Troubleshooting guide

Novell®
ZENworks® Linux Management

7.3 IR4

January 31, 2011

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 guide includes troubleshooting strategies that you can use and error messages that might be displayed for problems that could occur as you use Novell ZENworks 7.3 Linux Management in your production environment.

As administrators gain experience using Linux Management, some unusual or previously untested implementation scenarios and undocumented product limitations might surface. We will gather this feedback from Novell customers and add it to this guide as it becomes practical to do so.

The guide is intended for network administrators and is divided into the following sections:

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

For the latest documentation on installing or upgrading to ZENworks 7.3 Linux Management, see the *Novell ZENworks 7.3 Linux Management Installation Guide*.

For the latest documentation on configuring and managing ZENworks 7.3 Linux Management, see the *Novell ZENworks 7.3 Linux Management Administration Guide*.

Installation, Upgrade, and ZENworks Database

The following section provides solutions to problems you might encounter when installing the Novell ZENworks 7.3 Linux Management or when working with the ZENworks Database:

- Chapter 1, "Installation and Upgrade Troubleshooting Strategies," on page 13

Installation and Upgrade Troubleshooting Strategies

1

The following sections provide solutions to the problems you might encounter when installing or upgrading to Novell ZENworks Linux Management:

1.1 Troubleshooting the Installation

Install randomly fails when zlm-config fails to complete

      Source: ZENworks7.3 Linux Management, Installation of the ZENworks Agent.

      Action: Re-run `zlm-config`.

Zmd hangs randomly on the managed device

Source: ZENworks 7.3 Linux Management, Installation of the ZENworks Agent.

Explanation: The ZENworks Agent (`zmd`) hangs on the managed device and displays the message "zmd inactive" when the managed device is kept idle for more than a day.

Action: Restart `zmd` on the managed device.

Installation of signed packages using rug fails on SLES 9, NLD, and Red Hat platforms

Source: ZENworks 7.3 Linux Management, Installation

Explanation: If the zmd security- level preference is set to signature, the installation of a signed package using `rug` would fail with the following error: `Unable to verify package signature.`

Action: Do the following:

    1 Verify signature manually using the following rpm command:

```
 rpm --checksig -v package_name
```

    2 Change the security- level preference to checksum or none as shown below:

```
rug set security-level checksum
```

ZENworks Server installation on SLES 10 fails with the error, "Resolvable not found"

Source: ZENworks 7.3 Linux Management, ZENworks Server

Action: Do the following:

    1 Remove the `openldap2` package from the system by executing `rpm -e openldap2` command.

    2 Install the ZENworks Server. For detailed information on installing the ZENworks Server, see "Installation" in the *Novell ZENworks 7.3 Linux Management Installation Guide*.

How do I recover the password for the ZENworks Server?

Source: ZENworks 7.3 Linux Management, ZENworks Server

Action: Do the following:

    1 After successfully installing the ZENworks Server components, take a reliable backup of the following files:

- `/etc/opt/novell/zenworks/hibernate.cfg.xml`
- `/etc/opt/novell/zenworks/tomcat/base/server.xml`
- `/etc/opt/novell/zenworks/serversecret`

    2 Replace `/etc/opt/novell/zenworks/serversecret` with the `serversecret` file that you have backed up in Step 1.

3 In `/etc/opt/novell/zenworks/tomcat/base/server.xml`, change the value of `keystorePass` and `connectionPassword` to the values configured in backed up `serversecret` file.

4 In `/etc/opt/novell/zenworks/hibernate.cfg.xml`, change the value of `<property name="connection.password">` to the values configured in backed up `serversecret` file.

Executing the `rug ref` command on the PPC, IPF, and zSeries devices results in exceptions related to Inventory

Source: ZENworks 7.3 Linux Management; ZENworks Agent

Possible Cause: On the PPC, IPF, and zSeries devices, the `rug set hardware-inventory-enabled` preference is set to `True`.

Action: Do one of the following:

- Ignore the exceptions because Inventory is not supported for the PPC, IPF, and zSeries devices.

- To avoid the exceptions, set the `rug set hardware-inventory-enabled` preference is set to `False`.

ZENworks Linux Management installation hangs in an X session on a 32-bit SUSE Linux Enterprise 11

Source: ZENworks 7.3 Linux Management, Installation

Action 1: Download and install the gpg2 2.0.9-25.25.1or later package and the gpg2-lang 2.0.9-25.25.1or later package from Novell Update (https://nu.novell.com), then run the ZENworks 7.3 Linux Management installation.

Action 2: Install the ZENworks 7.3 Linux Management in one of the following ways:

- Log in to the device in the init 3 mode by using the following command, then run the ZENworks Linux Management installation:

  `/sbin/init 3`

- Remotely log in to the device by using either RSH or SSH and run the ZENworks Linux Management installation.

NOTE: This might close any applications that are open.

Unable to upgrade the default ZENworks Linux Management agent installed on SUSE Linux Enterprise Server 10 devices by using the upgrade bundles

Source: ZENworks 7.3 Linux Management; Installation

Explanation: The upgrade bundles do not contain the python-xml package to successfully upgrade the default ZENworks Linux Management agent.

Action: Manually add the python-xml package from the SUSE Linux Enterprise Server (SLES) 10 media to the upgrade bundle.

Upgrading from ZENworks 7.2 Linux Management with IR2 or later to ZENworks 7.3 Linux Management might fail on a SUSE Linux Enterprise Server 10 GM device

Source: ZENworks 7.3 Linux Management; Installation

Possible Cause: The Python version in the default ZENworks Linux Management installation is earlier than Python 2.4.2-18.7.

Action 1: Do the following:

1 Upgrade the appropriate Python package to version 2.4.2-18.7 by using the ZENworks 7.2 Linux Management with IR2 media or the SLES 10 SP1 media.

2 Install the nici package from the ZENworks 7.2 Linux Management with IR2 media.

3 Run the zlm-upgrade script again by using the ZENworks 7.3 Linux Management media.

Action 2: Before upgrading to ZENworks 7.3 Linux Management on a SLES 10 GM device, ensure that the Python package version that is installed is 2.4.2-18.7. If the Python package version is earlier, upgrade it to version 2.4.2-18.7 by using the ZENworks 7.2 Linux Management with IR2 media or the SLES 10 SP1 media.

During ZENworks Linux Management installation, the ndsd runlevel scripts from the eDirectory packages display warning messages

Source: ZENworks 7.3 Linux Management; Installation

Explanation: The `zmd-messages.log` file displays the warning messages if you are installing ZENworks Linux Management in debug mode (`--zlm-debug`), and the log-level setting for zmd is set to debug.

For example:

```
insserv: warning: script 'post_ndsd_stop' missing LSB tags
and overrides
insserv: Default-Start undefined, assuming default start
runlevel(s) for script `post_ndsd_stop
```

Action: Ignore the warning messages, and continue with the ZENworks Linux Management installation.

Unable to install the ZENworks 7.3 Linux Management with IR3 agent on ia64 and s390x devices that have a default installation of SLES 11 SP1

Source: ZENworks 7.3 Linux Management; Installation

Possible Cause: You cannot install the ZENworks 7.3 Linux Management with IR3 agent on ia64 and s390x devices that have a default installation of SLES 11 SP1 because the `novell-zenworks-gtk-sharp2` package requires the `libglade2` package, which is not a part of the default installation of SLES 11 SP1.

Action: Do the following on the ia64 and s390x devices on which you want to install the ZENworks 7.3 Linux Management with IR3 agent:

1 Install the `libglade2` package from the SLES 11 SP1 installation media.

2 Install the ZENworks 7.3 Linux Management with IR3 agent by running the `zlm-install` command.

The ZENworks Linux Management agent restores the old values of the deviceid and secret files on SLES 11 and SLED 11 managed devices even after deleting them

Source: ZENworks 7.3 Linux Management; Installation.

Explanation: If the SLES 11 or SLED 11 managed devices are registered to Novell Customer Center through YaST, the ZENworks Linux Management agent restores the old values of the `deviceid` and `secret` even after you delete them and restart the agent.

Action: See TID 7006537 on the Novell Support Web site (http://www.novell.com/support).

Unable to install SLES 9 patch bundles on a ZENworks Linux Management agent

Source: ZENworks 7.3 Linux Management; Installation.

Possible Cause: You might not be able to install patch bundles if the local YOU cache has obsolete SLES 9 patches.

Action: Do the following:

1 On the server, remirror the SLES 9 patches to the same folder that contains the old SLES 9 patches by using the `zlmmirror m -o -c conf.xml` command.

2 On the managed device, clear the YOU cached content present under `/var/lib/YaST2/you/mnt` directory by using rug command `rug you-clean-cache`.

3 Assign the bundle that you mirrored in Step 1 to the agent.

The SLES 9 patch bundles are installed on the agent.

ZENworks Control Center fails to load after successfully installing or upgrading the ZENworks 7.3 Linux Management Server or later on a 64-bit device

Source: ZENworks 7.3 Linux Management; Installation.

Explanation: The ZENworks Control Center Management Console does not load on the Web browser after you install the Primary Server or upgrade from the previous version. The Tomcat `/var/opt/novell/log/zenworks/tomcat/Catalina.start` log file displays the following exception:

```
LifecycleException:  Exception opening directory server
connection:  javax.naming.CommunicationException:
localhost:389 [Root exception is java.net.ConnectException:
Connection refused
```

The following error message is displayed when you execute any of the Novell eDirectory commands on a 64-bit ZENworks Linux Management Server.

```
Error when loading shared libraries
```

Possible Cause: On a 64-bit device, eDirectory 8.8.3 does not configure the 64-bit equivalent path to search for its shared libraries at run time. This shared path is configured incorrectly in the `/etc/ld.so.conf.d/novell-NDSbase.conf` file.

Action 1: Add a path for 64-bit libraries:

1 Edit the `/etc/ld.so.conf.d/novell-NDSbase.conf` file as follows:

- Replace `/opt/novell/eDirectory/lib` with `/opt/novell/eDirectory/lib64`.

- Replace `/opt/novell/eDirectory/lib/nds-modules` with `/opt/novell/eDirectory/lib64/nds-modules`.

- Append the `/opt/novell/lib` with the `/opt/novell/lib64` path to the file.

2 Run the `ldconfig` command.

3 Restart the eDirectory services by using the `/etc/init.d/ndsd restart` command.

Action 2: Before executing the eDirectory commands, execute the following command at the command prompt:

`. /opt/novell/eDirectory/bin/ndspath`

Unable to log in to ZENworks Control Center of the ZENworks Linux Management Server with the Primary or Secondary configuration because of no time synchronization

Source: ZENworks 7.3 Linux Management; Installation.

Explanation: You cannot log in to ZENworks Control Center because of no time synchronization between ZENworks Linux Management Servers (Primary or Secondary) with their eDirectory instances. Sometimes the objects in the eDirectory instances on the Primary or Secondary Server in the zone do not synchronize if they cannot communicate.

Action: To synchronize the time between ZENworks Linux Management Servers (Primary or Secondary) with their eDirectory instances:

1 Ensure that the Primary or Secondary Server device is configured to synchronize the time through the external NTP Server.

You can also update the Primary or Secondary Server time stamp by running the following command:

ntpdate - s <*NTP-server-host*>

2 Synchronize the time between the eDirectory instances on the ZENworks Linux Management Server by running the following command:

`. /opt/novell/eDirectory/bin/ndspath`

ndsrepair -T

3 Restart the ZENworks Linux Management services by running the following command:

zlm-config --restart

1.2 Troubleshooting the Upgrade Scripts

Execution of the Upgrade Script Fails on Managed Devices Other Than SLES 10 and SLED 10

Source: ZENworks7.3 Linux Management Upgrade.

Possible Cause: The Remote Execute policy is not implemented on the device. To verify that the policy has not been implemented, check that the `/var/opt/novell/zenworks/cache/zmd/policymanager/policies.xml` file does not have reference to the Remote Execute policy.

Action: Do the following on the managed device:

1 Ensure that the zmd version is 7.1.100 by executing `rpm -qi novell-zenworks-zmd`.

2 Restart the ZMDservice by executing `/etc/init.d/novell-zmd restart`.

Execution of the Upgrade Script Fails on the SLES 10 or SLED 10 Managed Devices

Source: ZENworks 7.3 Linux Management, Upgrade.

Action: Do the following on the managed device:

1 Ensure that the zmd version is 7.1.100 by executing `rpm -zmd`.

2 Restart the ZMD service by executing `/etc/init.d/novell-zmd restart`.

Policy Handlers

II
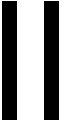
If the Policy Handlers component of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message, or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

- Chapter 2, "Policy Handlers Error Messages," on page 23
- Chapter 3, "Policy Handlers Troubleshooting Strategies," on page 31

Policy Handlers Error Messages

<div style="text-align: right; font-size: 3em;">2</div>

This section contains detailed explanations of the error messages you might encounter using the Novell ZENworks Linux Management Policy Handler component:

2.1 General Error Messages

The *policy_name* could not be enforced because it contains invalid keys

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: Some other application might have locked the settings that are defined in the policy they cannot be written to GConf.

Action: Ask the user to login again to the managed device.

The *policy_name* could not be enforced because few keys defined in the policy could not be cleared appropriately before enforcement

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: Some other application might have locked the settings that are defined in the policy. They could not be removed from GConf.

Action: Ask the user to log in again to the managed device.

The *policy_name* could not be enforced because the format of the policy data was invalid

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The policy details were corrupted while retrieving or applying it.

Action: Perform the following:

    1 To refresh the policy details, run the following command from the command line:

       `/opt/novell/zenworks/bin/rug refresh`

    2 If the policy is not enforced, stop zmd by running the following command from the command line:

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

    3 Remove the policy cache files from `/var/opt/novell/zenworks/ cache/zmd/PolicyManager/policies.xml`.

    4 Start zmd by running the following command from the command line:

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

    5 Ask the user to log in again to the managed device.

The *policy_name* could not be enforced because the user specified was invalid

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The user's login entry for device does not exist in the `/etc/passwd` file.

Action: Make sure that the user's entry exists in the `/etc/passwd` file.

Possible Cause: An internal error occurred while applying the policy.

Action: Perform the following:

1 Restart zmd by running the following command from the command line:

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

2 Ask the user to log in again to the managed device.

The *policy_name* could not be enforced because the username has not been specified in the policy

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: An internal error occurred while applying the policy.

Action: Perform the following:

1 Restart zmd by running the following command from the command line:

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

2 Ask the user to login again to the managed device.

The GConfEnforcer could not find any settings to read from the device

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The default schema files of GConf are corrupted or not valid.

Action: Ensure that the default schema files of GConf are valid.

Possible Cause: You might not have configured any specific GConf values for the user.

Action: Configure some values for the user.

For more information about configuring GConf values, refer "Understanding Policies" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

The GConfEnforcer could not read the requested settings from the device for the specified user

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The user's entry does not exist in the `/etc/passwd` file.

Action: Make sure that the user's entry exists in the `/etc/passwd` file.

The settings made by the *policy_name enforcers* could not be cleared completely. Settings made by policies of this type might still be in effect on the device

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: Some other application might have locked the settings that are defined in the policy, so cannot be removed from GConf.

Action: Perform the following:

1 Ask the user to log in again to the managed device.

2 Clear the policy enforcement again on the managed device.

The *policy_name* could not be enforced because there was an error in setting or unsetting the values into the configuration source

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The home directory of a user who has logged in to the managed device does not exist in the `/etc/passwd` file.

Action: Ensure that a valid home directory is specified for a user on the managed device in the `/etc/passwd`.

Possible Cause: Root has insufficient rights to access the home directory of a user on the managed device.

Action: Ensure that root has sufficient rights to access the home directory.

Possible Cause: Some other application might have locked the settings that are defined in the policy, so they cannot be written to GConf.

Action: Ask the user to log in again to the managed device.

The read settings operation could not be performed by the enforcer GConf Enforcer because there was an error in reading from the configuration source

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The home directory of a user whose settings are being retrieved from the managed device does not exist in the `/etc/passwd` file.

Action: Ensure that a valid home directory is specified for a user on the managed device in `/etc/passwd` file.

Possible Cause: The user does not have sufficient rights to access the directory from the ZENworks Management Daemon.

Action: Ensure that the user has sufficient rights to access the ZENworks Management Daemon.

Possible Cause: Some other application might have locked the settings that are defined in the policy, so they cannot be written to GConf.

Action: Retry importing the settings.

The enforcement of *policy_name* was unsuccessful and the application is not installed/compatible. The version of *name of the application* should be >= *minimum required version*

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The application (Firefox*, Epiphany*, or EvolutionTM) is not installed or the specified version is earlier than the minimum supported version.

Action: Upgrade the application to the minimum required version and try enforcing the policy again.

The enforcement of *name of the policy* was unsuccessful and the operating system distribution is not compatible. The distribution should be >= *distribution required version*. Only some keys might be enforced

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The distribution or version of the operating system is not compatible with the policy you are trying to enforce.

Action: Associate the policy to a device with the required distribution and version of the operating system.

The *policy_name* will not be enforced because the *name of the application* is not installed

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The policy might be associated to a device that does not have the application installed.

Action: Install the required application.

The *policy_name* will not be enforced because the operating system is not *required distribution version* or higher

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Critical

Possible Cause: The Novell Linux Desktop policy or the SUSE Linux Enterprise Desktop policy is associated to a device that does not have Novell Linux Desktop or SUSE Linux Enterprise Desktop operating system respectively.

Action: Associate the Novell Linux Desktop policy only to devices having Novell Linux Desktop operating system installed, and the SUSE Linux Enterprise Desktop policy only to the devices having the SUS Linux Enterprise Desktop operating system installed.

The *policy_name* was requested to be enforced, however, it is already executing, therefore, we will not start it again.

Source: ZENworks 7.3 Linux Management; Policy Handlers

Severity: Important

Explanation: If two or more users are logging into the device at the same time, the policy enforcement might not have finished for the first user before it started for the other user. The specified policy is not enforced for users other than the first user.

Possible Cause:	Two or more users have logged in to the device at the same time.
Action:	The users after the first user should login again for the policies to take effect.
Possible Cause:	One of the policies is taking a long time.
Action:	For Text File and Remote Execute policies, review any scripts/programs specified in the policy to see if they could take excessive time. Correct those situations to reduce the amount of time and try enforcing the policy again. For GConf-based policies, do not include any settings in the policy that are not relevant to you. If the policy data is correct, then restart ZMD and enforce the policy again.
Possible Cause:	The time interval for enforcing the policy is too small compared to the amount of time it takes to enforce the policy.
Action:	Increase the time interval.

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

  2 Click any Remote Execute or Text File policy for which you want to increase the time interval.

  3 On the *Summary* page, click *Relative to Refresh* in *Assignments* section.

  4 In the *Edit Schedule* dialog box, increase the time interval you have specified in *After Executing*, *Repeat Every* option.

Rescheduling the enforcement of *name of the policy* for 2 minutes later, because its type is not re-entrant and another policy of this type is already executing.

Source:	ZENworks 7.3 Linux Management; Policy Handlers
Severity:	Important
Possible Cause:	A read settings request was made to the managed device while a user was trying to login.
Action:	Ask the user to login again to the managed device.
Possible Cause:	There is an internal error.
Action:	Restart ZMD and ask the user to login again to the managed device.

The enforcer executable, *enforcer_name*, could not be located

Source:	ZENworks 7.3 Linux Management; Policy Handlers
Explanation:	The Policy Manger logs the error message in the ZENworks Control Center when you log into a managed device that does not have the GConf binaries installed.
Possible Cause:	The ZENworks Agent is installed with the -x option on the managed device that does not have GConf binaries installed.
Possible Cause:	The ZENworks Agent installation is corrupted.

Action: If the error message is displayed when a GConf based policy is assigned, do one of the following:

- To apply the GConf based policy, reinstall the ZENworks Agent without -x option.
- Remove the assignment between the policy and the device that does not have the Gconf binaries installed.

Action: If the error message is displayed when a GConf based policy is not assigned, ignore the message and acknowledge it in ZENworks Control Center.

2.2 Remote Execute Policy Error Messages

-

The *policy_name* was enforced and the program launched did not complete the execution

Explanation: This message indicates that the launched script or binary or Java* program didn't complete the execution when the enforcer returned, so the exit code returned by the launched program could not be reported in the message. This message does not mean that the launched program was terminated abnormally.

Possible Cause: While creating the policy, the *Maximum Time to Wait* setting was specified as *Do Not Wait* or *Wait For number of seconds Secs*.

Action: In the *Maximum Time to Wait* setting, select *Wait Till the Program Completes the Execution*.

Policy Handlers Troubleshooting Strategies

3

This section provides solutions to problems you might encounter when using Novell ZENworks Linux Management Policy Handler component.

- Section 3.1, "General Troubleshooting Strategies," on page 31
- Section 3.2, "Troubleshooting the Epiphany Policy," on page 34
- Section 3.3, "Troubleshooting the Generic GNOME Policy," on page 34
- Section 3.4, "Troubleshooting the Remote Execute Policy," on page 35
- Section 3.5, "Troubleshooting the Text File Policy," on page 37
- Section 3.6, "Troubleshooting SUSE Linux Enterprise Desktop Policy," on page 38

3.1 General Troubleshooting Strategies

- "The new policy is not enforced on the device after multiple refreshes" on page 31
- "The updated policy is not being enforced on the device after multiple refreshes" on page 33
- "A new policy is not enforced following an immediate manual refresh after policy assignment" on page 33
- "The assigned policies are enforced but applications do not reflect the specified behavior" on page 33
- "The policy is not displayed in the Effective Policies list" on page 34

The new policy is not enforced on the device after multiple refreshes

Source:	ZENworks 7.3 Linux Management; Policy Handlers
Possible Cause:	The policy does not display in the effective policies list of the device.
Action:	In the policy Summary page, assign the policy to the device by using Assignment section.
Possible Cause:	The minimum system requirements for the policy to be enforced on the device are not met.
Action:	Ensure that the minimum system requirement for the policy to be enforced on the managed device are met.
Possible Cause:	The policy enforcement schedule is not set.
Action:	For the Text File and Remote Execute policies, verify that the schedule to enforce a policy has been set.
Action:	For GNOME-based policies, verify that the User Login event has occurred by viewing the `/var/opt/novell/log/zenworks/zmd-messages.log` file.
Possible Cause:	For policies other than Remote Execute and Text File, there might be more than one policy of the same type associated with the device.

Action: Define all your settings only in one policy and associate it to the device.

Possible Cause: The policy was not refreshed on the device.

Action: Perform the following:

1 If you have recently assigned the policy to the managed device, wait for a few minutes to see if the policy is simply slow in being enforced.

2 If it is not enforced within a few minutes, on the ZENworks Control Center, go to the Devices page and select the device where you have assigned a policy.

3 In the Action menu, select Refresh Device.

4 On the managed device, open the file `/var/opt/novell/zenworks/cache/zmd/PolicyManager/Policies.xml`.

5 Search for the policy you have defined by using its name as the search string.

6 Refresh the device multiple times.

Possible Cause: You have not logged in through the user interface login on the device.

Explanation: If the policy is set to run on User Login, a user for whom the policy has not applied should log in by using the user interface on the device.

Action: Make sure that you log in through the user interface and verify the policy status again.

Possible Cause: The window manager is not GDM and KDM.

Action: By default, GConf-based policies support GDM, KDM, or XDM display managers. If you want your existing Display Manager to change to GDM, KDM, or XDM:

If you are using the Novell Linux Desktop or SUSE Linux and you want to change to GDM, KDM, or XDM:

1 Edit the `/etc/sysconfig/displaymanager` file as follows:

DISPLAYMANAGER=<<*GDM, KDM, or XDM*>>

For more details, refer to the GNOME Documentation (http://www.gnome.org/projects/gdm/docs.html)

2 Edit the `/usr/X11R6/bin/gnome` file and add the following to the beginning of the file:

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

If you are using Red Hat* and you want to change to GDM, KDM, or XDM:

1 Edit the `/etc/sysconfig/desktop` file as follows:

DISPLAYMANAGER=<<*GDM, KDM, or XDM*>>

2 Edit the `/etc/X11/xdm/Xsession` file and add the following to the beginning of the file:

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

NOTE: If you do not want to use the GDM, KDM, or XDM Display Manager, you must manually make changes in the configuration file. This delays the start of the desktop session and allows the enforcement of Gconf-based policies to be completed. To do this, you must create a file similar to `/usr/X11R6/bin/gnome` (on SuSE/NLD) or `/etc/X11/xdm/Xsession` (on Red Hat). These files must satisfy the following conditions:

- A user without the administrator privilege should not be able to edit the file.
- The file should be invoked every time a user logs in using the GUI

Add the following to the beginning of the file:

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

The updated policy is not being enforced on the device after multiple refreshes

Source: ZENworks 7.3 Linux Management; Policy Handlers

Possible Cause: The Revision number of the policy was not incremented.

Action: To increment the revision number:

1 In ZENworks Control Center, click *Policies*.
2 Click the policy for which you want to increment the revision number.
3 On the *Summary* page, increment the revision number and refresh the device.

To check the version of the policy available in the Cache:

1 Open the `/var/opt/novell/zenworks/cache/zmd/PolicyManager/Policies.xml` file.
2 Search for the policy name. The version should be listed in between <Version> </Version>.

A new policy is not enforced following an immediate manual refresh after policy assignment

Source: ZENworks 7.3 Linux Management; Policy Handlers

Possible Cause: The synchronization between a policy and the managed device might have been delayed.

Action: Wait for 5 minutes before manually refreshing after you update or assign a policy to the managed device.

The assigned policies are enforced but applications do not reflect the specified behavior

Source: ZENworks 7.3 Linux Management; Policy Handlers

Possible Cause: The desktop session has started before enforcement was complete.

Action: Log out and log in from the managed device where the policy has been enforced.

The policy is not displayed in the Effective Policies list

Source: ZENworks 7.3 Linux Management; Policy Handlers

Possible Cause: A schedule is not specified on the Policy Schedule page.

Action: Define a schedule:

1 In the ZENworks Control Center, click *Policies*.
2 Click the policy for which you want to define a schedule.
3 On the *Summary* page, click *Advanced* in the *Assignments* section.
4 In the *Edit Schedule* dialog box, specify an appropriate schedule, then click *OK*.

   The schedule is defined for the policy you have selected.

3.2 Troubleshooting the Epiphany Policy

Unable to find the downloaded file even after enforcing the Epiphany policy

Source: ZENworks 7.3 Linux Management; Policy Handlers

Possible Cause: You might have provided an incorrect path or you might not have the necessary rights to write to the directory.

Action: Perform the following:

1 Ensure that users have Read, Write, and Execute rights to the download directory.
2 If the absolute path is not specified in the download folder, specify only the directory name.

   A directory with this name is created in user's home directory and all downloaded files are saved in that directory.

3.3 Troubleshooting the Generic GNOME Policy

The Generic GNOME policy is not being enforced for some applications

Source: ZENworks 7.3 Linux Management; Policy Handlers; Generic GNOME Policy

Explanation: The Generic GNOME policy defines setting for many applications. Not all the applications reflect the settings that are defined in the policy.

Possible Cause: The applications that do not reflect the policy settings might not be working properly with GConf.

Action: To check if the problem is with the application and not with the ZENworks Linux Management, perform the following:

    1 Open the GConf Editor.

    2 Navigate to the settings that you have configured.

    3 Select the setting you have defined.

       If the GConf Editor displays that this value cannot be changed, the policy is enforced appropriately. The problem might be with the application. Refer to the application documentation to resolve the issue.

       If the GConf Editor displays that this value can be changed, see

Possible Cause: The application is started before the policy settings are enforced.

Action: Restart the application.

The warning is logged even if the distribution system requirements are met

Source: ZENworks 7.3 Linux Management; Policy Handlers; Generic GNOME Policy

Possible Cause: After the settings are imported from the managed device, the system requirements might have changed or removed before the policy was applied on the managed device.

Action: If the settings in the policy are not distribution dependent, ignore the warning.

If the policy is distribution dependent, add or modify system requirements on the Details page of the policy.

GNOME-based polices might not be enforced

Source: ZENworks 7.3 Linux Management; Policy Handlers; Generic GNOME Policy

Explanation: GNOME-based policies such as Epiphany*, Evolution*, Firefox*, Generic GNOME*, Novell Linux Desktop, and SUSE® Linux Enterprise Desktop might not be enforced.

Action: Log in as an administrator and remove all the hidden files (file names starts with '.') with .status.completed extension from the HOME directory of the user, for whom the policy enforcement is not working. The policy is enforced for the same user on subsequent logins.

3.4 Troubleshooting the Remote Execute Policy

An error occurs while executing a given script, binary, or Java program

Source: ZENworks 7.3 Linux Management; Policy Handlers; Remote Execute Policy

Possible Cause: The input parameters given in the policy are incorrect.

Action: If you have not defined your own script:

1 Combine the inputs for the following fields as one line in the policy:

```
InterpreterName InterpreterParameters ProgramName
ProgramParameters
```

2 On the managed device, execute the above statement from the command line.

3 If there is an error, give the correct parameters for InterpreterName, InterpreterParameters, ProgramName, and ProgramParameters.

If you have defined your Own Script, perform the following:

1 On the managed device, create a file containing the script you have specified in the policy.

2 Execute the script file from the command line.

3 If there is an error, give the correct parameters for InterpreterName, InterpreterParameters, ProgramName, and ProgramParameters.

4 Copy the correct script to the policy.

Possible Cause: In the Binary or Java executable type, shell or redirection operators are specified in the parameters.

Action: If you want to use shell or redirection operators with a Binary or Java executable, perform the following:

1 On the Remote Execute policy page, select Script as the Executable type.

2 In Script to Run field, select Define Your Own Script.

3 Combine the inputs for the following fields as one line in the policy:

```
InterpreterName InterpreterParameters ProgramName
ProgramParameters
```

Policy enforcement does not give the status of the launched program

Source: ZENworks 7.3 Linux Management; Policy Handlers; Remote Execute Policy

Possible Cause: The Maximum Waiting Time setting might not have the right value.

Action: On the Remote Execute policy page, in the Maximum Time to Wait field, select Wait Till the Program Completes the Execution.

Unable to install or enforce the available bundle or policy on the managed device according to the schedule when the ZENworks server is inactive

Source: ZENworks 7.3 Linux Management; Policy Handlers; Remote Execute Policy

Explanation: The assigned bundle or policy becomes available on the agent, gets installed at the configured scheduled time. However, during this period, if the ZMD goes to the normal sleep state because of its inactivity, or the ZENworks Linux Management services is down, then the bundle and policy capabilities or services cannot be processed from the inactive ZENworks Linux Management server on refreshing. The scheduled action data for the effective policy or bundle is not available with the agent to process the the required scheduled action.

Action: Ensure that all the ZENworks Linux Management services are active on the ZENworks server and are accessible from the agent.

3.5 Troubleshooting the Text File Policy

The Text File policy is not enforced

Source: ZENworks 7.3 Linux Management; Policy Handlers; Text File Policy

Possible Cause: Policy Enforcement might have failed.

Action: Ensure that the policy has been enforced correctly by checking the Event Log of the policy or of the managed device.

Possible Cause: The search string was not found in the file.

Action: Verify that the Additional Info field in a log message contains a list of changes that were not performed. Ensure that the search string specified in the changes which were not done is found in the file.

Possible Cause: The pre-change action that is specified in the policy failed and the Action When the Execution Fails field was set to Do Not Modify the Text File.

Action: Ensure that the pre-change action does not fail.

Unable to find the backup file after the Text File policy has modified the file

Source: ZENworks 7.3 Linux Management; Policy Handlers; Text File Policy

Possible Cause: There was an error while creating the backup of the modified file.

Action: Perform the following:

 1 Verify the value of the backup exit code in the message that is logged after policy was enforced.

 2 If the exit code is 1, it indicates that there was an error while taking the backup. Check the Additional Information field of the message to get more information on the error that is occurred.

Possible Cause: You might not be looking at the correct location of the backup.

Action: Perform the following:

 1 Verify the value of the backup exit code in the message that is logged after policy was enforced.

 2 If the exit code is 0, it indicates that the backup was taken successfully. Check to see if the backup file is in the same directory as the modified file.

Text File policy enforcement failed because of an error, but the file still appears modified or some unknown files appear in the same directory as the file

Source: ZENworks 7.3 Linux Management; Policy Handlers; Text File Policy

Possible Cause: When the text file enforcement failed, there was also an error while rolling back the changes in the files being modified.

Action: Perform the following:

1 Verify the value of the rollback exit code in the logged error message.

2 If the exit code is 1, it indicates that there was an error while rolling back the changes. Check the Additional Information field of the message to get more information the error that occurred during rollback.

Possible Cause: There might be another Text File policy that modifies the same file.

Action: Perform the following:

1 Verify the value of rollback exit code in the logged error message.

2 If the exit code is 0, it indicates that the rollback was done successfully. Check to see if there is another Text File policy that modifies the same file.

3 If the exit code is -1, it indicates that the rollback operation was not done because the file was not modified. Check to see if there is another Text File policy that modifies the same file.

How to ensure that the post-change action has been successful when the Text File policy was enforced

Source: ZENworks 7.3 Linux Management; Policy Handlers; Text File Policy

Action: Verify the value of the post-change action exit code in the message that was logged after policy was enforced. This value is the exit code, which was returned by the program or script launched in the post-change action.

3.6 Troubleshooting SUSE Linux Enterprise Desktop Policy

If you configure the SUSE Linux Enterprise Desktop policy for a SLED 10 or SLED 11 managed device, the Disable Launcher Creation option does not work

Source: ZENworks 7.3 Linux Management; Policy Handlers; SUSE Linux Enterprise Desktop Policy

Explanation: The *Disable Launcher Creation* option is not supported on SLED 10 or SLED 11 managed devices.

Event Monitoring

III
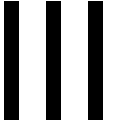
If the Event Monitoring component of Novell ZENworks Linux Management displays an error message or if specific instructions for an error message are not available, you can try the more general troubleshooting strategies to resolve the problem.

This section contains the following topic:

◆ Chapter 4, "Event Monitoring Troubleshooting Strategies," on page 41

Event Monitoring Troubleshooting Strategies 4

This section provides solutions to problems you might encounter when using Novell ZENworks Linux Management Event Monitoring component.

4.1 Troubleshooting Event Monitoring

-
-
-
-
-
-
-

Changing the severity level for a local log from the Centralized Message Logging setting in Novell Control Center is not taking effect

Severity:	ZENworks 7.3 Linux Management; Event Monitoring
Possible Cause:	The Debug and Above message severity set using the command line interface takes precedence over the severity defined using the Centralized Message Logging user interface.
Action:	Turn off the Debug and Above severity from command line interface using the following command:

```
set debug-level off
```

SMTP mail is not working for the GMail server

Severity:	ZENworks 7.3 Linux Management; Event Monitoring
Possible Cause:	The Event Monitoring component of ZENworks 7.3 Linux Management does not support SMTP on a Transport Layer Security (TLS) server.
Action:	For the GMail server, use only SMTP and Secure SMTP servers.

Unable to send e-mail to the specified e-mail address

Severity:	ZENworks 7.3 Linux Management; Event Monitoring
Possible Cause:	You might have defined filters or relays on the SMTP server.

Action: Clear the filters or relay that you have defined that block the SMTP packets from the ZENworks 7.3 Linux Management server.

Possible Cause: The authentication information you have provided in the E-mail Notification section of the Centralized Message Logging page is not correct.

Action: Ensure that the username and password you have specified are correct.

I am receiving unknown traps on the trap console

Severity: ZENworks 7.3 Linux Management; Event Monitoring

Possible Cause: The `messagelogger.mib` file is not compiled on the server.

Action: Compile the `messagelogger.mib` file located at `/opt/novell/zenworks/share/messagelogger`.

For example, if you want to compile messagelogger.mib on the Management and Monitoring Services console of ZENworks 7 Server Management, do the following:

1 Right-click the ConsoleOne Site Serve object, then click *Properties*.

2 In Properties of *name of the Site Server* dialog box, select the *MIB Pool* page.

3 Click *Modify Pool*.

4 In the *Add/Remove MIBs* dialog box, click *Add*, then select the MIB that needs to be compiled.

5 Click *Compile*.

Unable to send the traps to the trap console

Severity: ZENworks 7.3 Linux Management; Event Monitoring

Possible Cause: You might have defined filters on the trap console.

Action: Clear the filters you have defined that block the traps generated from ZENworks 7.3 Linux Management server.

Possible Cause: The port number you have specified is not correct.

Action: To specify the correct port number:

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

2 In *Management Zone Settings*, click *Centralized Message Logging*.

3 Specify the correct SNMP port number of the trap console in the *SNMP Trap* section.

The log-level setting for a managed device is set to the default value info whenever the managed device is refreshed

Source: ZENworks 7.3 Linux Management; Event Monitoring

Action: Do the following:

1 In ZENworks Control Center, click *Configuration*

2 In *Management Zone Settings*, click *Local Device Logging*.

3 Deselect the *Log message to a local file if severity is* check box.

4 Click *Apply*.

After upgrading to ZENworks 7.3 Linux Management with IR2, the Number of backup files per day option does not display the new default value on the Local Device Logging page

Source: ZENworks 7.3 Linux Management; Event Monitoring

Explanation: After upgrading to ZENworks 7.3 Linux Management with IR2 from an earlier version of ZENworks Linux Management, the *Number of backup files per day* field displays the value that you selected before upgrading to ZENworks 7.3 Linux Management with IR2.

Action: After upgrading to ZENworks 7.3 Linux Management with IR2:

    1 In ZENworks Control Center, click *Configuration > Local Device Logging*.

    2 Select the *Log message to a local file if severity is* check box.

    3 (Optional) Change the value of the *Number of backup files per day*.

Inventory

IV

If the Inventory component of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

Inventory Roll-Up Error Messages

5

This section contains detailed explanations of the error messages you might encounter using the Inventory Roll-Up component of Novell ZENworks Linux Management.

Incorrect input for the time interval between roll-ups

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Informational

Action: Specify a valid value in hours. If you do not specify a value, the Inventory Roll-up component takes the default time interval (168 hrs).

DNS name not found. Will exit now.

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Possible Cause: Unable to get the DNS name of the local machine.

Action: Ensure that the local machine has a valid DNS name.

The IP address of destination Inventory server has not been configured in the Inventory Roll-Up Configuration page

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Informational

Action: To enable the roll-up:

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

2 In the *Management Zone Settings* pane, click the *Device Inventory* category.

3 In the *Inventory Roll-Up Settings* pane, specify the IP address of the destination server.

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

The time interval between inventory roll-ups has not been set. By default, the time interval is set for 7 days.

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Informational

***filename* is deleted as it is older than RollupInitTime**

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Informational

Explanation: Based on the Discard Scan Data Time in the Inventory Service object properties of the Receiver, the Sender deletes the compressed .zip files in the entpushdir directory that have been created earlier than the specified discard scan data time.

Unable to get zeninvRollupTime from the destination inventory server

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Ensure that the ZENworks Web Server is running on the ZENworks Server Management or the ZENworks Desktop Management destination Inventory server.

Action: On the destination Inventory server, start the Receiver from the Service Manager.

Action: If the Sender fails to connect to the Receiver even after the retries, contact Novell Support (http://support.novell.com).

Action: Ensure that the network connection between the ZENworks Linux Management server and the ZENworks Desktop Management or ZENworks Server Management server is working.

Unable to initiate the file transfer

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Ensure that the ZENworks Web Server is running on the ZENworks Server Management or the ZENworks Desktop Management destination Inventory server.

Action: On the destination Inventory server, start the Receiver from the Service Manager.

Action: If the Sender fails to connect to the Receiver even after the retries, contact Novell Support (http://support.novell.com).

Action: Ensure that the network connection between the ZENworks Linux Management server and the ZENworks Desktop Management or ZENworks Server Management server is working.

Unable to rename the *filename*.str file

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Explanation: The str files in the entmerge directory cannot be transferred to entpushdir.

Action: Ensure that the entmerge directory exists.

Action: Ensure that you have rights to transfer the str files to the entpushdir directory.

Error while creating inner zip file

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Possible Cause: The disk on the Inventory server is full.

Action: Ensure that there is free disk space on the server.

Possible Cause: The directory containing the `.str` files does not exist.

Action: Ensure that the directory exists on the Inventory server.

Possible Cause: There is no Read and Write access to the files in the directory.

Action: Ensure that the directory has Read and Write access for the files in the directory.

Sanity check for prp file *filename* failed. The file may be corrupt

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

The name format of the *filename* str file is incorrect

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Could not get service DN from the prp file

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Unable to retrieve the server name from prp file

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Unable to procure/retrieve the schedule time from prp file

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Informational

Action: Contact Novell Support (http://support.novell.com).

Irrecoverable internal error: *error_message*. State machine crashed

Source: ZENworks Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Compression error while compressing and deleting str files

Source: ZENworks 7.3 Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

The conversion of Deviceinfo to STR format has failed

Source: ZENworks 7.3 Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Datamodel Exception occurred while extracting devices from the Inventory database

Source: ZENworks 7.3 Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

An exception occurred while writing to an STR file

Source: ZENworks 7.3 Linux Management; Inventory Roll-Up

Severity: Critical

Action: Contact Novell Support (http://support.novell.com).

Inventory Troubleshooting Strategies

6

This section provides solutions to problems you might encounter when using the Inventory Roll-Up component of Novell ZENworks Linux Management.

- Section 6.1, "Troubleshooting Inventory Roll-Up," on page 51
- Section 6.2, "Troubleshooting Hardware Inventory," on page 52

6.1 Troubleshooting Inventory Roll-Up

- "Inventory Roll-up fails to roll up the inventory data" on page 51

Inventory Roll-up fails to roll up the inventory data

Source:	ZENworks 7.3 Linux Management; Inventory Roll-Up
Possible Cause:	The IP address or the DNS name of the destination server is incorrect.
Action:	Ensure that the correct IP address or the DNS name of the destination server has been configured in the Inventory Roll-Up settings pane of the ZENworks Control Center.
Possible Cause:	The Receiver might not be running on the destination Inventory server of ZENworks Server Management or ZENworks Desktop Management.
Action:	On the destination Inventory server, start the Receiver from the Service Manager.
Action:	If the Sender fails to connect to the Receiver even after the retries, contact Novell Support (http://support.novell.com).
Possible Cause:	The ZENworks Web Server is not running on the ZENworks Server Management or the ZENworks Desktop Management destination Inventory server.
Action:	Ensure that the ZENworks Web Server is running on the ZENworks Server Management or the ZENworks Desktop Management destination Inventory server.
Possible Cause:	The network connection between the ZENworks Linux Management server and the ZENworks Desktop Management or ZENworks Server Management server is not working.
Action:	Ensure that the network connection between the ZENworks Linux Management server and the ZENworks Desktop Management or ZENworks Server Management server is working.
Possible Cause:	The ZENworks 7.3 Linux Management database is not running.
Action:	Ensure that the ZENworks 7.3 Linux Management database is up and running.

6.2 Troubleshooting Hardware Inventory

inventory-scanner-option can be set to an invalid value on the managed device

Source: ZENworks Linux Management; Inventory

Explanation: The `inventory-scanner-option` is passed to the hardware scanner 'hwinfo' to control the probing of certain hardware component.typically used for problematic or unsupported hardware. The default value is `-braille`.

This option does not uniformly controls probing of all hardware components under hwinfo.The `inventory-scanner-option` can be set to an invalid value.

The ZENworks Linux Management resets wireless network configuration on SLES 10 and SLED 10

Source: ZENworks Linux Management; Inventory

Explanation: The default setting for the `hwinfo zmd` preferences is set to `--nowpa` for SLES 10 and SLED 10.If this zmd preference value is not set to `--nowpa`, then the `hwinfo` command resets the wireless configuration settings on SLES 10 and SLED 10.

On SLES 9 and NLD, `hwinfo-option` is set to null by default and should be null always.

Action: `rug set hwinfo-options '--nowpa'`

Hardware Inventory of the registered devices is not updated successfully to the server

Source: ZENworks Linux Management; Inventory

Action: Do the following:

* Ensure that the Inventory module is loaded by executing the `rug ping` command. If the module is loaded, the `zmd-messages.log` file contains the following message:

```
INFO ModuleLoader Loaded 'Inventory' - 'Software and
Hardware inventory module for Linux'
```

◆ Execute the `hwinfo --all > hwinventory.log` command, and check
the log file to ensure that the Inventory Scanner runs successfully on the
managed device.

◆ Ensure that the `hardware-inventory-enabled` zmd setting is set to
`true`.

◆ Execute the `rug sch` command to verify the current Hardware Inventory
refresh schedule.

The Hardware inventory on the device is collected and updated based on
this schedule. If a new refresh schedule is not added, do the following:

1. Use `rug sl` to check if the managed device is successfully
   registered to the server, and is active.

2. Stop and start the ZENworks agent service, `/etc/init.d/novell-
   zmd`, and verify that the new schedule is now added.

◆ Ensure that the hardware inventory is collected and sent successfully
from the managed device.

◆ Set the following zmd options: `log-soap-xml` to `true` and `log-
level` to `debug` to procure the logged SOAP messages when
hardware inventory module service runs.

◆ Examine the debug log messages, `zmd-messages.log`, and search
for "HardwareInventoryCapability" as per timestamp. The following
messages are logged when delay schedule for hardware inventory is
triggered:

```
DEBUG HardwareInventoryCapability Starting to send
hardware inventory
```

```
(SOAP packets here)
```

```
DEBUG HardwareInventoryCapability Done sending
hardware inventory
```

This indicate that the hardware inventory of the managed device is
now updated to the ZENworks server.

Hardware inventory of the RHEL 4.x/5.x managed devices is not updated successfully to the server

Source: ZENworks Linux Management; Inventory

Possible Cause: The hardware inventory of RHEL 4.x / 5.x managed devices is not
successfully updated to the ZENworks Linux Management Server if the setting
for the `hwinfo` zmd preference is set to `--nowpa`. This is because the --nowpa
preference is not supported by the older version of the `hwinfo` package that is
installed as part of the managed device installation.

Action: Set the `hwinfo-options` to null by running the `rug set hwinfo-options
""` command.

How do I control the interval of hardware inventory update to the server?

Source: ZENworks Linux Management; Inventory

Action: Do the following:

- Change the `refresh-interval-hardware` zmd setting to the desired value in seconds.

  A new hardware inventory refresh schedule is created for the registered device.

- (Optional) Reset the `delay` zmd setting to send hardware inventory within new 'delay' interval.

  The random delayed schedule "Hardware Inventory delay" is added when the refresh schedule triggers to update the Hardware Inventory. The default 'delay' value is 900. All inventory delayed schedules are affected by changing the zmd setting 'delay'.

How do I control the probing of hardware information of specific component on managed device?

Source: ZENworks Linux Management; Inventory

Action: Change the `inventory-scanner-options` zmd setting to a particular hardware component. This option is passed to the hardware scanner, 'hwinfo --all', to control the probing of specific hardware components.

For example, hwprobe=inventory-scanner-options hwinfo --all.

For more information, see the hwinfo readme located in `/usr/share/doc/packages/hwinfo`.

How to control delayed schedules for updating inventory on the ZENworks Linux Management server?

Source: ZENworks Linux Management; Inventory

Action: The inventory delayed schedules for a registered device is affected when you change the zmd setting, delay. The default value is 900. The random delayed schedules to update inventory at the server are created using the delay setting. The new delay settings affect the next random delayed schedule only after the next refresh schedule.

All delayed schedules for inventory are added during the device registration and subsequently, when refresh schedules are triggered. The "Software Inventory delay" schedule is added to update inventory when packages are installed or removed on a client.

Disaster Recovery

V

If the Disaster Recovery component of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

Disaster Recovery

<div align="right">7</div>

This section explains how to restore a Novell ZENworks Linux Management system after the failure of a ZENworks Primary Server.

Restoration consists of the following:

1. Converting a ZENworks Secondary Server with an eDirectory read/write replica to a ZENworks Primary Server.

2. Moving all the devices that were managed by the old ZENworks Primary Server to the new ZENworks Primary Server. For more information, see "Registering Devices" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

The following sections provide additional information:

7.1 Safeguarding Your System through Backups

To restore your ZENworks Linux Management environment if the ZENworks Primary Server fails, you need backups of the Data Store, the Object Store, the package repository, and the zlmmirror configuration files.

7.1.1 The Data Store

ZENworks Linux Management supports both PostgreSQL and Oracle* databases as the ZENworks Data Store; both engines provide backup mechanisms that should be implemented. For information on backing up and restoring the Data Store, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

7.1.2 The Object Store

The ZENworks Object Store is Novell eDirectory 8.8.3. For information on backing up and restoring the ZENworks Object Store, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

7.1.3 The Package Repository

The package repository is the `/var/opt/novell/zenworks/pkg-repo` directory on the ZENworks Primary Server. You need to make a periodic backup of this directory. For more information on package management, see "Package and Content Management" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

7.1.4 The zlmmirror Configuration Files

If zlmmirror has been configured, you should back up the zlmmirror configuration files that the administrator has created. Because the names of the configuration files for zlmmirror and their locations are determined by the administrator, it is the administrator's responsibility to keep them backed up. For more information on zlmmirror, see "Mirroring Software" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

7.2 Safeguarding Your System through Server Configuration

When ZENworks Linux Management is installed, a Management Zone is created. The Zone is managed by a group of ZENworks servers; the first server is the ZENworks Primary Server and the others are ZENworks Secondary Servers. The Management Zone is highly dependent on the availability of the Data Store and the Object Store to function properly. Thus, it becomes important to understand how to configure your environment to provide fault tolerance and higher availability.

7.2.1 Data Store

The ZENworks Linux Management software provides an option to install the Data Store locally onto the ZENworks Primary Server. This option is generally sufficient in an environment where fault tolerance is not required. However, if the ZENworks Primary Server is lost, all of the data is lost unless there is a backup of the Data Store prior to the disaster. When the Primary Server fails, ZENworks Secondary Servers lose connectivity to the Data Store, which causes much of the data in the ZENworks Control Center to become unreadable. The ZENworks Linux Management system continues to function, but no data is recorded.

To provide fault tolerance, we recommend locating the Data Store on a machine that is remote from the ZENworks Primary and Secondary Servers. The ZENworks Linux Management software provides an option to install to a remote PostgreSQL or Oracle database. In this case, when the ZENworks Primary Server is lost, the Secondary Servers continue to have access to the Data Store.

7.2.2 Object Store

The ZENworks Object Store is Novell eDirectory . The ZENworks Primary Server holds a master replica of the Object Store and the next two consecutive ZENworks Secondary Servers installed in the Management Zone hold a read/write replica of the Object Store. The rest of the Secondary Servers do not hold a replica of the Object Store.

When the ZENworks Primary Server is disconnected, removed for maintenance, or otherwise lost, the ZENworks Secondary Servers with the read/write replicas act as a live backup of the ZENworks Object Store to the other ZENworks Secondary Servers that have no replica. By default, Secondary Servers with no replica go through the Primary Server to obtain Object Store information; as a temporary solution, eDirectory on those Secondary Servers might need to be restarted to provide functionality while the Primary Server is out. zlmmirror and content replication are functions of the Primary Server, so those services remain interrupted until the Primary Server is brought back up.

If the Primary Server is lost, the master replica of the Object Store is also lost. This situation is remedied by converting one of the two Secondary Servers with a read/write replica of the Object Store to a Primary Server, then by creating another read/write replica on another Secondary Server.

7.2.3 Package Repository

Creation of bundles or packages either manually or through zlmmirror or content replication are all functions that are performed through the ZENworks Primary Server.

When the ZENworks Primary Server is disconnected, removed for maintenance, or otherwise lost, bundles and packages cannot be created on the ZENworks Primary Server or replicated to ZENworks Secondary Servers. Existing assignment of replicated bundles and packages remains available to devices registered to ZENworks Secondary Servers. New assignments of replicated bundles and packages can also be made to those devices. However, new assignments of non-replicated bundles and packages, although they can be made, fail to distribute until the bundles and packages have been replicated to the ZENworks Secondary Server to which the device is registered.

If zlmmirror has been configured in the environment and content replication has taken place, the package repository on the ZENworks Primary Server is replicated onto all ZENworks Secondary Servers. Information about the new bundles and packages is also written to the Data Store. Therefore, when the ZENworks Primary Server is lost and a ZENworks Secondary Server is converted into a new ZENworks Primary Server, the bundles and packages from the zlmmirror operation would already be local to the new ZENworks Primary Server; all that is necessary is to re-create or restore the zlmmirror configuration files onto the new ZENworks Primary Server.

If zlmmirror has been configured in the environment but no content replication has taken place when the ZENworks Primary Server is lost, the zlmmirror operation causes new bundles and packages to be downloaded locally onto the ZENworks Primary Server and their information to be written into the Data Store. When a ZENworks Secondary Server is converted into a new ZENworks Primary Server, the package repository on the new Primary Server is out of sync with the Data Store. Because the package repository is out of sync with the Data Store, content replication and zlmmirror will fail. Unless you have a backup of these bundles and packages, their information must be removed from the database. This operation also causes any user-created packages to be lost.

7.2.4 Message Logger

The Message Logger continues to function normally regardless of which servers are down. But if the Data Store is local to the Primary Server and the Primary Server is down, no database logging occurs until a new Data Store is restored to the environment. Additionally, if the Data Store is down, the conversion does not function properly. For more information on the Message Logger, see "Message Logger" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

7.3 Disaster Recovery for a Single ZENworks Linux Management Primary Server

If you have only one primary server and no secondary server in your zone, do the following tasks in the order listed below:

7.3.1 Backup Requirements

The backups need to be obtained on a daily or weekly basis from your running ZENworks Linux Management Server. This backup information is collected from two different classes.

The first class contains some basic configuration information such as the hostname, ZENworks Linux Management zone name, configuration files, object store login information and so forth.

The second class contains information from the object store, data store, and package repository. Ensure that the backup information is recent and is collected within a short time frame to maintain consistency of data. For more information on configuring these backups, see Section 7.1, "Safeguarding Your System through Backups," on page 57.

NOTE: During the package repository backup, ensure that the links to the package files are restored.

A sample script for creating the backups is as follows:

```
# cat zlm-backup-all.sh
#!/bin/bash
BACKUPDIR='/images/backup'
DAT=`date +%Y%m%d`

mkdir -p ${BACKUPDIR}
cd ${BACKUPDIR}

# CLASS ONE DATA #

#Taking backup of deviceid and secret files

if [ -e /etc/opt/novell/zenworks/zmd/deviceid ];
then
  cp /etc/opt/novell/zenworks/zmd/deviceid ${BACKUPDIR}
  cp /etc/opt/novell/zenworks/zmd/secret ${BACKUPDIR}
else
  cp /etc/zmd/deviceid ${BACKUPDIR}
  cp /etc/zmd/secret ${BACKUPDIR}
fi

# some disk / mount information that the new system can be partitioned
#similarly
df  > disk-layout.log
df  > mount.log

#Taking backup of edirectory
cp /opt/novell/zenworks/datamodel/share/ldap-certs ${BACKUPDIR}
cp /etc/opt/novell/zenworks/zlm.conf ${BACKUPDIR}
cp -rp /var/opt/novell/nici .
cp -rp /var/nds/dib .
rm dib/dsbk.pipe
cp /etc/opt/novell/nici* .

#Taking backup of conf files
cp -rp /etc/opt/novell/zenworks .
cp -rp /etc/crontab .

# CLASS TWO DATA #
```

```
# Taking backup of data store
zlm_dbbackup.sh -H localhost -D ${BACKUPDIR}/zlm_dbbackup-${DAT}

# Taking backup of object store - you need to provide the ZLM Administrator
#password
zlm_ndsbackup.sh -U admin.system -D ${BACKUPDIR}/zlm_ndsbackup-${DAT} -B

# Taking backup of package repository
tar -cvzf bundles.tar.gz /var/opt/novell/zenworks/pkg-repo/bundles
tar -cvzf catalogs.tar.gz /var/opt/novell/zenworks/pkg-repo/catalogs
cp -Rp /var/opt/novell/zenworks/pkg-repo/files .
cp -Rp /var/opt/novell/zenworks/pkg-repo/packages .
```

7.3.2 Installating and Configuring a New ZENworks Linux Management Server

1 Install the new SLES server by using the SLES distribution, patch level, and architecture same as that were used before server failure.

2 Assign the server, the hostname, domain name, and IP address same as that were used earlier.

3 Install the same version of the Novell ZENworks Linux Management system by using the same Management zone name and hostname used by the old server. You can see this information in the `/etc/opt/novell/zenworks/zlm.conf` file.

  3a Run the configuration as a part of the installation, or run it manually later. Until the configuration is complete, ensure that the agents do not communicate with the new server by executing the `/etc/init.d/novell-zmd stop` command.

4 Restore the package repository in the `/var/opt/novell/zenworks/pkg-repo` directory and ensure that the ownership rights are with the zenworks users and the zenworks group.

  4a On restoring the package repository, verify if the `package` files in the `bundles` directory contains the correct path.

  4b To check for broken links, run the following command:

    ```
    find /var/opt/novell/zenworks/pkg-repo -type l | (while read FN ; do
    test -e "$FN" || ls -ld "$FN"; done)
    ```

    For more information on restoring packages, see "Package and Content Management" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

5 Restore the ZENworks Linux Management Object Store (eDirectory) backup by executing the following command with the administrator credentials:

    ```
    zlm_ndsrestore.sh -U admin.system -F <backup file with full path> -B
    ```

  5a Verify the log file `/var/opt/novell/logzenworks/ndsrestore.log` and ensure that there are no error messages and the restoring process is successful.

  5b Verify if the eDirectory Security Objects (Certificate Authority and SSL certificates) are properly restored by executing the following commands:

    ```
    /etc/init.d/ndsd restart
    ```

    ```
    netstat -tanpu | grep 10636
    ```

The LISTEN line display in the output indicates that the Security Objects are properly restored and the eDirectory is active and listening on the secure LDAP port.

If the restoration is not successful and eDirectory is not active, see Section 7.3.3, "Restoring the eDirectory Security Objects," on page 62.

6 Restore the ZENworks Linux Management server configuration files you added as backups earlier by using the following commands:

```
cp {BACUP_PATH}/zenworks/serverid /etc/opt/novell/zenworks
```

```
cp {BACUP_PATH}/zenworks/serversecret /etc/opt/novell/zenworks
```

```
cp {BACUP_PATH}/deviceid /etc/zmd/
```

```
cp {BACUP_PATH}/secret /etc/zmd/
```

For SLES 9 and RHEL 5 devices, the restoration path of `the deviceid` and `secret` files is `/etc/opt/novell/zenworks/zmd`. Verify the log files to ensure that there are no error messages and the restoration of files is successful.

7 From the `server.xml` backup file that was used in the old server, copy the lines starting with the words `connectionName` and `connectionPassword` into your current `server.xml` file in the `/etc/opt/novell/zenworks/tomcat/base` directory.

8 Restore the database backup by using the current datastore (postgresql) password from the new server. You can obtain the current database password using the following command:

```
grep password /etc/opt/novell/zenworks/hibernate.cfg.xml
```

Restore the backup by using the following command:

```
zlm_dbrestore.sh -d zenworks -U zenadmin -F <BACKUP-FILE>
```

For information on backing up and restoring the Data Store, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

9 Restart the ZENworks Linux Management services by using the `zlm-config --restart` command and test the restored ZENworks Linux Management system.

Verify the log files to ensure that there are no errors.

10 Copy the ZENworks Linux Management mirror configuration files from the backup directory to the new ZENworks Linux Management server machine.

7.3.3 Restoring the eDirectory Security Objects

While restoring the eDirectory Security Objects, the Certificate Authority can fail to register properly and the SSL certificate of the LDAP server might not work. To verify this, run the `/etc/init.d/ndsd restart` command. The LISTEN line display ensures proper restoration of the Security Objects and proper functioning of your ZENworks Linux Management server.

Scenario1: Restoring the eDirectory Security Objects on a 64-bit device

1 Stop the eDirectory path by using the `/etc/init.d/ndsd stop` command.

2 Add a library path by using the `vi /etc/ld.so.conf.d/novell-NDSbase.conf` command.

3 Modify the file from:

```
/opt/novell/eDirectory/lib
```

```
/opt/novell/eDirectory/lib/nds-modules
```

to:

`/opt/novell/eDirectory/lib64`

`/opt/novell/eDirectory/lib64/nds-modules`

`/opt/novell/lib64`

4 Run the `ldconfig` command.

5 Restart the eDirectory by using the `/etc/init.d/ndsd start` command.

Scenario 2: Restoring eDirectory Security Objects by using LDAP

If you are not using a 64-bit device, use the following method to restore the eDirectory Security Objects when the `LISTEN` line does not display on running the `/etc/init.d/ndsd restart` command:

1 Run the following command:

```
 ldapconfig set 'Require TLS for Simple Binds with Password=no' -a
admin.system
```

2 Delete the eDirectory certificate authority by using the `ldap` delete command. Ensure that you insert the same ZENworks Linux Management zone name in the delete command that you used during the backup of the `zlm.conf` file.

```
 ldapdelete -H ldap://localhost:10389 -D cn=admin,o=system -W -Z -x
'cn=<ZLM management zone name> -TREE CA,cn=Security'
```

3 Re-create the certificate authority and all server certificates by executing the `ndsconfig upgrade` command using the administrator context as `admin.system` and the ZCC administrator password.

4 Migrate the eDirectory configuration file to the original location:

```
 mv /etc/opt/novell/eDirectory/conf/nds.conf /etc
```

Delete the line `/etc/opt/novell/eDirectory/conf/nds.conf` from the file `/etc/opt/novell/eDirectory/conf/.edir/instances.0`

5 Run the `/etc/init.d/ndsd restart` command and verify if the `LISTEN` line displays on the `ldap` port.

6 Run the following command to set the Password value to 'yes':

```
ldapconfig set 'Require TLS for Simple Binds with Password=yes' -a
admin.system
```

7 Capture the `keystorePass` public key of the eDirectory certificate authority by using the following command:

```
 cat /etc/opt/novell/zenworks/tomcat/base/server.xml | grep keystorePass
```

8 Run the `openssl s_client -connect localhost:10636 -showcerts -keyform DER` command. The certificates used by the new ZENworks Linux Manangement server are displayed.

9 Copy the second certificate in the displayed list into the `ca.b64` file.

NOTE: An example certificate, such as `1 s:/OU=Organizational CA/O=ZONE-TREE`, where `ZONE` is the Management zone name, starts from `--BEGIN CERTIFICATE--` to `--END CERTIFICATE--`

10 Create a new keystore and copy it to the appropriate location. This step needs to be done outside the backup directory. Provide the password obtained in Step 7 as the keystore password.

```
/opt/novell/eDirectory/lib64/nds-modules/embox/jre/bin/keytool -import -
file ca.b64 -alias 127.0.0.1 -keystore ldap-certs

cp ldap-certs /opt/novell/zenworks/datamodel/share/ldap-certs
```

7.4 Restoring Your System after a Primary Server Failure

7.4.1 Restoring a Primary Server for a Remote Data Store

This section is applicable only if the PostgreSQL or Oracle data store is hosted remotely. Before starting the process of converting a Secondary Server to a Primary Server, all the Secondary Servers that don't have a read/write replica of the ZENworks Object Store need to have eDirectory restarted. When it is restarted, eDirectory recognizes that the Primary Server is lost and no longer tries to communicate with it.

To restart eDirectory:

1 Type `/etc/init.d/ndsd restart` on each Secondary Server that doesn't have a read/write replica of eDirectory.

Converting a Secondary Server to a Primary Server

To convert a ZENworks Secondary Server to a ZENworks Primary Server:

1 Choose a Secondary Server with a read/write replica to be the new Primary Server and change the ZENworks Object Store replica on that server to be the master replica by typing `ndsrepair -P -Ad`.

2 On all the Secondary Servers, copy `var/opt/novell/zenworks/zfs/pds/security/csr/*.csr` to `var/opt/novell/zenworks/zfs/pds/security/*.cer`.

3 If required, restore the ZENworks Data Store (for instructions, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*).

4 From within the `/opt/novell/convertserver` directory, type `./convertserver` on the server that is being promoted to the Primary Server, then follow the prompts. You'll need the administrator password.

5 If you want to have all the devices that were using the old Primary Server, change the address of the old Primary Server name on the DNS server to that of the new Primary Server.

6 Restore or re-create any zlmmirror configuration files that existed previously.

7 Restore the package and bundle directories if they have been backed up.

8 If you haven't done so already, install ConsoleOne for Linux.

   8a Download the Linux version of ConsoleOne from the Novell Downloads Web site (http://download.novell.com/). You are prompted to enter your Novell account username and password. If you don't have a Novell account, use the "create new account" link.

8b Save the ConsoleOne compressed file to disk and uncompress it.

8c Run the `cl-install` installation script. Install all the snap-ins.

9 Use ConsoleOne to remove the old Primary Server object from the ZENworks Object Store.

9a Start ConsoleOne by running the ConsoleOne executable located under `/usr/ConsoleOne/bin`.

9b Authenticate to eDirectory by clicking the tree icon. You are prompted with a login credential dialog box. Log in to your server with the following information:

- Login name: admin
- Password: Password from the ZENworks Linux Management installation
- Tree: IP address of a Secondary Server that holds a read/write replica of the ZENworks Object Store
- Context: system

9b1 Under My World/NDS/.ZONENAME-TREE/system, select your old Primary Server object. Right-click and select Delete NDS object. Answer Yes.

10 After a Secondary Server has been promoted to be the Primary Server, a read/write replica of the ZENworks Data Store needs to be created on one of the other Secondary Servers. Use ConsoleOne to create a new read/write eDirectory partition on one of the Secondary Servers that has no replica.

10a In the left pane of ConsoleOne, expand NDS. The new zone name is appended with -TREE.

10b Click the new zone name. Click *View* from the menu, then click *Partition and Replica View*. The servers and their replica types are listed.

10c Select any server. Right-click it and select *Add Replica*.

10d Select a server using the browse button. Navigate to the system container, then click the server object that will be your new read/write replica. Click *OK*.

10e Click *OK* twice.

11 Run the `/opt/novell/zenworks/sbin/dbsync.sh` script to synchronize the database with eDirectory.

7.4.2 Restoring a Primary Server for a Local Data Store

This section is applicable only if the PostgreSQL ZENworks data store is hosted locally.

To recover a crashed ZENworks 7.3 Linux Management Primary Server, you must restore the PostgreSQL database to a Secondary Server and then promote the server to be a Primary Server. The Secondary Server must have a read/write eDirectory replica for the ZENworks Object Store.

You must ensure that the following prerequisites are met before you begin the restoration process:

- There must be at least one Secondary Server in the Primary Server's Management Zone.
- Make sure that all the contents of the ZENworks package repository of the Primary Server are replicated to all the Secondary Servers in the Management Zone.
- You must have a reliable backup of the `/var/lib/pgsql/data/pg_hba.conf` file from the Primary Server.

- You must have a recent backup of the zenworks database. For more information on backing up, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.
- You must have a recent backup of the ZENworks object store. For more information on backing up, see "ZENworks Object Store and Data Store Maintenance" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

Do the following on the ZENworks Primary Server before you begin the restoration process:

1 Stop all the ZENworks services by using the following command:

`zlm-config --stop`

2 Stop the PostgreSQL database by using the following command:

`/etc/init.d/postgresql stop`

3 Disconnect the device from the network.

Perform the following tasks in the order listed:

1. "Recovering the ZENworks Data Store" on page 66
2. "Re-configuring the ZENworks Object Store" on page 68
3. "Re-configuring Content Replication" on page 69

Recovering the ZENworks Data Store

Do the following on the Secondary Server to recover the Primary Server data store:

1 Choose a Secondary Server with a Read/Write replica to be promoted as the new Primary Server. The Secondary Server must contain the Read/Write replicas of the master replica located on the Primary Server.

2 Verify if the following RPM packages, which contain the PostgreSQL server and its client libraries, are installed on the Secondary Server. If the RPMs are not installed, you must install them.

- postgresql-server
- postgresql
- postgresql-jdbc
- postgresql-libs

3 Stop all the ZENworks services by using the following command:

`zlm-config --stop`

4 Start the PostgreSQL service by using the following command:

`/etc/init.d/postgresql start`

If this is the first time you are starting the PostgreSQL service, the PostgreSQL default configuration and database files are created.

5 In the PostgreSQL configuration file `/var/lib/pgsql/data/postgresql.conf`, edit or add the following parameters for the default PostgreSQL 8.0 database on a SLES 10 device. You need to optimize them based on the server load in your environment.

- max_connections = 500
- authentication_timeout = 1

- shared_buffers = 2048
- work_mem = 2048
- max_fsm_pages = 40000
- maintenance_work_mem = 16384
- listen_addresses = '*'
- timezone = GMT
- unix_socket_permissions = 0770

The PostgreSQL configuration settings such as sort_mem, vacuum_mem, and tcpip_socket in PostgreSQL 7.4 on SLES 9 devices have changed to work_mem, maintenance_work_mem, and listen_addresses in PostgresSQL 8.0 and above on SLES 10 devices. For SLES 9 servers with PostgreSQL 7.4, ensure to set the value of tcpip_socket to True.

6 Edit the `/etc/opt/novell/zenworks/hibernate.cfg.xml` file as follows. These modifications point the ZENworks services to the newly created local PostgreSQL database.

  6a Change the value of the database `connection.url` parameter to `jdbc:postgresql://127.0.0.1:5432/zenworks`

  6b Change the value of the database `connection.password` parameter to the content of the file `/etc/opt/novell/zenworks/serversecret.`

7 Restore the `pg_hba.conf` file that you backed up on the Primary Server to the following path on this Secondary Server:

`/var/lib/pgsql/data/pg_hba.conf`

This overwrites the default PostgreSQL client authentication configuration file.

After the restoration process is complete, the database is locally available.

8 From the `pg_hba.conf` file, remove the line containing the IP address of this Secondary Server.

9 Ensure that you retain the `pg_hba.conf` file rights. The owner must be the user `postgresql`, the group must be `postgresql`, and the rights scheme for the file must be `0600`.

10 Edit the `~/.pgpass` file to replace the IP address of the old Primary Server with `localhost` as follows:

`localhost:5432:zenworks:zenadmin:<serversecret>`

The value of `serversecret` must be the content of the file `/etc/opt/novell/zenworks/serversecret,` located on the promoted Secondary Server.

11 Restart the postgreSQL service by using the following command:

`/etc/init.d/postgresql restart`

12 Rename the database backup file created on the Primary Server without the time stamp.

For example, if the database backup filename is `11:59:08-zenworks-backup.tar.gz,` rename the file as `zenworks-backup.tar.gz.`

13 Copy the renamed database backup file to the `/tmp` directory.

14 From within the `/opt/novell/convertserver` directory, run the script `zlm_create_restore_pgdb` as follows:

`./zlm_create_restore_pgdb -F *Path_to_zenworks_dbbackup_file*`

This script creates the zenworks database schema on the Secondary Server. It also restores the database from the zenworks database backup file in verbose mode by default. If you are prompted for a password, use the value of `/etc/opt/novell/zenworks/serversecret` that is located on the Secondary Server.

15 If there are additional Secondary Servers connected to this zone, do the following on each of the Secondary Servers:

15a Edit the `/etc/opt/novell/zenworks/hibernate.cfg.xml` file as follows to direct all the Secondary Servers to the new Primary Server data store:

- Edit the database `connection.url` parameter value to `jdbc:postgresql://New_Primary_Server_IP_Address:5432/zenworks`

- Change the database `connection.password` parameter value to the content of the new Primary Server's file `/etc/opt/novell/zenworks/serversecret`

15b Edit the `~/.pgpass` file to point to the new Primary Server's IP address, and set the `connection password` to the value of the `/etc/opt/novell/zenworks/serversecret` file.

Re-configuring the ZENworks Object Store

The ZENworks Object Store is based on Novell's eDirectory. Before starting the process of converting a Secondary Server to a Primary Server, all the Secondary Servers that do not have a read/write replica of the ZENworks Object Store need to have eDirectory restarted.When it is restarted, eDirectory recognizes that the Primary Server is lost and no longer tries to communicate with it. To restart the eDirectory, run the `/etc/init.d/ndsd restart` command on each secondary server that doesn't have a read/write replica of eDirectory.

Do the following on the Secondary Server that you are promoting to a Primary Server:

1 Start the ndsd daemon on the Secondary Server by using the following command:

`/etc/init.d/ndsd start`

2 Do the following during the NDS Repair process to change the ZENworks Object Store's Read/Write replica state to Master replica state:

2a Run the `ndsrepair -P -Ad` command.

2b Enter a replica number based on the partition name.

For example, enter the replica number as 1 based on the partition name.

2c Enter the replica operation option value for the option *Designate this server as the new master replica*.

For example, the corresponding value of the option is 5.

IMPORTANT: Do not start the old Primary Server back up as it might corrupt the Object Store information and might also conflict with another master replica in the same zone.

3 Remove the old Primary Server from the eDirectory Replication schema:

3a Run the `ndsrepair -P -Ad` command.

3b Enter the replica number based on the partition name.

For example, enter the replica number as 1 based on the partition name.

3c Enter the replica operation option value for View Replica Ring.

For example, enter the value as 5.

3d Enter the number for the old Primary Server's server name.

3e Enter the server option value for Remove this server from replica ring.

For example, enter the value as 6.

4 Restart the zlm services on the promoted Secondary Server by using the following command:

```
zlm-config --restart
```

5 Ensure that the local postgreSQL database service is running by using the following command:

```
/etc/init.d/postgresql status
```

6 Execute the following commands to check the status of the server back-end modules, health and datastore respectively:

```
zlman ping
zlman si
zlman sh server_name
```

7 From within the `/opt/novell/convertserver` directory, run the `./convertserver` command on the Secondary Server, and provide the administrator password to continue.

The Secondary Server is promoted to a Primary Server and all the ZENworks services are automatically restarted.

8 Restart the ZENworks Linux Management services on all the Secondary Servers by using the following command:

```
zlm-config --restart
```

Re-configuring Content Replication

The content replication can be re-configured if no change has been made to the Primary Server's DNS Name or IP address is unchanged.

Do the following to configure the content replication between the new Primary Server and the remaining Secondary Servers:

1 Stop the ZENworks Server Management (TED) service on any additional Secondary Server by using the following command:

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

2 Delete the `.keystore` file from the `/var/opt/novell/zenworks/zfs/pds/security/private/` directory located on the other Secondary Servers.

3 From the new Primary Server, copy the `/var/opt/novell/zenworks/zfs/pds/security/csr/*.csr` files to the `/var/opt/novell/zenworks/zfs/pds/security/` on all other Secondary Servers.

4 Rename the `.csr` files to `.cer` on all the Secondary Servers.

5 In the `etc/opt/novell/zenworks/zfs-startup.xml` file, set the `<Value>` tag of the parameter `<Parameter Name="eDirectory Servers">` to the IP address of the new Primary Server.

6 Start the TED services by using the following command on all the Secondary Servers:

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

Disaster Recovery Error Messages

<div style="text-align: right; font-size: 3em;">8</div>

This section contains detailed explanations of the error messages you might encounter using the Novell ZENworks Linux Management's Disaster Recovery component:

- "Error Encountered, Cannot Proceed." on page 71
- "Could not authenticate to the eDirectory server. Please check your password." on page 71
- "The zlm_create_restore_pgdb script fails while restoring and creating the database on a Secondary Server being promoted to a Primary Server" on page 71

Error Encountered, Cannot Proceed.

Source:	ZENworks Linux Management; Disaster Recovery
Severity:	Critical
Possible Cause:	The zlm.conf file that is required to obtain the LDAP connection information does not exist in `/etc/opt/novell/zenworks`.
Action:	Ensure that the zlm.conf file exists in `/etc/opt/novell/zenworks`.
Possible Cause:	The `hibernate.cfg.xml` file that is required to obtain database connection and configuration information does not exist in `/etc/opt/novell/zenworks`.
Action:	Ensure that the `hibernate.cfg.xml` file exists in `/etc/opt/novell/zenworks`.
Possible Cause:	While copying the password from the `hibernate.cfg.xml` file, you entered an incorrect password to authenticate to the database.
Action:	Refer the password that is specified in the `hibernate.cfg.xml` file and ensure that you specify a correct password.

Could not authenticate to the eDirectory server. Please check your password.

Source:	ZENworks Linux Management; Disaster Recovery
Severity:	Informational
Possible Cause:	When you attempted to authenticate to eDirectory, you might have entered an incorrect password at the shell prompt.
Action:	Ensure that you have entered a correct password.

The zlm_create_restore_pgdb script fails while restoring and creating the database on a Secondary Server being promoted to a Primary Server

Source:	ZENworks Linux Management; Disaster Recovery
Action:	Use the following command to run the `/opt/novell/zenworks/sbin/zlm_dbrestore.sh` script on the Secondary Server that is being promoted to Primary Server. It uses the database backup file that was created on the old Primary Server:

```
zlm_dbrestore.sh -d zenworks -U zenadmin -H localhost -F
zenworks-backup.tar.gz
```

If you are prompted for a password, use the content of the `/etc/opt/novell/zenworks/serversecret` file or the content of the `/etc/opt/novell/zenworks/hibernate.cfg.xml` file.

Remote Management

VI

If the Remote Management component of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

Remote Management Error Messages

9

This section contains detailed explanations of the error messages you might encounter using the Novell ZENworks Linux Management Remote Management component:

- "Network error:could not connect to server:port number of the Remote Management service" on page 75
- "Unable to initiate a remote session because the Remote Management settings cannot be read on the Managed device. Contact your ZENworks administrator." on page 76
- "Unable to initiate a remote session because the authentication to the X server, which is running on the managed device, could not succeed. Contact your ZENworks administrator." on page 76
- "host post is not an RFB Server" on page 76
- "Unable to initiate a remote session because the Remote Management settings cannot be read on the Managed Device" on page 77

Network error:could not connect to server:*port number of the Remote Management service*

Source:	ZENworks Linux Management; Remote Management
Severity:	Informational
Possible Cause:	The network firewall of the managed device blocks the required port.
Action:	Configure the firewall on the managed device to allow incoming connections for the required port.

For example, to configure the firewall on Novell Linux Desktop:

1 In the *System* menu, click *Administrator Settings* to launch YaST.

2 In the YaST Control Center, click *Security and Users*.

3 In the right pane, click *Firewall*.

4 In *Firewall Configuration: Basic Settings*, select the *Internal Interfac*e according to your preference.

5 In *Firewall Configuration: Services*, click *Expert*.

6 In the *Edit Additional Services* dialog box, specify the Remote Management port numbers in *Additional TCP Services*, then click *OK*.

7 Click *Next*.

8 In *Firewall Configuration: Features*, click *Next*.

9 In *Firewall Configuration: Logging Options*, click *Next*.

10 In the *Save Settings and Activate Firewall* dialog box, click *Continue*.

Possible Cause:	The Remote Control service (or Remote Login service) might not be running on the specified port.

Action: Start the Remote Control service (or Remote Login service) on the managed device using the following command:

```
/etc/init.d/xinetd start
```

NOTE: This may start other services enabled under xinetd. Refer xinetd man pages for more details.

Possible Cause: The port number you have specified in the Remote Management dialog box is not correct.

Action: Specify the correct port number in the Remote Management dialog box.

Unable to initiate a remote session because the Remote Management settings cannot be read on the Managed device. Contact your ZENworks administrator.

Source: ZENworks Linux Management; Remote Management

Severity: Important

Possible Cause: Remote Management settings are not available on the managed device.

Action: Do the following:

1 In ZENworks Control Center, click *Devices*.

2 Click *Servers* or *Workstations*.

3 Select the device you want to refresh.

4 In *Action* menu, click *Refresh Device*.

Unable to initiate a remote session because the authentication to the X server, which is running on the managed device, could not succeed. Contact your ZENworks administrator.

Source: ZENworks Linux Management; Remote Management

Severity: Informational

Possible Cause: You might have changed the X Server configuration.

Action: Restart the Display Manager.

For example, you can restart the Display Manager as follows:

1 Switch to any one of the text consoles by pressing Ctrl + Alt + F1 in your graphical session.

2 Change the runlevel of the managed device to 3 by entering the following command at the shell prompt:

```
init 3
```

3 Change the runlevel back to 5 by entering the following command at the shell prompt:

```
init 5
```

host post is not an RFB Server

Source: ZENworks Linux Management; Remote Management

Severity: Important

Possible Cause: The Remote Control Service has failed to authenticate to the X server.

Action: Restart the Display Manager.

1 Switch to any one of the text consoles by pressing Ctrl + Alt + F1 in your graphical session.

2 Change the runlevel of the managed device to 3 by entering the following command at the shell prompt:

```
init 3
```

3 Change the runlevel back to 5 by entering the following command at the shell prompt:

```
init 5
```

Unable to initiate a remote session because the Remote Management settings cannot be read on the Managed Device

Source: ZENworks Linux Management; Remote Management

Possible Cause: On Linux, the http and https IP addresses are different in the system-wide proxy setting.

Action: Use the same proxy for both http and https.

Remote Management Troubleshooting Strategies

10

This section provides solutions to problems you might encounter when using the Novell ZENworks Linux Management Remote Management component:

- "Multiple Remote Login sessions to the same managed device fail" on page 79
- "The Remote Management session does not proceed if the managed device is displaying the GNOME logout dialog box" on page 79
- "The Remote Management Viewer window fails to refresh after multiple Remote Management sessions from the same browser session" on page 80
- "The Password dialog box loses focus during a Remote Management session" on page 80
- "Unable to continue with the Remote Control operation because the Remote Management Viewer freezes" on page 80
- "Authentication to the X Server fails" on page 80
- "Only a grey screen is displayed while performing a Remote Login session" on page 81
- "Unable to perform a Remote Login session to a RHEL 5 managed device from a ZENworks Linux Management Server" on page 82
- "Unable to perform Remote Login session to a SLES 11 or a SLED 11 managed device" on page 82
- "Unable to automatically reboot a managed device by pressing the Send Ctrl+Alt+Del button in the management console during a Remote Login session" on page 83

Multiple Remote Login sessions to the same managed device fail

Severity: ZENworks Linux Management; Remote Management

Possible Cause: The limitation on the maximum number of Remote Sessions configured for XDMCP causes this.

Action: Configure the XDMCP settings on the managed device to allow more multiple Remote Sessions to the agent.

For example, if you want to configure XDMCP on GDM display manager:

1 Run `gdmsetup` at the shell prompt.

2 In Login Screen Setup window, Click *XDMCP*.

3 Select the *Maximum Remote Sessions* option.

4 Configure XDMCP for the number of remote sessions you want to use simultaneously.

The Remote Management session does not proceed if the managed device is displaying the GNOME logout dialog box

Severity: ZENworks Linux Management; Remote Management

Possible Cause: The GNOME session manager freezes all other processes on the logout dialog box by controlling the X Server.

Action: Start the Remote Management session after the user performs an operation in the dialog box on the managed device.

The Remote Management Viewer window fails to refresh after multiple Remote Management sessions from the same browser session

Severity: ZENworks Linux Management; Remote Management

Action: Clear the browser cache.

To clear the browser cache in the Firefox Web browser:

1 In *Tools* menu of the Firefox browser, select *Options*.

2 In the right pane, click *Privacy*.

3 For Cache, click *Clear*.

4 Restart the browser.

To clear the browser cache in the Internet Explorer Web browser:

1 In the *Tools* menu of the Internet Explorer browser, select *Internet Options*.

2 In the *General* page, click *Delete Files* in the *Temporary Internet Files* section.

3 Restart the browser.

The Password dialog box loses focus during a Remote Management session

Severity: ZENworks Linux Management; Remote Management

Explanation: If you launch the ZENworks Control Center using Firefox and establish a Remote Management session, sometimes the focus is not on the password dialog box.

Possible Cause: Incompatibilities between the Java 1.4.x Focus Management and Remote Management Viewer causes the loss of focus of password dialog box.

Action: Click the title bar of the Remote Management Viewer window.

Unable to continue with the Remote Control operation because the Remote Management Viewer freezes

Severity: ZENworks Linux Management; Remote Management

Possible Cause: The current encoding that you have selected might not be able to handle numerous screen updates.

Action: In Remote Management Viewer window, select Hextile encoding in the Options tab and retry.

Authentication to the X Server fails

Severity: ZENworks Linux Management; Remote Management

Explanation: A Remote Control session to a Managed Device fails with an error message "*host port* is not an RFB Server".

Possible Cause: The Remote Control Service has failed to authenticate to the X Server.

Action: Restart the Display Manager.

> **1** Switch to any one of the text console.
>
> **2** Change the runlevel of the managed device to 3 by entering the following command at the shell prompt:
>
> init 3
>
> **3** Change the runlevel back to 5 by entering the following command at the shell prompt:
>
> init 5

Only a grey screen is displayed while performing a Remote Login session

Severity: ZENworks Linux Management; Remote Management

Explanation: If you select the Remote Login operation in the Remote Management dialog box, the launched session shows only a grey screen with an X cursor.

Possible Cause: XDMCP was not enabled on the managed device.

Action: On devices other than SUSE Linux Enterprise Server (SLES) 11 and SUSE Linux Enterprise Desktop (SLED) 11, manually enable XDMCP. You must have installed the gdm package on the device to enable XDMCP.

> **1** Run gdmsetup at the shell prompt.
>
> **2** In the Login Screen Setup window, Click *XDMCP*.
>
> **3** Select the *Enable XDMCP* check box.
>
> **4** Run /opt/novell/zenworks/bin/novell-rm-fixrl.sh with the required options.

On SLES 11 and SLED 11, run /usr/bin/novell-rm-fixrl.sh with the required options.

If you use the -restartdm option, make sure that all applications are closed, then run the script from the text console.

Example 1: If you use the GDM display manager with the configuration file that is located at /etc/opt/gnome/gdm/gdm.conf on devices other than SLES 11 and SLED 11, you can enable XDMCP by using the following command:

#/opt/novell/zenworks/bin/novell-rm-fixrl.sh -dm gdm -cf /
etc/opt/gnome/gdm/gdm.conf enable

Example 2: If you use the GDM display manager with the configuration file that is located at /etc/dbus-1/system.d/gdm.conf on SLES 11 or SLED 11, you can enable XDMCP by using the following command:

#/usr/bin/novell-rm-fixrl.sh -dm gdm -cf /etc/dbus-1/
system.d/gdm.conf enable

After enabling XDMCP by executing remote login script, the device should start with the gdm as its current display manager.

Unable to perform a Remote Login session to a RHEL 5 managed device from a ZENworks Linux Management Server

Severity: ZENworks Linux Management; Remote Management

Action: Do the following at the shell prompt of the RHEL 5 managed device:

1 Create a `fonts` directory by using the following command:

```
mkdir -p /usr/X11R6/lib/X11/fonts
```

2 Link the `/usr/share/X11/fonts` file to `/usr/X11R6/lib/X11/fonts` file by using the following command:

```
ln -s /usr/share/X11/fonts /usr/X11R6/lib/X11/fonts
```

3 Run `gdmsetup.`

4 In the GDM Setup window, do the following:

  4a Click *Remote*.

  4b Select the *Same as Local* option from the pop-up menu.

  4c Click *Security*.

  4d Select the *Allow Remote System Administrator Login* option.

5 Close the GDM Setup window.

6 Reboot the managed device.

Unable to perform Remote Login session to a SLES 11 or a SLED 11 managed device

Source: ZENworks Linux Management; Remote Management.

Action: Do the following at the shell prompt of the SLES 11 or SLED 11 managed device:

1 Create an `X11` directory by using the following command:

```
mkdir -p /usr/X11R6/lib/X11
```

2 Link the `/usr/share/fonts` file to `/usr/X11R6/lib/X11/fonts` file by using the following command:

```
ln -s /usr/share/fonts /usr/X11R6/lib/X11/fonts
```

3 Enable XDMCP by using the following command:

```
/usr/bin/novell-rm-fixrl.sh -dm gdm -cf /etc/dbus-1/
system.d/gdm.conf enable
```

4 Run the following commands in the order listed to set the value of `DISPLAYMANAGER_REMOTE_ACCESS` to `yes` in the `/etc/sysconfig/displaymanager` file :

- ◆ `sed "s/^DISPLAYMANAGER_REMOTE_ACCESS=\"no\"/DISPLAYMANAGER_REMOTE_ACCESS=\"yes\"/" < /etc/sysconfig/displaymanager > /tmp/dm`

- ◆ `mv /tmp/dm  /etc/sysconfig/displaymanager`

5 Restart the Display Manager by using the `/etc/init.d/xdm restart` command. By default, the Display Manager is GDM.

These steps can be automated on SUSE Linux Enterprise 11 managed devices by using the Remote Execute Policy.

Unable to automatically reboot a managed device by pressing the Send Ctrl+Alt+Del button in the management console during a Remote Login session

Source: ZENworks Linux Management; Remote Management.

Action: None.

Dell DTK

VII

If the Dell OpenManage Deployment Toolkit (DTK) component of Novell ZENworks Linux Management displays an error message, or if specific instructions for an error message are not available, you can try the more general troubleshooting strategies to resolve the problem.

◆ Chapter 11, "Dell Configuration Bundle Troubleshooting Strategies," on page 87

Dell Configuration Bundle Troubleshooting Strategies

<div style="text-align: right; font-size: 3em;">11</div>

The following procedure provides a scenario for troubleshooting a Dell Configuration Preboot bundle:

1 Create or modify a Dell Configuration bundle.

For steps to do this, see "Creating Dell Configuration Bundles" in the *Novell ZENworks 7.3 Linux Management Administration Guide*.

2 Do one of the following:

- Assign the bundle to a managed device (see "Creating Dell Configuration Bundles" in the *Novell ZENworks 7.3 Linux Management Administration Guide*).

- Create a Preboot Work Assignment rule for an unmanaged device (see "Creating Dell Configuration Bundles" in the *Novell ZENworks 7.3 Linux Management Administration Guide*).

3 In the TFTP directory, locate the `.../dell-dtk/dell-dtk.s` file and open it in an editor.

4 Modify this file by adding a # character at the beginning of each of the last two lines to comment them out:

```
./dtask
reboot
```

5 Save the edited file.

6 Allow the device to boot through PXE.

The device should be assigned work and boot into the DTK environment, but the assigned work will not be executed, because the `./dtask` and `reboot` lines in the `dell-dtk.s` file were disabled.

7 After the device has booted to the Dell DTK in maintenance mode, press Alt-F2 to obtain a usable console.

8 Check the following items to determine if the Dell Configuration bundle worked correctly:

- A directory named `/tmp/dell-dtk` should have been created.

  A script named `dell-dtk-maint.s` that is downloaded from `/srv/tftp/dell-dtk` creates the `/tmp/dell-dtk` directory.

- A utility named `dtktask` should have been placed in the `/tmp/dell-dtk` directory.

- To determine whether various environment variables have been set appropriately, enter the following commands to see if the TFTPIP and PROXYADDR variables display the IP address of your ZENworks Imaging server:

  ```
  echo $TFTPIP
  echo $PROXYADDR
  ```

9 If all of these items show no problems, change to the `/tmp/dell-dtk` directory.

10 Run the dtktask utility:

```
./dtktask -v
```

The verbose option (-v) is optional. It causes the information being sent to the `dtktask.log` file to be displayed on screen.

11 To further determine any problems, examine the following log file:

`/var/log/dtktask.log`

If the log file doesn't resolve the problem, determine what action to take from the information in the log file.

To troubleshoot, you could manually download the files, run the utilities, and look for error messages on screen.

12 After each trial run, reboot the device or reassign the Preboot work so that your troubleshooting starts at a known state, then repeat these steps to troubleshoot a different Dell Configuration bundle.

Package and Content Management

VIII

If the Package and Content Management features of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message, or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

Package and Content Management Error Messages

This section contains detailed explanations of the error messages you might encounter using the Novell ZENworks Linux Management Package and Content Management features:

- "Error receiving message: Unknown response message from server, status: CancelSignal" on page 91
- "Error receiving message: Read failure" on page 91
- "Error receiving message: Cannot deploy this version because one or more packages have been deleted" on page 91
- "Error receiving message: More than one bundle exists with the name bundle_name. Use -g option to install the bundle by GUID" on page 92
- "Error receiving message: duplicate key value violates unique constraint "dup_devices_pkey" "" on page 92
- "Error receiving message: Invalid URI scheme. Supported : http, ftp and absolute path" on page 92

Error receiving message: Unknown response message from server, status: CancelSignal

Source: ZENworks 7.3 Linux Management; Package and Content Management

Action: Do the following:.

> **1** Increase the `memory-threshold` value in the `zmd.conf` file. The `zmd.conf` file is located in `/etc/zmd/` on SLES 10 and SLED 10 devices, and in `/etc/opt/novell/zenworks/zmd/` on other devices.
>
> **2** Restart the zmd.

Error receiving message: Read failure

Source: ZENworks 7.3 Linux Management; Package and Content Management

Action: Do the following:.

> **1** Increase the `memory-threshold` value in the `zmd.conf` file. The `zmd.conf` file is located in `/etc/zmd/` on SLES 10 and SLED 10 devices, and in `/etc/opt/novell/zenworks/zmd/` on other devices.
>
> **2** Restart the zmd.

Error receiving message: Cannot deploy this version because one or more packages have been deleted

Source: ZENworks 7.3 Linux Management; Package and Content Management

Explanation: The error message is displayed on the Secondary Server for all packages after content replication. But you can assign this bundle to all the managed devices that are registered to the Secondary Server.

Action:	Ignore the message.

Error receiving message: More than one bundle exists with the name *bundle_name*. Use -g option to install the bundle by GUID

Source:	ZENworks 7.3 Linux Management; Package and Content Management
Possible Cause:	There is more than one bundle with the same name in different folders in ZENworks Control Center, and you are trying to install one of them.
Action:	On the managed device, use the `rug bin -g GUID` command to install the required bundle.

Error receiving message: duplicate key value violates unique constraint "dup_devices_pkey" "

Source:	ZENworks 7.3 Linux Management; Package and Content Management
Explanation:	The `loadermessages.log` file displays the error message when you mirror the DUP bundle.
Action:	Ignore the message.

Error receiving message: Invalid URI scheme. Supported : http, ftp and absolute path

Source:	ZENworks 7.3 Linux Management; Package and Content Management
Explanation:	The error message is displayed when services with the NFS URL scheme are added to zmd on SLES 11 or SLED 11 by using the following command:

`rug sa -t zypp URL_of_the_NFS_server`

Action:	Do the following:

    1 Mount the NFS source to a local directory by using the following command:

       `mount URL_of_the_NFS_server path_to_the_local_directory`

    2 Add the local directory as a zypp service by using the following command:

       `rug sa -t zypp mounted_directory_path service_name`

Package and Content Management Troubleshooting Strategies

13

This section provides solutions to problems you might encounter when using Novell ZENworks Linux Management Package and Content Management features:

- "Installing updates that were mirrored from the Update sites, such as http://updates.novell.com (http://updates.novell.com/), using the rug up command fails with dependency errors" on page 93
- "Rug refresh hangs" on page 94
- "Bundle or package installation might fail with the error message, "Resolvable ID (number) does not exist"" on page 94
- "The zlman push-now option does not install the bundle on the device" on page 94
- "The command to set the password on the managed device is truncated in the error message" on page 94
- "Adding a custom repository fails with an error" on page 94
- "Installing the YOU patches without any particular order using the rug command fails" on page 95
- "Mirroring more than 400 bundles simultaneously between ZENworks Linux Management servers located in different management zones fails" on page 95
- "Content Replication overwrites the symbolic links of all the files located in the package repository on the Secondary Server" on page 95
- "Unable to list more than 500 packages from a ZENworks repository by using the zlman lp command" on page 96

Installing updates that were mirrored from the Update sites, such as http:// updates.novell.com (http://updates.novell.com/), using the rug up command fails with dependency errors

Source:	ZENworks 7.3 Linux Management; Package and Content Management
Possible Cause:	The dependent packages are not available on the ZENworks Linux Management server.
Action:	To distribute and install RPMs to managed devices, you need to ensure that all packages the RPMs depend on, and all packages dependent on the RPM are also imported to the ZLM server. For example, to distribute updates to the SLES 10 devices mirrored from updates.novell.com, you need to ensure that all the packages from the SLES 10 media are imported to the ZENworks Linux Management server. You need not assign the bundles or catalogs containing the dependent RPMs to the managed devices.

Rug refresh hangs

Source: ZENworks 7.3 Linux Management; Package and Content Management

Explanation: The `rug refresh` command sometimes hangs.

Action: Execute the `rug restart` command.

Bundle or package installation might fail with the error message, "Resolvable ID (number) does not exist"

Source: ZENworks 7.3 Linux Management; Package and Content Management

Possible Cause: The `zmd.db` file is corrupt.

Action: Regenerate `zmd.db`.

Enter the following at the command line:

```
rug restart --clean
```

The zlman push-now option does not install the bundle on the device

Source: ZENworks 7.3 Linux Management; Package and Content Management

Explanation: When you try to install a bundle by using the `zlman push-now` command, the bundle is not installed.

Possible Cause: You might have locked the device through the `rug set device-locked true` command or through the `blackout-interval` preference.

Action: Check to see if the device is locked by using the command `rug get device-locked`. Unlock the device by using the `rug set device-locked false` command.

The command to set the password on the managed device is truncated in the error message

Source: ZENworks 7.3 Linux Management; Package and Content Management

Explanation: When you try to initiate a remote session, the following message is displayed if the password is not set on the managed device:

```
Unable to initiate a remote session because a password has not
been set on the managed device. To set the password, run
"zrmservice --pas"
```

The command displayed by the message is truncated.

Action: The complete message is as follows.

```
Unable to initiate a remote session because a password has not
been set on the managed device. To set the password, run
"zrmservice --passwd".
```

Adding a custom repository fails with an error

Source: ZENworks Linux Management; Package and Content Management

Explanation: The following error message might be displayed when you add a custom repository:

```
ERROR: Could not add 'http://foobar.com/sled-10-i586': Failed
to parse XML metadata: Unsigned file '/repodata/repomd.xml
(file:/var/cache/zmd/web/files/foobar.com/sled-10-i586/)'
```

Action: Log in as root, and execute the following command: `rug set security-level checksum`.

Installing the YOU patches without any particular order using the rug command fails

Source: ZENworks 7.3 Linux Management; Package and Content Management

Explanation: If you try to install the YOU patches from a catalog by using wildcard characters in the patch name (For example, `rug bin catlog_name patch*`), then you might encounter issues because of the order in which the patches get installed.

Possible Cause: The usage of wildcard characters change the installation order of the YOU patches. The patched numbered higher could depend on the lower numbered patches.

Action: Do not use wildcard characters for installing a set of patches that are dependent on each other.

Mirroring more than 400 bundles simultaneously between ZENworks Linux Management servers located in different management zones fails

Source: ZENworks 7.3 Linux Management; Package and Content Management.

Explanation: The following error message is displayed when you mirror more than 400 bundles between ZENworks Linux Management servers located in different management zones:

```
Exception in thread "main" java.lang.OutOfMemoryError
```

Possible Cause: The JVM heap memory is only 128 MB.

Action: Increase the JVM heap memory capacity on the local Primary Server:

1 In the `/opt/novell/zenworks/bin/zlmmirror` file, change the value of `-Xmx` to 256 or 512 in the following line, depending on the memory capacity of your device and the load on the server:

```
/opt/novell/zenworks/lib/java/bin/java $ZLMMIRROR_OPTS -
Xmx128m com.novell.zenworks.zlmmirror.ZLMMirror --temp-
args-file $ZLMMIRROR_ARGS_FILE
```

2 Save the file.

3 Restart the ZENworks Linux Management service by using the following command:

```
zlm-config --restart
```

Content Replication overwrites the symbolic links of all the files located in the package repository on the Secondary Server

Source: ZENworks 7.3 Linux Management; Package and Content Management.

Action: None.

Unable to list more than 500 packages from a ZENworks repository by using the zlman lp command

Source: ZENworks 7.3 Linux Management; Package and Content Management.

Action: Apply ZENworks 7.3 Linux Management Hot Patch 1.

Preboot Services

IX

If the Preboot Services features of Novell ZENworks Linux Management displays an error message, you can look it up in the Error Messages section. If a problem is not accompanied by an error message, or if specific instructions for an error message are not available, you can try more general troubleshooting strategies to resolve the problem.

This section contains the following topics:

- Chapter 14, "Preboot Services Error Messages," on page 99
- Chapter 15, "Preboot Services Troubleshooting Strategies," on page 101

Preboot Services Error Messages

14

This section contains detailed explanations of the error messages you might encounter using the Novell ZENworks Linux Management Preboot Services:

- "Error Receiving Message: Not an authorized path for storing images" on page 99

Error Receiving Message: Not an authorized path for storing images

Source: ZENworks 7.3 Linux Management; Preboot Services

Possible Cause: You might encounter this error if the directory path to upload the images is appended with a / (forward slash).

1 Log in to ZENworks Control Center, and click the *Configuration* tab.
2 Click *Preboot Services*.
3 In the *Image Storage Security* panel, select the *Only allow uploads to the following directories* check box.
4 Enter the full path of the directory, and click *Add*.

Action: Remove the forward slash at the end of the path.

Preboot Services Troubleshooting Strategies

15

This section provides solutions to problems you might encounter when using Novell ZENworks Linux Management Preboot Services:

- "The zislnx service fails to shut down on a RHEL 3 device" on page 101
- "After restoring RHEL 5 image, the device does not boot" on page 101
- "How to take and restore the image on RHEL 6 devices with ext3 file system" on page 102

The zislnx service fails to shut down on a RHEL 3 device

Source: ZENworks 7.3 Linux Management; Preboot Services

Possible Cause: RHEL 3 does not follow Linux Standard Base (LSB) standards, and therefore the zislnx service fails to shut down when you run the following command:

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

Action: None.

After restoring RHEL 5 image, the device does not boot

Source: ZENworks 7.3 Linux Management; Preboot Services

Explanation: When you try to restore an image on RHEL 5, the grub command fails to load the bootable files.

Possible Cause: Due to incompatible staging files in the latest Imaging distro.

Action: Do the following:

1 Edit the image file by using Image Explorer, replace the files *e2fs_stage1_5*, *stage2* and *message* under boot folder with the files available in TID 7006480 at Novell Support (http://www.novell.com/support/microsites/microsite.do).

2 Save the image.

3 Restore the image on the device.

4 Before rebooting the device, run the following commands:

```
mount <active partition> <mount directory>
```

For example: `mount /dev/sda1 /mnt/`

```
grub-install.unsupported --root-directory=<mount directory> --recheck <hard disk>
```

For example: `grub-install.unsupported --root-directory=/mnt --recheck /dev/sda`

5 Reboot the device.

How to take and restore the image on RHEL 6 devices with ext3 file system

Source: ZENworks 7.3 Linux Management; Preboot Services

Explanation: You cannot restore an image on RHEL 6 device, because RHEL uses GUIDs to identify the partitions in the device, which will modify the GUID of the partition while restoring the image.

Possible Cause: RHEL 6 assigns GUID to access the mount directories instead of partitions.

Action 1:   Before taking an image, do the following:

1 Edit the files `/boot/grub/menu.lst` and `/etc/fstab`, replace the GUIDs in the files with appropriate mount partition.

`/boot/grub/menu.lst`

Replace the entry root=*<GUID>* with root=*<active partition>*.

For example: Replace root=UUID=873fd0f0-9a0b-4d09-bbfb-3b82a2e46f71 with root=/dev/sda1.

/etc/fstab

Replace the entry *<GUID>* with *<active partition>*.

For example: Replace UUID=d6196feb-eba6-4798-a11b-45a6b1e940fd with /dev/sda1.

NOTE: If there are many mount points defined in `/etc/fstab` with GUIDs, replace them appropriately with the partitions.

2 Take and restore the image.

3 Reboot the device.

Action 2:   After taking an image without modifying `/boot/grub/menu.lst and /etc/fstab`, do the following:

1 Edit the image file by using Image Explorer.

2 Extract the files `/boot/grub/menu.lst` and `/etc/fstab`, and edit the files.

`/boot/grub/menu.lst`

Replace the entry root=*<GUID>* with root=*<active partition>*.

For example: Replace root=UUID=873fd0f0-9a0b-4d09-bbfb-3b82a2e46f71 with root=/dev/sda1.

/etc/fstab

Replace the entry *<GUID>* with *<active partition>*.

For example: Replace UUID=d6196feb-eba6-4798-a11b-45a6b1e940fd with /dev/sda1.

NOTE: If there are many mount points defined in `/etc/fstab` with GUIDs, replace them appropriately with the partitions.

3 Replace the files and save the image file.

4 Restore the image and reboot the device.

Registration

X

The following section provides solutions to porblems you might encounter while working with the Registration component in ZENworks 7.3 Linux Management:

◆ Chapter 16, "Registration Troubleshooting Strategies," on page 105

Registration Troubleshooting Strategies

16

The following section provides solutions to the problems you might encounter when using Novell ZENworks Linux Management Registration services:

The Device Registered Date column in the device registration reports might display a future date

Source: ZENworks 7.3 Linux Management; Registration.

Explanation: The *Device Registered Date* column displays a future date when compared to the date on which the device was registered to the server.

Action: Set the date of those devices that are registered with a future date to the current date:

1 Connect to the PostgreSQL Server's `zenworks` database as a PostgreSQL user by entering the following commands in the order listed:

```
su postgres

psql zenworks
```

2 Run the following query to set the date to the current date:

```
update zen_device set added_date = 'current date' where
deviceguid in( SELECT deviceguid from zen_device where
added_date > NOW() ) ;
```

You must specify the current date in the format 'yyyy-mm-dd hh:mm:ss'.

3 Disconnect from the PostgreSQL database by using the `\q` command.

4 Exit the PostgreSQL session by using the `exit` command.

Error receiving message:Unknown response message from server, status: CancelSignal

Source: ZENworks 7.3 Linux Management; Registration

Explanation: The error message is displayed when you delete a registered service by using the `zmd` command.

Possible Cause: When you start the zmd service, all its underlying modules might not be completely initialized to allow deletion of the requested zmd service. You should delete any registered service after the `rug ping -a` command is successfully completed.

Action: Do the following:

1 Restart the zmd service.

2 Run the `rug ping -a` command.

ZENworks Linux Management Generic Messages

XI

The following section contains detailed explanations of the generic error messages you might encounter while using ZENworks Linux Management:

-

Generic Error Messages

<div style="text-align: right; font-size: 3em;">17</div>

The following sections contain the detailed explanations of the generic error messages you might encounter while using the Novell eDirectory services:

- "Error while loading shared libraries" on page 109
- "eDir result: 255. Unable to configure eDirectory. Please verify the address of your master server along with the organization name and password" on page 109
- "An error occurred while trying to create the bundle. (The object could not be created. This could be because the name is too long, or the object is too deep in the folder hierarchy)" on page 110

Error while loading shared libraries

Source: ZENworks 7.3 Linux Management

Explanation: The error message is displayed when you execute any of the Novell eDirectory commands on a 64-bit ZENworks Linux Management server.

Action 1: Do the following:

1 Edit the `/etc/ld.so.conf.d/novell-NDSbase.conf` file as follows:
- Replace `/opt/novell/eDirectory/lib` with `/opt/novell/eDirectory/lib64`.
- Replace `/opt/novell/eDirectory/lib/nds-modules` with `/opt/novell/eDirectory/lib64/nds-modules`.
- Append the file with the `/opt/novell/lib` with `/opt/novell/lib64` path.

2 Run the `ldconfig` command.

3 Restart the eDirectory services by using the `/etc/init.d/ndsd restart` command.

Action 2: Before executing the eDirectory commands, execute the following command at the command prompt:

`. /opt/novell/eDirectory/bin/ndspath`

eDir result: 255. Unable to configure eDirectory. Please verify the address of your master server along with the organization name and password

Source: ZENworks 7.3 Linux Management

Explanation: The error message is displayed when you run the `zlm-config` command during the ZENworks 7.3 Linux Management installation on SUSE Linux Enterprise Server 11 (SLES 11).

Action: Do the following:

1 Delete the `nds.conf` files from the system by using the `rm -f /etc/nds.conf*` command.

2 Delete the `dib` directory from the system by using the `rm -rf /var/nds/dib/` command.

3 Delete the existing `/etc/opt/novell/eDirectory/conf/.edir/instance.0` file by using the `rm /etc/opt/novell/eDirectory/conf/.edir/instance.0` command.

4 On the ZENworks 7.3 Linux Management server, start the ZENworks services by using the `zlm-config --start` command.

5 Run the `zlm-config` command again to reconfigure ZENworks Linux Management on your device.

An error occurred while trying to create the bundle. (The object could not be created. This could be because the name is too long, or the object is too deep in the folder hierarchy)

Source: ZENworks 7.3 Linux Management.

Explanation: The error message is displayed because of the object FDN (Fully Distinguished Name) limitation of 256 characters in eDirectory when you create a bundle object either in ZENworks Control Center or by using the `zlman` command, or during mirroring.

Action: Do any of the following:

- Do not create the bundle object deeper in the folder hierarchy, or with long names.

- Ensure that the total FDN of the bundle object from its root container in eDirectory does not exceed 256 characters.

Documentation Updates

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

This section contains information on documentation content changes that were made in this *Troubleshooting Guide* after the initial release of Novell ZENworks 7.3 Linux Management. The information can help you to keep current on updates to the documentation.

All changes that are noted in this section are also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes are published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the guide.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains its publish date on the front title page.

The documentation was updated on the following dates:

A.1 January 31, 2011

A.1.1 Installation, Upgrade, ZENworks Database

The following changes were made to this section:

Location	Change
Section 1.1, "Troubleshooting the Installation," on page 13	Added the following scenarios: ◆ "ZENworks Control Center fails to load after successfully installing or upgrading the ZENworks 7.3 Linux Management Server or later on a 64-bit device" on page 17. ◆ "Unable to log in to ZENworks Control Center of the ZENworks Linux Management Server with the Primary or Secondary configuration because of no time synchronization" on page 18.

Location	Change
Section 3.4, "Troubleshooting the Remote Execute Policy," on page 35	Added the following scenarios: ◆ "Unable to install or enforce the available bundle or policy on the managed device according to the schedule when the ZENworks server is inactive" on page 36.
Chapter 7, "Disaster Recovery," on page 57	Updated the following section: ◆ "Disaster Recovery for a Single ZENworks Linux Management Primary Server" on page 59.
Chapter 16, "Registration Troubleshooting Strategies," on page 105	Added the following scenarios: ◆ "Error receiving message:Unknown response message from server, status: CancelSignal" on page 105.

A.2 August 09, 2010

A.2.1 Installation, Upgrade, ZENworks Database

The following changes were made to this section:

Location	Change
Section 1.1, "Troubleshooting the Installation," on page 13	Added the following scenarios: ◆ "The ZENworks Linux Management agent restores the old values of the deviceid and secret files on SLES 11 and SLED 11 managed devices even after deleting them" on page 17. ◆ "Unable to install SLES 9 patch bundles on a ZENworks Linux Management agent" on page 17.

A.3 June 02, 2010 (Interim Release 3)

Updates were made to the following section. The changes are explained below:

- ◆ Section A.3.1, "Installation, Upgrade, ZENworks Database," on page 112
- ◆ Section A.3.2, "Inventory," on page 113

A.3.1 Installation, Upgrade, ZENworks Database

The following changes were made to this section:

Location	Change
Section 1.1, "Troubleshooting the Installation," on page 13	Added the following scenario: ◆ "Unable to install the ZENworks 7.3 Linux Management with IR3 agent on ia64 and s390x devices that have a default installation of SLES 11 SP1" on page 16

A.3.2 Inventory

The following changes were made in this section:

Location	Change
"Troubleshooting Hardware Inventory" on page 52	Added the following scenario: "Hardware inventory of the RHEL 4.x/5.x managed devices is not updated successfully to the server" on page 53

A.4 December 24, 2009

Updates were made to the following section. The changes are explained below:

- Section A.4.1, "Installation, Upgrade, ZENworks Database," on page 113
- Section A.4.2, "ZENworks Linux Management Generic Messages," on page 113

A.4.1 Installation, Upgrade, ZENworks Database

The following changes were made to this section:

Location	Change
Section 1.1, "Troubleshooting the Installation," on page 13	Added the following scenarios: ◆ "Upgrading from ZENworks 7.2 Linux Management with IR2 or later to ZENworks 7.3 Linux Management might fail on a SUSE Linux Enterprise Server 10 GM device" on page 16 ◆ "During ZENworks Linux Management installation, the ndsd runlevel scripts from the eDirectory packages display warning messages" on page 16

A.4.2 ZENworks Linux Management Generic Messages

The following changes were made to this section:

Location	Change
"Generic Error Messages" on page 109	Added the following error message: ◆ An error occurred while trying to create the bundle. (The object could not be created. This could be because the name is too long, or the object is too deep in the folder hierarchy).

A.5 November 19, 2009

Updates were made to the following sections. The changes are explained below:

- Section A.5.1, "ZENworks Linux Management Generic Messages," on page 114

A.5.1 ZENworks Linux Management Generic Messages

The following changes were made to this section:

Location	Change
"Generic Error Messages" on page 109	Added the following error message: ◆ eDir result: 255. Unable to configure eDirectory. Please verify the address of your master server along with the organization name and password.

A.6 October 12, 2009 (Interim Release 1)

Updates were made to the following sections. The changes are explained below:

- Section A.6.1, "Event Monitoring," on page 114
- Section A.6.2, "Remote Management," on page 114
- Section A.6.3, "ZENworks Linux Management Generic Messages," on page 115

A.6.1 Event Monitoring

The following changes were made to this section:

Location	Change
"Troubleshooting Event Monitoring" on page 41	Added the following scenario: ◆ After upgrading to ZENworks 7.3 Linux Management with IR2, the Number of backup files per day option does not display the new default value on the Local Device Logging page

A.6.2 Remote Management

The following changes were made to this section:

Location	Change
"Remote Management Troubleshooting Strategies" on page 79	Added the following scenario: ◆ Unable to automatically reboot a managed device by pressing the Send Ctrl+Alt+Del button in the management console during a Remote Login session
Chapter 10, "Remote Management Troubleshooting Strategies," on page 79	Updated the following scenario: ◆ "Unable to perform Remote Login session to a SLES 11 or a SLED 11 managed device" on page 82

A.6.3 ZENworks Linux Management Generic Messages

The following changes were made to this section:

Location	Change
"Error while loading shared libraries" on page 109	Updated this section.

A.7 May 26, 2009 (Hot Patch 1)

Updated were made to the following sections. The changes are explained below.

- Section A.7.1, "Installation, Upgrade, ZENworks Database," on page 115
- Section A.7.2, "Policy Handlers," on page 115
- Section A.7.3, "Event Monitoring," on page 115
- Section A.7.4, "Package and Content Management," on page 116
- Section A.7.5, "Registration," on page 116

A.7.1 Installation, Upgrade, ZENworks Database

The following changes were made to this section:

Location	Change
Section 1.1, "Troubleshooting the Installation," on page 13	Updated the following scenario: - "ZENworks Linux Management installation hangs in an X session on a 32-bit SUSE Linux Enterprise 11" on page 15

A.7.2 Policy Handlers

The following changes were made to this section:

Location	Change
Section 3.6, "Troubleshooting SUSE Linux Enterprise Desktop Policy," on page 38.	Updated the following scenario: - "If you configure the SUSE Linux Enterprise Desktop policy for a SLED 10 or SLED 11 managed device, the Disable Launcher Creation option does not work" on page 38

A.7.3 Event Monitoring

The following changes were made to this section:

Location	Change
Section 4.1, "Troubleshooting Event Monitoring," on page 41	Added the following scenario: ◆ "The log-level setting for a managed device is set to the default value info whenever the managed device is refreshed" on page 42.

A.7.4 Package and Content Management

The following changes were made to this section:

Location	Change
Chapter 12, "Package and Content Management Error Messages," on page 91	Added the following scenario: ◆ "Error receiving message: Invalid URI scheme. Supported : http, ftp and absolute path" on page 92.
Chapter 13, "Package and Content Management Troubleshooting Strategies," on page 93	Updated the following scenario: ◆ "Unable to list more than 500 packages from a ZENworks repository by using the zlman lp command" on page 96.

A.7.5 Registration

The following changes were made to this section:

Location	Change
Chapter 16, "Registration Troubleshooting Strategies," on page 105	Added the following scenario: ◆ "The Device Registered Date column in the device registration reports might display a future date" on page 105.