts.

10 After the database is successfully migrated, continue with .

22.7.3 Post-Migration Tasks

If there is only one server in the Management Zone, all ZENworks services are automatically started after the data is successfully migrated to an Oracle database.

If there are multiple servers in the Management Zone:

1 On the device where you ran the migration utility, copy the following files to the appropriate directory on all the servers:

```
zdm.xml
dmaccounts.properties
dmmappings.properties
```

The files are located in the *ZENworks_installation_path*\conf\datamodel directory on Windows and in the /etc/opt/novell/zenworks/datamodel directory on Linux.

2 Restart the ZENworks services.

- **On Windows:** Do the following:

    1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

    2. Double-click *Administrative Tools > Services*.

    3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

    - /etc/init.d/./novell-zenmntr restart

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

    - /etc/init.d/./novell-zenloader restart

3 Migrate the ZENworks Reports from the Sybase SQL Anywhere database to an Oracle database:

   3a Install the Oracle client on a Primary Server that does not have an instance of the ZENworks Reporting Server.

   3b Install a new instance of the ZENworks Reporting Server on the device on which you have installed the Oracle client.

   3c Copy the reports to the device where the new instance of the Reporting Server is running. These are the ZENworks Reports that you saved before migrating them. For more information, see Section 22.7.1, "Preparing to Move the Data," on page 210.

   3d Publish the reports and restore the reporting rights and the ownership details of the reports by using the following command:

```
zman rpld path_of_directory_containing_rights.xml_and_ownership.xml
```

   3e Uninstall the ZENworks Reporting Server instance that was installed prior to migrating the database.

The ZENworks Server now points to the new database.

For the Oracle 10g database, any administrator name is case sensitive, including login names from user sources. The default ZENworks administrator account automatically created during installation uses an initial capital, so in order to log in to ZENworks Control Center, you must enter `Administrator`.

22.7.4 Troubleshooting Database Migration

- "Troubleshooting a Java Heap Space Exception" on page 214
- "Troubleshooting an Oracle Database Crash" on page 215
- "Troubleshooting an Oracle Tablespace Issue" on page 215
- "Troubleshooting the Database Migration Failure Issue" on page 216
- "Troubleshooting the Database Migration by Using An Existing User Schema" on page 216

Troubleshooting a Java Heap Space Exception

If you encounter a Java Heap Space exception during the database migration because of low memory:

1 Edit the *ZENworks_installation_path*\bin\novell-zenworks-configure.bat file on Windows or /opt/novell/zenworks/bin/novell-zenworks-configure on Linux to change the heap space value in the following line, depending upon the RAM of the device where the migration utility is running:

```
"%JAVA_HOME%\bin\java" -Djava.library.path=%ZENLIB% -cp "%MYCP%"
%DEBUG_OPTS% %JAVA_OPTS% -Xmx128m
com.novell.zenworks.configure.ConfigureLoader %CONFIG_OPTS%
```

The heap space value is represented in megabytes (MB) within -Xmx128m. By default, it is 128.

For example, if the RAM of the device is 512 MB, then the line in the novell-zenworks-configure.bat file can be updated as follows:

```
"%JAVA_HOME%\bin\java" -Djava.library.path=%ZENLIB% -cp "%MYCP%"
%DEBUG_OPTS% %JAVA_OPTS% -Xmx512m
com.novell.zenworks.configure.ConfigureLoader %CONFIG_OPTS%
```

IMPORTANT: The heap space value must be either equivalent to or less than the RAM of the device.

2 At the console prompt, run the `ZENworks_installation_path\bin\novell-zenworks-configure.bat` file on Windows or `/opt/novell/zenworks/bin/novell-zenworks-configure` on Linux.

3 Follow the prompts.

When you are prompted to enter the location of the file required for resuming the migration, enter the the complete path of `DBMigration.xml`. The file is located in the `ZENworks_installtion_path\bin` directory on Windows, and in the `/opt/novell/zenworks/bin` directory on Linux.

The XML file contains a list of tables and a flag indicating whether the table was successfully migrated or not. When the database migration resumes, only the tables with flag value set to False are migrated.

Troubleshooting an Oracle Database Crash

If the Oracle database crashes during the database migration:

1 At the console prompt, run the `ZENworks_installation_path\bin\novell-zenworks-configure.bat` file on Windows or `/opt/novell/zenworks/bin/novell-zenworks-configure` on Linux.

2 Follow the prompts.

When you are prompted to enter the location of the file required for resuming the migration, enter the the complete path of `DBMigration.xml`. The file is located in the `ZENworks_installtion_path\bin` directory on Windows, and in the `/opt/novell/zenworks/bin` directory on Linux.

The XML file contains a list of tables and a flag indicating whether the table was successfully migrated or not. When the database migration resumes, only the tables with flag value set to False are migrated.

IMPORTANT: Do not edit the contents of `DBMigration.xml`.

Troubleshooting an Oracle Tablespace Issue

If the Oracle USERS tablespace does not have sufficient space to create and store the ZENworks database schema, the database migration fails with the following error messages while trying to create the tables:

```
SEVERE: Terminating the database migration...
SEVERE: An error has occurred while migrating the database.
```

To resolve this issue, the Oracle database administrator must increase the size of the USERS tablespace. Ensure that the tablespace has a minimum of 100 MB to create ZENworks database schema without any data in it and an appropriate additional space depending upon the size of the database to be migrated.

Troubleshooting the Database Migration Failure Issue

If the NLS_CHARACTERSET parameter is not set to AL32UTF8 and the NLS_NCHAR_CHARACTERSET parameter is not set to AL16UTF16, the database migration fails with the following error messages:

```
Failed to run the sql script: localization-updater.sql,
message:Failed to execute the SQL command: insert into
zLocalizedMessage(messageid,lang,messagestr)
values('POLICYHANDLERS.EPE.INVALID_VALUE_FORMAT','fr','La stratégie {0} n''a
pas pu être appliquée du fait que la valeur de la variable "{1}" n''est pas
dans un format valide.'),
message:ORA-00600: internal error code, arguments: [ktfbbsearch-7], [8], [],
[], [], [], [], []
```

To resolve this issue, set the NLS_CHARACTERSET parameter to AL32UTF8 and the NLS_NCHAR_CHARACTERSET parameter to AL16UTF16. To ensure that the character set parameters are configured with the recommended values, run the following query at the database prompt:

```
select parameter, value from nls_database_parameters where parameter like
'%CHARACTERSET%';
```

Troubleshooting the Database Migration by Using An Existing User Schema

If you choose to migrate the database by using an existing user schema, the database migration utility creates the ZENworks database but it might fail to migrate the data.

To resolve this issue:

1 Make sure that the ZENworks tables, views, and user sequence are deleted from the newly created ZENworks database by the database administrator. Later on, clear the user_recyclebin database table.

2 Start the database migration again by using the same user schema. For more information, see "Migrating the Data from the Sybase SQL Anywhere Database to an Oracle Database" on page 212.

22.7.5 Reverting to the Sybase Database

If you want to return to using the Sybase database:

1 On the device where you run the migration utility, rename the following files:

zdm.xml.bak to zdm.xml

dmaccounts.properties.bak to dmaccounts.properties

dmmappings.properties.bak to dmmappings.properties

The files are located in the *ZENworks_installation_path*\conf\datamodel directory on Windows and in the /etc/opt/novell/zenworks/datamodel directory on Linux.

2 Restart all the ZENworks Services:

◆ **On Windows:** Do the following:

1. From the Windows desktop *Start* menu, click *Settings* > *Control Panel*.

2. Double-click *Administrative Tools > Services*.

3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

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

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

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

External Database Maintenance

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

23

</div>

- ◆ Section 23.1, "Moving the Data from One External Sybase Database to another External Sybase Database," on page 219
- ◆ Section 23.2, "Configuring the ZENworks Server to Point to the New MS SQL Database Containing Data Moved from Another MS SQL Database," on page 220
- ◆ Section 23.3, "Configuring the ZENworks Server to Point to the New Oracle Database Containing Data Moved from Another Oracle Database," on page 222

23.1 Moving the Data from One External Sybase Database to another External Sybase Database

ZENworks® 10 Asset Management allows you move the data from one OEM Sybase database (external Sybase database) to another external Sybase database.

- ◆ Section 23.1.1, "Preparing to Move the Data," on page 219
- ◆ Section 23.1.2, "Moving the Data from One External Sybase to Another External Sybase," on page 219

23.1.1 Preparing to Move the Data

Before moving the data from one external Sybase database to another external Sybase database, do the following:

- ◆ Make sure that ZENworks 10 Asset Management is installed with an external Sybase database on a Windows or Linux device. The data is moved from this database to another external database.
- ◆ Make sure that you have another Windows or Linux device with an external Sybase database installed. For more information on how to install an external Sybase database, see "Installing an External ZENworks Database" in the *ZENworks 10 Asset Management Installation Guide*.

23.1.2 Moving the Data from One External Sybase to Another External Sybase

In the following procedure, assume that the device you are moving the data from is EDB1 and the device you are moving the data to is EDB2.

1. On the EDB1 device from which you want to move the data, stop the Novell® ZENworks Embedded Datastore service.
   - ◆ **On Windows:** Do the following:
     1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.
     2. Double-click *Administrative Tools > Services*.
     3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Stop*, or select the *Novell ZENworks Embedded Datastore* service, then click ■ on the toolbar.
   - ◆ **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa stop`.

2 From the EDB1 device, copy `zenworks_database.conf` and all files within the `database` directory to the appropriate directories on the EDB2 device.

The `zenworks_database.conf` is located in the `ZENworks_installation_path\conf\` directory on Windows and in the `/etc/opt/novell/zenworks/` directory on Linux.

The `database` directory is located in `ZENworks_installation_path` by default on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

3 On the EDB2 device, open `zenworks_database.conf` and make sure that it contains the correct path of the database file.

4 On the EDB1 device, edit `zdm.xml` (located in `ZENworks_installation_path\conf\datamodel` on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux):

- Set the value of the `Server` entry key to the IP address of the EDB2 device.

- Make sure that the value of the `Port` entry key is the port number on which the EDB2 device is running.

5 On the EDB2 device, start the Novell ZENworks Embedded Datastore service:

- **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

  2. Double-click *Administrative Tools > Services*.

  3. Right-click the *Novell ZENworks Embedded Datastore* service, then click *Start*, or select the *Novell ZENworks Embedded Datastore* service, then click ▶ on the toolbar.

- **On Linux:** At the console prompt, enter `/etc/init.d/./sybase-asa start`.

6 On the EDB1 device, restart the ZENworks services:

- **On Windows:** Do the following:

  1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.

  2. Double-click *Administrative Tools > Services*.

  3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

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

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

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

The ZENworks Server now points to new database (EDB2).

23.2 Configuring the ZENworks Server to Point to the New MS SQL Database Containing Data Moved from Another MS SQL Database

If you move the data from one MS SQL database to another MS SQL database, the ZENworks Server must be configured to point to the new MS SQL database.

The following sections provide detailed information:

23.2.1 Preparing to Move the Data

Before configuring the server to point the new MS SQL database, do the following:

- Make sure that ZENworks 10 Asset Management is installed (on Windows or Linux) with an MS SQL database. The data is migrated from this database to another MS SQL database. Assume that this device is called MSDB1.

- Make sure that you have another Windows device with an MS SQL database installed. Assume that this device is called MSDB2. For more information on how to install an MS SQL database, see "Installing an External ZENworks Database" in the *ZENworks 10 Asset Management Installation Guide*.

- Move the data from MSDB1 to MSDB2. For more information about moving the data, see the MS SQL database documentation.

23.2.2 Configuring the ZENworks Server to Point to the New MS SQL Database

To configure the ZENworks Server to point to the new database (MSDB2):

1 On the MSDB1 device, edit `zdm.xml` (located in `ZENworks_installation_path\conf\datamodel` on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux) to do the following:

- Make sure that the value of the `Port` entry key is the port number on which the MS SQL database is running.
- Set the value of the `Server` entry key to the IP address of the MSDB2 device.
- Set the value of the `Database` entry key to path of the database directory of the MSDB2 device.

2 On the MSDB1 device, restart the ZENworks services.

- **On Windows:** Do the following:

   1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.
   2. Double-click *Administrative Tools > Services*.
   3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:

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

23.3 Configuring the ZENworks Server to Point to the New Oracle Database Containing Data Moved from Another Oracle Database

If you move the data from one Oracle database to another Oracle database, the ZENworks Server must be configured to point to the new Oracle database.

The following sections provide detailed information:

23.3.1 Preparing to Move the Data

Before configuring the server to point the new Oracle database, do the following:

- Make sure that ZENworks 10 Asset Management is installed (on Windows or Linux) with an Oracle database. The data is migrated from this database to another Oracle database. Assume that this device is called ORDB1.
- Make sure that you have another Windows device with an Oracle database installed with the same database credentials as the ORDB1. Assume that this device is called ORDB2. For more information on how to install an Oracle database, see "Installing an External ZENworks Database" in the *ZENworks 10 Asset Management Installation Guide*.
- Move the data from ORDB1 to ORDB2. For more information about moving the data, see the Oracle database documentation.

23.3.2 Configuring the ZENworks Server to Point to the New Oracle Database

To configure the ZENworks Server to point to the new Oracle database (ORDB2):

1 On the ORDB1 device, edit `zdm.xml` (located in `ZENworks_installation_path\conf\datamodel` on Windows and in `/etc/opt/novell/zenworks/datamodel` on Linux) to do the following:

- Make sure that the value of the `Port` entry key is the port number on which the Oracle database is running.
- Set the value of the `Server` entry key to the IP address of the ORDB2 device.
- Set the value of the `Database` entry key to net service name of the Oracle database installed on the ORDB2 device.

2 On the ORDB1 device, restart the ZENworks services.

- **On Windows:** Do the following:

    1. From the Windows desktop *Start* menu, click *Settings > Control Panel*.
    2. Double-click *Administrative Tools > Services*.
    3. Start the following services: *Novell ZENworks Server*, *Novell ZENworks Services Monitor*, and *Novell ZENworks Agent Service*.

- **On Linux:** At the console prompt, enter the following commands:
  - `/etc/init.d/./novell-zenmntr restart`
  - `/etc/init.d/./novell-zenserver restart`
  - `/etc/init.d/./novell-zenloader restart`

Zone Administration

VII

This section contains information about Management Zone configuration settings that let you control a wide range of functionality for your Zone.

◆ Chapter 24, "Management Zone Configuration Settings," on page 227

Management Zone Configuration Settings

<div style="text-align: right; font-size: 3em;">24</div>

The Management Zone configuration settings enable you to control a wide range of functionality for your Zone. There are Device Management settings that let you control how often devices access a ZENworks Server for refreshed information, how often dynamic groups are refreshed, and what levels of messages (informational, warning, or error) are logged by the ZENworks Adaptive Agent. There are Inventory settings, Discovery and Deployment settings, and much more.

The configuration settings are grouped into categories:

24.1 Accessing Configuration Settings

Management Zone settings that apply to devices are inherited by all devices in the zone. You can override zone settings by configuring them on device folders or on individual devices. This allows you to establish zone settings that apply to the largest number of devices and then, as necessary, override the settings on folders and devices.

By default, your zone settings are preconfigured with values that provide common functionality. You can, however, change the settings to best adapt them to the behavior you need in your environment.

24.1.1 Modifying Configuration Settings at the Zone

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

2 In the Management Zone Settings panel, click the settings category (*Device Management*, *Discovery and Deployment*, *Event and Messaging*, and so forth) whose settings you want to modify.

3 Click the setting to display its details page.

4 Modify the setting as desired.

For information about the settings, click the *Help* button in ZENworks Control Center or see the following sections:

- ◆ "Device Management Settings" on page 230
- ◆ "Discovery and Deployment Settings" on page 231
- ◆ "Event and Messaging Settings" on page 231
- ◆ "Infrastructure Management Settings" on page 232
- ◆ "Inventory Settings" on page 232
- ◆ "Reporting Services Settings" on page 233
- ◆ "Asset Management Settings" on page 233

5 When you have finished modifying the setting, click *OK* (or *Apply*) to save your changes.

If the configuration setting applies to devices, the setting is inherited by all devices in the zone unless the setting is overridden at a folder level or a device level.

24.1.2 Modifying Configuration Settings on a Folder

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

2 In the Devices panel (on the *Managed* tab), browse for the folder whose settings you want to modify.

3 When you find the folder, click *Details* next to the folder name to display the folder's details.

4 Click the *Settings* tab.

5 In the Settings panel, click the settings category (, *Device Management*, *Infrastructure Management*, and so forth) whose settings you want to modify.

6 Click the setting to display its details page.

7 Modify the setting as desired.

For information about the setting, click the *Help* button in ZENworks Control Center or see the following sections:

- "Device Management Settings" on page 230
- "Discovery and Deployment Settings" on page 231
- "Event and Messaging Settings" on page 231
- "Infrastructure Management Settings" on page 232
- "Inventory Settings" on page 232
- "Reporting Services Settings" on page 233
- "Asset Management Settings" on page 233

8 When you have finished modifying the setting, click *OK* (or *Apply*) to save your changes.

The configuration setting is inherited by all devices in the folder, including any devices contained in subfolders, unless the setting is overridden on a subfolder or individual device.

24.1.3 Modifying Configuration Settings on a Device

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

2 In the Devices panel (on the *Managed* tab), browse for the device whose settings you want to modify.

3 When you find the device, click the device name to display the its details.

4 Click the *Settings* tab.

5 In the Settings panel, click the settings category (*Device Management*, *Infrastructure Management*, and so forth) whose settings you want to modify.

Devices > Workstations > zendocwks1

zendocwks1

| Summary | Inventory | Relationships | Settings |

Settings

Device Management

Category	Description	Inherited From
Local Device Logging	Enable and configure local logging of warnings and errors encountered by managed devices.	(System)
Device Refresh Schedule	Configure the device refresh interval.	(System)
ZENworks Agent	ZENworks Agent Configuration.	(System)
ZENworks Explorer Configuration	Configure the behavior of the ZENworks Explorer on managed devices.	(System)
System Variables	Configure system variables.	---
Primary User	Configure the setting for how the primary user is determined.	---

Infrastructure Management

Inventory

Asset Management

6 Click the setting to display its details page.

7 Modify the setting as desired.

For information about the setting, click the *Help* button in ZENworks Control Center or see the following sections:

- "Device Management Settings" on page 230
- "Discovery and Deployment Settings" on page 231
- "Event and Messaging Settings" on page 231
- "Infrastructure Management Settings" on page 232
- "Inventory Settings" on page 232
- "Reporting Services Settings" on page 233
- "Asset Management Settings" on page 233

8 When you have finished modifying the setting, click *OK* (or *Apply*) to save your changes.

24.2 Device Management Settings

The Device Management section contains the following settings:

Local Device Logging: Configure logging of messages to a managed device's local drive. You can determine what severity level messages are logged and when the log file is backed up. You can also determine what severity level messages are sent to the ZENworks server for viewing in ZENworks Control Center. For more information, see Local Device Logging (../../resources/help/settings_syslocallogging.html).

Device Refresh Schedule: Specify how often a device contacts a ZENworks Server to update information. You can also specify what to do with a device when it has not contacted a ZENworks Server within a certain number of days. For more information, see Device Refresh Schedule (../../resources/help/settings_sysrefreshsched.html).

ZENworks Agent: Configure uninstall and caching settings for the ZENworks Adaptive Agent as well as enable or disable specific Adaptive Agent modules. For more information, see ZENworks Agent (../../resources/help/settings_agent.html).

Registration: Control the settings used when registering devices, including how registered devices are named, whether registration rules are enabled, and whether device objects in ZENworks Control Center can be renamed as they update their registration information. For more information, see Registration (../../resources/help/settings_registration.html).

System Variables: Define variables that can be used to replace paths, names, and so forth as you enter information in ZENworks Control Center. For more information, see System Variables (../../resources/help/settings_systemvariables.html).

Primary User: Determine how and when a device's primary user is calculated. For more information, see Primary User (../../resources/help/settings_primaryuser.html).

Primary Workstation: Determine how and when a device's primary workstation is calculated. You can also disable the calculation by selecting the *None (do not calculate)* option. For more information, see Primary Workstation (../../resources/help/settings_primaryws.html).

Dynamic Group Refresh Schedule: Determine how often a dynamic group's criteria are applied to devices in order to update membership in the group. Membership in a dynamic group is determined by applying the dynamic group's criteria to devices. If a device meets the criteria, it is added to the group; you cannot manually add devices to a dynamic group or remove them from a dynamic group. For more information, see Dynamic Group Refresh Schedule (../../resources/help/settings_dynamicgroupschedule.html).

Wake-on-LAN: Configure the number of retry attempts to wake up a device and the time interval between the retry attempts. For more information, see Wake-on-LAN (../../resources/help/settings_wakeonlan.html).

24.3 Discovery and Deployment Settings

The Discovery and Deployment section contains the following settings:

Advertised Discovery Settings: Specify how often you want your ZENworks system to attempt to discover devices on your network that have the ZENworks pre-agent installed. For more information, see Advertised Discovery Settings (../../resources/help/settings_discovery_advertised.html).

Discovery: Control the settings used during the discovery processes, including the maximum number of discovery requests that can be running at one time and the technologies to use for the discovery. You can also specify IP and SNMP settings used by the WMI (Windows Management Instrumentation) and SNMP discovery technologies. For more information, see Discovery (../../resources/help/settings_discoverysettings.html).

Windows Proxy: Specify a managed Windows device in your zone to perform discovery and deployment tasks in place of a ZENworks Server. This is designed primarily to enable ZENworks Servers running on Linux to offload discovery tasks that use Windows-specific discovery technologies such as WMI and WinAPI and deployment tasks that involve Windows managed devices. For more information, see Windows Proxy (../../resources/help/settings_winproxysettings.html).

24.4 Event and Messaging Settings

The Event and Messaging section contains the following settings:

Centralized Message Logging: Configure the settings related to message logging performed by the Primary Server, including automatic message cleanup, e-mail notification, SNMP traps, and UDP forwarding. For more information, see Centralized Message Logging (../../resources/help/settings_syscentralizedlogging.html).

SMTP Settings: Configure the SMTP server for sending the e-mail notifications to ZENworks administrators. For more information, see SMTP Settings (../../resources/help/settings_smtpsettings.html).

24.5 Infrastructure Management Settings

The Infrastructure Management section contains the following settings:

Closest Server Default Rule: Define the rule that is used by a device to determine the closest collection, content, and configuration servers when no Closest Server rules have been defined or when none apply. This rule is simply a listing of the servers in the order you want devices to contact them. You cannot add or remove servers from the lists. For more information, see Closest Server Default Rule (../../resources/help/settings_closestserverdefaultrule.html).

Closest Server Rules: Create rules that are used to determine which servers a device contacts for the collection, content, and configuration functions, if your ZENworks Management Zone includes more than one server. For more information, see Closest Server Rules (../../resources/help/settings_closestserverrules.html).

HTTP Proxy Settings: Define proxy servers you want to use. A proxy server lets a device connect indirectly to a ZENworks Server through the proxy server. The device's ZENworks Adaptive Agent connects to the proxy server, then requests resources from a ZENworks Server. The proxy provides the resource either by connecting to the ZENworks Server or by serving it from a cache. For more information, see HTTP Proxy Settings (../../resources/help/settings_httpproxy.html).

System Update Settings: Configure how you want to use the System Updates feature, including how often to check for updates, specifying a download schedule, configuring e-mail notifications, and more. For more information, see System Update Settings (../../resources/help/settings_systemupdate.html).

ZENworks News Settings: Configures the server and the schedule for downloading the ZENworks News. For more information, see ZENworks News Settings (../../resources/help/settings_zenworksnews.html).

24.6 Inventory Settings

The Inventory section contains the following settings:

Inventory: Configure inventory scanning settings, including on-demand scans, first scans, and recurring scans. You can also specify directories to skip when performing scans and identify software applications that are not contained in the ZENworks Knowledgebase. For more information, see Inventory (../../resources/help/settings_sysinventory.html).

Inventory Schedule: Specify when to run an inventory scan, including specifying that scans do not run automatically or specifying a date-specific, recurring, or event-driven scan. For more information, see Inventory Schedule (../../resources/help/settings_sysinventoryschedule.html).

Collection Data Form: Configure which demographic data to collect for a device or devices, such as a user's name or telephone, which department the user belongs to, and so on. For more information, see Collection Data Form (../../resources/help/ settings_sysinventorycollectwizard.html).

Collection Data Form Schedule: Configure how you send out the Collection Data Form. You can schedule it as part of a regular inventory scan, you can use a Device Quick Task, or you can use the Collection Data Form Schedule. For more information, see Collection Data Form Schedule (../../ resources/help/settings_sysinventorywizardschedule.html).

Inventory Only: Configure inventory scan settings for devices in the zone that don't have the ZENworks Adaptive Agent installed but do have the Inventory Module installed. This type of scan is useful for devices running Windows NT, Windows 95, Windows 98, Windows Me, NetWare, and Mac OS* X. For more information, see Inventory Only (../../resources/help/settings_sysumi.html).

Inventory Only Schedule: Configure when to run an Inventory Only scan. For more information, see Inventory Only Schedule (../../resources/help/settings_sysumischedule.html).

Inventory Only Reconciliation: Control whether and how new workstations are reconciled to avoid the possibility of duplicates in the database. When a scan is made of a workstation that is new to the Management Zone, it is assigned an identifier. If the identifier is lost, such as by a disk crash, it is assigned a new identifier during the next scan. Reconciliation allows you to check whether the workstation is already in the database. If it is, the identifier in the database is changed to match the new identifier. For more information, see Inventory Only Reconciliation (../../resources/help/ settings_sysinventoryreconcile.html).

24.7 Reporting Services Settings

The Reporting Services section contains the following settings:

E-mail Notification Settings: Configure the ZENworks Reporting Server for sending e-mail notifications to the ZENworks administrator. For more information, see E-mail Notification Settings (../../resources/help/cfg_mzset_reptsvr_set.html).

Folder Sync Schedule: Define the refresh interval when the Custom Report folders that are created in the ZENworks Reporting Server InfoView must synchronize with the ZENworks Control Center. For more information, see Folder Sync Schedule (../../resources/help/cfg_report_foldersync.html).

Reset the Passphrase of the ZENworks Reporting Server: Allow the user to reset the Passphrase of the ZENworks Reporting Server. For more information, see Reset the Passphrase (../../resources/ help/cfg_report_resetpassphrase.html).

File Location Notification Settings: Specify the destination directory for the report instances on the ZENworks Reporting Server or on any other remote server. For more information, see File Location Notification Settings (../../resources/help/cfg_report_filelocsettings.html).

FTP Server Notification Settings: Specify the destination on the FTP server where you want to transfer the reporting instances. For more information, see FTP Server Notification Settings (../../ resources/help/cfg_report_ftpsrvrsettings.html).

24.8 Asset Management Settings

The Asset Management section contains the following settings:

Reports: Configure report settings for Asset Management. For more information, see Reports (../../
resources/help/settings_sysamreport.html).

Compliance: Set the time of day that license compliance data is refreshed. For more information,
see Compliance (../../resources/help/settings_sysamcompliance.html).

Usage Monitoring: Enable software usage monitoring. For more information, see Usage
Monitoring (../../resources/help/am_usagemonitor.html).

Usage Display: Configure whether or not usage data is displayed on License Management pages
(Asset Management > License Management tab) in the ZENworks Control Center.. For more
information, see Usage Display (../../resources/help/am_usagedisplay.html).

Message Logging

VIII

This section includes information about Message Logger features and procedures to help you configure and maintain your Novell® ZENworks® system.

Overview

25

The Message Logger component of Novell® ZENworks® 10 Asset Management lets the other ZENworks components such as zenloader, webservices, and ZENworks Management Daemon (ZMD) log messages to different output targets. The output targets includes the system log, local log, database, SMTP, SNMP trap, and UDP.

The following sections provide additional information on the Message Logger component:

25.1 Functionalities of Message Logger

Message Logger performs the following functions:

- Writes messages to local log files.
- Writes messages to a system log or event log.
- Writes messages to the Management console.
- Sends messages to the Management server.
- Sends messages as SMTP mail to SMTP servers from the Primary Server.
- Sends messages as SNMP traps to remote or local machines from the Primary Server.
- Sends messages as UDP packets to UDP destinations.
- Writes messages to the ZENworks database.
- Automatically purges database entries from the ZENworks database.
- Automatically acknowledges the messages in the ZENworks database.

25.2 Message Severity

A message is an event that is generated by different components and modules. These events can be exceptions such as errors, warnings, information to a user, or a debug statement to debug a module.

Messages are classified based on the following severity levels:

Error: Indicates that an action cannot be completed because of a user or system error. These messages are critical and require immediate attention from an administrator.

Warning: Indicates 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.

Debug: Provides debug information to troubleshoot and solve problems that might occur. The debug messages are stored only in the local file.

25.3 Message Format

Messages are logged in different formats depending on the output targets. For more information on message formats see, Section 27.1, "Understanding Message Formats," on page 245.

Configuring Message Logger Settings

26

The following sections provide information on configuring the settings of the Message Logger component of Novell® ZENworks® 10 Asset Management.

26.1 Configuring the Message Logger Settings at the Zone Level

The following sections contain information to help you configure the settings in the Management Zone to enable message logging:

26.1.1 Local Device Logging

In ZENworks Control Center, the Local Device Logging page lets you configure the message logging to a local drive and the system log file of the managed device.

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Device Management*, then click *Local Device Logging*.

3 Configure the following options in the Local File panel:

Log Message to a Local File if Severity Is: Choose from one of the following:

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

- **Warning and Above:** Stores messages with a severity of Warning and Error.

- **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.

If you need to troubleshoot a ZENworks Adaptive Agent issue on an individual device, you can change the severity setting so that additional information is logged. On the device, double-click the Z icon in the notification area, click *Logging* in the left navigation pane, then select an option from the *Log Messages if Severity Is* drop-down list.

Rolling Based on Size: Closes the current log file and starts a new file based on the file size:

 - **Limit File Size to:** Specify the maximum size of the log file, in either kilobytes (KB) or megabytes (MB). The log file is closed after the size of the file reaches the specified limit and a new file is started.

 - **Number of Backup Files:** Specify the number of closed files to be backed up. The maximum number of backup files is 13.

Rolling Based on Date: Closes the current log file and starts a new file based on the following schedules:

 - **Daily Pattern:** Starts a new file daily.

 - **Monthly Pattern:** Starts a new file monthly.

On a Windows managed device, the local files include the following:

 - `zmd-messages.log` located in `\novell\zenworks\logs\localstore`

 - `loader-messages.log` located in `\novell\zenworks\logs`

 - `services-messages.log` located in `\novell\zenworks\logs`

On a Linux managed device, the local files include the following:

 - `loader-messages.log` located in `/var/opt/novell/log/zenworks`

 - `services-messages.log` located in `/var/opt/novell/log/zenworks`

4 Configure the following options in the System Log panel.

Send Message to Local System Log if Severity Is: Choose from one of the following:

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

 - **Warning and Above:** Stores messages with a severity of Warning and Error.

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

This setting lets you determine the message types that are added to the local system log. The local system log is the `\var\log\messages` directory on Linux devices and the `zenworks/logs/centralstore` directory on Windows devices.

Messages added to this system log directory are sent to the ZENworks Server for viewing in ZENworks Control Center on the *Configuration > System Information* page or by viewing the Summary page for the server or workstation.

26.1.2 Centralized Message Logging

In ZENworks Control Center, the Centralized Message Logging page lets you configure the settings related to message logging performed by the Primary Server.

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Event and Messaging*, then click *Centralized Message Logging*.

3 In the Automatic Message Cleanup panel, configure the settings to automatically acknowledge or remove the logged messages from the ZENworks server:

Preferred Maintenance Server: Specify the IP address of the preferred server on which the Message Cleanup actions runs to acknowledge or delete the logged messages from database.

Information: Allows you to configure the following settings for the informational messages:

◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are acknowledged. By default, all the informational messages older than 60 days are automatically acknowledged.

◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged informational messages that are older than the number of days you specify. For example, if you specify 30 days, then all the informational messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the informational messages dated until today are deleted. By default, all the informational messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Warnings: Allows you to configure the following settings for the warning messages:

◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are acknowledged. By default, all the warning messages older than 60 days are automatically acknowledged.

◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged warning messages that are older than the number of days you specify. For example, if you specify 30 days, then all the warning messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then the warning messages dated until today are deleted. By default, all the warning messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Errors: Allows you to configure the following settings for the error messages:

◆ **Auto acknowledge when older than [ ] days:** Allows you to automatically acknowledge the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are acknowledged when the Message Cleanup activity is scheduled to run. If you specify zero, then the error messages dated until today are acknowledged. By default, all the error messages older than 60 days are automatically acknowledged.

◆ **Auto delete when older than [ ] days:** Allows you to automatically delete the logged error messages that are older than the number of days you specify. For example, if you specify 30 days, then all the error messages logged before 30 days from the current date are deleted when the Message Cleanup activity is scheduled to run. If you specify zero, then error messages dated until today are deleted. By default, all the error messages older than 60 days are automatically deleted.

If you want to specify both the auto-acknowledge and auto-delete days, then the number of auto-acknowledge days should always be less than the number for auto-delete days.

Select the Days of the Week and the Time to Perform the Message Cleanup: Allows you to specify the time and the days of the week to run the Message Cleanup action. The administrator can set a daily schedule for Message Cleanup action.

Use Coordinated Universal Time: Allows you to convert the specified time to UTC (GMT) time. By default, this option is selected.

4 In the E-mail Notification panel, configure the settings to send the error messages to the administrators through e-mail:

Send Log Message via E-mail if Severity Is: Allows you to select the severity of the message to trigger sending the log messages through e-mail.

From: Specify the sender's e-mail address.

To: Specify the e-mail address of the recipients. You can specify more than one e-mail address by separating them with commas.

Subject: Specify the subject to be included while sending the e-mail from the Primary Server. You can customize the *Subject* field with macro values. For more information on customizing the subject field, see Section 27.1.2, "E-Mail Format," on page 245.

5 In the SNMP Traps panel, configure the SNMP traps on the ZENworks Server to send log messages:

Send as SNMP Trap if Severity Is: Sends an SNMP trap if the logged message's severity is Error.

Trap Target: Specify the IP address or DNS name of the SNMP server.

Port: Specify the port number of the SNMP server configured for this operation. By default, the port number is 162.

Community String: Specify the community string of the SNMP trap that is to be sent.

6 In the UDP Forwarder panel, configure the settings to send logged messages through the UDP services. The following table contains information on the options available:

Send Message via UDP: Sends messages to the UDP destinations if the logged message's severity is Error.

UDP Destinations: You can perform the following tasks with the *Add*, *Edit*, and *Remove* options:

- ◆ **Add a Server**
    1. Click *Add* to display the Add UDP Destination Address dialog box.
    2. Specify the server name and the UDP port number configured for this operation.
    3. Click *OK*.
- ◆ **Remove a Server**
    1. Select the check box next to the server (or servers).
    2. Click *Remove*.
- ◆ **Edit Server Details**
    1. Select the check box next to the server.
    2. Click *Edit* to display the Edit UDP Destination dialog box.
    3. Modify the settings as desired, then click *OK*.

26.2 Configuring the Message Logger Settings at the Folder Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for all the devices within a folder:

1 In ZENworks Control Center, click *Devices*.

2 Click the *Folder (Details)* option for which you want to configure the Message Logger settings.

3 Click *Settings*, then click *Device Management > Local Device Logging*.

4 Click *Override*.

5 Edit the logging settings as required.

6 To apply the changes, click *Apply*.

or

To revert to the Local Device Logging settings configured at the zone level, click *Revert*.

7 Click *OK*.

26.3 Configuring the Message Logger Settings at the Device Level

By default, the Message Logger settings configured at the zone level are applied to all the managed devices. However, you can modify the Local Device Logging settings for the managed device:

1 In ZENworks Control Center, click *Devices*.

2 Click *Servers* or *Workstations* to display the list of managed devices.

3 Click the device for which you want to configure the Message Logger settings.

4 Click *Settings*, then click *Device Management > Local Device Logging*.

5 Click *Override*.

6 Edit the logging settings as required.

7 To apply the changes click *Apply*.

or

To revert to the Local Device Logging settings configured at the zone level, click *Revert*.

8 Click *OK*.

26.4 Turning on the Debug Messages

To turn on the logging of debug messages for all components:

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Device Management*, then click *Local Device Logging.*

3 In the local file panel, select the *Log message to a local file if severity is* option, then select the severity as *Debug and above*.

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

Managing Messages

27

The Message Logger component lets you manage the messages logged by the other components of Novell® ZENworks® 10 Asset Management.

- Section 27.1, "Understanding Message Formats," on page 245
- Section 27.2, "Viewing the Message Status," on page 247
- Section 27.3, "Viewing the Messages," on page 249
- Section 27.4, "Acknowledging Messages," on page 250
- Section 27.5, "Deleting Messages," on page 252
- Section 27.6, "Viewing the Predefined Reports," on page 254

27.1 Understanding Message Formats

- Section 27.1.1, "Local Log File Format," on page 245
- Section 27.1.2, "E-Mail Format," on page 245
- Section 27.1.3, "SNMP Message Format," on page 246
- Section 27.1.4, "UDP Payload Format," on page 247

Messages are logged in different formats depending on the output targets such as local log, e-mail notification, SNMP traps, and UDP notification.

All error messages log the component name on which the error is generated. To troubleshoot the error, refer to the component's Reference Guide.

27.1.1 Local Log File Format

Messages are logged on the managed device and ZENworks Server in the following format:

```
[severity] [loggingTime] [userGUID] [componentName] [MessageID]
[MessageString] [additionalInfo] [RelatedGUID].
```

For example, `[DEBUG] [1/22/2007 12:09:15 PM] [] [ZMD] [] [refreshing QuickTaskRefresh(GeneralRefresh)] [] [].`

27.1.2 E-Mail Format

An e-mail message consists of the message header and the message body:

- "Message Header" on page 245
- "Message Body" on page 246

Message Header

The subject field in the e-mail can be customized as required by using keyword substitution macros:

Macro	Value
%s	Severity of the message.
%c	Name of the component.
%d	ID of the device at which the message is generated.
%t	Time of the message generation.
%a	Alias name of the device where the message is generated.

For example, if you want the subject line to display as "ERROR occurred on device Testifies at 4/1/ 07 5:31:01 PM", then specify "*%s occurred on device %a at %t*" in the *Subject* field.

Message Body

The message body consists of the following fields:

- ◆ **Device Alias:** Name of the device where the message is generated.
- ◆ **Device IP Address:** IP Address of the device where the message is generated.
- ◆ **Error:** [Date] Component name Message ID localized message string.
- ◆ **Additional Information:** (Optional) Any additional information.

27.1.3 SNMP Message Format

The SNMP messages consists of the following two parts:

- ◆ "SNMP Message Header" on page 246
- ◆ "Protocol Data Unit (PDU)" on page 246

SNMP Message Header

The following fields are contained in the header:

Version Number: Specifies the version of SNMP used. ZENworks 10 Asset Management uses SNMPv1.

Community String: Defines an access environment for a group of network-management systems (NMS).

Protocol Data Unit (PDU)

The following fields are contained in the PDU:

Enterprise: Identifies the type of managed object generating the trap. ZENworks 10 Asset Management uses 1.3.6.1.4.1.23.2.80.100.

Agent Address: Provides the IP address of the machine where the trap was generated.

GenerIc Trap Type: Contains the integer value 6. Type 6 is an enterprise-specific trap type, which has no standard interpretation in SNMP. The interpretation of the trap depends upon the value in the specific trap type field, which is defined by the Message Logger MIB.

Specific Trap Code: For enterprise-specific traps generated by ZENworks 10 Asset Management, the values in the specific trap type fields are as follows:

- For a severity level of MessageLogger.ERROR, the specific trap is 1.
- For a severity level of MessageLogger.WARN, the specific trap is 2.
- For a severity level of MessageLogger.INFO, the specific trap is 3.

Time Stamp: The time stamp indicating when the trap occurred.

Variable Bindings: Provides additional information pertaining to the trap. This field consists of the following name/value pairs:

- For trap ID 1.3.6.1.4.1.23.2.80.100.0.1, the value is the device GUID.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.2, the value is the device name.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.3, the value is the component name.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.4, the value is the time when the message was logged.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.5, the value is the message ID.
- For trap ID 1.3.6.1.4.1.23.2.80.100.0.6, the value is the probable cause.

27.1.4 UDP Payload Format

The payload is a byte array with null-terminated delimiters such as \0 or 0 x 00 (hexadecimal) for each element. Each element's data is presented as UTF-8 encoded strings and is explained below:

- The first element is the ZENworks version information. For example, 10.
- The second element is the value of severity of the message. The severity values are 4 for Informational, 6 for Warning, and 8 for Debug messages.
- The third element is the message date. The date is not locally specific and is represented as a UTF-8 string. For example, 09-Mar-2008 14:15:44.
- The fourth element is the user ID.
- The fifth element is the component name.
- The sixth element is the non-localized message ID.
- The seventh element is the localized message string.
- The eighth element is the additional information.
- The ninth element is the probable cause URL.
- The tenth element is the related GUID objects separated by commas.

NOTE: If the element does not have any data, it is represented as \0\0.

27.2 Viewing the Message Status

In ZENworks Control Center, you can view the status of the logged messages in the following panels on the home page.

27.2.1 Message Summary

The Message Summary panel displays the number of critical, warning, and normal messages generated on the main objects in the Management Zone.

Figure 27-1 *Message Summary*

Message Summary				
	⊗	◇	●	**Total**
🗄 Servers	3	0	5	8
🖥 Workstations	9	1	1	11

In the Message Summary panel, you can do the following:

* Click an object type to display its root folder. For example, click *Servers* to display the Servers root folder.

* For any object type, click the number in one of its status columns (⊗◇ ●) to display a listing of all the objects that currently have that status. For example, to see the list of servers that have a normal status, click the number in the column of the *Servers*.

* For any object type, click the number in the *Total* column to display all of the objects of that type having critical, warning, or normal messages. For example, click the Total count for *Servers* to display a list of all servers having messages logged.

27.2.2 Device Hot List

The Device Hot List displays a list of the devices that have a noncompliant ⊠ status or have generated critical ⊗ or warning ◇ messages. The device remains in the hot list until you resolve the compliancy problem and acknowledge the messages. You can use this list as a summary of problems that need attention on the device.

To view the Device Hot List:

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

Device Hot List					
⊠	⊗	◇	Type	Item	
3	45	22	🖥	blr-nrm-r6a	
2	28	27	🖥	blr-nrm-r9a	
2	25	23	🖥	blr-nrm-r5v2	
2	0	0	🗄	blr-nrm-r3f	
1	52	1	🖥	blr-nrm-r11d	
◄ ► 1 - 5 of 15					show 5 ▼ items

* ⊠ This column indicates the number of bundles or policies that could not be applied to the device because an error occurred. You must review the error and warning messages to discover the compliance problem. The noncompliant status applies only to ZENworks Configuration Management. ZENworks Asset Management does not use this status.

◆ ❌ This column indicates the number or unacknowledged error messages generated for the device. An error is any action that fails so the ZENworks Adaptive Agent cannot complete the action on the device.

◆ 🔶 This column indicates the number of unacknowledged warning messages generated for the device. A warning is any action that encounters a problem; the problem might or might not result in the ZENworks Adaptive Agent completing the action on the device.

2 Click the device to display its message log.

27.3 Viewing the Messages

In the ZENworks Control Center, you can view the logged messages as follows:

◆ Section 27.3.1, "Message Log," on page 249
◆ Section 27.3.2, "System Message Log," on page 250

27.3.1 Message Log

The Message Log displays all unacknowledged messages generated for the object.

To view the message logs:

1 In ZENworks Control Center, click the *Device Hot List* on the home page, then click the device to view its message log.

You can also use the *Devices* menu to view the logs:

1 In ZENworks Control Center, click *Devices*.

2 Click *Servers* or *Workstations* to display the list of managed devices.

3 Click the name of a device, then click the *Summary* tab to display:

Status: Displays an icon indicating the type of message:

❌ Critical Message
🔶 Warning
🟢 Normal

Message: Displays a brief description of the event that occurred.

Date: Displays the date and time the event occurred.

4 To view the log messages in the advanced view, click *Advanced* on the right corner of the Memory Log panel.

You can acknowledge or delete messages from the message log. For more information on acknowledging messages, see Section 27.4, "Acknowledging Messages," on page 250, and for information on deleting messages, see Section 27.5, "Deleting Messages," on page 252.

27.3.2 System Message Log

The System Message Log panel displays the unacknowledged messages generated by the ZENworks Servers and managed devices in the Management Zone.

1 In ZENworks Control Center, click *Configuration*.

2 Click *System Information* to display the System Message Log.

System Message Log			Advanced
Status	Message	Date	Source
🟢	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess/http://164.9	10:24 AM	🖥 blr-nrm-r5v2
🟢	POLICYHANDLERS.PrinterPolicy.LocalPrinterAddSuccess(printerlocal)	10:23 AM	🖥 blr-nrm-r5v2
🟢	Printer \\164.99.154.214\share already exists for user , hence n	10:23 AM	🖥 blr-nrm-r5v2
🔶	The action printer policy (ID:printer policy) failed, but the ac	10:23 AM	🖥 blr-nrm-r5v2
🟢	iPrint client is already installed in the device, not reinstall	10:23 AM	🖥 blr-nrm-r5v2
◀ ▶	1 - 5 of 820		show 5 ▾ items

Status: Displays an icon indicating the type of message:

❌ Critical Message

🔶 Warning

🟢 Normal

Message: Displays a brief description of the event that occurred.

Date: Displays the date and time the event occurred.

3 To view the log messages in the advanced view, click *Advanced* on the right corner of the System Memory Log panel.

You can acknowledge or delete messages from the system message log. For more information on acknowledging messages, see Section 27.4, "Acknowledging Messages," on page 250, for information on deleting messages, see Section 27.5, "Deleting Messages," on page 252.
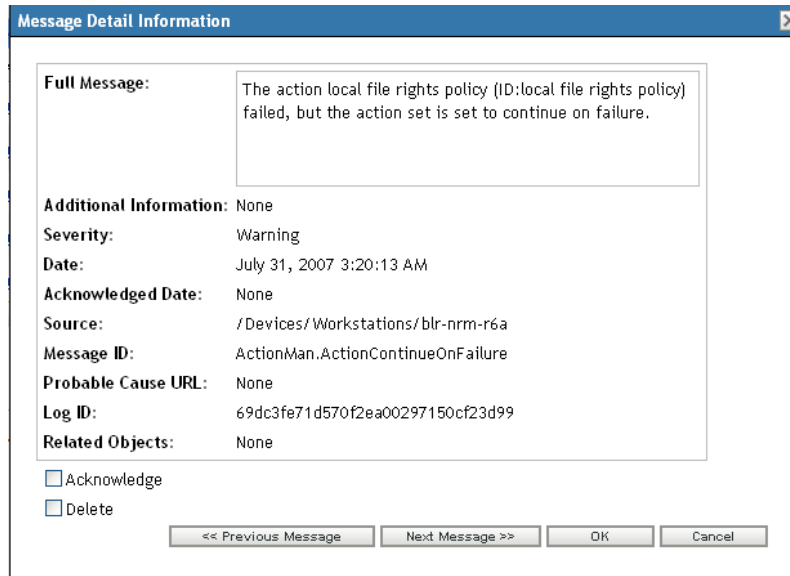
27.4 Acknowledging Messages

An acknowledged message is one that you have reviewed and marked as acknowledged (✔).

27.4.1 Acknowledging a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to acknowledge.

2 In the Message Detail Information dialog box, select the *Acknowledge* option, then click *OK*:

The acknowledged messages are removed from the Message Log panel or the System Message Log panel, depending on which panel you selected in Step 1.

The acknowledged messages continue to be listed in the Advanced view of these logs, marked with a check mark (✔).

27.4.2 Acknowledging Multiple Messages

1 In the Message Log panel or the System Message Log panel, click *Advanced* on the right corner of the panel.

2 Select the messages to acknowledge, then click *Acknowledge*:

The acknowledged messages are marked with a check mark (✔).

27.4.3 Acknowledging Messages Logged During a Specified Time

1 In ZENworks Control Center, click *Configuration*.

2 In the *Configuration Tasks*, click *Message Cleanup* to display:
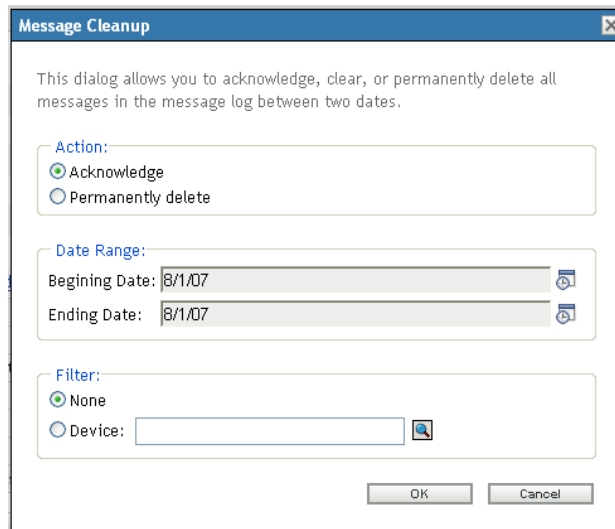
3 In the Message Cleanup dialog box, select *Acknowledge*.

4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.

5 Select the *Filter* option:

None: Cleans up the messages in selected date range from all the devices.

Device: Cleans up the messages in selected date range from the selected device.

6 Click *OK*.

A message cleanup action is initiated and a system message is logged after the cleanup action is completed. For more information on viewing system logs, see Section 27.3.2, "System Message Log," on page 250.

27.5 Deleting Messages

Deleting a message completely removes the message from your ZENworks system.

- Section 27.5.1, "Deleting a Message," on page 252
- Section 27.5.2, "Deleting Multiple Messages," on page 253
- Section 27.5.3, "Deleting Messages Logged During a Specified Time," on page 253

27.5.1 Deleting a Message

1 In the Message Log panel or the System Message Log panel, click the message you want to delete.

2 In the Message Detail Information dialog box, select the *Delete* option, then click *OK*:

27.5.2 Deleting Multiple Messages

1 In the Message Log panel or the System Message Log panel, click *Advanced* on the right corner of the panel.

2 Select the messages to delete, then click *Delete*.

27.5.3 Deleting Messages Logged During a Specified Time

1 In ZENworks Control Center, click *Configuration*.

2 In the *Configuration Tasks*, click *Message Cleanup*.
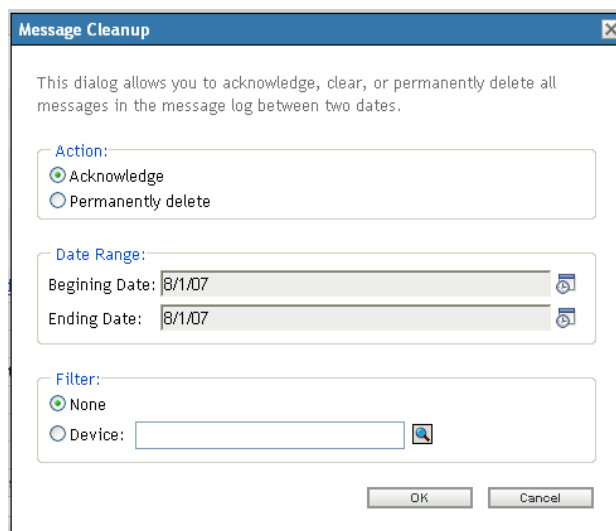
3 In the Message Cleanup dialog box, select *Permanently Delete*.

4 In the *Date Range* option, select the *Beginning Date* and the *Ending Date*.

5 Select the *Filter* option:

None: Cleans up the messages in selected date range from all the devices.

Device: Cleans up the messages in selected date range from the selected device.

6 Click *OK*.

7 In the Confirm Delete Dialog box, click *OK* to delete the message.

A system message is logged after the cleanup action is completed. For more information on viewing the system log see, Section 27.3.2, "System Message Log," on page 250.

27.6 Viewing the Predefined Reports

You must have installed ZENworks Reporting Server to view the predefined reports. For more information on how to install ZENworks Reporting Server, see the *ZENworks 10 Asset Management Reporting Server Installation Guide*.

To view the predefined reports for messages:

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

2 In the ZENworks Reporting Server Reporting panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView.

3 Navigate to the *Novell ZENworks Reports* folder > *Predefined Reports* > *ZENworks System* folder.

4 The following predefined report is included for Messages:

ZENworks Messages: Displays message details such as the log time and description for all the ZENworks System messages.

For more information on creating and managing reports, see the *ZENworks 10 Asset Management System Reporting Reference* documentation.

Naming Conventions in ZENworks Control Center

A

When you name an object in the ZENworks® Control Center (folders, groups, registration keys, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.

- Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks 10 Asset Management is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.

- If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose reg key 1 in quotes ("reg key 1") when entering it in the zman utility.

- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

Schedule Types

B

The following schedules are available:

B.1 Date Specific

The Date Specific scheduling option lets you specify one or more dates on which to run the event.

Figure B-1   *Date Specific Schedule*

Start Dates: Click ▢ to display a calendar you can use to select a date for the event. You can add multiple dates one at a time.

Run Event Every Year: Select this option to run the event every year on the dates shown in the *Start Date(s)* list.

Select When Schedule Execution Should Start: Select one of the following options:

- **Start Immediately at Start Time:** Starts the event at the time you specify in the *Start Time* field.

- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the *Start Time* and *End Time* fields. You can use this option to avoid possible network overload from concurrently scheduled events.

Use Coordinated Universal Time (UTC): The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

B.2 Event

This scheduling option lets you specify the event you want to trigger the scheduled action.

Figure B-2 *Event Schedule*

Select from the following triggers:

User Login: A user logs in to the device's operating system.

User Logout: A user logs out of the device's operating system.

Device Boot: The device powers on.

Device Shutdown: The device powers off.

On Device Lock: The device's operating system is locked.

On Device Unlock: The device's operating system is unlocked.

ZENworks Login: A user logs in to the ZENworks® Management Zone.

ZENworks Logout: A user logs in out of the ZENworks Management Zone.

Device Connecting to Network (Windows Only): The disconnected device detects a new wired or wireless network connection.

NOTE: At device startup, the ZENworks® Adaptive Agent contacts a ZENworks Server according to the device's refresh schedule to refresh its bundle, policy, configuration, and registration information. If information changes, the Adaptive Agent must refresh its information before the

changes can show up on the device, even if one of the event triggers occur. By default, devices refresh randomly between 300 and 360 seconds after device startup with a full refresh every 12 hours.

For example, if you create a bundle and schedule it to launch when the device connects to the network, the device must be manually refreshed or refreshed according to schedule before the Adaptive Agent can upload or launch the bundle, even if the device connects to the network.

B.3 Now

Select this scheduling option to run the event immediately.

B.4 Recurring

The Recurring scheduling option lets you repeat the event at a specified interval.

NOTE: The following sections describe all of the Recurring schedule options. Depending on the event or action you are scheduling, some options might not be available.

Figure B-3 *Recurring Schedule*

When a Device Is Refreshed: This schedule causes the event to occur each time the ZENworks Adaptive Agent performs a refresh on the device. If you want to delay the event so that it does not happen immediately upon refresh, select the *Delay execution after refresh* option and specify the number of days, hours, or minutes you want to delay the event.

Days of the Week: This schedule lets you specify the days during the week that you want the event to run. The event is run on these same days each week.

Select *Days of the Week*, then fill in the following fields:

- ◆ **Sun... Sat:** Specifies the days of the week you want to run the event.
- ◆ **Start Time:** Specifies the time you want to run the event.
- ◆ **Process Immediately if Device Unable to Execute on Schedule:** The event is run immediately if, for some reason, the schedule you configured results in the event not being able to run.
- ◆ **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- ◆ **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the *Start Time* and *End Time* fields. You can use this option to avoid possible network overload from concurrently scheduled events.
- ◆ **Restrict Schedule Execution to the Following Date Range:** Limits running the event to the time period specified by the starting and ending dates.

Monthly: This schedule lets you specify one or more days during the month to run the event.

Select *Monthly*, then fill in the following fields:.

- ◆ **Day of the Month:** Specifies the day of the month to run the event. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the event is not run that month.
- ◆ **Last Day of the Month:** Runs the event on the last day of the month, regardless of its date (28, 30, or 31).
- ◆ *First Sunday*: Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click █ to add multiple days.
- ◆ **Start Time:** Specifies the time you want to run the event.
- ◆ **Process Immediately if Device Unable to Execute on Schedule:** The event is run immediately if, for some reason, the schedule you configured results in the event not being able to run.
- ◆ **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.

- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the starting and ending dates.

Fixed Interval: This schedule lets you specify an interval between days to run the event. For example, you can run the event every 14 days.

Select *Fixed Interval*, then fill in the following fields:.

- **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the event is run. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.

- **Start Date:** Specifies the initial start date for the interval.

- **Start Time:** Specifies the initial start time for the interval.

- **Process Immediately if Device Unable to Execute on Schedule:** The event is run immediately if, for some reason, the schedule you configured results in the event not being able to run.

- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the start date, end date, and end time.

Documentation Updates

C

This section contains information on documentation content changes that were made in this *System Administration Reference* after the initial release of Novell® ZENworks® 10 Configuration Management. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

C.1 August 17, 2009: Update for ZENworks 10 Configuration Management (10.2.1)

Location	Update
Section 8.4, "Backing Up Closest Server Rules," on page 97	Added entire section.
"Agent Features" on page 103	Added note about using ZENworks 10 Asset Management with ZENworks 7 Desktop Management installed in your environment.
"Agent Features" on page 103	Updated the section to add the effects of enabling, disabling, or uninstalling the Agent modules.
Section 11.4, "Tasks to Be Performed after Changing the DNS Name of a Primary Server," on page 116	Added Step 3.
Section 14.1, "Understanding Available Updates," on page 141	Added first three paragraphs in section.
Section 21.6, "Using ZENworks 10 Asset Management with ZENworks 7 Desktop Management," on page 192	Added entire section.

C.2 August 6, 2008: SP1 (10.1)

Updates were made to the following sections:

Location	Update
Section 2.4, "Managing Administrator Roles," on page 37	Added this section for the new Roles feature.
Chapter 7, "Server Hierarchy," on page 81	Updated this section with the new Satellite feature.
Section 20.2, "Credential Storage," on page 181 and Chapter 4, "Credential Vault," on page 57	Added these new sections for the new Credential Vault feature.
Section 20.4, "Troubleshooting User Authentication," on page 182	Added this section for troubleshooting user authentication.
Chapter 12, "Introduction to ZENworks System Updates," on page 121	This section was updated when the newer version of the System Updates feature was released with version 10.0.3.
Chapter 22, "Embedded Database Maintenance," on page 197Chapter 22, "Embedded Database Maintenance," on page 197	Added the following sections: ◆ Section 22.2, "Changing the Ports Used by the Embedded Sybase SQL Anywhere Database," on page 197 ◆ Section 22.5, "Moving the Data from an Embedded Sybase Database to an External Sybase Database," on page 205 ◆ Section 23.1, "Moving the Data from One External Sybase Database to another External Sybase Database," on page 219 ◆ Section 22.7, "Migrating the Data from an Embedded Sybase SQL Anywhere to an External Oracle Database," on page 209 ◆ Section 23.2, "Configuring the ZENworks Server to Point to the New MS SQL Database Containing Data Moved from Another MS SQL Database," on page 220
Chapter 10, "Backing Up and Restoring the ZENworks Server and Certificate Authority," on page 107	Added the following sections on backing up and restoring Certificate Authority: ◆ Section 10.3, "Backing Up the Certificate Authority," on page 109 ◆ Section 10.4, "Restoring the Certificate Authority," on page 109